Microsoft
Secure Software Development

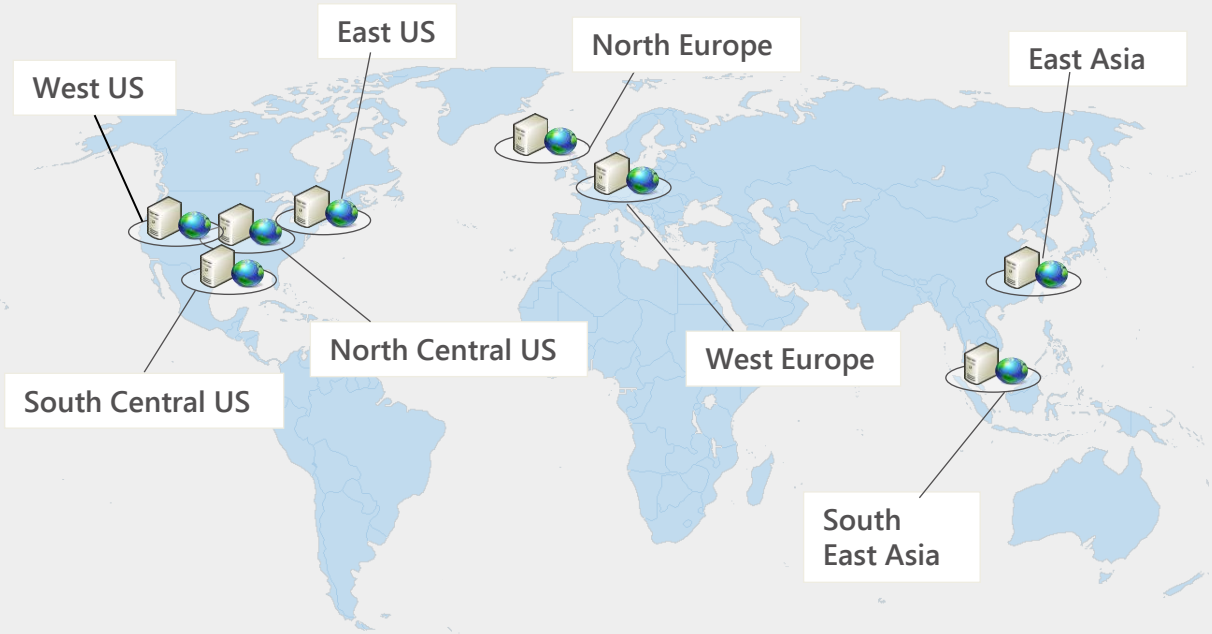
# Windows Azure – облачные сервисы и безопасность данных

Alexey Bokov
Windows Azure Evangelist, Microsoft

# План

- Облачная платформа Windows Azure
- Сервисы авторизации Windows Azure
- Сценарии использования Active Directory
- Сервисы SQL Azure Labs
- Примеры решений на базе Windows Azure
- Q/A

# Windows Azure - инфраструктура

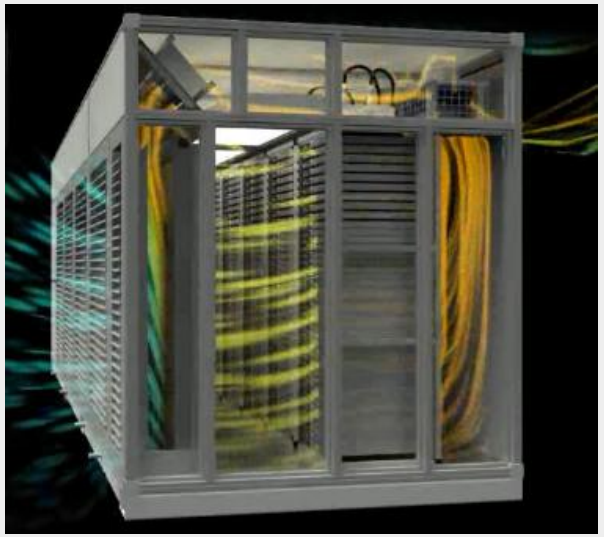



*8 датацентров:*
*- 4 поколение на ITPAC*
*- площадь~ 28 100 кв*
*- мощность ~ 16 МВт*
*- PUE ~ 1.05-1.22*
*- стоимость ~ 500M $*


***24 узла в CDN:*** *Ashburn, San Francisco, Chicago, San Antonio, Los Angeles, Miami, Newark, Seattle, Amsterdam, Dublin, London,* ***Moscow****, Paris, Stockholm, Vienna, Zurich, Hong Kong,* ***Sao Paulo****, Seoul, Singapore,* ***Sydney****, Taipei,* ***Tokyo****, Doha*

Microsoft

# Secure Software Development



Microsoft

# Secure Software Development

Microsoft .NET | Java | php | nodeJS

CDN | кэш данных | интеграция | бизнес аналитика | Сервисы авторизации | Медиа | HPC | E-commerce

## Вычислительные ресурсы

cloud services | VMs | websites

## Данные

SQL базы данных | noSQL решения | блобы

## Сеть

connect | virtual network | traffic manager

Автоматизация | Управление ресурсами

Гибкость | Оплата по использованию

## Глобальная инфраструктура

*серверы/сеть/датацентры*


## Windows Azure предоставляет управление идентификацией и доступом идентификацией для облачных приложений на уровне платформы

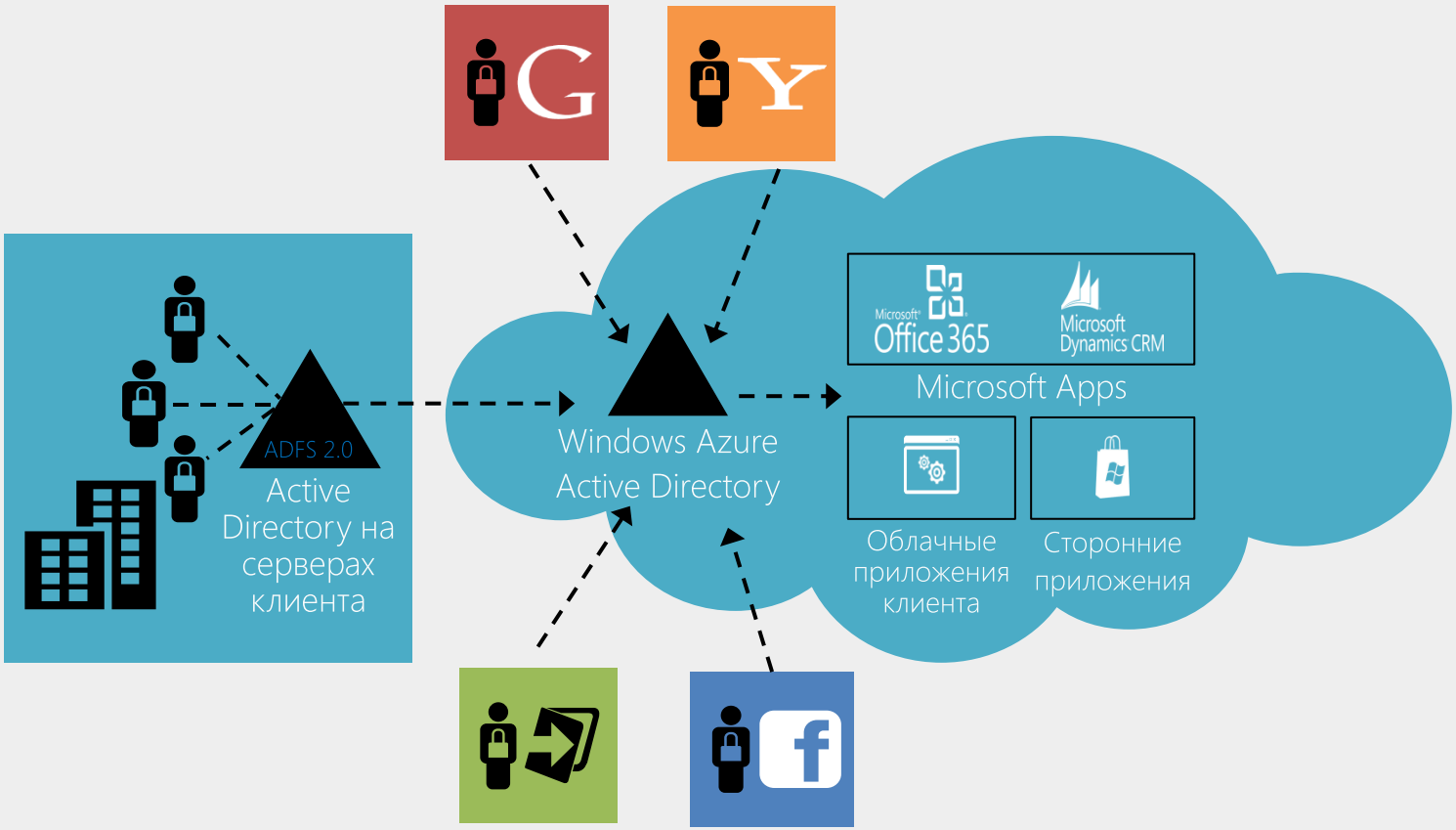
Использование Windows Azure Active Directory предоставляет управление доступом для облачных приложений и широкие возможности по интеграции с Microsoft Office 365, Dynamics CRM Online, Windows Intune или другими сторонними облачными сервисами.

Простая реализация Single Sign On – с использованием Live ID, Facebook, Yahoo, Google & Active Directory

Поддержка индустриальных стандартов и существующих .NET API

CDN | кэш данных | интеграция | бизнес аналитика | **Сервисы авторизации** | Медиа | HPC | E-commerce

# Windows Azure Active Directory – идентификация и управление доступом



# Active Directory Domain Services в Windows Azure это :

- Возможность быть ближе к пользователю ( 8 ДЦ по всему миру )
- Более высокая отказоустойчивость к техногенным катастрофам- Disaster recovery
- Оптимизация архитектуры облачных сервисов в случае если нет необходимости обращения к on-premise AD

# Особенности AD в Windows Azure:

- В целом использование AD контроллера доменов в виртуализованной среде Windows Azure аналогично использованию под Hyper-V on-premise
- Привязка только к динамически выданному Windows Azure IP ( адрес существует всё время жизни виртуальной машины )
- Данные AD должны быть на Data disk ( максимальный размер 1 ТБ ) – он более медленный ( write-throught caching )
- Вместо Copy/restore всей системы в VHD рекомендуется использовать бэкапирование данных

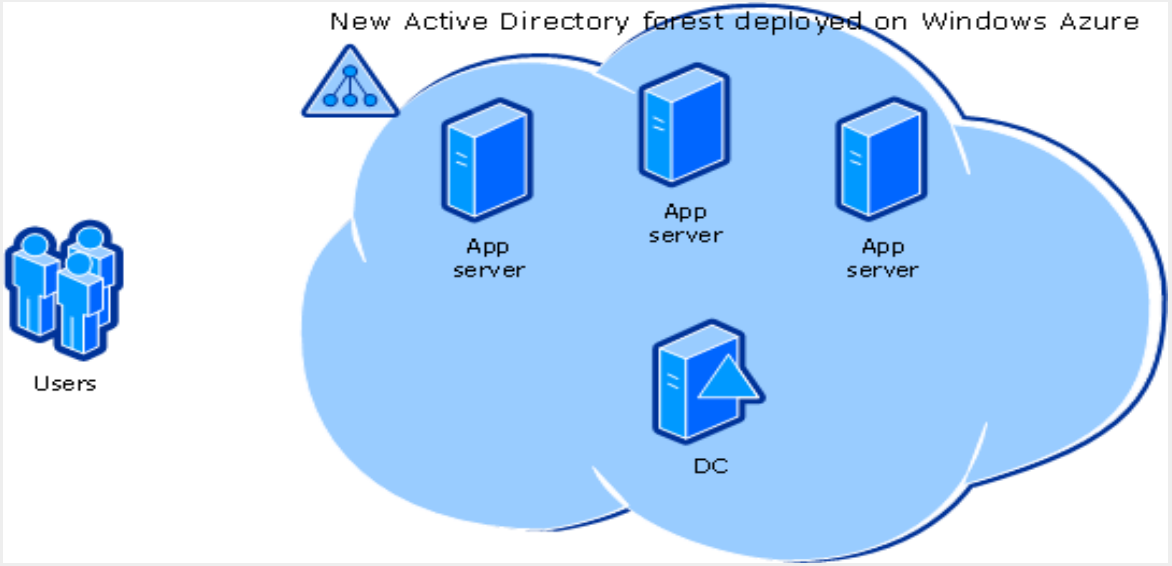
# AD Domain Controller в Windows Azure и on-premise

- При необходимости обращения к on-premise надо использовать VPN
- Весь исходящий трафик – платный
- Нет возможности прямого взаимодействия между разными VPN в Windows Azure
- В Windows Azure конфигурации виртуальных машин являются фиксированными ( RAM, CPU, сеть, дисковая подсистема )
- Safeguards и клонирование DC - не поддерживаются

# AD Federation Services в Windows Azure это:

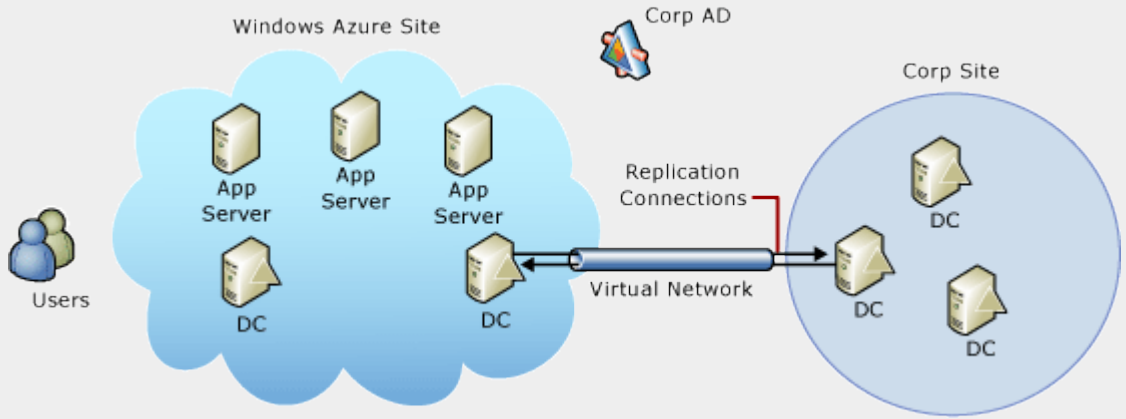
- Высокая доступность может достигаться встроеными средствами load-balancing Windows Azure
- Управление ( создание, настройка) федерациями в Windows Azure проще
- Но не забываем про тарификацию исходящего наружу трафика, например от AD FS proxy в Windows Azure

# Active Directory в Windows Azure – всё в облаке



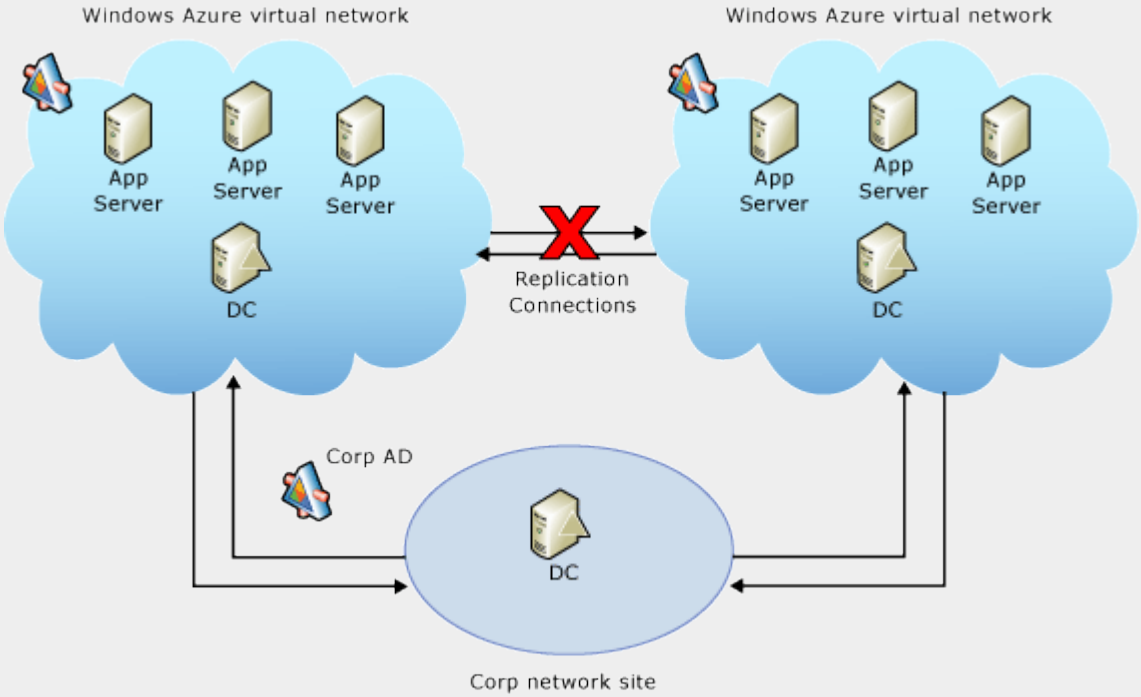

- Все пользователи, приложения и AD используют Windows Azure.
- Нет необходимости в соединении с корпоративной сетью ( например sharepoint инсталлированный в Windows Azure использует AD из Windows Azure )

# Active Directory в Windows Azure – гибридный сценарий



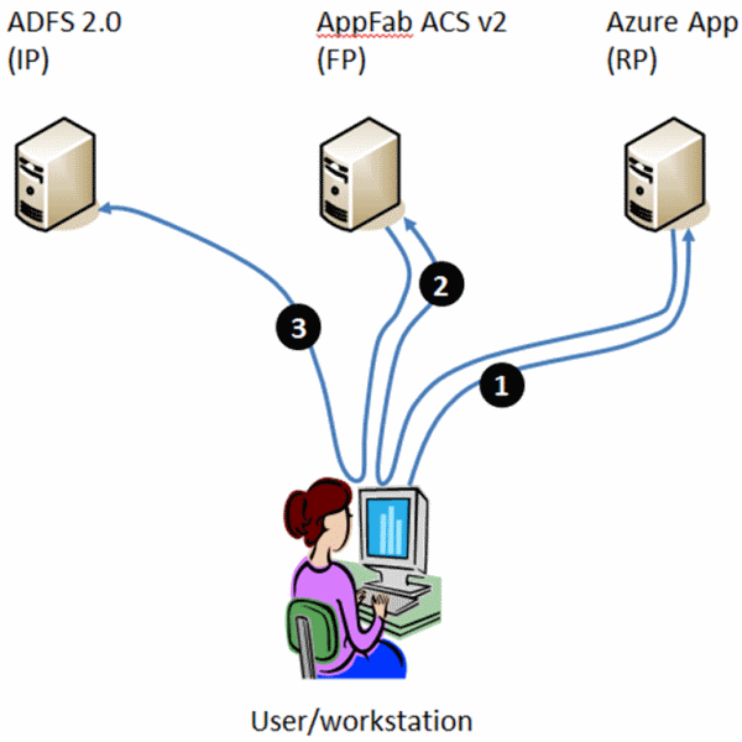

- Пользователям нужен доступ к приложениям в корпоративной сети через Интернет
- Облачные приложения также часто обращаются к ресурсам внутри корпоративной сети
- Для оптимизации архитектуры к AD внутри корпоративной сети добавляется несколько AD в клауде Windows Azure

# Active Directory в Windows Azure – георасределённое решение




- Оптимизация сетевой latency – пользователи обращаются к ближайшему ДЦ Windows Azure
- Высокая отказоустойчивость кластера в целом, в т.ч. к техногенным катастрофам
- Минус решения – прямого взаимодействия между разными VPN нет, все через корпоративную сеть ( исходящий из Windows Azuretрафик будет тарифицироваться )

# Пример облачного приложения с использованием AD из корпоративной сети



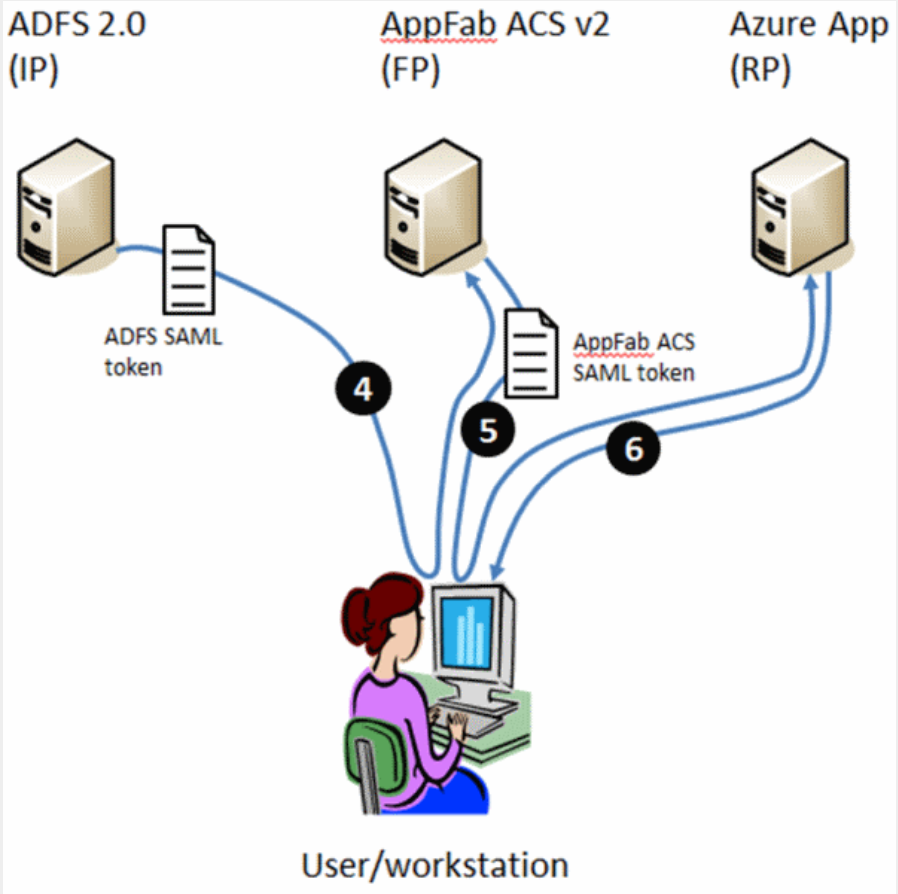

- Пользователь обращается к Azure App и приложение редиректит его на Azure Access Control Services
- ACS видит что пользователь не авторизован и перенаправляет его в ADFS
- ADFS отвечает контекстом юзера ( UPN ~ user@domain.com )

ADFS – Identity provider ( выдает SAML токены )

ACS – Federation provider ( получает SAML от ADFS и выдает свои SAML

Azure App – relying party ( использует WIF )

# Пример облачного приложения с использованием AD из корпоративной сети



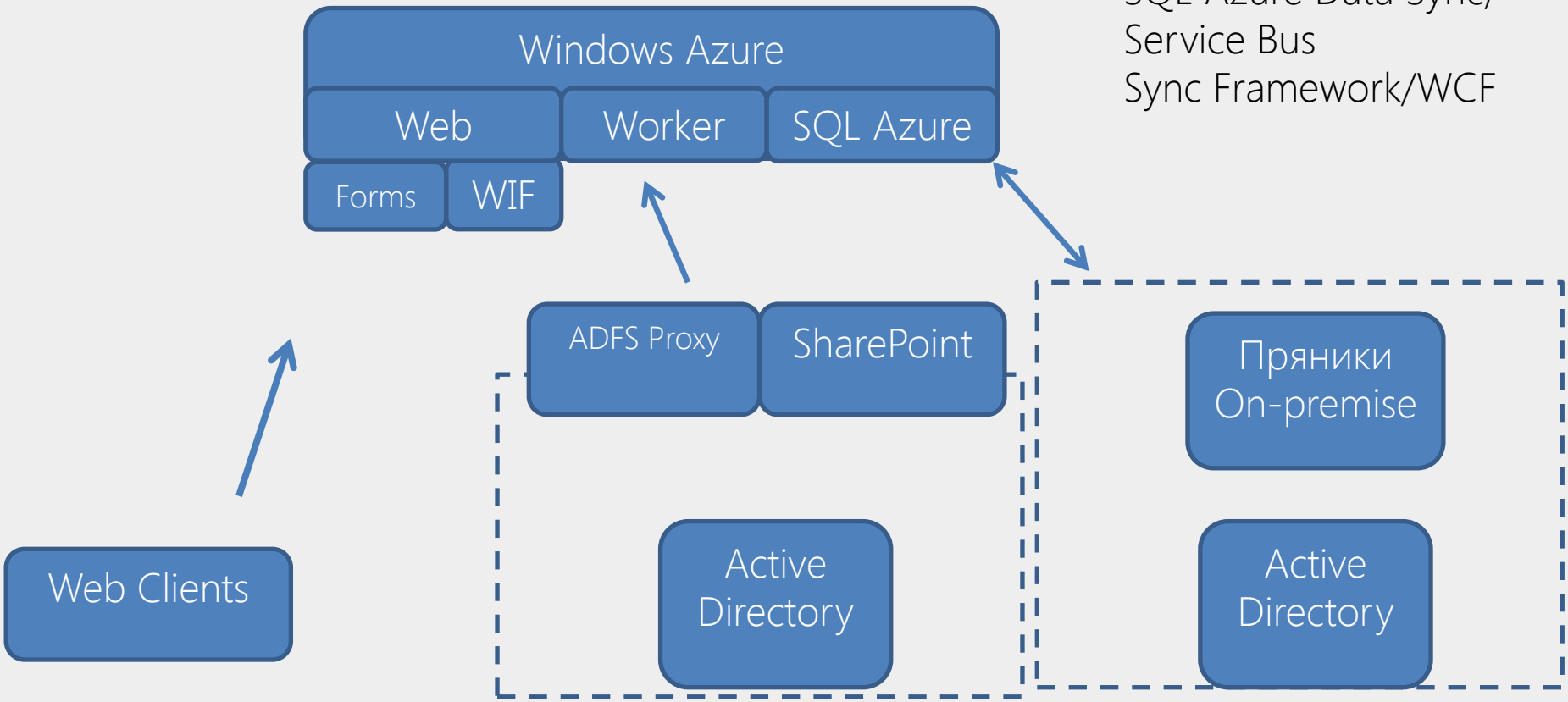

- ADFS выдает SAML для ACS и делает редирект обратно на ACS ( SAML в POST данных)
- ACS на основе SAML от ADFS делает свой SAML и выполняет аналогичный редирект обратно в Azure App ( новый SAML от ACS в POST данных )
- Azure App получает SAML, выдает пользователю запрашиваемую страницу, создает cockie для следующих запросов на авторизацию

# Гибридное решение - Пряники

- Сервис нематериальной мотивации персонала
- Реализован гибридный сценарий через ServiceBus – часть данных в ДЦ клиента
- Поддержка авторизации через Active Directory ( сервер AD у клиента )

http://pryaniky.com

SQL Azure Data Sync,
Service Bus
Sync Framework/WCF

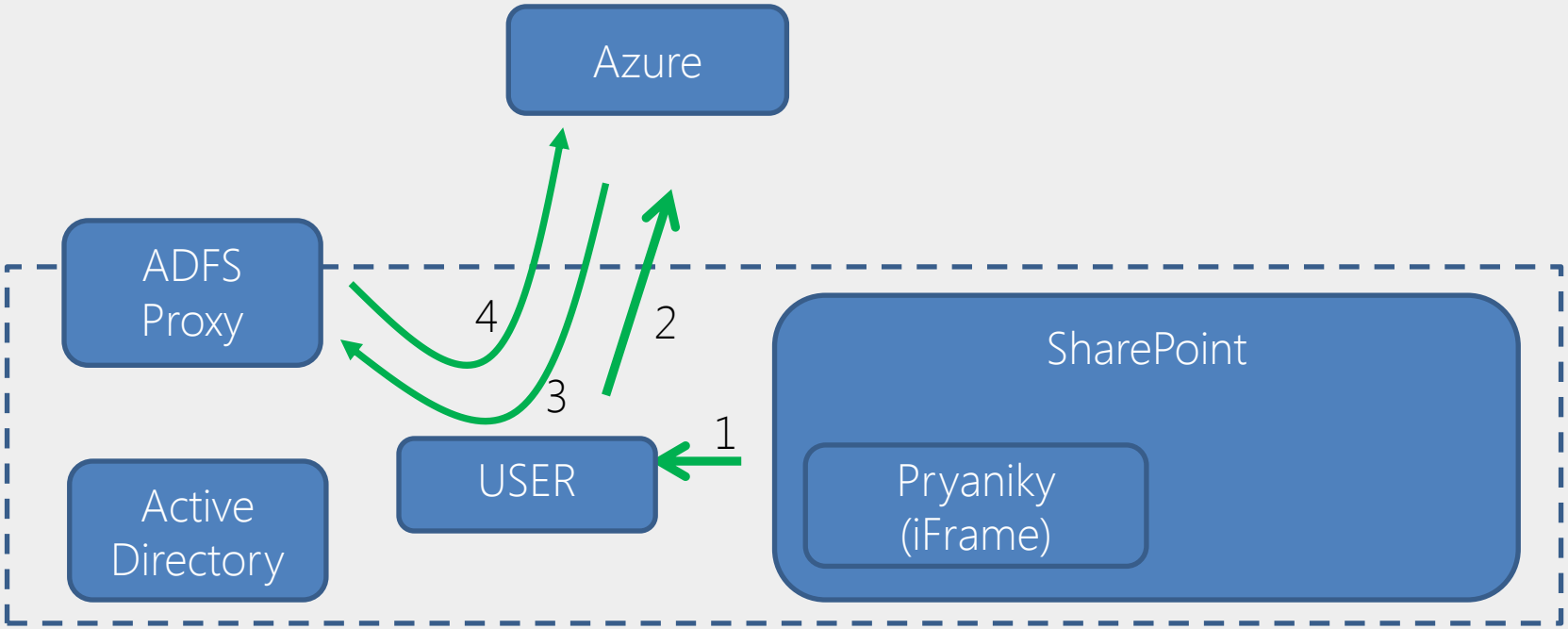


# Сервис Пряники – аутентификация

1. User запрашивает страницу SharePoint, на которой есть WebParts, представляющие собой обычные iFrame.
2. WebParts пробуют начать загруать содерджимое с Azure
3. в этот момент Azure возвращает Redirect на ADFS или ADFS Proxy для аутентификации
4. Пользователь вводит учетные данные или аутентифицируется автоматически (для зоны Intranet) - его вместе с токеном передают обратно в Azure

Плюсы - простая реализация

Минусы - редирект пользователя, невозмодность закешировать данные на стороне клиента

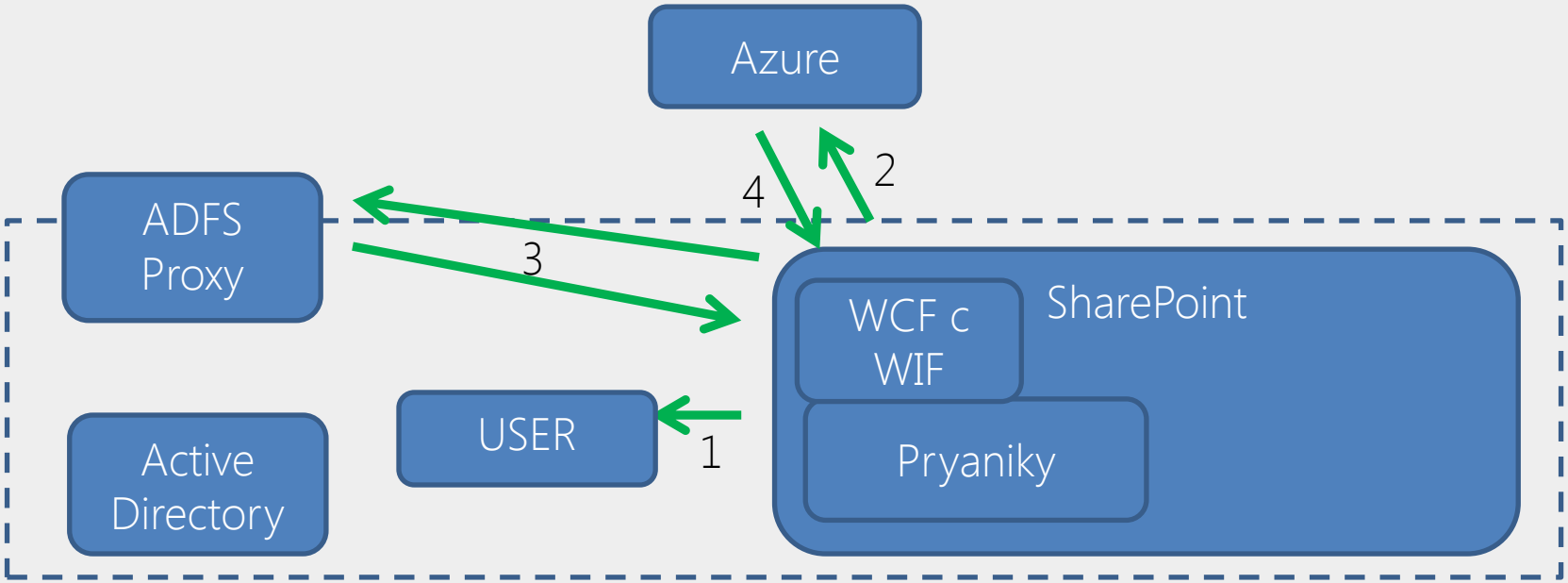


# Сервис Пряники – аутентификация

**WCF +ADFS: позволяет аутентифицировать пользователей из домена в облачном сервисе без активного участия пользователей**

1. Пользователь получает страницу SharePoint
2. При генерации страницы вызывается WCF/WIF компонена которая делает запрос к Azure
3. В процессе установки защищенного соединения и аутентификации пользователя на сервисе требуется токен, который получается WCF-клиентом от ADFS или ADFS-Proxy
4. В результате после аутентификации клиента WebParts получает необходинмые данные для отображения

Данный подход позволяет не только кешировать данные, но и сохранить полученный токен для аутентификации в последующих запросах



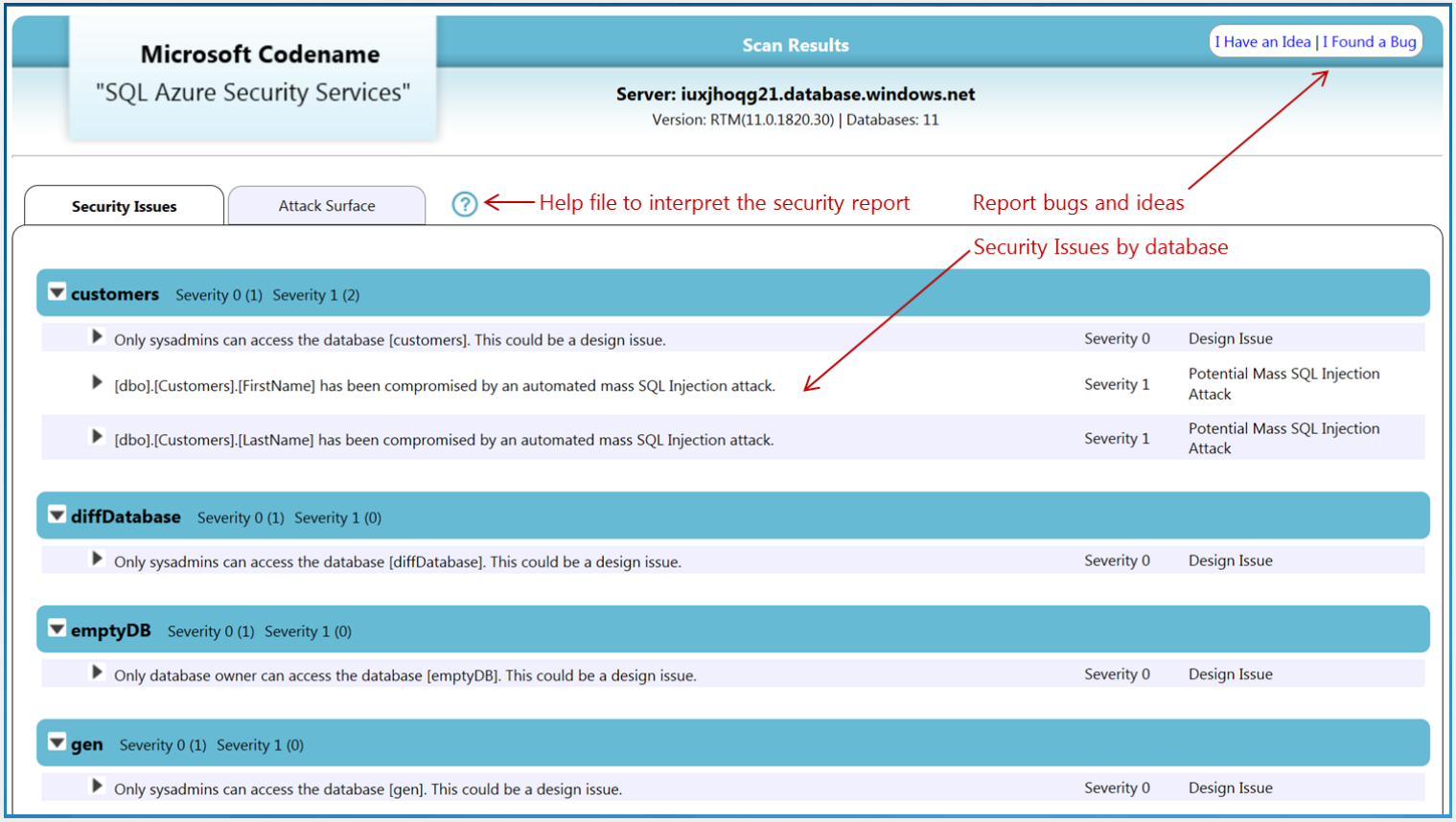
# Облачная база данных SQL Azure

- Защищенное соединение с сервисом ( SSL )
- SQL Azure Firewall ограничивает доступ к сервису с определенных IP
- Аутентфикация SQL Server
- Полезные сервисы:
  - SQL Azure Security Services
  - SQL Azure Trust Services

# SQL Azure security services

Microsoft SQL Azure Labs

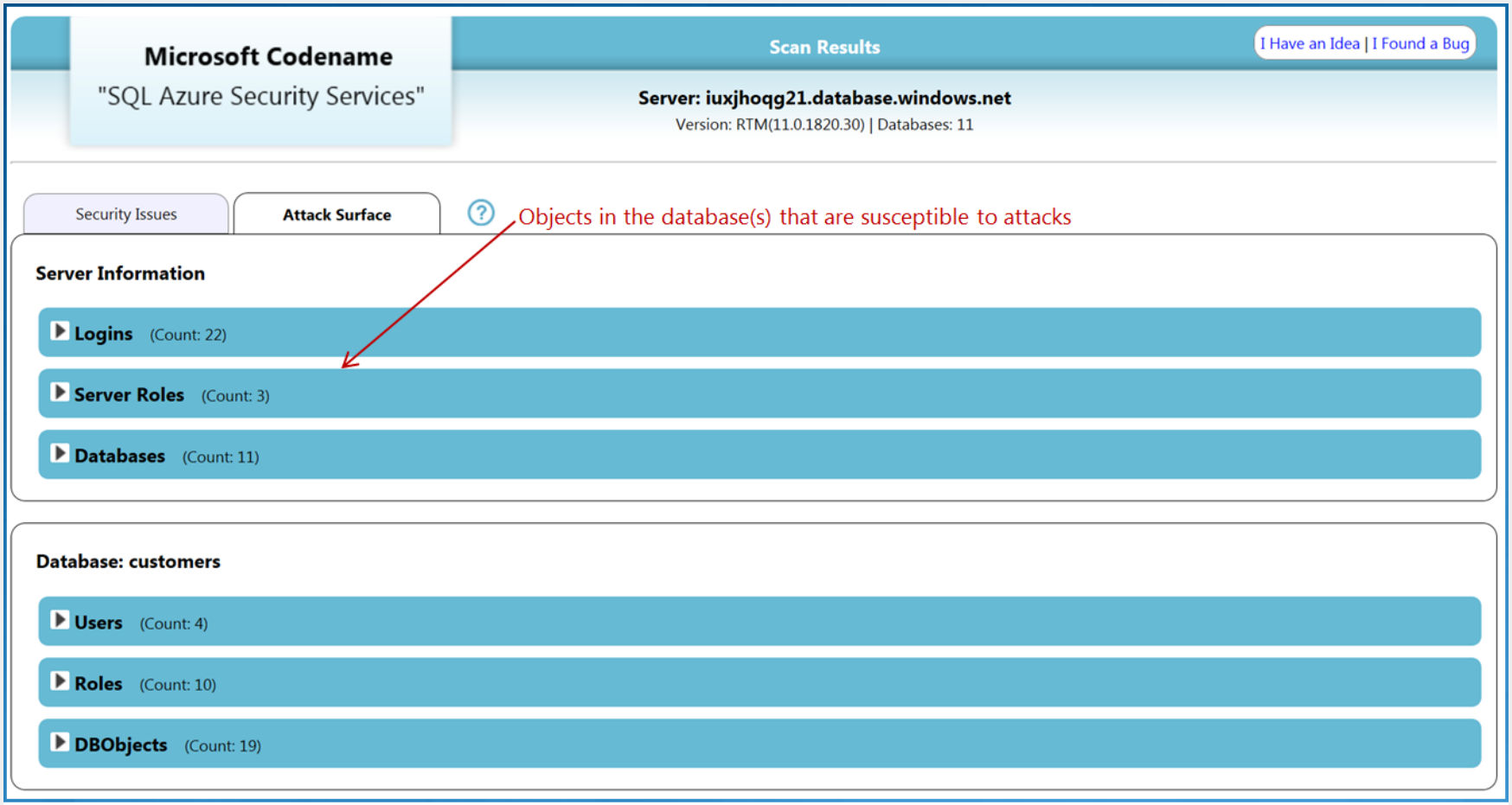
- Анализ архитектуры базы



# SQL Azure security services

Microsoft SQL Azure Labs

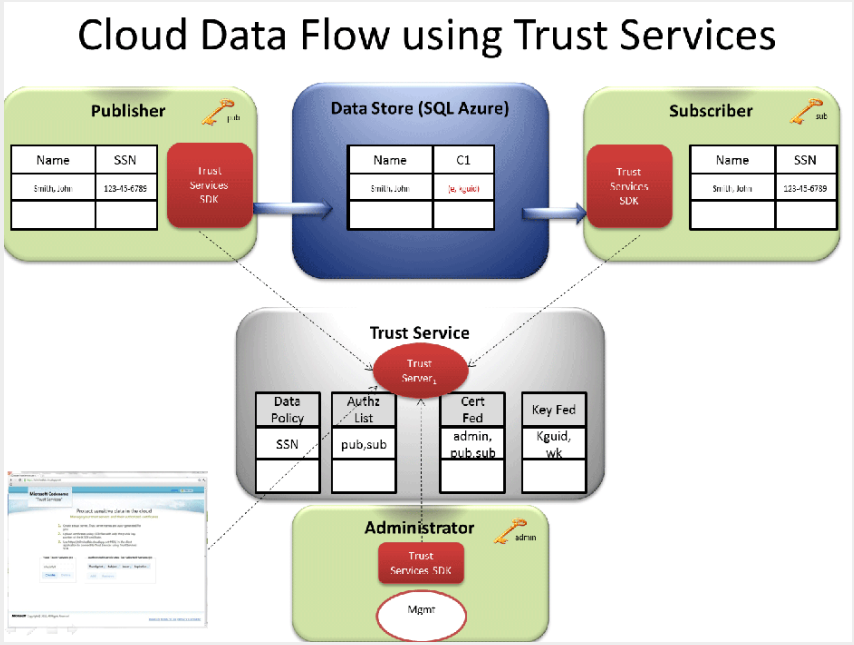
- Анализ объектов базы данных на потенциальные уязвимости



# SQL Azure Trust Services

Microsoft SQL Azure Labs

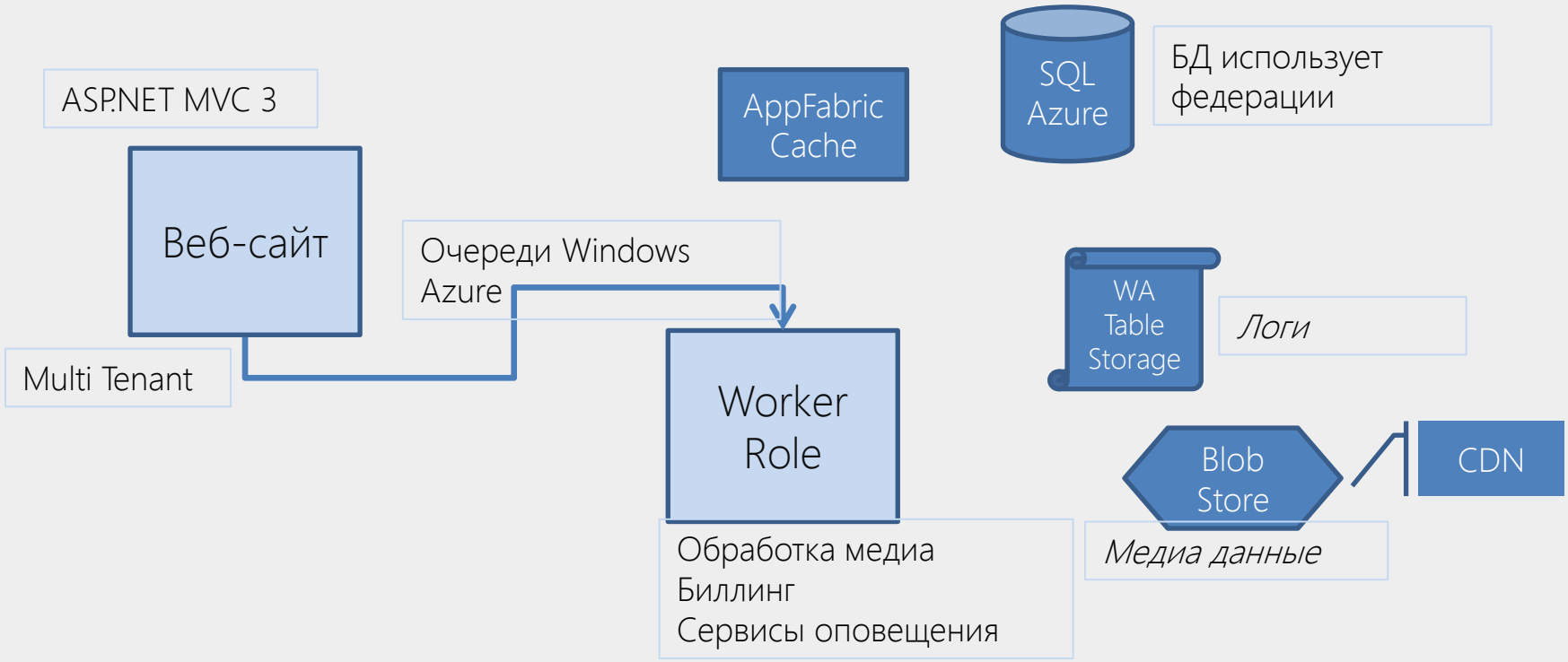
- Фреймворк для шифрованной обработки данных
- Данные хранятся в облаке уже в зашифрованном виде
- Удобное управление доступом к данным через портал



# Облачная CMS

SPORTFORT
http://sportfort.ru

- SportFort – CMS для спортсменов любителей и непрофессиональных спортивных команд ( сейчас более 1200 спортивных команд )
- Windows Azure используется как надежный и удобный веб-хостинг
- Стек технологий: ASP.NET, SQL Azure, Blob для медиа данных

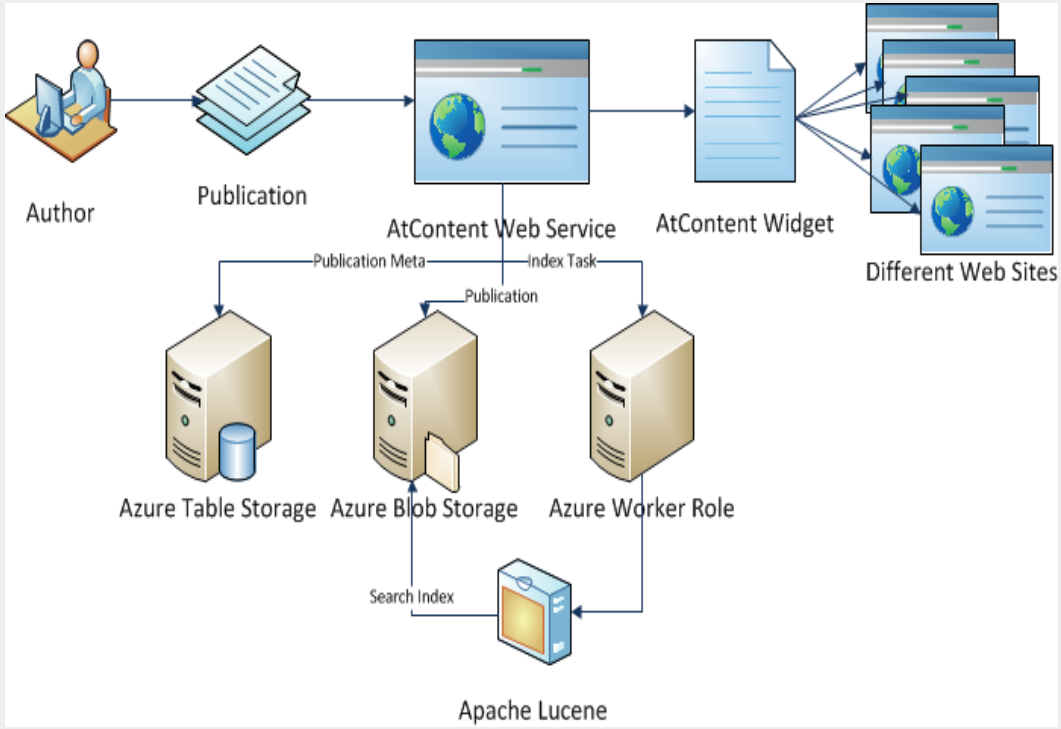


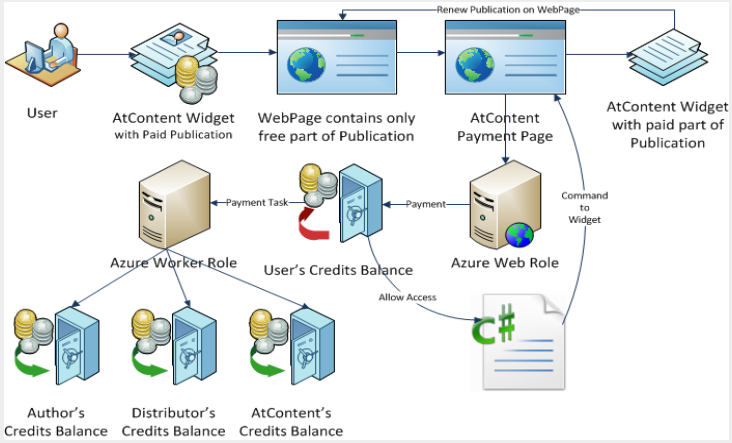
# Open-source технологии

AtContent™

http://atcontent.com

- Облачный сервис для создания, распространения и продажи авторского контента с использованием виджетов
- Как основная БД используется NoSQL TableStorage, Apache Lucene как движок для поиска
- Оплата авторам контента через PayPal



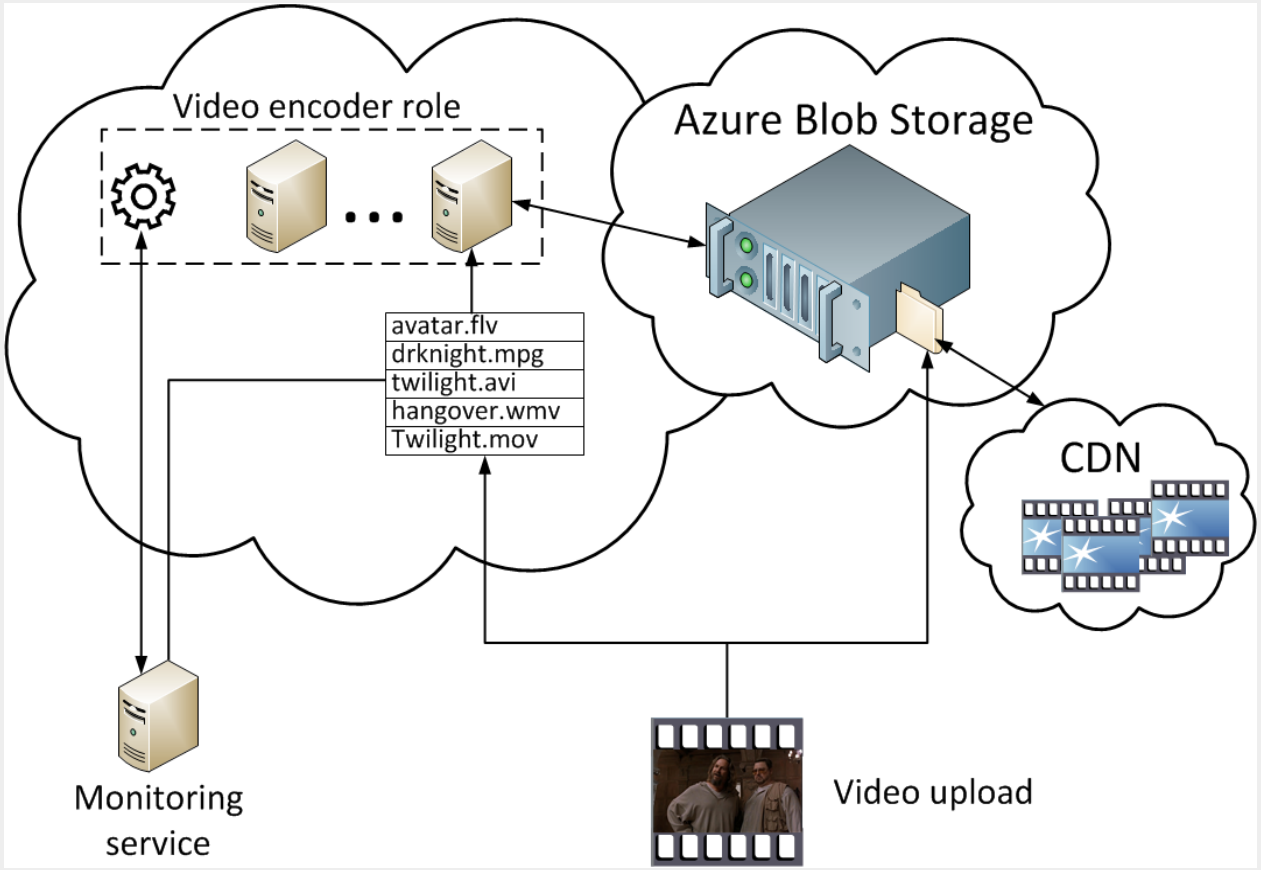




Интеграция с PayPal и механизм оплаты

# Надежность и автомасштабирование

- Всероссийская школьная образовательная сеть ( 19 620 школ, 2.4 млн учеников )
- Реализовано автоматическое масштабирование сервиса в зависимости от нагрузки
- Используется геобалансировка для повышения отказоустойчивости

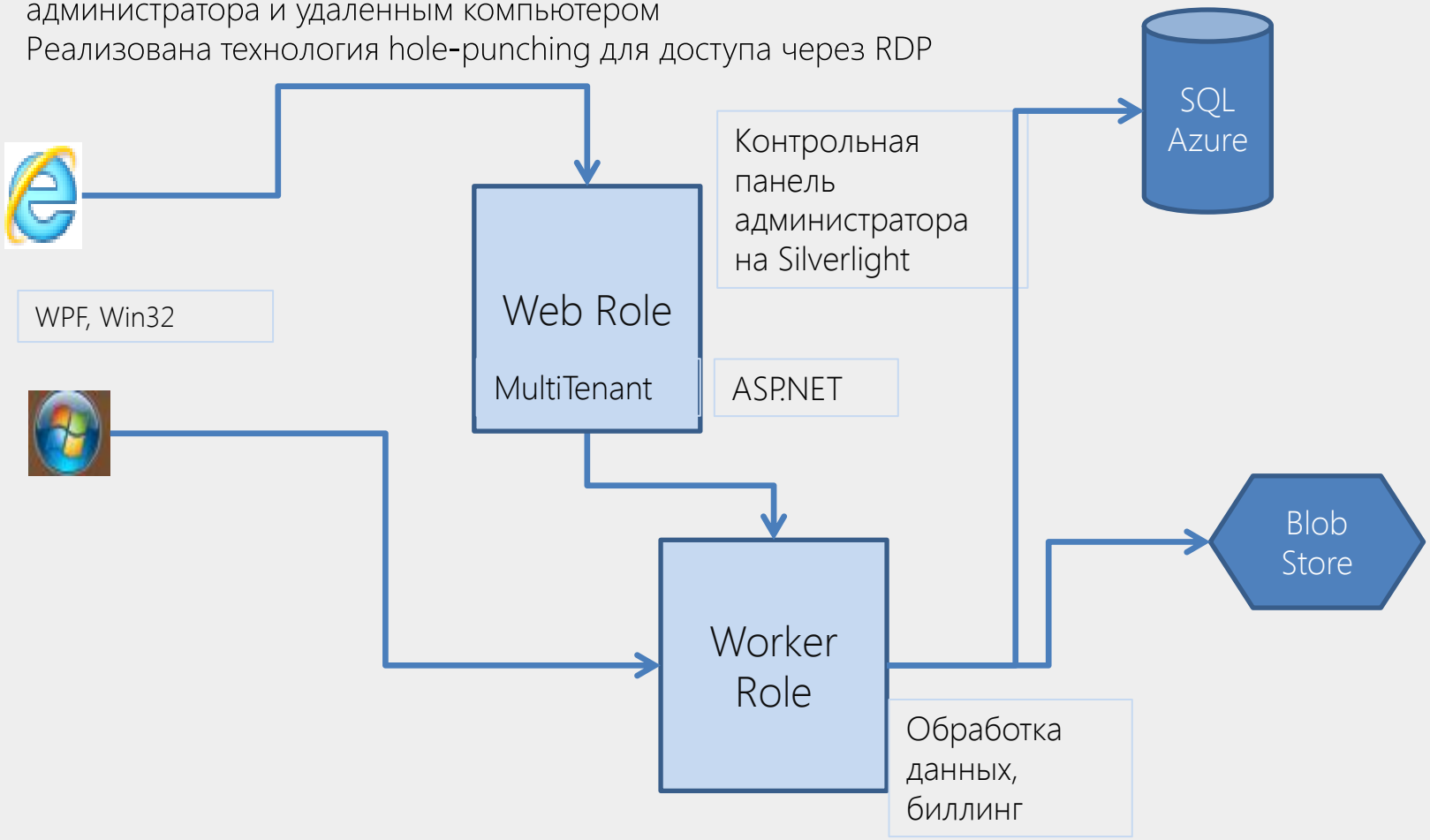
Дневник
http://dnevnik.ru



# Облако как связующее звено

ria-media software
SysAdmin Anywhere
http://ria-media.net

- Сервис для удаленного администрирования компьютерами Windows
- Windows Azure используется как связующее звено между лэптопом администратора и удаленным компьютером
- Реализована технология hole-punching для доступа через RDP



# Powered by Windows Azure: сделано в России

SPORTFORT
Веб платформа для спортивных команд


Пряники – сервис для нематериальной мотивации персонала

ria-media software
SysAdmin Anywhere
Сервис для удаленного управления IT ресурсами


Wizee Шопинг – мобильный гид по торговым центрам

Всероссийская школьная образовательная сеть

WebProfessionals.ru
Инструмент для выбора надежного партнера по разработке веб-сайтов

ABBYY
Облачный сервис по извлечению данных

Облачный сервис для организации и проведения онлайн мероприятий

Сервис для путешественников

Сервис для поиска работы

Управление процессом подбора персонала

Трансляция премии “Золотой граммофон” онлайн

Онлайн трансляции представлений

Тегирование изображений

# Powered by Windows Azure: сделано в России

RPserver
Платформа создания бизнес-приложений

ARTEZIO
Сервис создания и обработки диаграмм

AtContent™
Облачный сервис для дистрибуции авторского контента

wobot
Инструмент поиска по социальным медиа

Acumatica
ERP в облаке

magora
Портал для малого бизнеса

ClickBerry
Сервис создания динамического видео

news360
Новостной сервис на всех платформах

ЛАЙВ!
1С через интернет

WebSoft
IT-решения для управления эффективностью персонала

COMDI
Видео-трансляции

hyperclap
Социальная сеть интересных мест

SMEOn
Small and Medium Enterprises On-line
Универсальный SaaS для малого бизнеса

BOSS-Referent
Электронный документооборот

spellabs influence maps
Аналитическая система построения карт влияния

blogscloud
Облачный хостинг блогов

# Powered by Windows Azure: сделано в России


Система управления и контроль внутренних процессов


Мониторинг и аналитика брендов


Рейтинг блогосферы


Википедия бизнес-контактов


Обмен информацией о продуктах и технологиях

# 19 Июня – Windows Azure Workshop в Екатеринбурге

- Адрес : Большакова 70, офис Microsoft
- Начало в 13-00
- В програме – сервисы и возможности облачной плафтормы, примеры успешных внедрений облака в России, секция ответов на вопросы.

# Полезные ресурсы

- Windows Azure Trust Center: ou.gs/trust
- SQL Azure Labs: ou.gs/labs
- Группа разработчиков Windows Azure: ou.gs/user
- Сообщество по безопасности IT Security: ou.gs/itsec
- Блог Windows Azure в MSDN: ou.gs/msdn
- Наш твиттер Windows Azure: @windowsazure_ru
- Контактный email: azurerus@microsoft.com

# Спасибо за внимание!

# Thank you!

Алексей Боков, эксперт по платформе Windows Azure

e-mail: abokov@microsoft.com

Twitter: @abokov

## Ваши вопросы…