MVA jumpstart

Расширение возможностей ЦОД с помощью Microsoft Azure

Microsoft

Александр Шаповал | Эксперт по стратегическим технологиям

Александр Шаповал

Эксперт по стратегическим технологиям

Email: ashapo@microsoft.com

Blog: http://blogs.technet.com/b/ashapo

Twitter: @ashapoval

IT Camps, весна 2016

- IT Camp – это
  - Технологические семинары для ИТ-специалистов
  - Проводятся экспертами Microsoft
  - Предполагают выполнение лабораторных работ

- Материалы: http://1drv.ms/1kLGFB9
  - Что нового в Windows 10 Enterprise
  - Расширение возможностей ЦОД с помощью Microsoft Azure
  - Модернизация ИТ-инфраструктуры

Программа мероприятия

09:30 - 10:00	Регистрация
10:00 - 11:00	**Развертывание ресурсов в Azure с помощью ARM-шаблонов и GIT**
11:00 - 12:00	**Проектирование инфраструктуры Azure для высокопроизводительных вычислений и хранения данных**
12:00 - 12:15	Перерыв
12:15 - 13:15	**Проектирование сетевой инфраструктуры Azure для повышения безопасности**
13:15 - 14:00	Обед
14:00 - 15:15	**Использование Azure Site Recovery для защиты и миграции из локальной сети**
15:15 - 15:30	Перерыв
15:30 - 17:00	**Управление идентификационными данными с помощью Azure Active Directory**

MVA jumpstart

01 | Развертывание ресурсов в Azure с помощью ARM-шаблонов и GIT

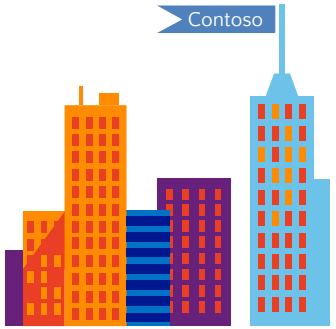
Microsoft

Александр Шаповал | Эксперт по стратегическим технологиям

Azure Resource Manager (ARM)

Уровень управления

Инструменты



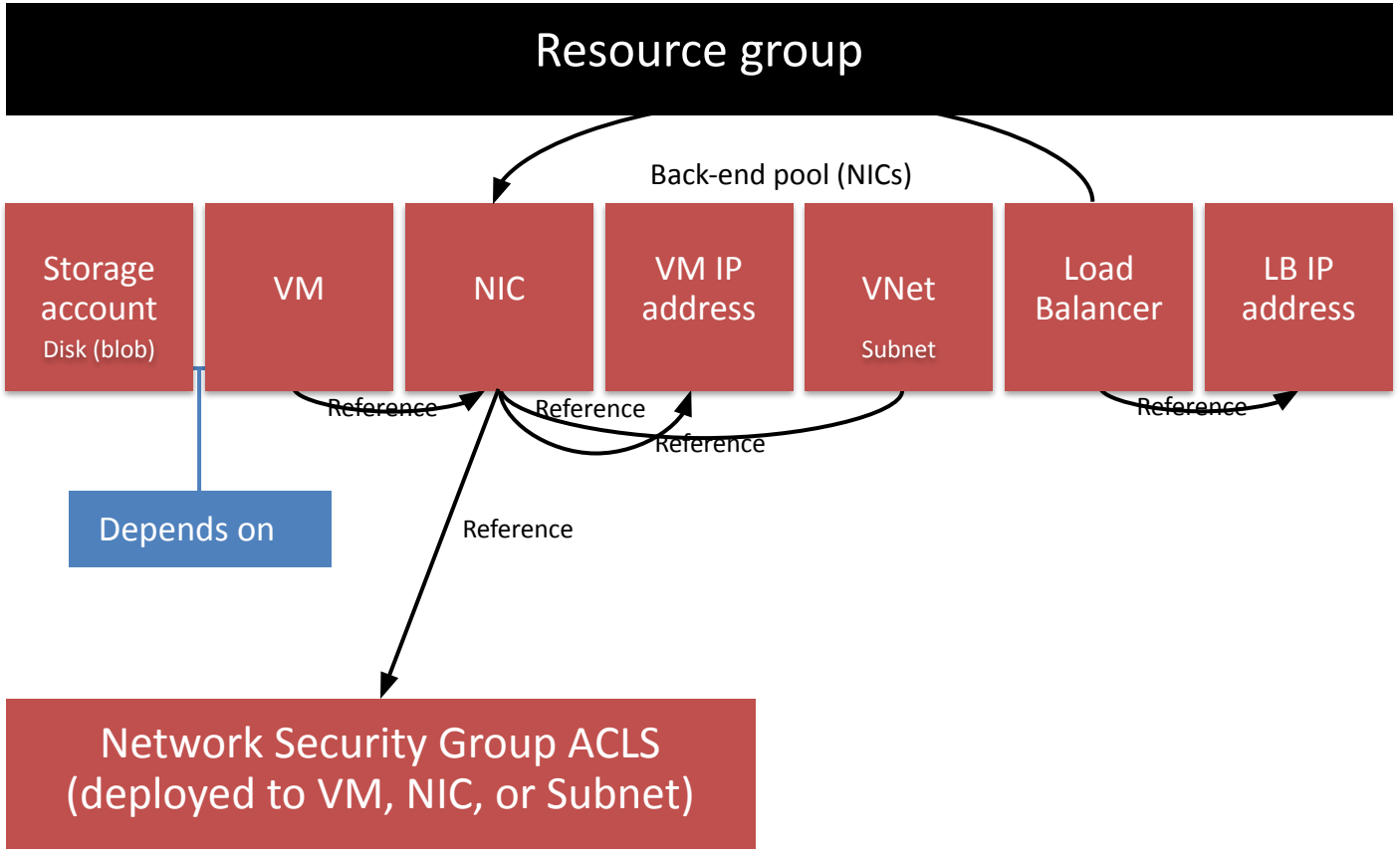
Расширения

Провай-деры

Пример использования Resource Manager

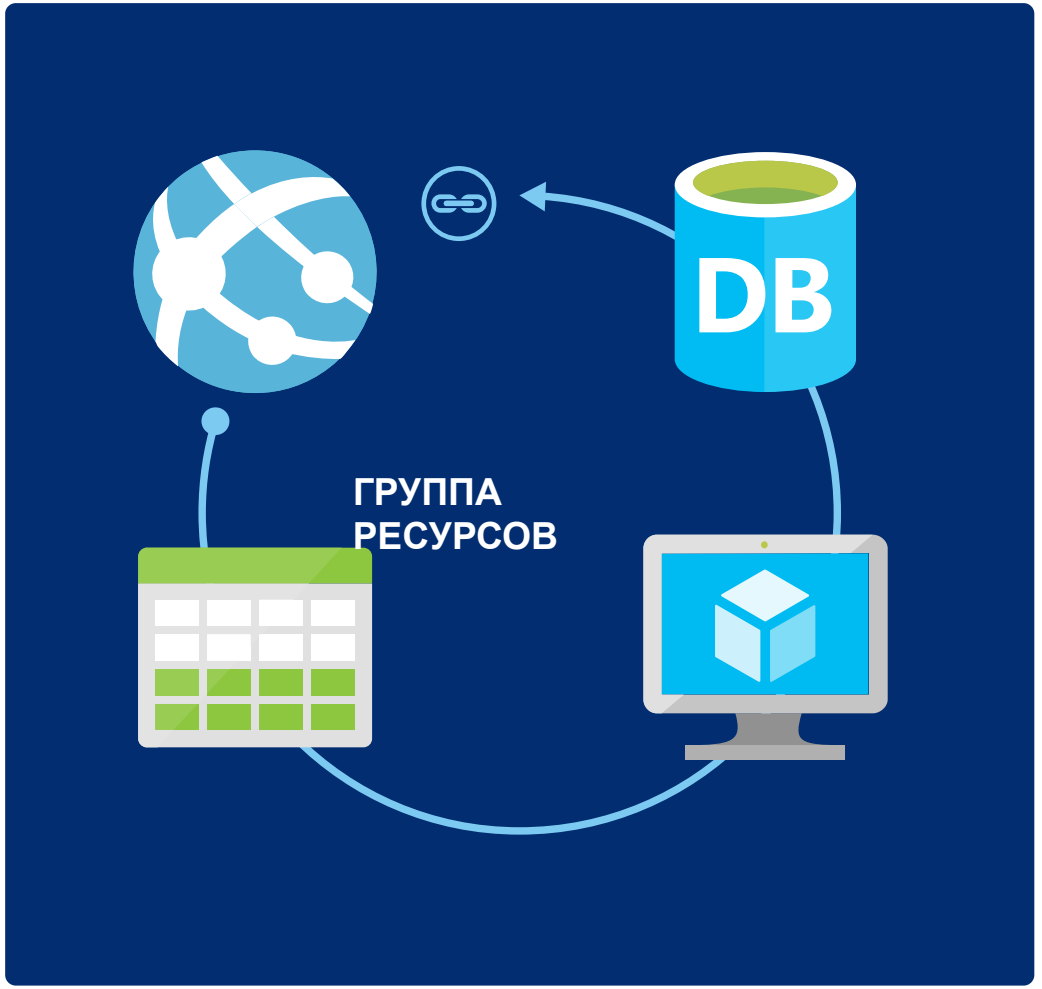
Классическая модель (v1)

Resource Manager (v2)



Группы ресурсов

- Контейнеры с множеством экземпляров ресурсов
- Каждый экземпляр относится к определенному типу ресурса
- Типы ресурсов определяются провайдерами ресурсов
- Каждый ресурс *должен* принадлежать одной и только одной группе ресурсов



Группа ресурсов: контейнер управления

- Жизненный цикл: развертывание, обновление, удаление, статус
- Группировка: учет, оплата, квота, интерфейс (портал, PowerShell, CLI)
- Контроль доступа: область применения разрешений RBAC
- Идентификационные данные: ресурсы могут взаимодействовать друг с другом

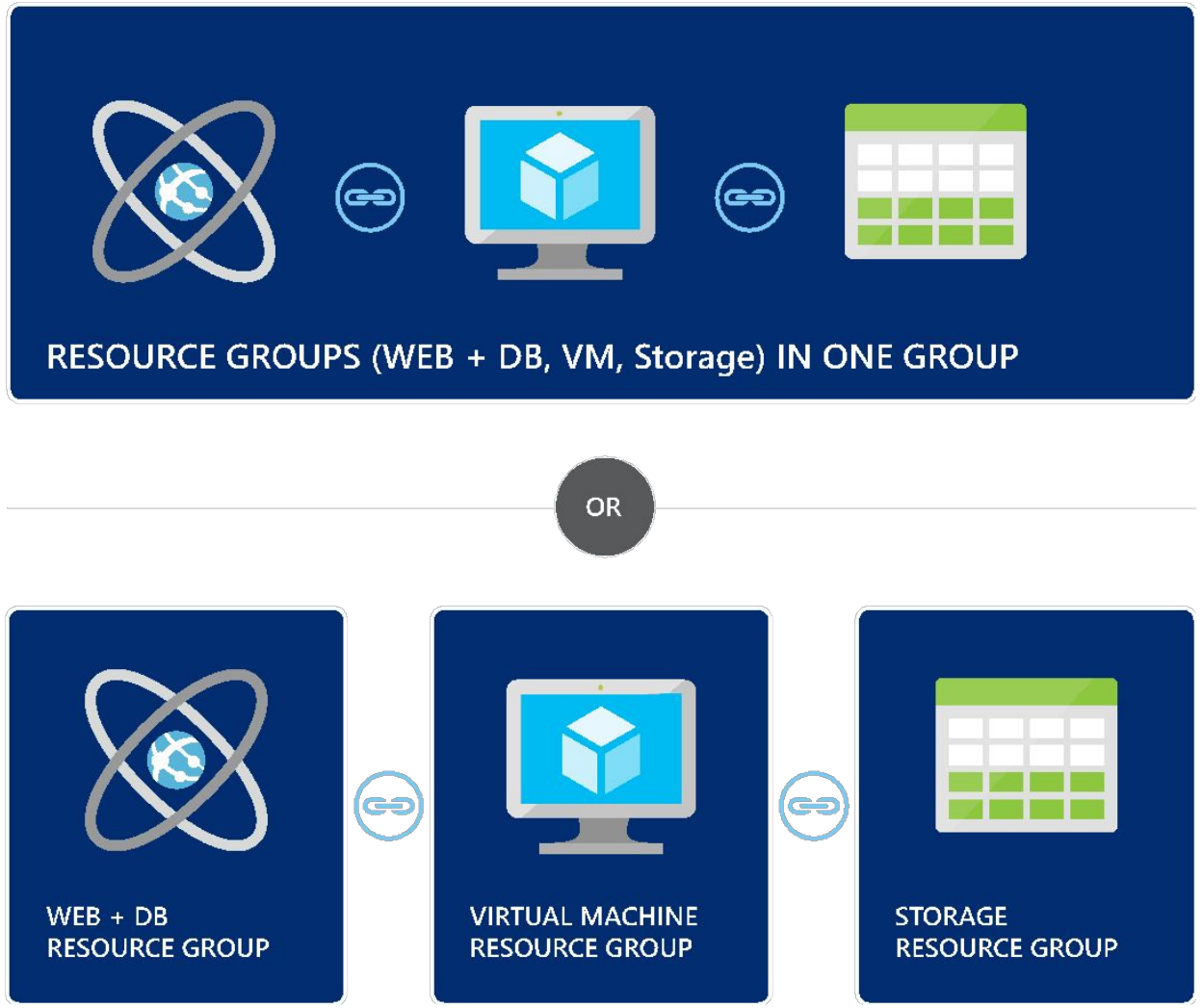
Жизненный цикл группы ресурсов

Вопрос:

Должны некоторые ресурсы принадлежать одной группе или разным?

Ответ:

Определяется тем, имеют ли они общий жизненный цикл и общее управление

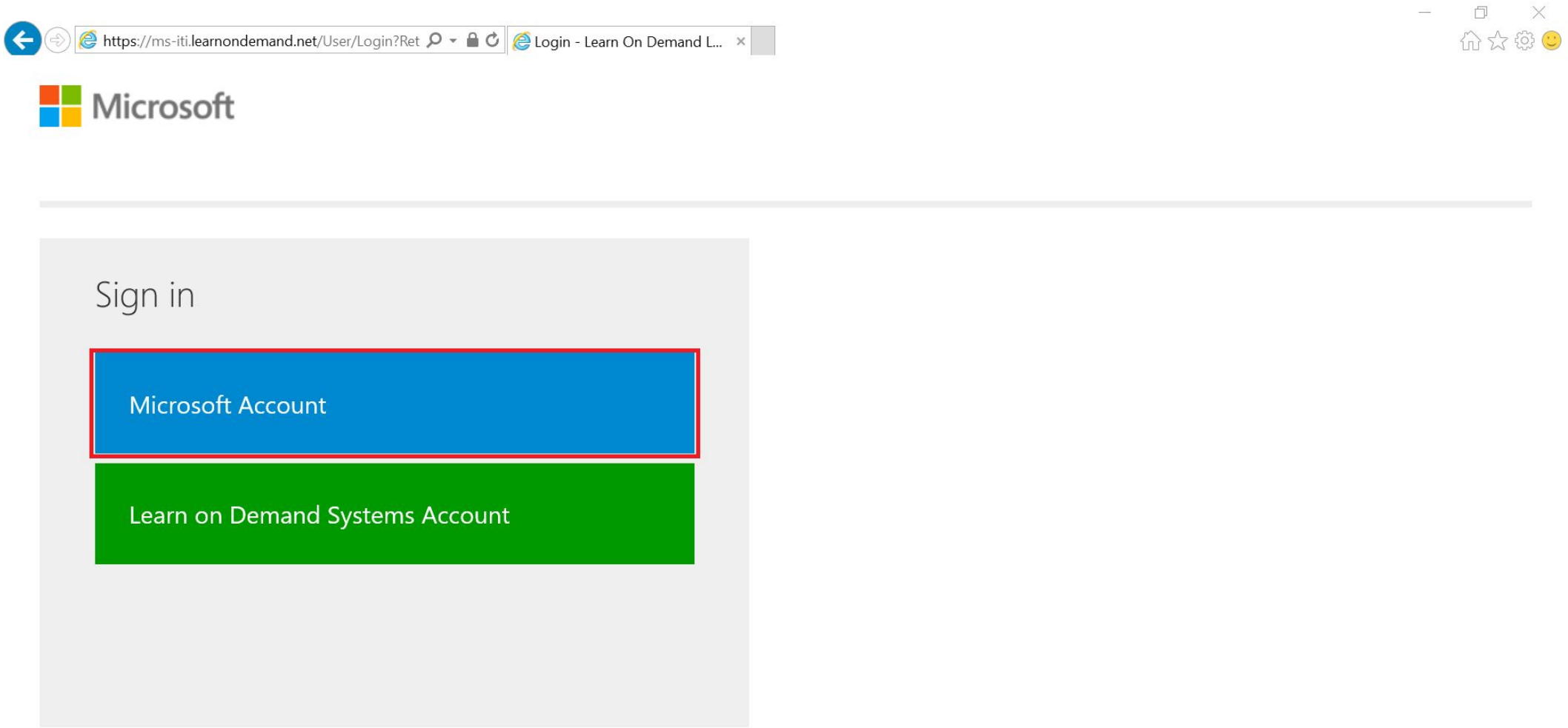


DEMO

Виртуальная машина на базе группы ресурсов

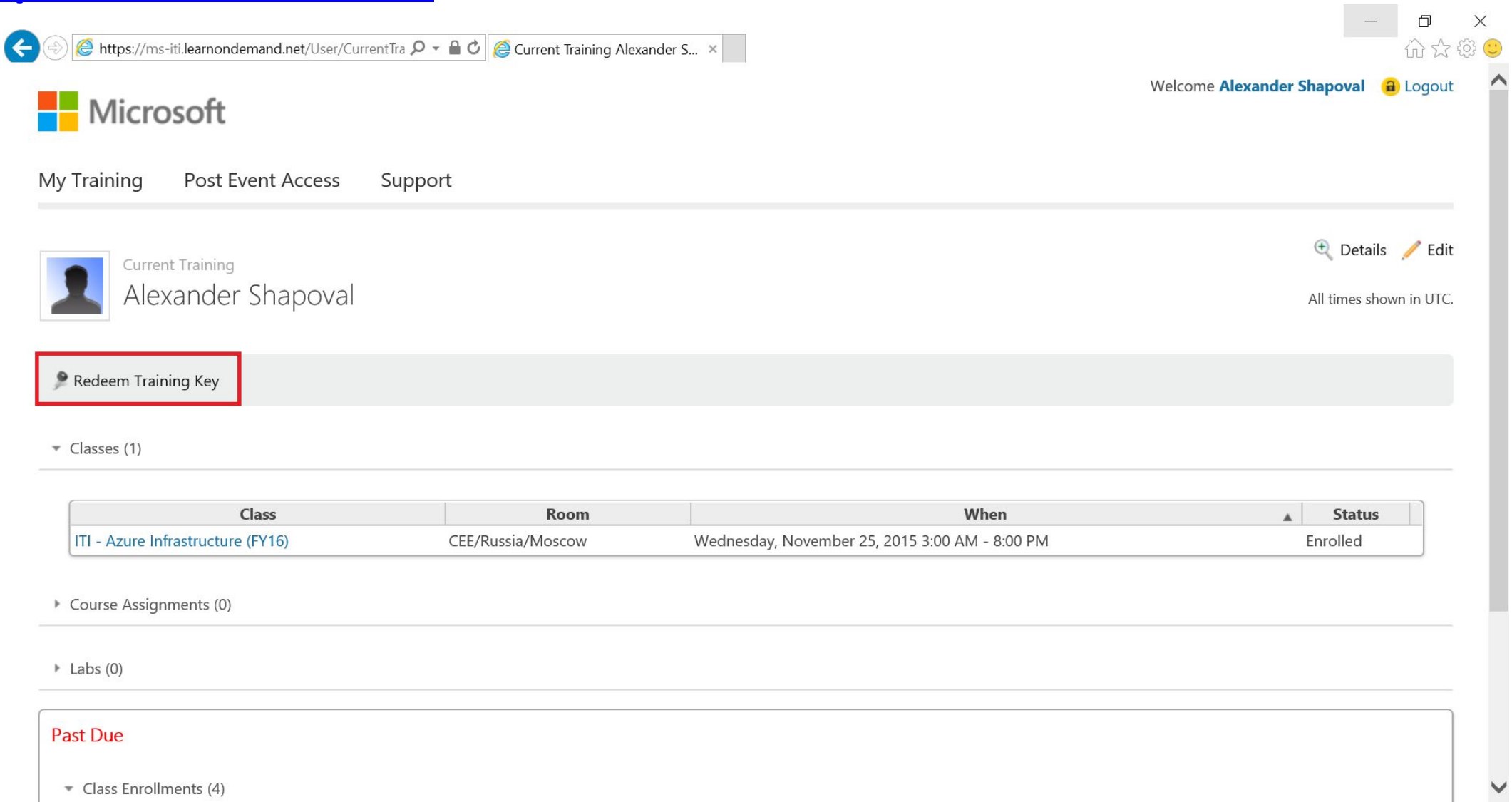
Подключение к лаб. работам

http://aka.ms/iti



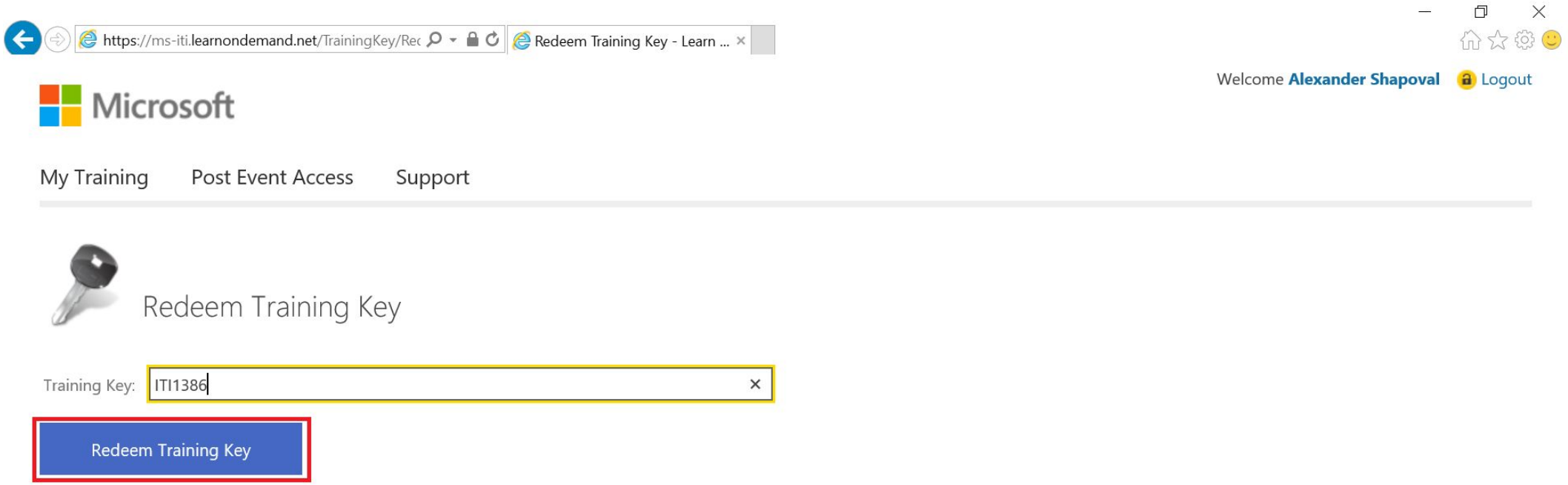
Подключение к лаб. работам

http://aka.ms/iti



Подключение к лаб. работам

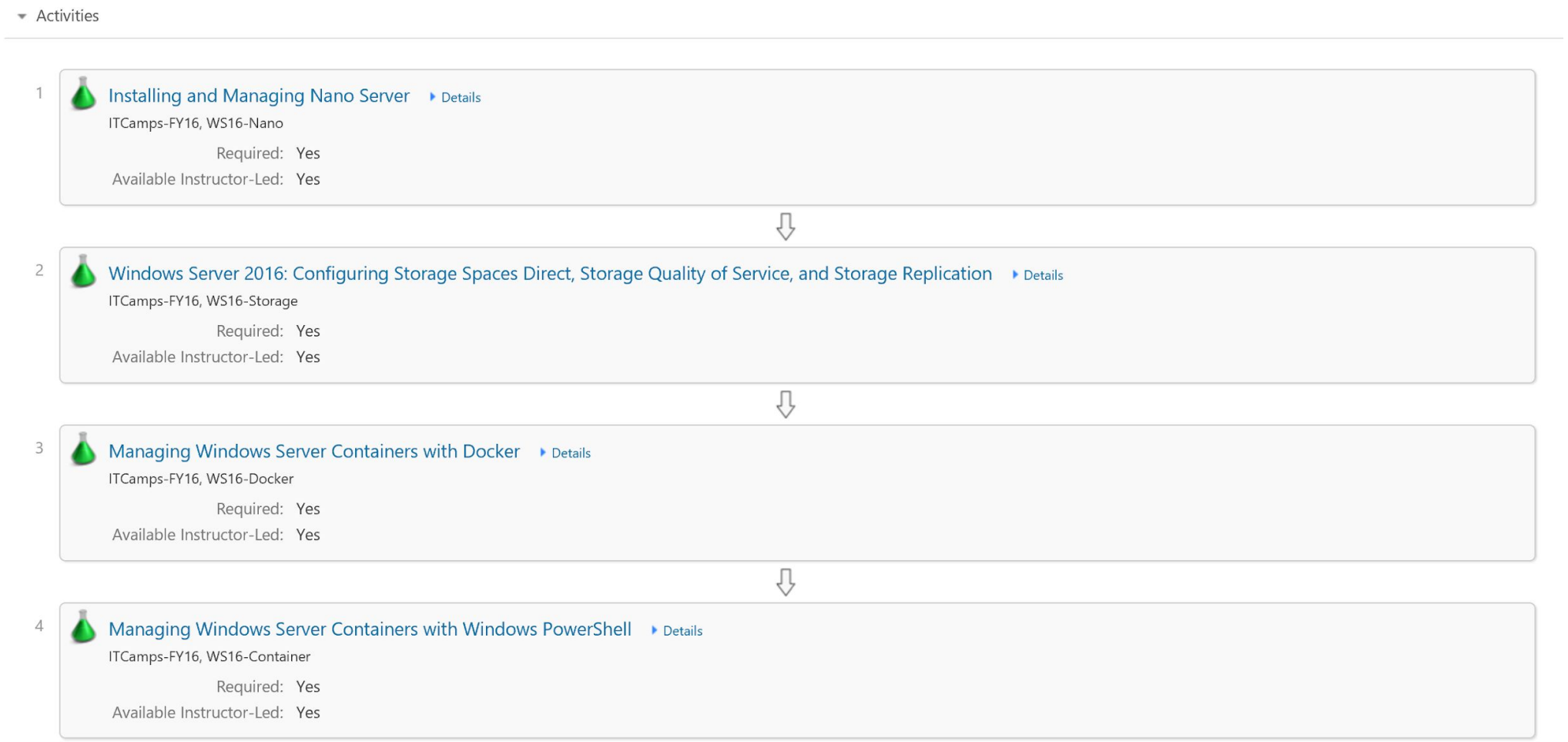
http://aka.ms/iti



Training Key: ITI2C856485

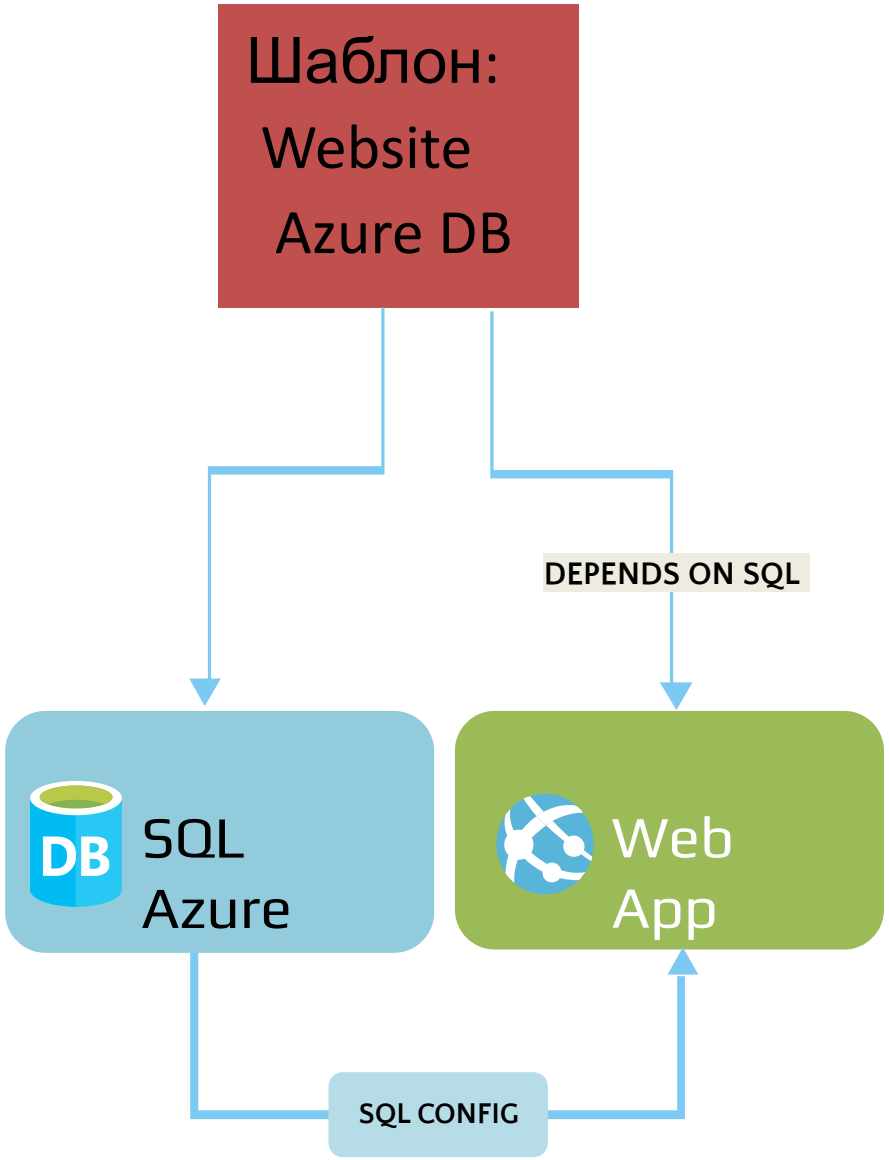
Подключение к лаб. работам

http://aka.ms/iti



Шаблоны ресурсов

- Основанная на модели декларативная спецификация ресурсов, их конфигурации, кода, расширений
- Многократная применимость
- Согласованное развертывание
- Использование в системах контроля версий
- Параметризация ввода/вывода

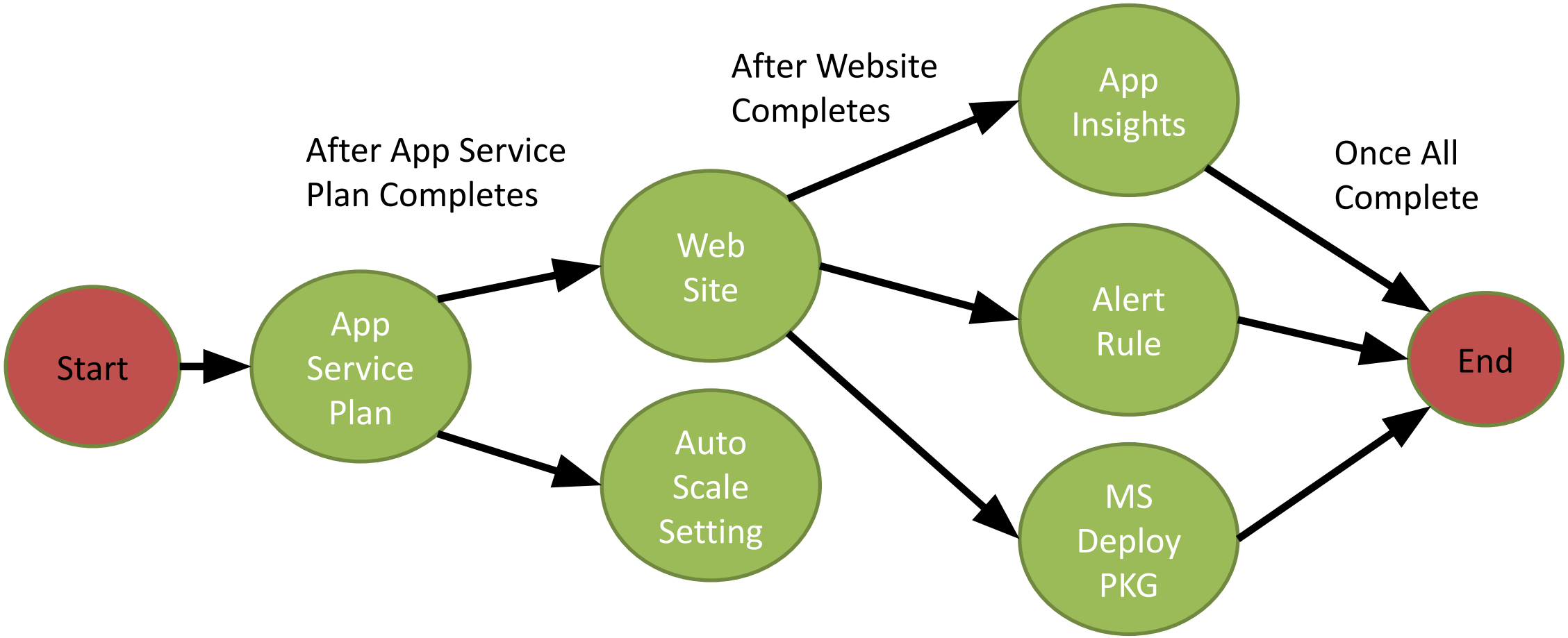


Разделы шаблона

- Параметры (Parameters): входные данные шаблона
- Переменные (Variables): переиспользование и сопоставление информации (например, выбор образа на основе региона)
- Ресурсы (Resources): описание всех ресурсов в группе
- Выходные данные (Outputs): фиксация информации в процессе выполнения (например, DNS-имя созданного блога)

Реализация шаблона

- Модуль выполнения строит машину состояния
- dependsOn() и reference() определяют зависимости



DEMO

Шаблоны группы ресурсов

MVA jumpstart

02 | Проектирование инфраструктуры Azure для высокопроизводительных вычислений и хранения данных

Microsoft

Александр Шаповал | Эксперт по стратегическим технологиям

Группы ресурсов

Контейнер для нескольких ресурсов

Управление ресурсами как единым целым

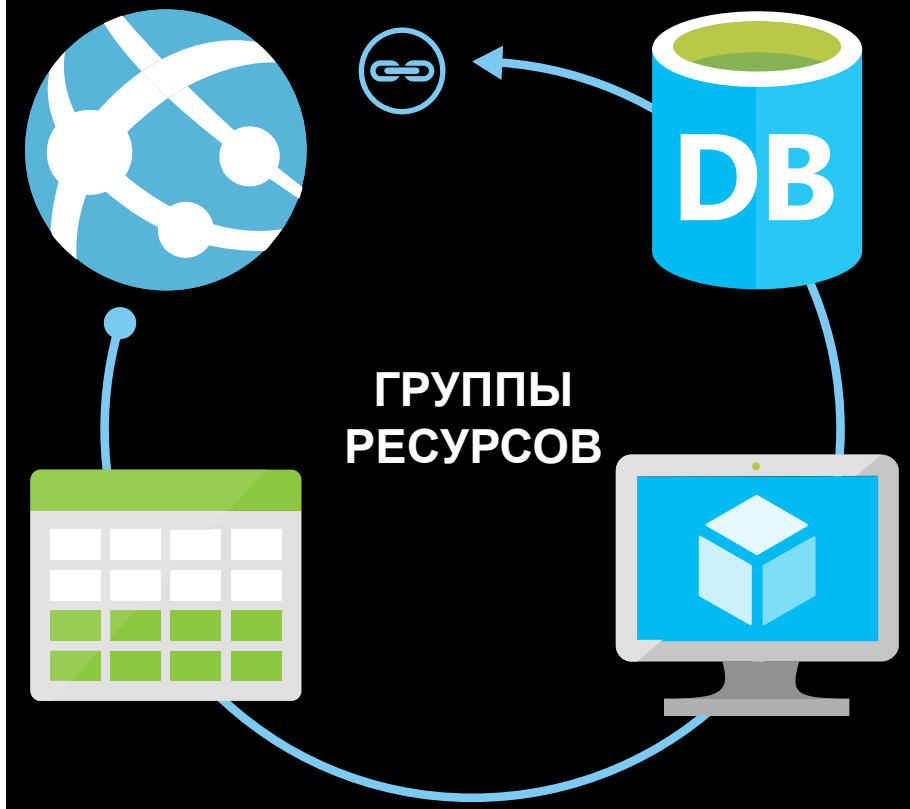
Ресурсы представлены в виде одной* группы

Группа ресурсов может охватывать разные регионы

Группа ресурсов может охватывать различные службы

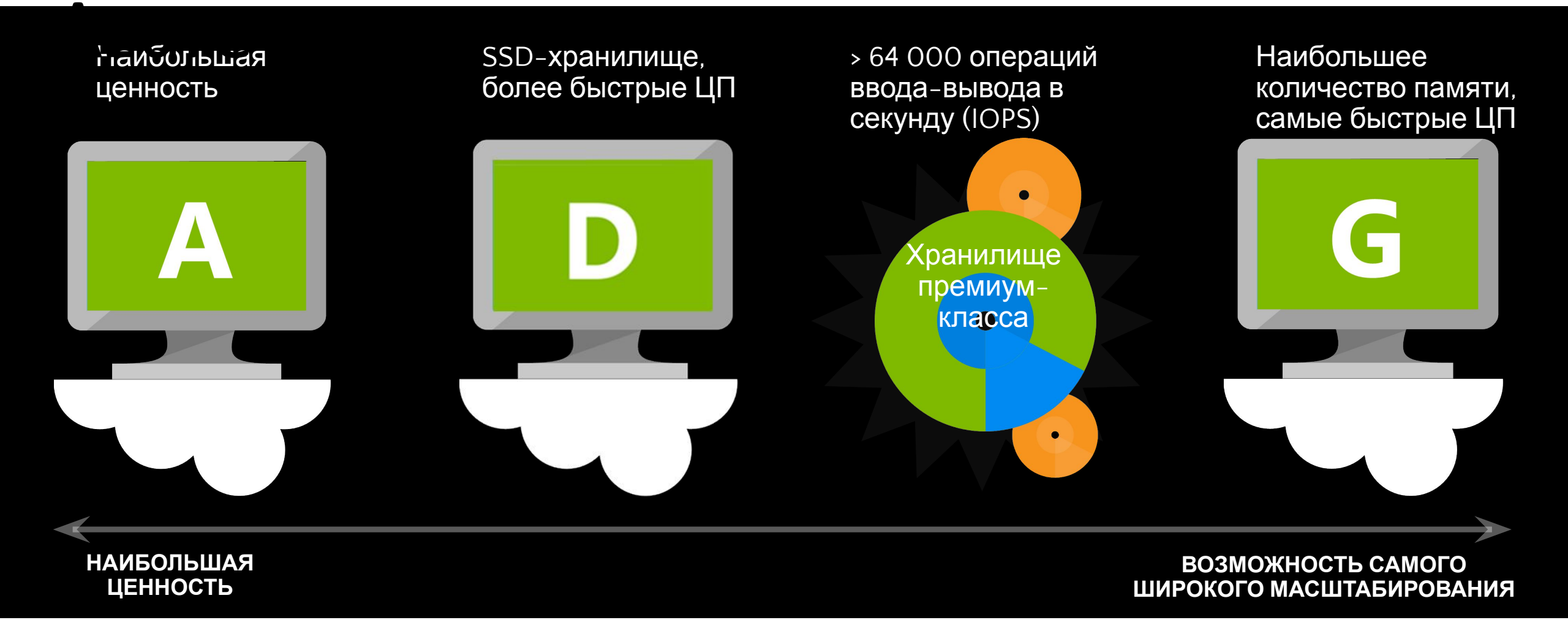
Управление доступом на основе ролей (RBAC) для групп или ресурсов

Присвоение тегов группам или ресурсам учета потребления



*и только одной

Семейства виртуальных машин



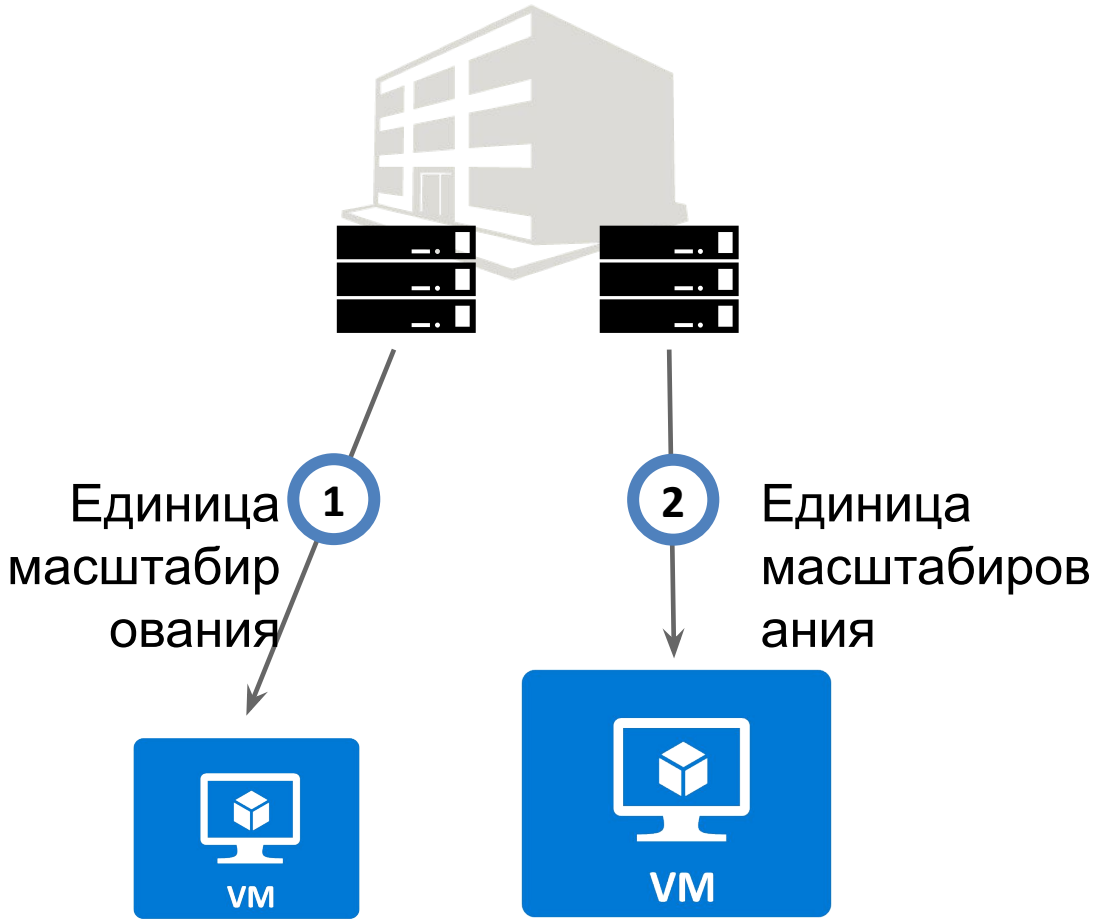
Единица масштабирования Azure (Azure scale unit)

Определение

Вычислительная единица, осуществляющая поддержку виртуальных машин определенных размеров

Каждая **облачная служба** привязана к одной единице масштабирования

Каждая **территориальная группа** с одной или более ВМ привязана к одной единице масштабирования



Влияние размера

Размер ВМ может изменяться только в рамках поддерживаемого диапазона и в той же единице масштабирования, где развернута ВМ

Единицы масштабирования и уровни ВМ

Basic

Единица масштабирования 1:
A0-A4
(первоначальные размеры ВМ)

- Без балансировки нагрузки, без автомасштабирования (масштабирование только в пределах A0-A4)
- Для небольших и средних приложений или рабочих нагрузок

Standard

Единица масштабирования 2:
A0-A7 (как SU1, но с A5-A7)

Единица масштабирования 3:
A8/A9 (ВМ “HPC”, оптимизированная сеть с Infiniband)

Единица масштабирования 4:
A0-A7 и D1-D14 (D-серии с SSD и улучшенными ЦП и все A0-A7)

Единица масштабирования 5:
G1-G5 (сверхмощные ВМ с ЦП Xeon до 32 ядер/448 ГБ ОЗУ/SSD-хранилищем объемом 6596 ГБ/64 дисками с данными)

Premium

Доступно для ВМ серий DS и GS

Хранилище премиум-класса

Высокая пропускная способность и низкая задержка

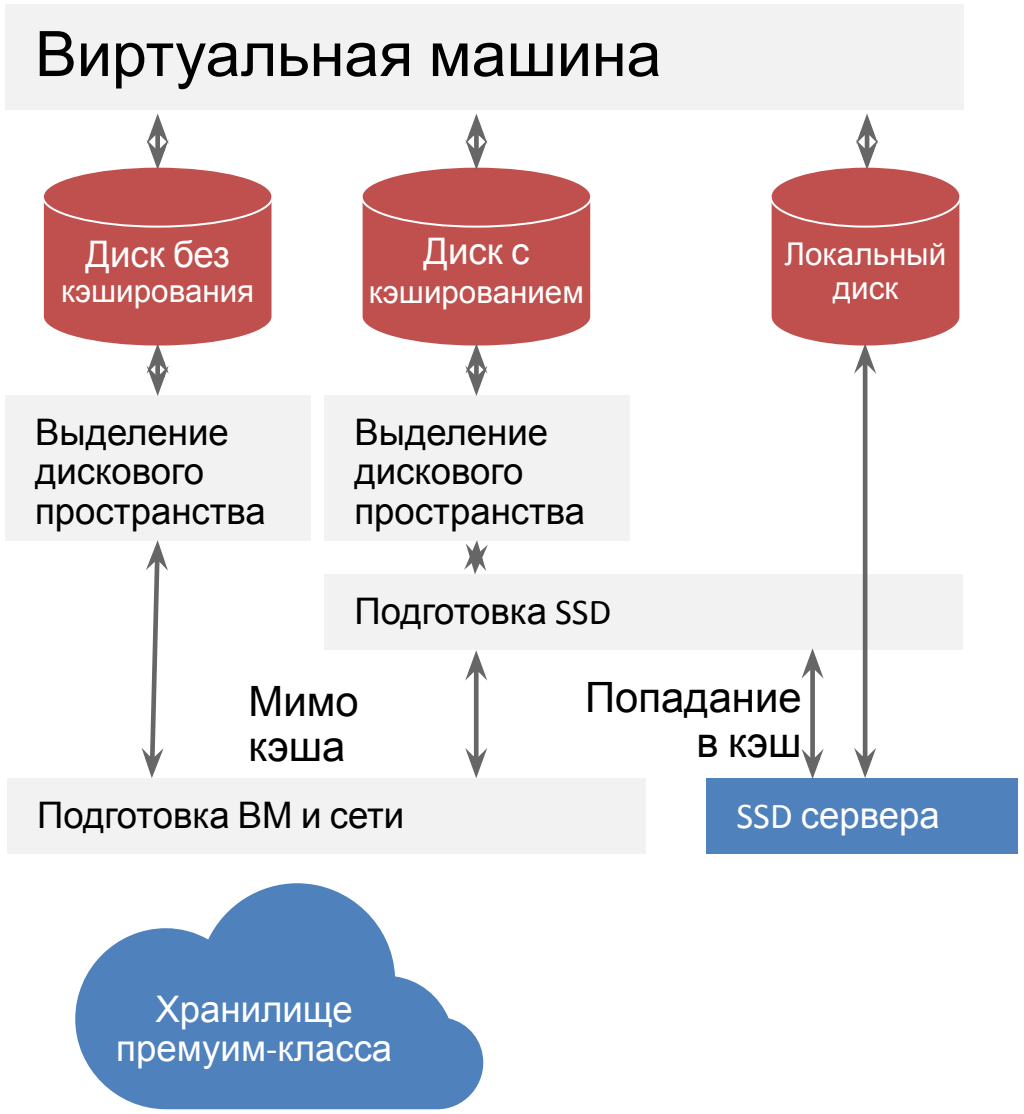
Емкость хранилища (Premium storage account) до 35 ТБ

До 80 000 операций ввода-вывода в секунду для ВМ

До 5000 операций ввода-вывода в секунду для диска

Около 5 мс на операции чтения и записи (без кэша)

Задержка при операции чтения менее 1 мс (кэш)



Анализ параметров производительности и существующих ограничений

Существуют лимиты на количество IOPS и на пропускную способность диска

Лимиты установлены на диск, на ВМ и на учетную запись хранения

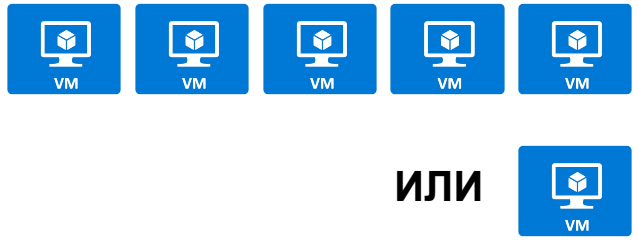
Не более 20 000 IOPS на учетную запись хранения (premium storage

Тип диска хранения	P10	P20	P30
Размер диска	128 ГБ	512 ГБ	1024 ГБ (1 ТБ)
Количество операций ввода-вывода в секунду для каждого диска	500	2300	5000
Пропускная способность диска	100 МБ в секунду	150 МБ в секунду	200 МБ в секунду

Размер ВМ	Число ядер ЦП	Макс. число операций ввода-вывода в секунду для диска (на одну ВМ)	Максимальная пропускная способность диска (на одну ВМ)	Размер кэша (ГБ)
STANDARD_DS1	1	3200	32 МБ в секунду	43
STANDARD_DS2	2	6400	64 МБ в секунду	86
STANDARD_DS3	4	12 800	128 МБ в секунду	172
STANDARD_DS4	8	25 600	256 МБ в секунду	344
STANDARD_DS11	2	6400	64 МБ в секунду	72
STANDARD_DS12	4	12 800	128 МБ в секунду	144
STANDARD_DS13	8	25 600	256 МБ в секунду	288
STANDARD_DS14	16	50 000	512 МБ в секунду	576
STANDARD_GS1	2	5000	125 МБ в секунду	264
STANDARD_GS2	4	10 000	250 МБ в секунду	528
STANDARD_GS3	8	20 000	500 МБ в секунду	1056
STANDARD_GS4	16	40 000	1000 МБ в секунду	2112
STANDARD_GS5	32	80 000	2000 МБ в секунду	4224

Сколько учетных записей хранения требуется?

Это зависит от ограничений (диск или ВМ)...

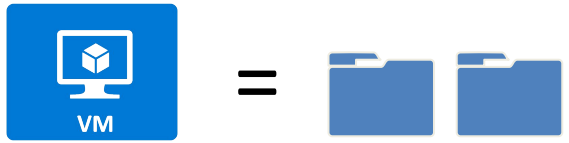


ПРИМЕР:

5 ВМ на дисках P30 (макс. 5000 операций ввода-вывода в секунду) **ИЛИ**

Одна ВМ с пятью чередующимися дисками P30 = 25 000 операций ввода-вывода в секунду

Значит, в обоих случаях понадобятся две учетные записи хранения, чтобы достичь уровня 25 000 операций ввода-вывода в секунду

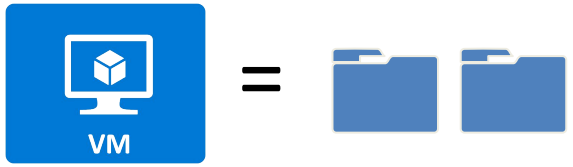


12 000 IOPS

ПРИМЕР:

ВМ поддерживают до 12 000 операций ввода-вывода в секунду **Нам нужно три таких машины...**

~~(3 x 12 000 = 36 000) : 20 000 = 2 учетные записи хранения~~



Максимум: 35 ТБ

ПРИМЕР:

Максимальное допустимое дисковое пространство для учетных записей премиум-класса – 35 ТБ

Чтобы получить 64 дисков по 1 ТБ (это допустимо для ВМ GS5), понадобятся две учетные записи хранения

Типы хранилищ Azure

Двоичные объекты (blobs) блоков и страниц, диски, таблицы, очереди, файлы

	Локальное отказоустойчивое хранилище (LRS)	Хранилище с механизмом отказоустойчивости по зонам (ZRS)	Хранилище с географическим механизмом отказоустойчивости (GRS)	Хранилище с географическим механизмом отказоустойчивости с доступом для чтения (RA-GRS)
Как это работает	Создается множество синхронных копий данных в рамках одного ЦОД	В нескольких ЦОД или в разных регионах хранится три копии данных Только для больших двоичных объектов блоков	Аналогично LRS, но с несколькими асинхронными копиями, хранящимися во втором ЦОД за несколько сотен километров от первого	Аналогично GRS, но с правом чтения, представляемого второму ЦОД
Всего копий	3	3	6	6
Зачем это нужно	Для экономичного хранения данных в локальной среде или с целью соответствия требованиям, предъявляемым к управлению данными	Экономичный способ хранения больших двоичных объектов блоков с повышенной устойчивостью	Для защиты от наиболее распространенных сбоев и аварий ЦОД	Обеспечивает доступ с правом чтения к данным во время сбоя; максимальная доступность и устойчивость данных
Соглашение об уровне обслуживания, регламентирующее доступность	99,9 % чтение и запись	99,9 % чтение и запись	99,9 % чтение и запись	99,9 % запись 99,9 % чтение

https://azure.microsoft.com/en-us/pricing/details/storage/

Работа с временным диском

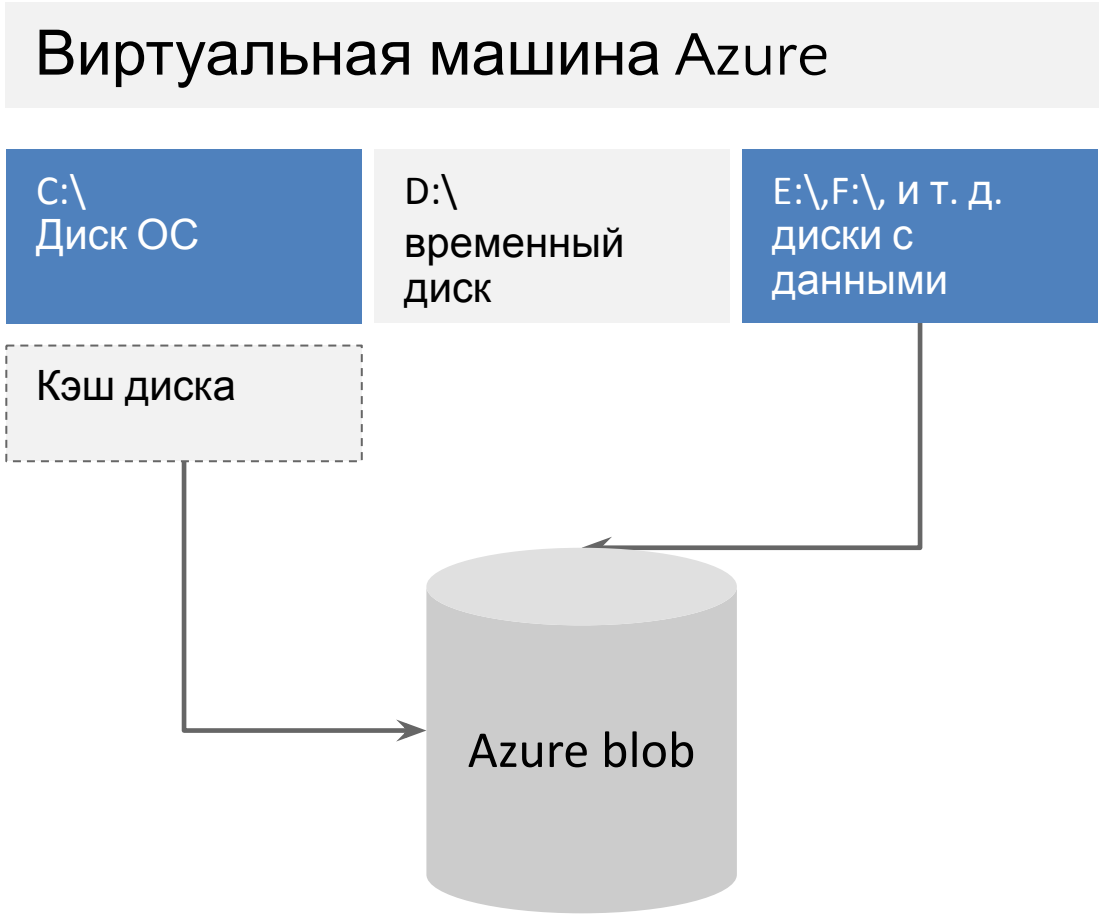
Никогда не размещайте критически важные непродублированные данные на временном диске!

Используйте его только для работы с SQL TempDB и Buffer Pool Extensions на ВМ серий D и G (временные диски SSD)

http://blogs.technet.com/b/dataplatforminsider/archive/2014/09/25/using-ssds-in-azure-vms-to-store-sql-server-tempdb-and-buffer-pool-extensions.aspx

Используйте планировщик для задач на временных дисках

Тестируйте запланированные задачи при помощи операции по изменению размера ВМ



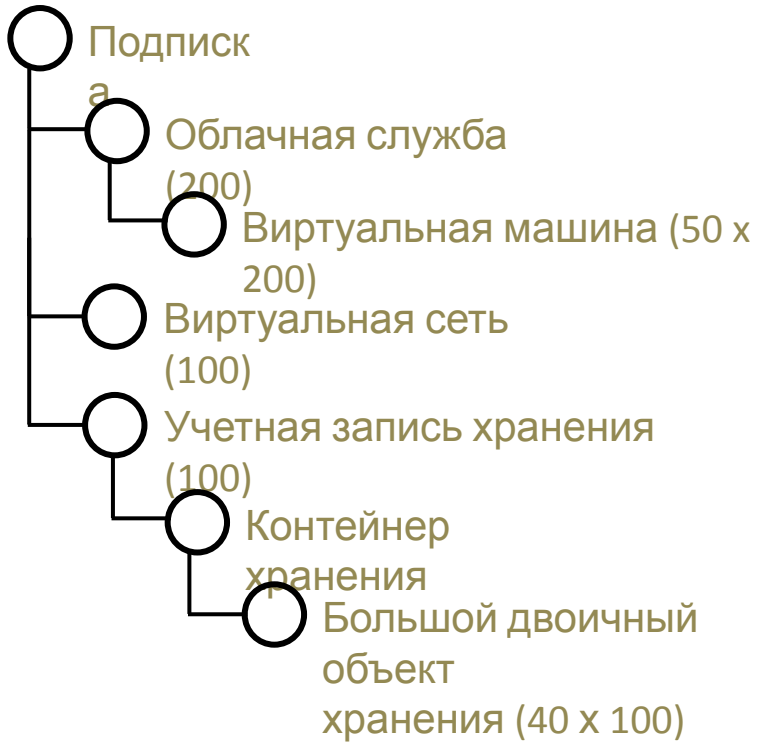
Производительность временного диска (серия D)

Кол-во ядер	Размеры ВМ	Размер временного диска (ГБ)	Макс. число операций ввода-вывода в секунду	Макс. скорость считывания (МБ/с)	Макс. скорость записи (МБ/с)
1	Standard_D1	50	3000	48	24
2	Standard_D2 Standard_D11	100	6000	96	48
4	Standard_D3 Standard_D12	200	12 000	192	96
8	Standard_D4 Standard_D13	400	24 000	384	192
16	Standard_D14	800	48 000	768	384

http://azure.microsoft.com/blog/2014/10/06/d-series-performance-expectations/

Основные понятия

Иерархия



Лимиты и блокировка

Объект	Лимит	Блокировка
Подписка	120 операций создания и (или) добавления в 5-минутном окне	Нет данных
Облачная служба	200 на подписку	~ 3 мин на обновление
Виртуальная машина	50 на облачную службу 2048 на виртуальную сеть	Нет
Виртуальная сеть	100 на подписку	Единый API для изменений
Учетная запись хранилища	100 на подписку	Нет
Контейнер хранения	Без ограничений	Нет
Большой двоичный объект для хранения	40 на учетную запись хранения	Один большой двоичный объект на контейнер в единицу времени для учетной записи хранения

http://azure.microsoft.com/en-us/documentation/articles/azure-subscription-service-limits/

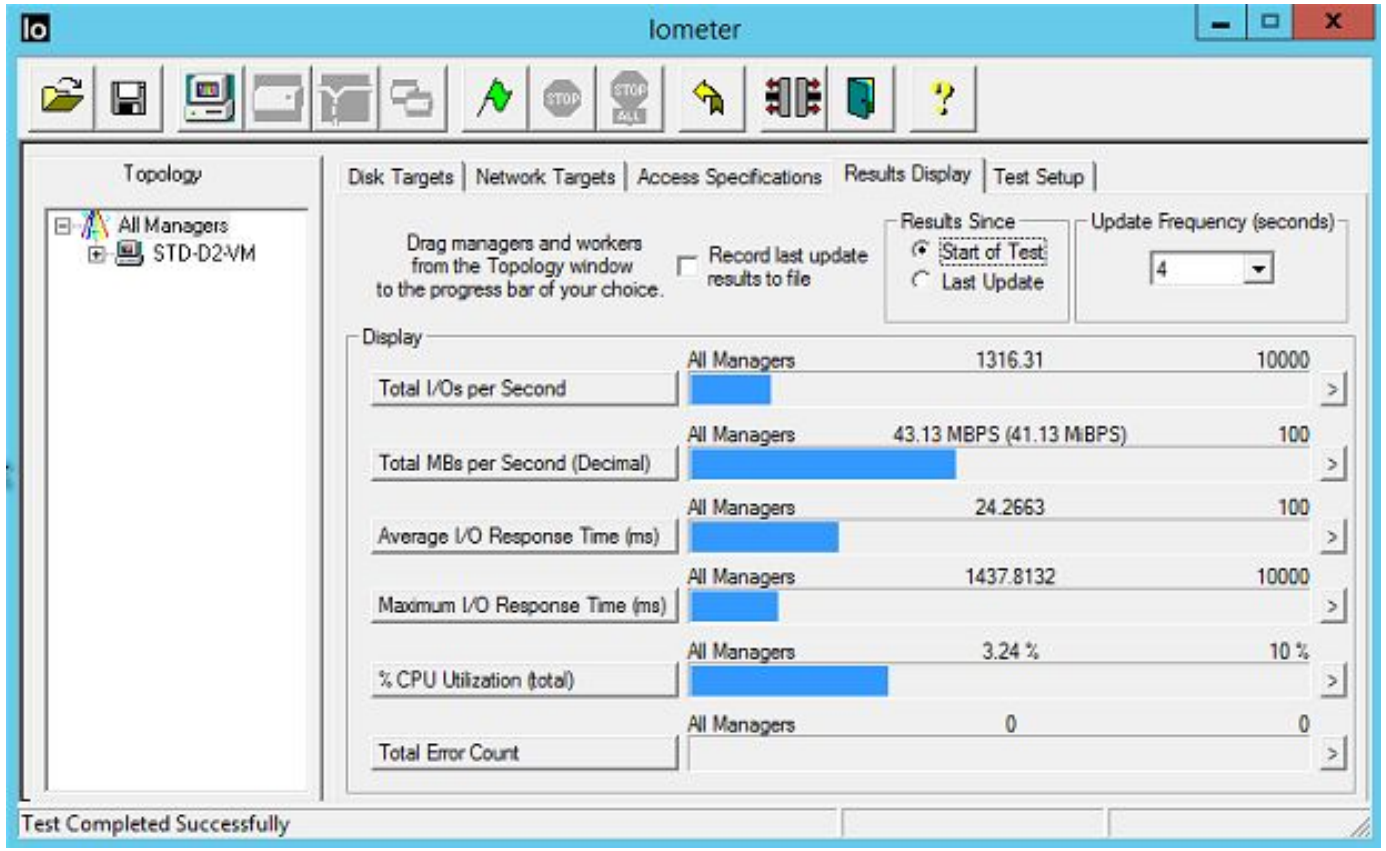
Iometer

Инструмент для измерения скорости ввода-вывода подсистемы и определения параметров отдельных и кластерных систем

Используется для оценки производительности и устранения неполадок

Простая настройка для репликации поведения любого популярного приложения

Одно из наиболее часто проводимых измерений – определение количества операций ввода-вывода в секунду



MVA jumpstart

03 | Проектирование сетевой инфраструктуры Azure для повышения безопасности

Microsoft

Александр Шаповал | Эксперт по стратегическим технологиям

Виртуальная сеть Azure

Стройте собственные сети

Логическая изоляция с контролем сетевых операций

Создавайте подсети с частными или общедоступными IP-адресами

Используйте собственную DNS или DNS Azure

Защитите ВМ с помощью групп сетевой безопасности

Запускайте высокодоступные внутренние службы с подсистемой балансировки нагрузки

Адресация в классической модели

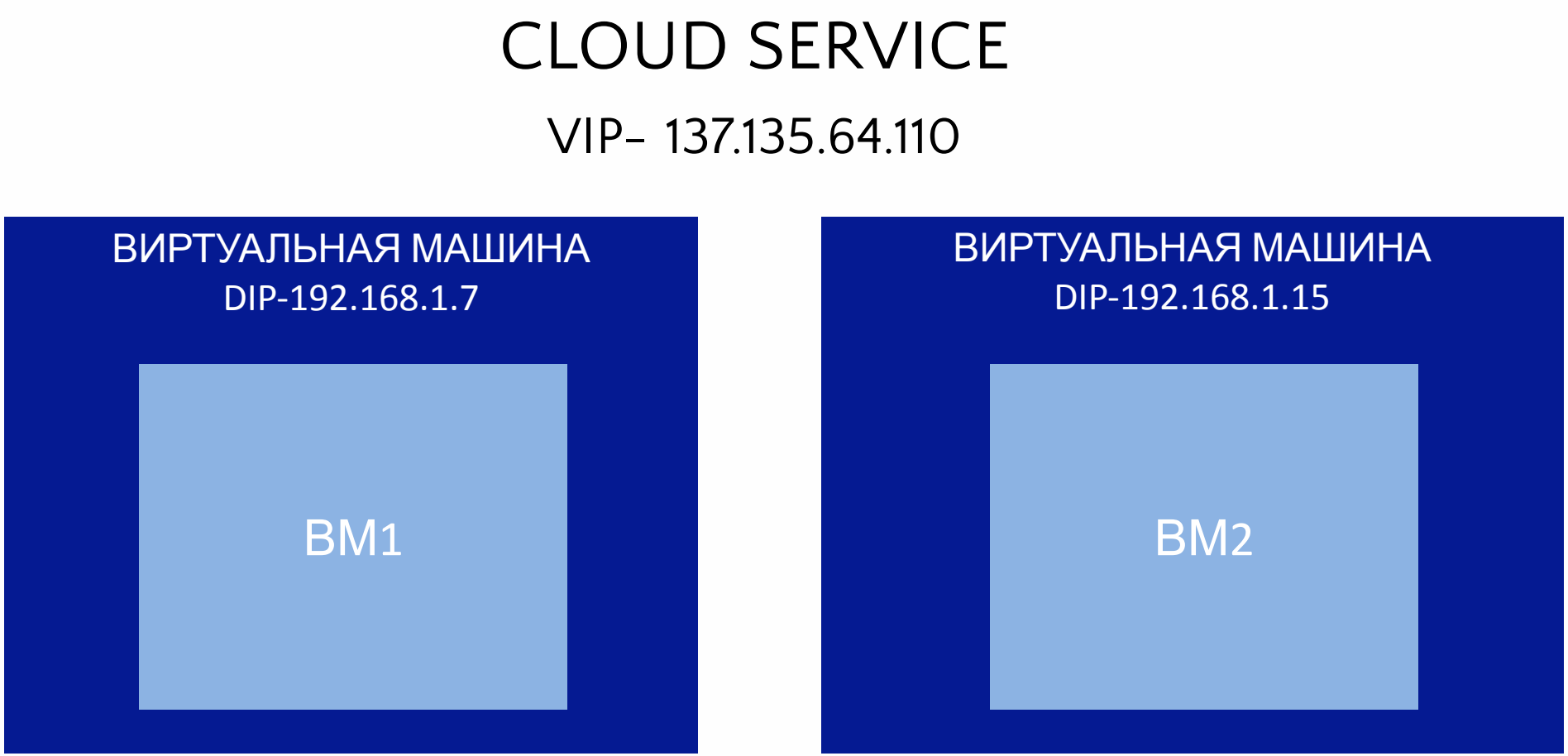
VIP – Virtual IP address

- Публичный IP, не привязан к конкретной ВМ или сетевому адаптеру.
- Присваивается облачной службе.
- Облачная служба может включать в себя несколько ВМ, которые, таким образом, разделяют VIP.

DIP – Dynamic IP address

- Динамически (с помощью DHCP) присваивается ВМ. Не меняйте этот адрес вручную!
- Срок аренды равен сроку жизни ВМ.
- При создании в виртуальной сети ВМ получает DIP из диапазона этой сети.

Адресация в классической модели



Зарезервированные IP-адреса можно перемещать!

Сохраните свои IP-адреса

Можно резервировать IP-адреса в имеющихся службах

IP-адреса можно перемещать между службами за секунды

IP-адреса и балансировка нагрузки в ARM

Публичные IP-адреса в Azure

Присваиваются ВМ, балансировщикам, VPN-шлюзам, шлюзам приложений

Public IP для ВМ

IP-адрес, эксклюзивно выделенный одной ВМ

Весь диапазон портов доступен по умолчанию

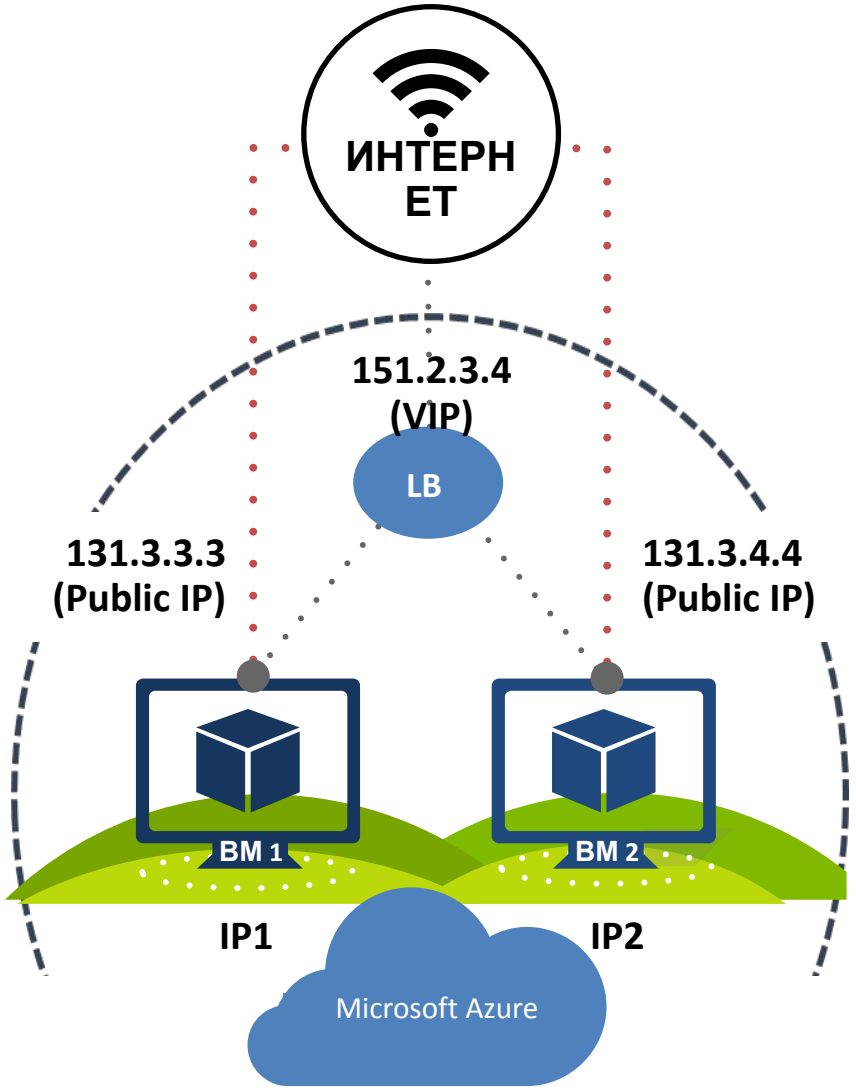
Выделяется динамически (по умолчанию) или статически

IP для балансировкой нагрузки (VIP)

IP-адрес для балансировкой нагрузки одного и более экземпляров ВМ

Перенаправление портов

В основном, для высокодоступных сценариев с балансировкой нагрузки или автоматическим масштабированием



IP-адреса и разрешение имен в ARM

Частные IP-адреса в Azure

Присваиваются ВМ, внутренним балансировщикам, шлюзам приложений

Private IP для ВМ

IP-адрес из диапазона виртуальной подсети

Выделяется динамически (по умолчанию) или статически

Разрешение имен с помощью Azure DNS

Private IP разрешаются в пределах виртуальной сети

Public IP могут быть присвоены имена *domainnamelabel.location*.cloudapp.azure.com

Имена должны быть уникальны в пределах location

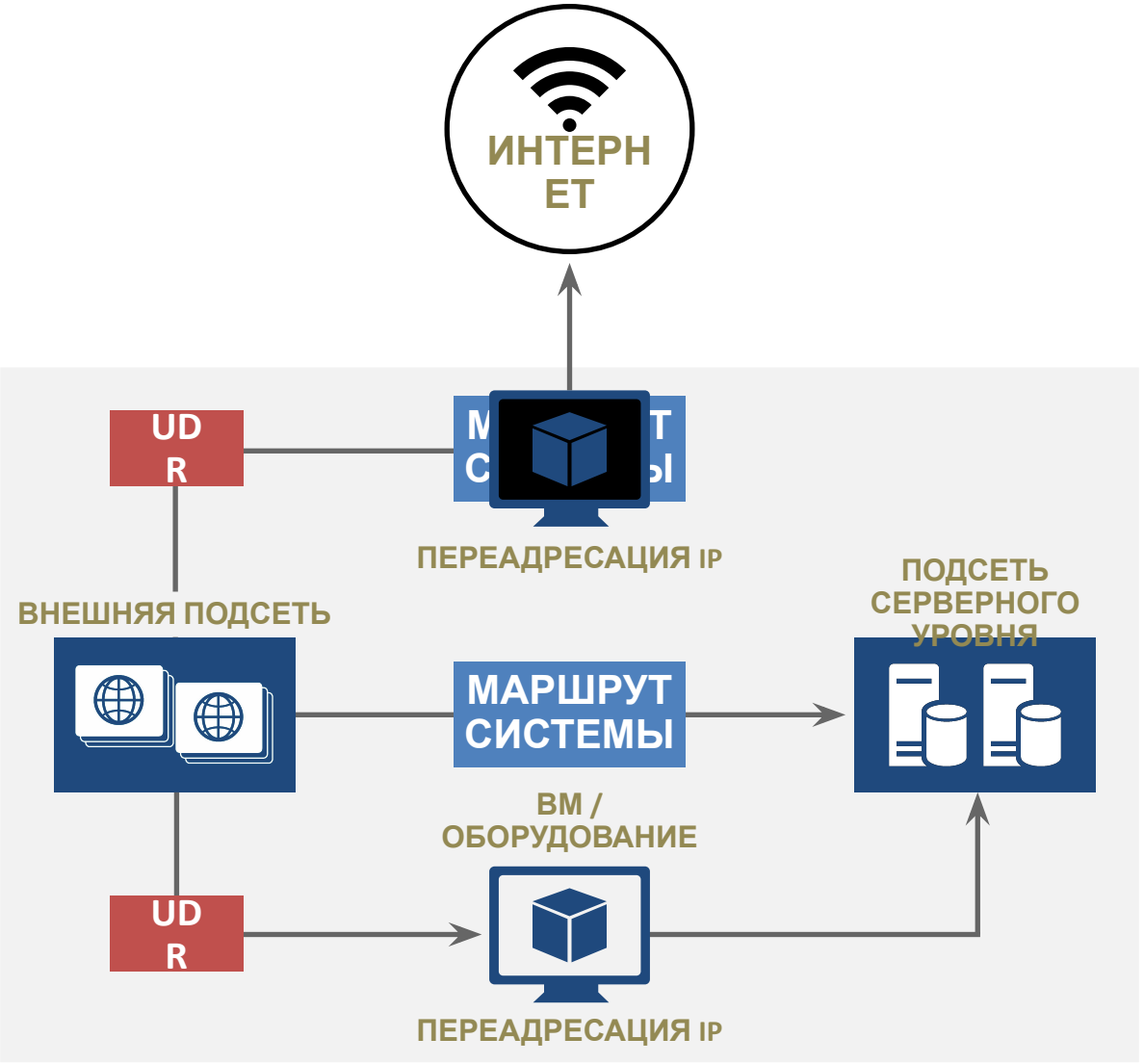
Пользовательские маршруты (UDR)

Контролируйте сетевой трафик с помощью пользовательских маршрутов

Назначайте подсетям таблицы маршрутов

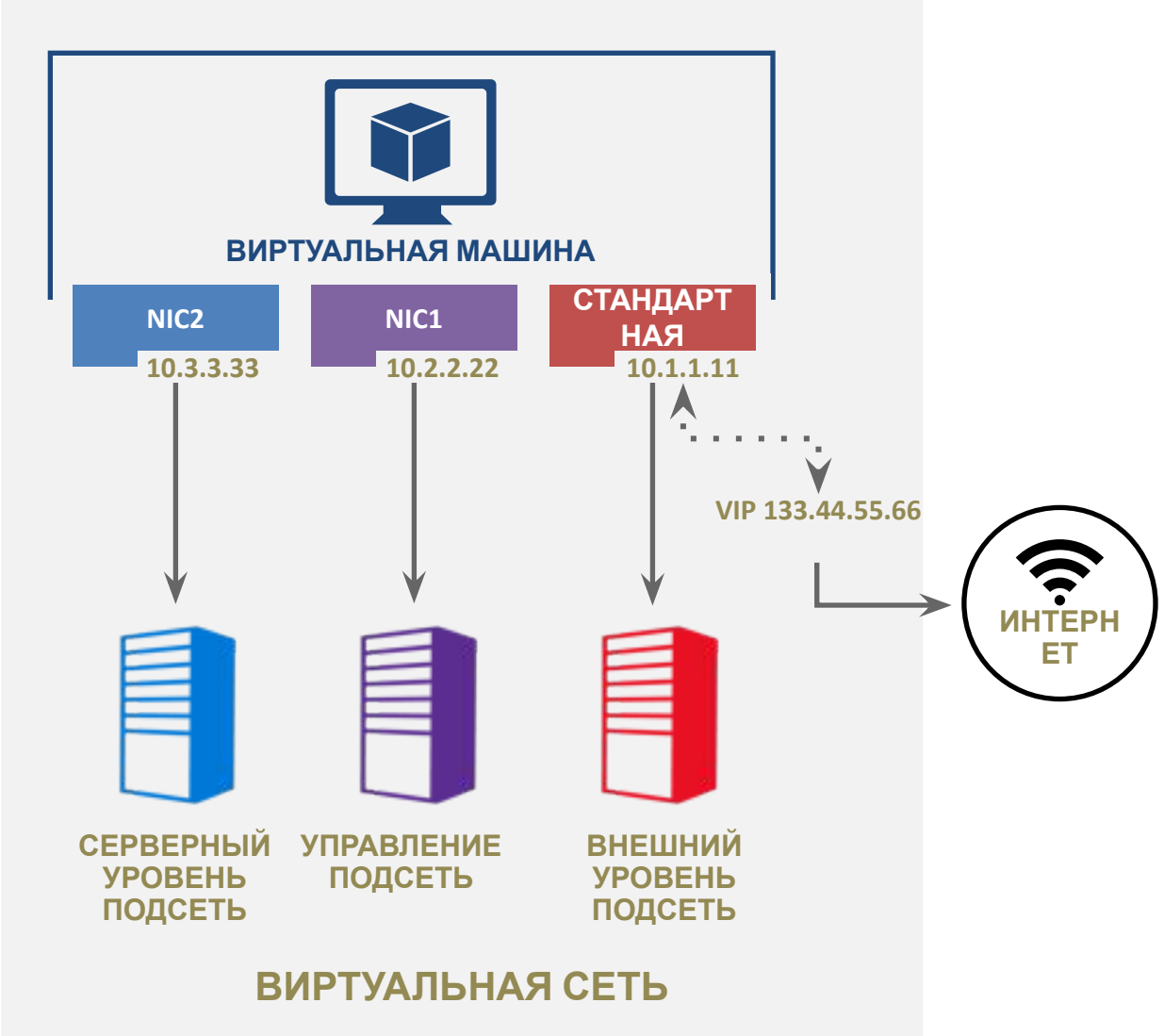
Указывайте следующий сетевой сегмент для любого префикса адреса

Задайте маршрут 0/0 для принудительного туннелирования трафика



ВМ с несколькими NIC в Azure

- **До 16 NIC на одну ВМ**
- **NSG и маршруты на всех NIC**
- **Разделение внешней подсети, подсети серверного уровня и уровня управления**



Выбор правильной модели подключения

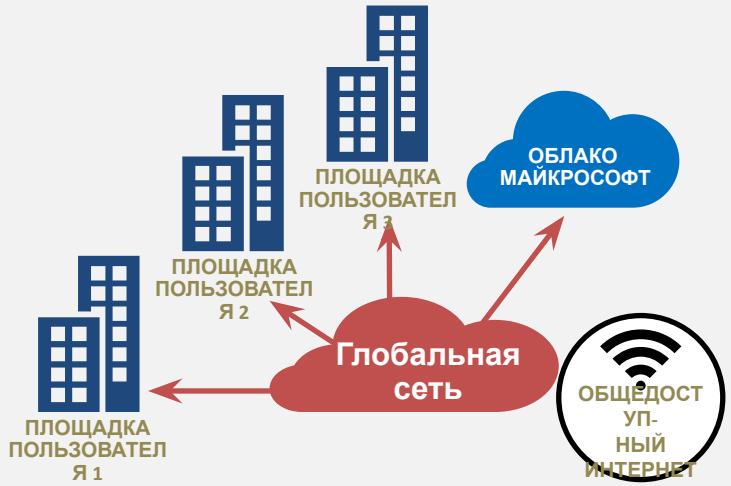
ШЛЮЗЫ ИНТЕРНЕТ / VPN

- Подключение через зашифрованное соединение общедоступного Интернета

ПОСТАВЩИК УСЛУГ

- Подключение к Azure с помощью услуги ExpressRoute, предоставляемой партнером на своей площадке

ПОСТАВЩИК УСЛУГ



- Подключение из глобальной сети поставщика сетевых услуг
- Azure становится одной из площадок пользователя в глобальной сети

ПОДКЛЮЧЕНИЕ ЧЕРЕЗ ИНТЕРНЕТ

EXPRESSROUTE –
ПРЕДОСТАВЛЯЕТ ПОЛЬЗОВАТЕЛЮ ВОЗМОЖНОСТЬ ВЫБОРА С ДОСТУПОМ КО ВСЕМ ОБЛАЧНЫМ СЛУЖБАМ МАЙКРОСОФТ

VPN-шлюзы для виртуальной сети

Для доступа к виртуальной сети необходим шлюз ExpressRoute или шлюз VPN

Возможно использование различных SKU

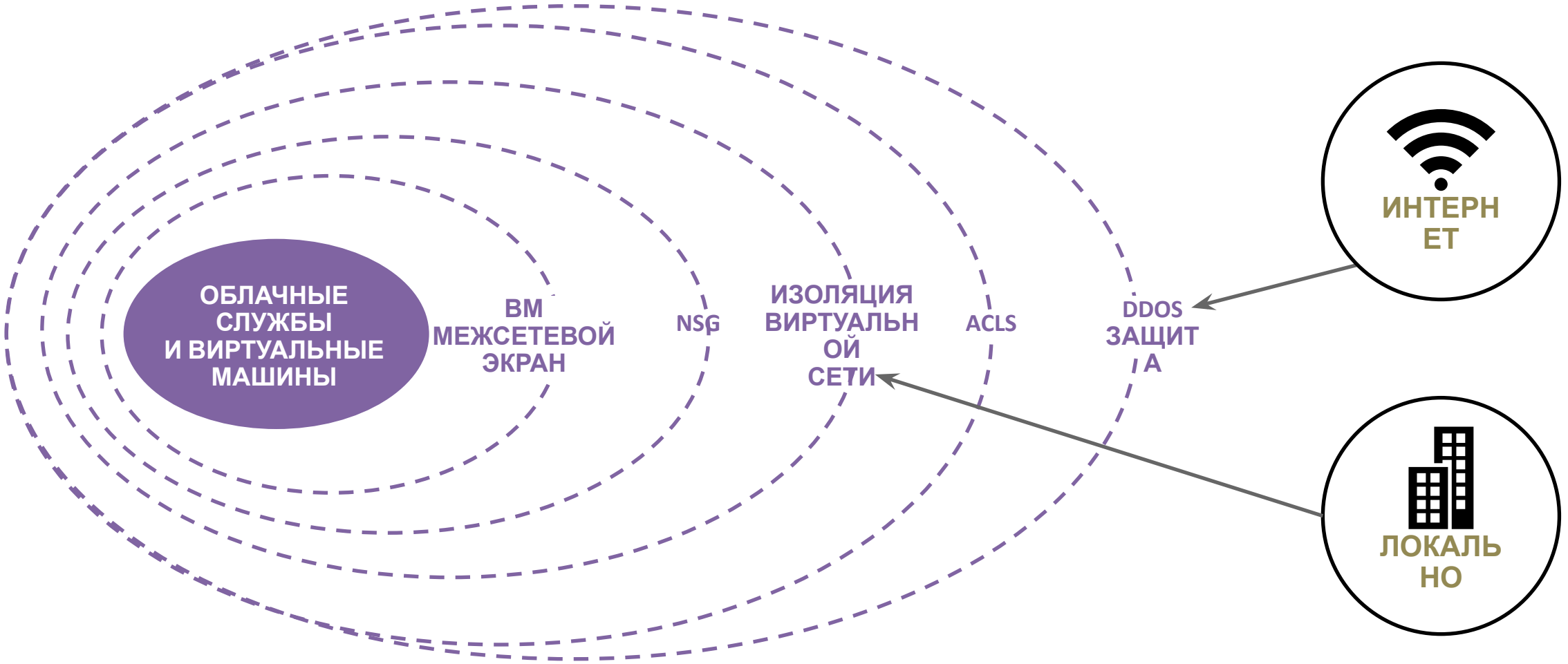
Поддержка совместной работы ExpressRoute и VPN

Повышенная пропускная способность ExpressRoute

SKU ШЛЮЗА ВИРТУАЛЬНОЙ СЕТИ	ПРОПУСКНАЯ СПОСОБНОСТЬ ШЛЮЗА EXPRESSROUTE	ШЛЮЗ VPN – EXPRESSROUTE СОВМЕСТНАЯ РАБОТА	ПРОПУСКНАЯ СПОСОБНОСТЬ ШЛЮЗА VPN	ШЛЮЗ VPN МАКС. ТУННЕЛЕЙ IPSec	ЗАТРАТЫ (В ДОЛЛАРАХ США) В ЧАС
BASIC	500 Мбит/с	НЕТ	100 Мбит/с	10	0,04
STANDARD	1000 Мбит/с	ДА	100 Мбит/с	10	0,19
PERFORMANCE	2000 Мбит/с	ДА	200 Мбит/с	30	0,49

СЛЕДУЕТ ИМЕТЬ В ВИДУ, ЧТО ТРАФИК EXPRESSROUTE ОБЩЕДОСТУПНЫХ СЕРВИСОВ AZURE, O365 И SKYPE ДЛЯ БИЗНЕСА **НЕ** ПРОХОДИТ ЧЕРЕЗ ШЛЮЗ ВИРТУАЛЬНОЙ СЕТИ

Уровни безопасности, защита и изоляция



Группы сетевой безопасности (Network Security Group, NSG)

Сегментация сети для обеспечения безопасности

Набор правил с приоритетами

Стандартные правила: 65 000 и более

Применяются к ВМ и (или) подсети

Применяются к внутреннему и внешнему трафику

Стандартные тэги:
VIRTUAL_NETWORK, INTERNET, AZURE_LOADBALANCER

API журналов аудита

MVA jumpstart

04 | Использование Azure Site Recovery для защиты и миграции из локальной сети

Microsoft

Александр Шаповал | Эксперт по стратегическим технологиям

Microsoft Operations Management Suite (OMS)

Анализ журналов

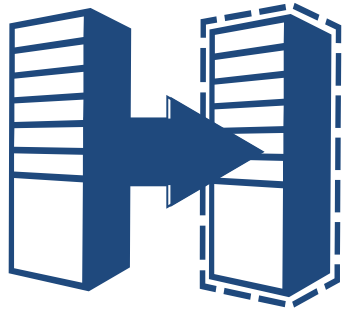
Наглядное представление всей гибридной среды

Автоматизация

Управление сложными и цикличными процедурами

Доступность

Надежная защита данных и высокая доступность приложений



Безопасность

Безопасность рабочих нагрузок, серверов и пользователей

Enterprise Mobility Suite (EMS)

Включен **Forefront Identity Management**

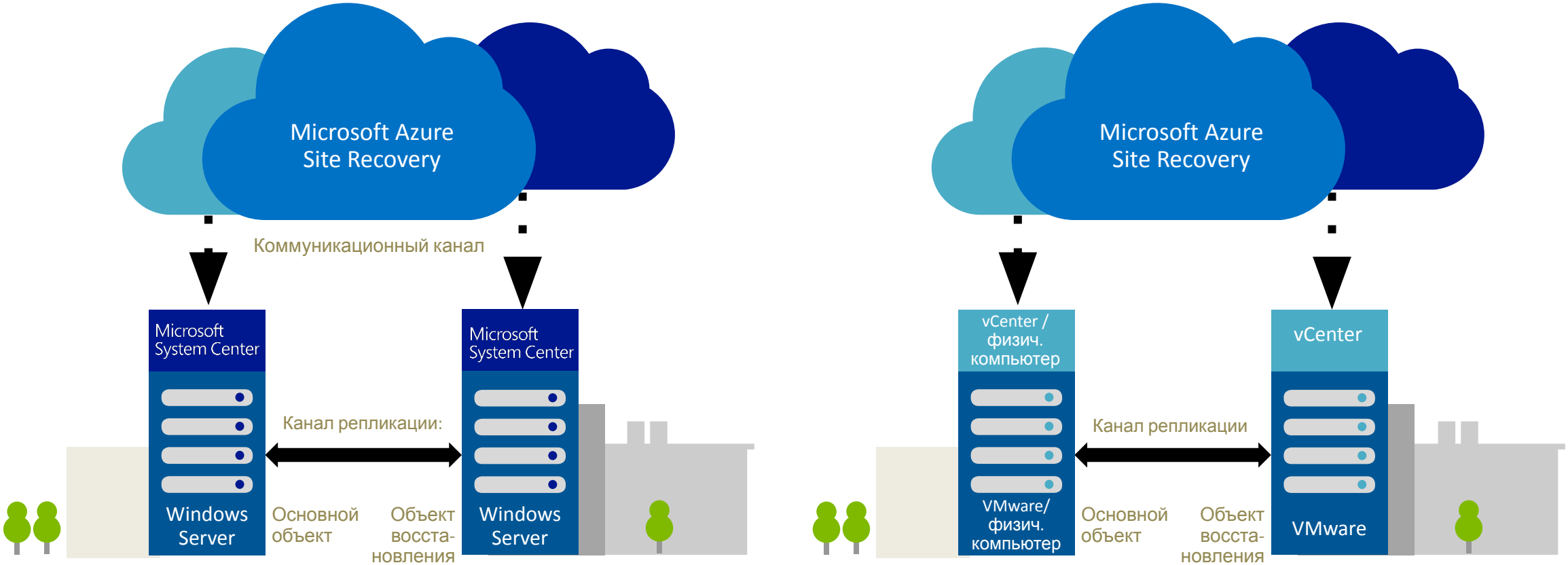
Azure Active Directory Premium	**Гибридное управление идентификацией**	*Благодаря Azure Active Directory Premium:* · Управление группами и обеспечение их безопасности, аудиторские отчеты · Самостоятельный сброс пароля и многофакторная аутентификация · Взаимодействие между AD и Azure AD
Microsoft Intune	**Управление мобильными устройствами Mobile Device Management**	*Благодаря Microsoft Intune:* • Управление параметрами и настройками мобильных устройств • Управление жизненным циклом мобильных приложений • Очистка и удаление данных с устройства
Azure Rights Management Service	**Защита данных**	*Благодаря Azure Rights Management Service:* • Защита информации • Условный доступ
Microsoft Advanced Threat Analytics	Расширенная защита от кибер-угроз	*Благодаря* Microsoft Advanced Threat Analytics*:* • Поведенческий анализ • Обнаружение известных атак и проблем • Обнаружение новых атак и угроз

С 1 августа 2015

Права на использование WS RMS CAL

Защитите приложения пользователей

Защита на локальном уровне с помощью службы Azure Site Recovery



Ключевые функции:

- Автоматизированная защита и репликация ВМ
- Удаленный мониторинг состояния
- Настраиваемые планы восстановления
- Интеграция с уже сделанными вложениями
- Поддержка гетерогенных сред
- Тестирование плана восстановления без влияния на производственную среду
- Управляемое восстановление многоуровневых приложений

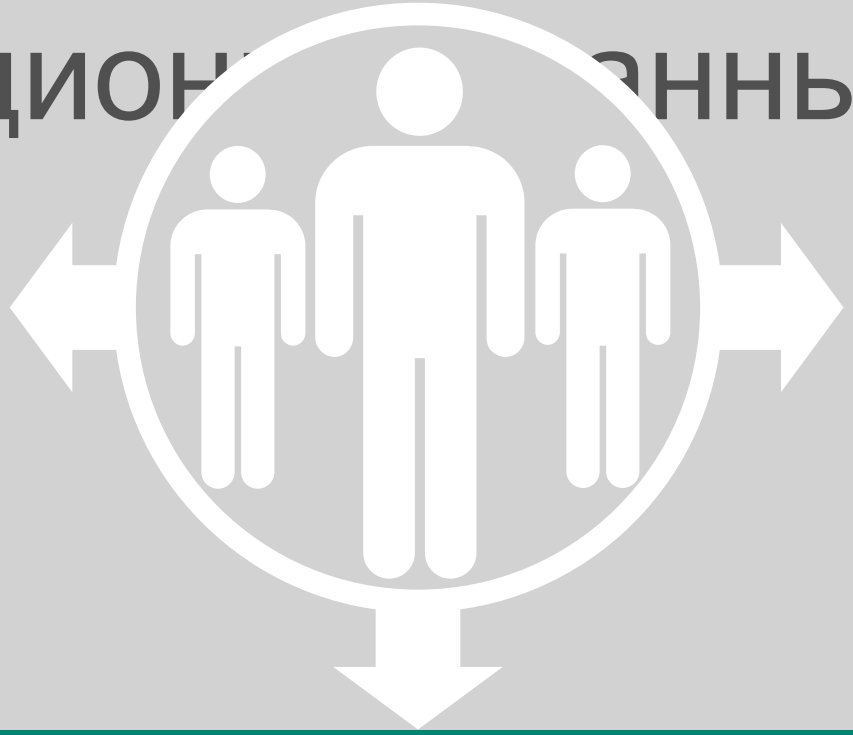
MVA jumpstart

05 | Управление идентификационными данными с помощью Azure Active Directory

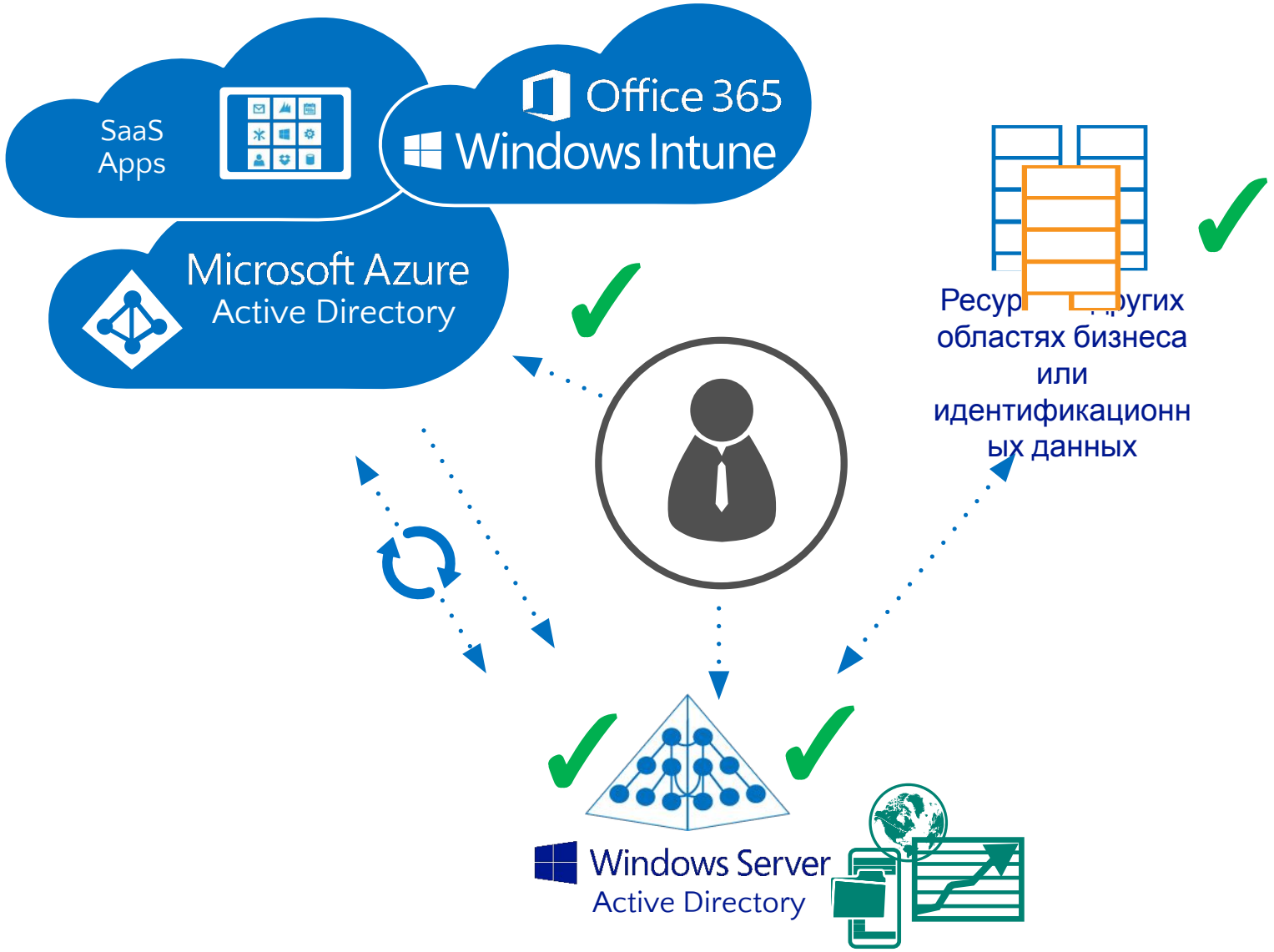
Microsoft

Александр Шаповал | Эксперт по стратегическим технологиям

Пользователям нужны **общие** локальные **и** облачные идентификационные данные



Идентификационные данные: облачные, синхронизированные или объединенные?



Облачные идентификационные данные – решение, при котором все идентификационные данные находятся в облаке

Синхронизированные идентификационные данные поддерживают копию существующих идентиф-ых. данных с облаком

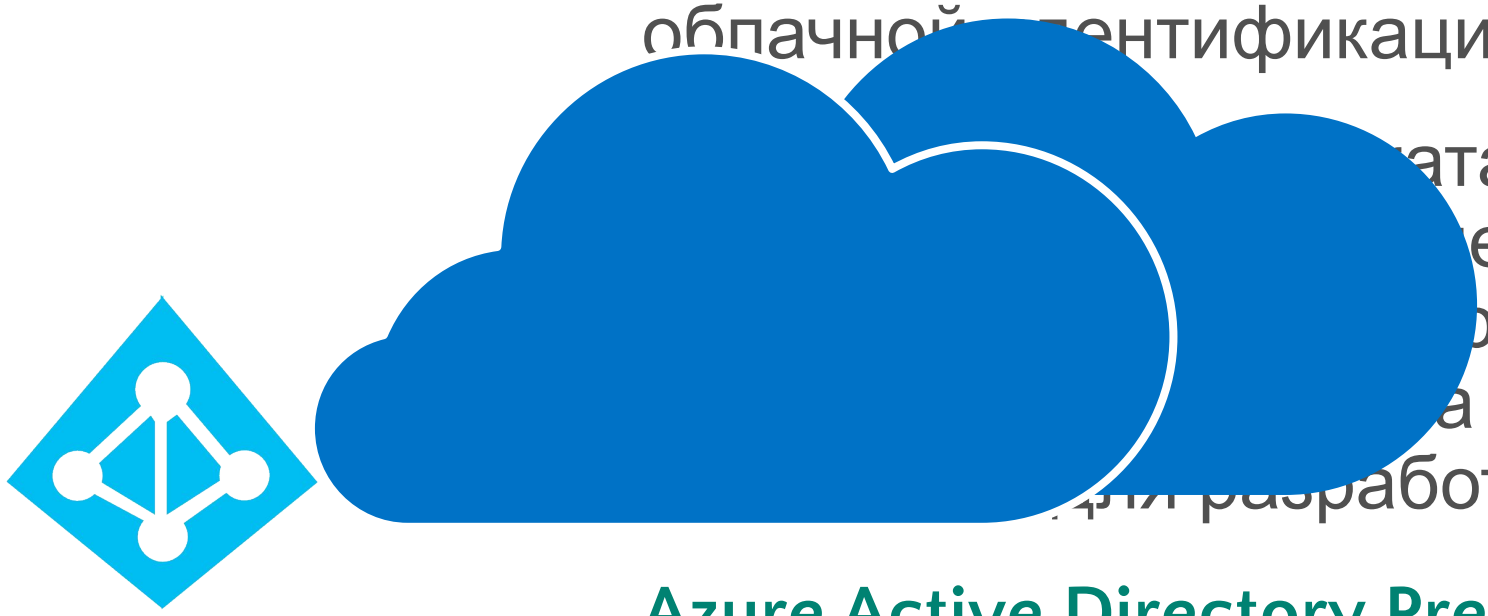
Объединенные идентификационные данные позволяют сохранить всю аутентификацию локально

Объединенные идентификационные данные B2B позволяют клиентам безопасно взаимодействовать друг с другом

Что такое Azure Active Directory?

Комплексное решение по управлению
облачной [illegible]ентификацией и облаком.

[illegible]аталогов,
[illegible]е удостоверениями,
[illegible]риложений и
[illegible]а стандартах,
[illegible] для разработчиков.

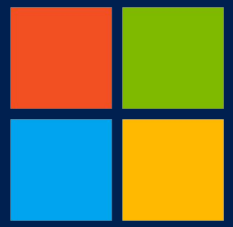


Azure Active Directory Premium – продвинутое предложение, которое включает возможность IAM для локальных, гибридных и облачных сред

https://azure.microsoft.com/en-us/pricing/details/active-directory/

Ресурсы

- Channel 9
  - https://channel9.msdn.com/
- Microsoft Virtual Academy
  - https://mva.microsoft.com/
- Microsoft Azure
  - https://azure.microsoft.com/



Microsoft