Бешков Андрей
Менеджер программ ИБ
Microsoft
abeshkov@microsoft.com

БЕЗОПАСНОСТЬ ГИБРИДНЫХ ОБЛАКОВ

Безопасность Гибридных облаков

- В чем проблема с облаками?
  - При чем тут трансграничная передача?
- Как с этим жить
  - Что делать если облачные ЦОДы не на территории страны.
- Проблемы
  - Какие у решения недостатки и как с ними бороться

Один тип облака не может всем подойти

- Некоторые облачные провайдеры хотят чтобы верили что:
  - Вам не нужно частное облако. Все должно быть в публичном облаке.
  - Публичные облака это миф. Все должно быть в частных облаках.
  - Бери что дают и будь счастлив. Мы лучше знаем что нужно. Мы прогрессивнее! Мы появились в век Интернета!
- Так получается потому что они не могу удовлетворить нужды разных категорий клиентов

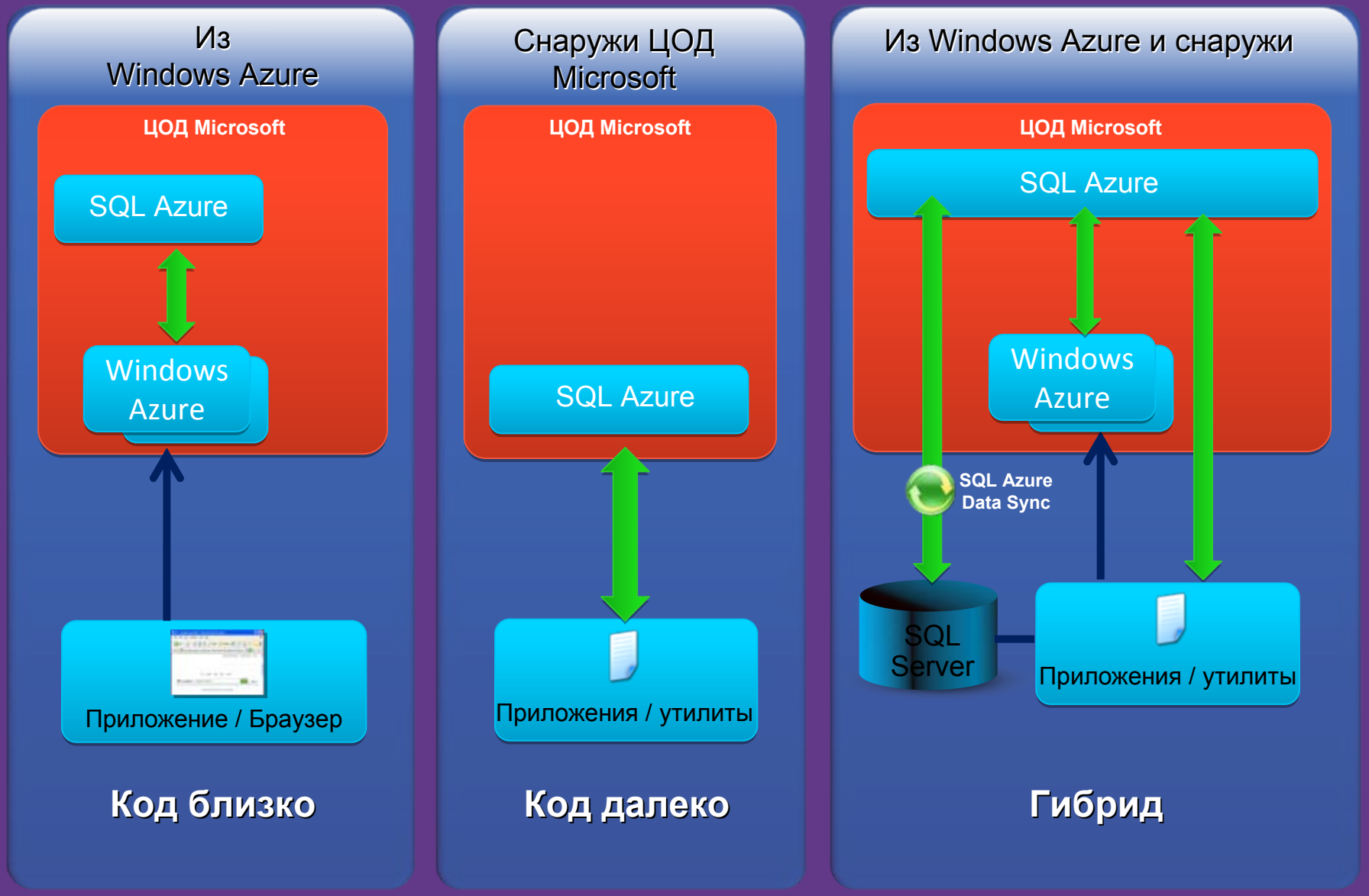
Риски в соответствии с Gartner…

Privileged User Access	• Получите как можно больше данных об уровне доступа персонала провайдера к вашим данным.
Regulatory Compliance	• Многие не понимают что клиент в ответе за безопасность и целостность своих данных.
Data location (Data Sovereignty)	• Можно ли проводить обработку данных только в определенных странах?
Data Segregation	• Как изолируются данные разных клиентов?
Recovery	• Как делается резервное копирование и восстановление?
Investigative support	• Какой тип поддержки доступен при расследовании инцидентов?
Long-term viability	• Останется ли это провайдер на рынке?

Начните с классификации данных

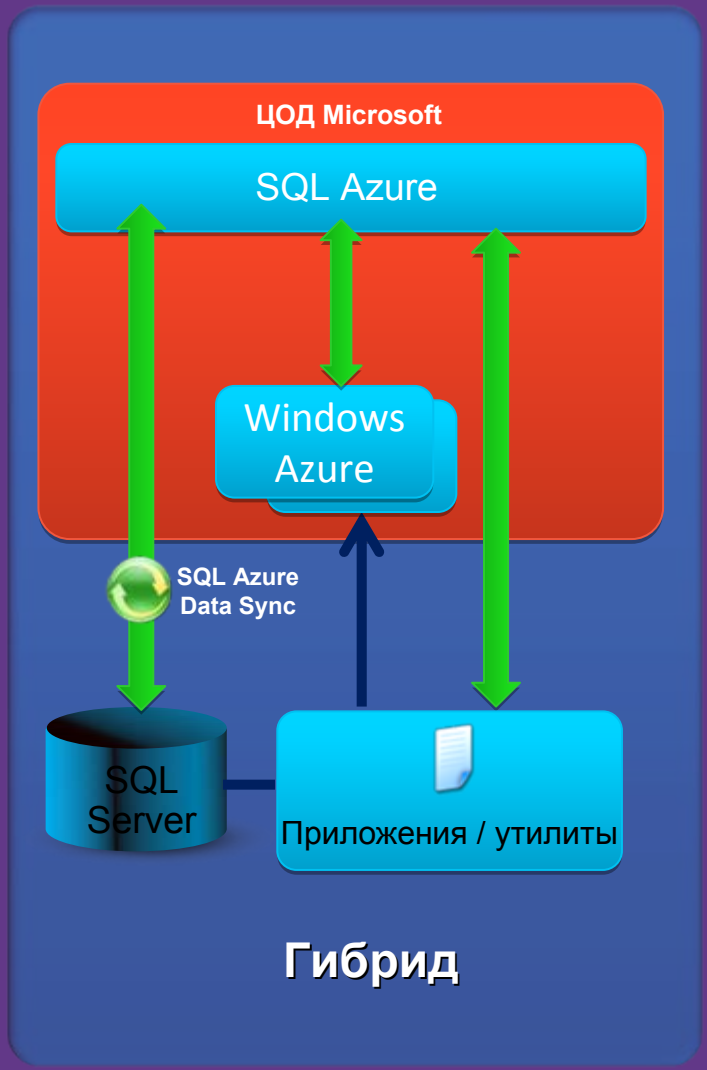
- Если вы не знаете что у вас есть, то как вы будете это защищать?
- Вы должны быть способны сказать что можно вынести в облако, а что останется в инфраструктуре предприятия.
- Классификация должна быть проста. В Microsoft всего 3 типа данных.
- Почти все что не HBI можно разместить в облаке.

Приложения и облачные топологии



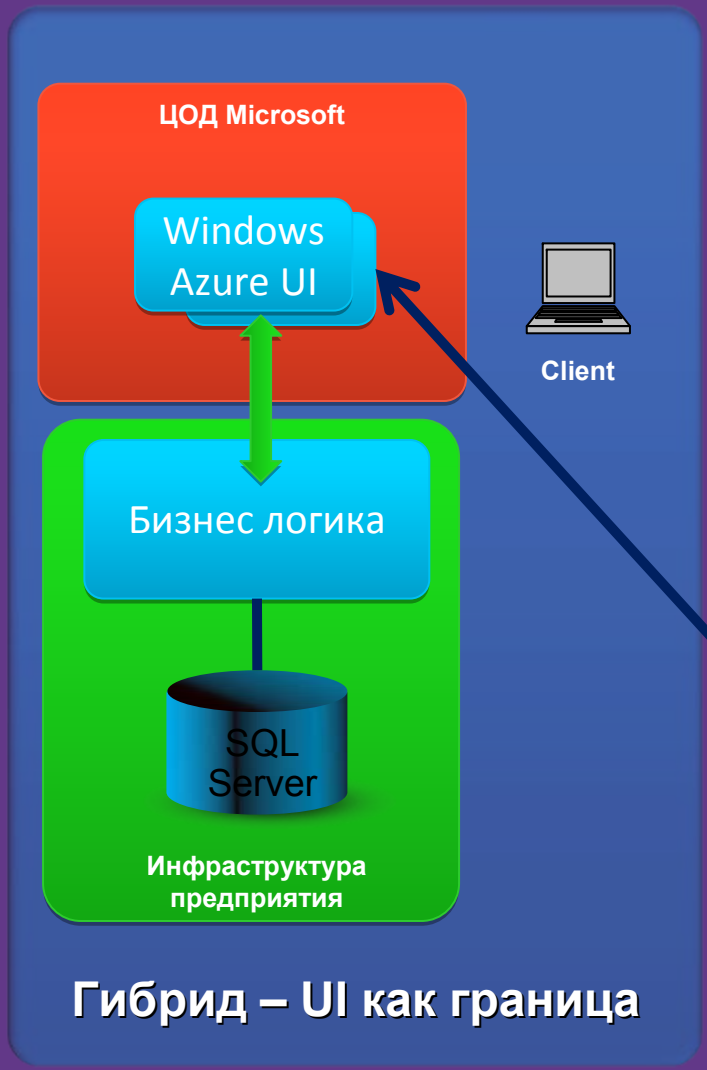
Пристальный взгляд на гибридные облака

- Комбинация кода и данных расположенные в облаках и инфраструктуре предприятия
- Код из облака может получить доступ к системам предприятия и наоборот
- Наиболее гибкий подход в отношении безопасности данных и инфраструктуры



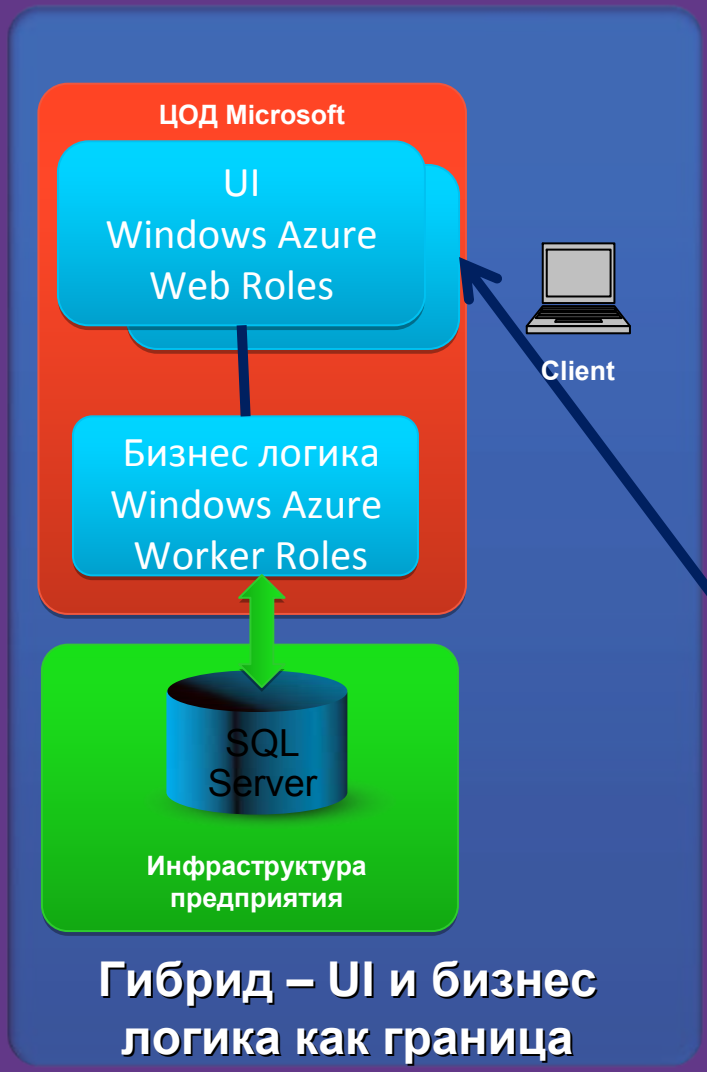
Типовые способы развертывания

- UI в облаке включая статический контент в (CDN)
- Хорошо для приложений с небольшой нагрузкой на бэкэнд
- Веб сервисы и бизнес логика в инфраструктуре предприятия
- Не пускаем клиентов и злоумышленников к себе в инфраструктуру



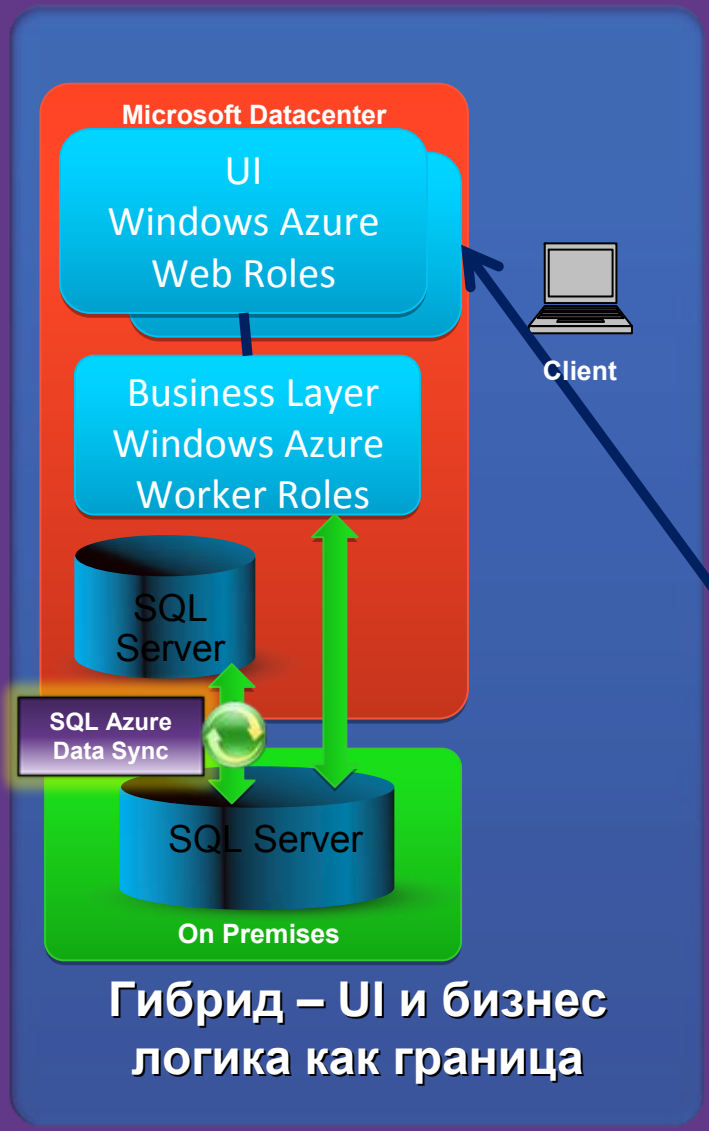
Типовые способы развертывания

- UI и бизнес логика в облаке
- Хорошо для приложений с заполнением форм или интенсивными вычислениями
- Веб сервисы бизнес логики в облаке
- Не пускаем клиентов, злоумышленников и их запросы к себе в инфраструктуру



Типовые способы развертывания

- UI, бизнес логика и некритичные данные в облаке
- Хорошо для приложений с заполнением форм или интенсивными вычислениями
- Веб сервисы бизнес логики в облаке
- Не пускаем клиентов, злоумышленников и их запросы к себе в инфраструктуру

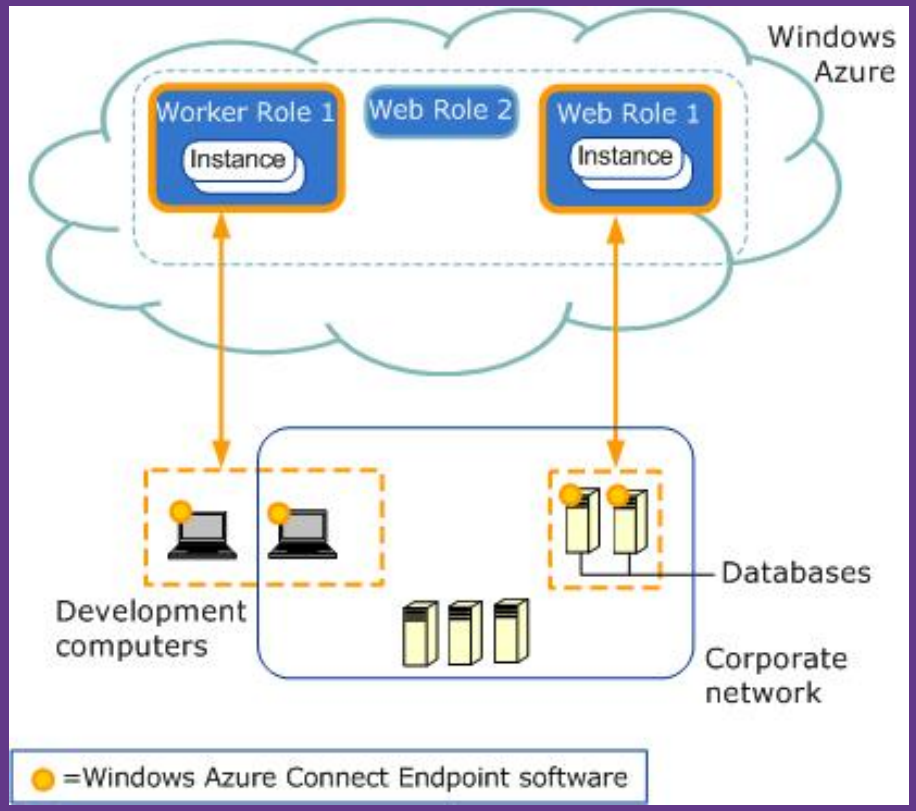


Как это помогает безопасности?

- Отличная защита от DDoS
- Изолирует инфраструктуру предприятия от злоумышленников
- Позволяет хранить и обрабатывать критичные данные в вашем ЦОД и пользоваться выгодами облаков
- Принимает входящие соединения только от доверенных системам

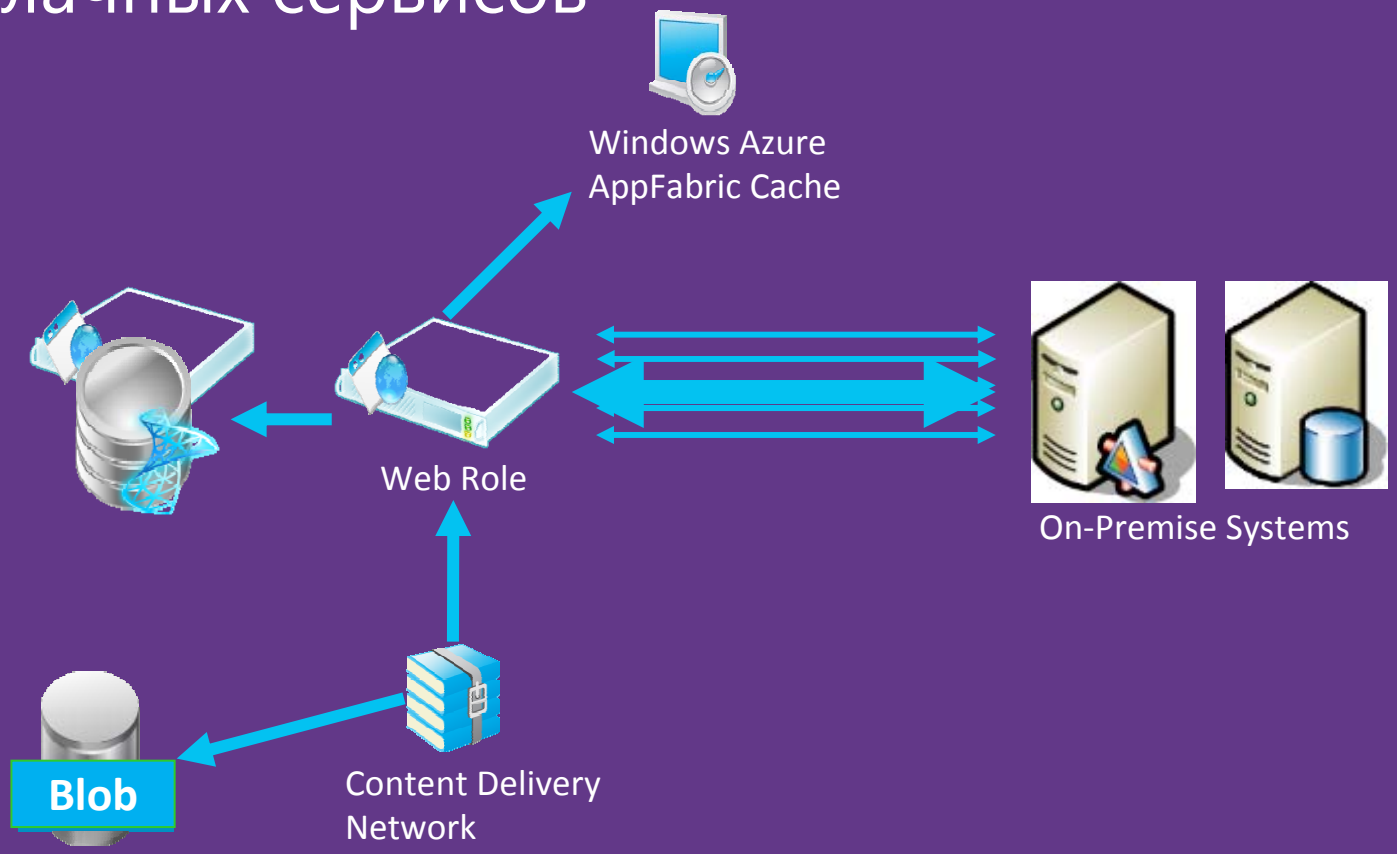
Защита коммуникаций
Windows Azure Connect

- Защищает сетевой траффик между предприятием и облаком с помощью IPv6 и IPsec
- Дает доступ гибридным приложениям только к определенным объектам инфраструктуры предприятия
- Позволяет удаленное управление приложениями в Azure
- Легкое развертывание и управлениет
  - Интегрирован с сервисной моделью Azure
  - Поддерживает Web, Worker и VM роли



Проблема: Задержки в сети

- Минимизация задержек для пользователей облачных сервисов

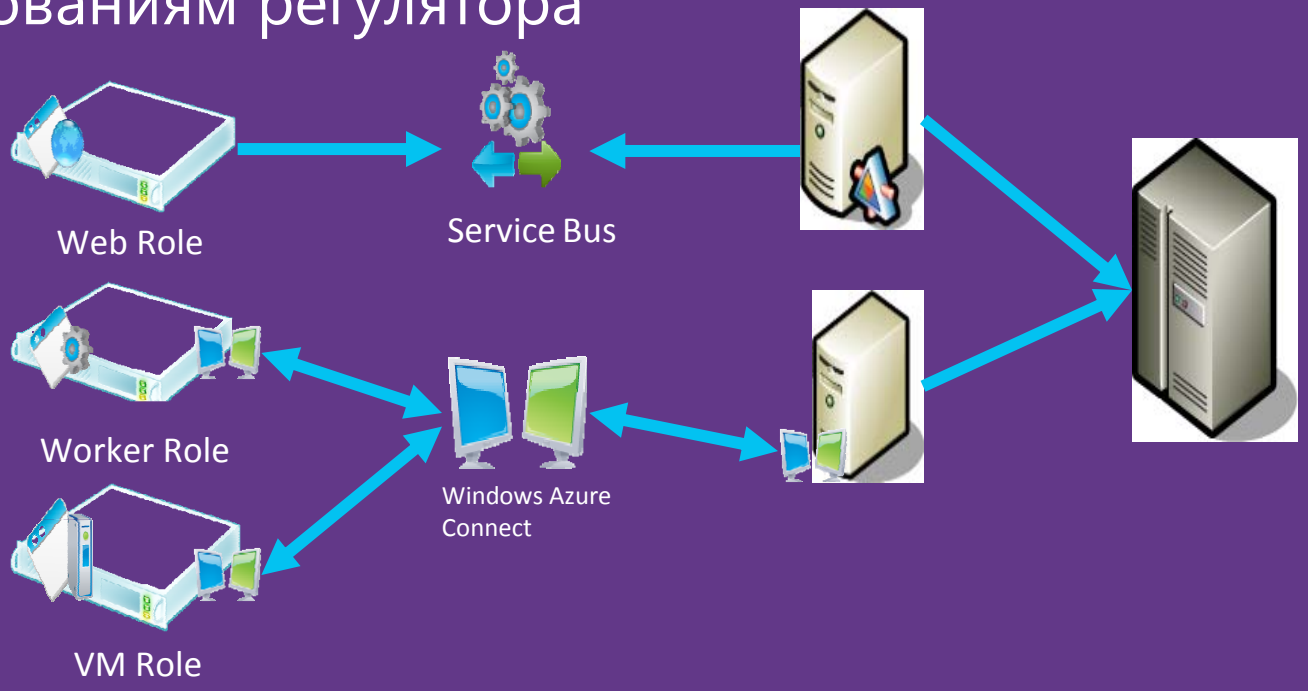


Windows Azure Content Delivery Network (CDN)

Более 2 террабайт в секунду с уровнем доступности 99.95% из 22 точек. CDN масштабируется автоматически без вмешательства пользователя

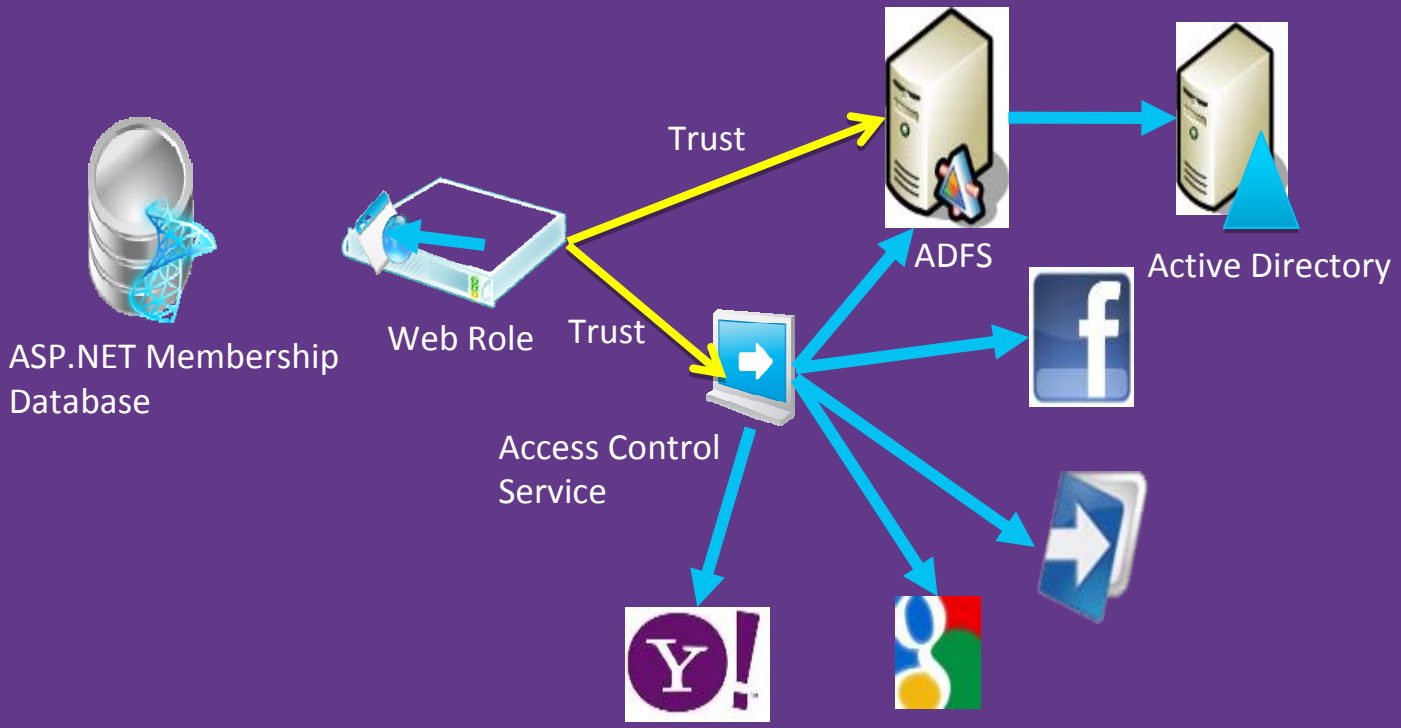
Проблема: Зависимость систем

- Устаревшие системы (мейнфреймы)
- Другие системы и сервисы
- Данные и системы которые должны находиться в инфраструктуре предприятия для соответствия требованиям регулятора



Проблема: Аутентификация и авторизация

- Управление и аутентификация пользователей в облаке
- Интеграция м Active Directory
- Федерация с партнерами или другими источниками идентификационных данных Facebook или Windows Live ID

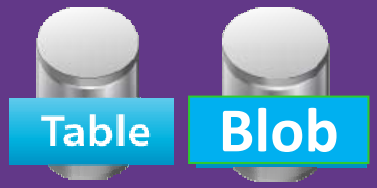


Проблема: Очень большие базы

- Хранение >150GB данных в БД

Множественные БД SQL Azure

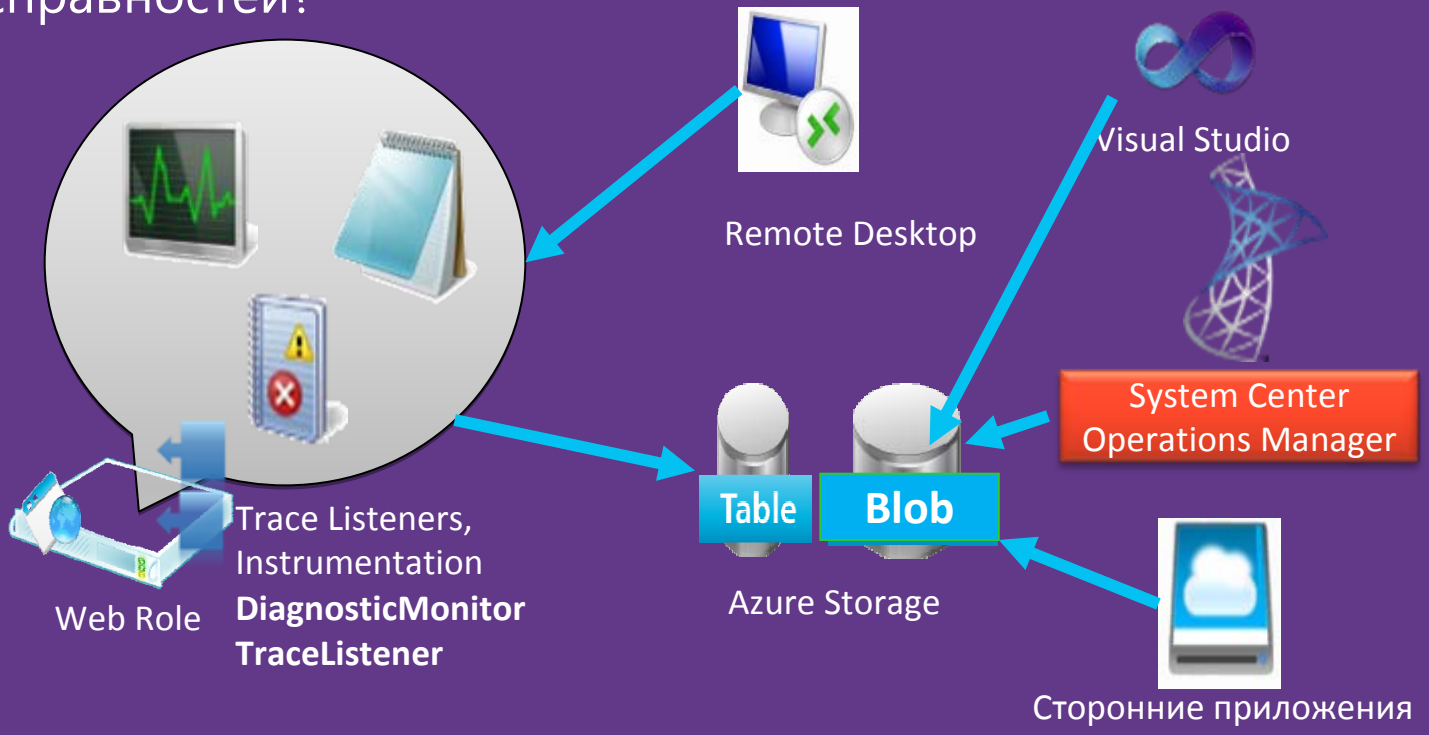
Разделяемые БД SQL Azure



Azure Storage

Проблема: Управление и мониторинг

- Microsoft обслуживает оборудование и ОС в облаке … но приложение обслуживаете вы!
- Как отслеживать производительность и выполнять поиск неисправностей?



Технические тонкости

- Какие приложения легче мигрировать в облако?
  - Обладающие веб интерфейсами
  - Способные к горизонтальному масштабированию
  - Работающие на Windows Server 2008+
  - Построенные на самописном коде
  - Использующие SQL Server
  - Не зависящие от сохраненных состояний

Технические тонкости

- Каких приложений стоит избегать?
  - С интерфейсом толстых клиентов (RDP)
  - Требующих сложной топологии для масштабирования
  - Не работающих на Windows Server 2008+
  - Требующих коробочных приложений Microsoft или сторонних производителей
  - Требующих продвинутых функций Oracle/DB2/MySQL или SQL Server
  - Требующих сохранения состояния за пределами БД

Безопасность данных – лучше?

- Конфиденциальность
  - Приблизительно такая же или лучше чем у вас сейчас. Сильно зависит от приложений и процедур организации.
- Целостность
  - Лучше чем у вас сейчас.
- Доступность
  - Возможно лучше чем у вас сейчас. Вряд ли вы превзойдете защиту провайдера облака от DDoS.

Ресурсы

- Information Classification Framework (Excel)
- Forrester: The Data Security And Privacy Playbook
- Forrester: Q&A: EU Privacy Regulations
- Gartner - In a Diverse Europe, Cloud Adoption Will Be Slower
- Cloud Security Alliance
- Securing the Microsoft Cloud Infrastructure
- Information Risk Executive Council: Security Strategy for Cloud Computing
- Legal issues in the Cloud Part 1 | Part 2 | Part 3 | Part 4
- Whitepapers about data sovereignty
- Microsoft Data Classification Toolkit
- AD RMS File API