МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»
Институт Информационных систем и геотехнологий
Кафедра Прикладной информатики

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

(БАКАЛАВЕРСКАЯ РАБОТА)

Специальность 38.03.05 «Бизнес-информатика»

На тему: Совершенствование бизнес-модели компании на основе внедрения информационных систем и технологий.

Исполнитель: Аль-Там Талеб Талеб
(фамилия, имя, отчество)
Руководитель: к.т.н., доцен
(ученая степень, ученое звание)
Попов Николай Николаевич
(фамилия, имя, отчество)

«К защите допускаю»
Заведующий кафедрой _____
(подпись)
И.о. директора института
(ученая степень, ученое звание)
Истомин Евгений Петрович
(фамилия, имя, отчество)
«___»_____2022 г.

Санкт – Петербург
2022

Оглавление

Введение 3

1.Теоретическая часть 4

1. 1.Информационные системы 4

1.1.1. Основные понятия и сущность информационных систем 4

1.1.2 Основные задачи информационных систем 6

1.1.3. Структура и классификация информационных систем....7

2. Описание и характеристики сервисов Azure. 11

2.1.Описание основных понятий Azure 11

2.2Службы Azure....13

2.3.Начало работы с учетными записями Azure 21

2.4.Обсуждение различных типов моделей облака 21

2.5.Описание преимуществ и особенностей облака 23

2.6.Описание различных облачных служб 24

3. Применение сервисов Azure для совершенствования процессов компании. 29

3.1.Ресурсы Azure и Azure Resource Manager 29

3.2.Подписки и группы управления Azure 31

3.3.Обзор вычислительных служб в Azure 35

3.4. Виртуальная сеть Azure....37

3.4.1. Основы виртуальной сети Azure....37

3.4.**2**. Основные сведения о VPN-шлюзе Azure....40

3.4.3. Основные сведения об Azure ExpressRoute 46

3.5. Изучение служб хранилища Azure....49

3.5.1. Основные принципы учетной записи службы хранилища Azure....49

3.5.2. Основные принципы хранилища дисков 50

3.5.3. Основные принципы хранилища BLOB-объектов Azure....51

3.5.4. Основы работы с файлами Azure....52

3.5.5. Основные сведения об уровнях доступа к BLOB-объектам 53

3.6. Базы данных SQL Azure 55

3.7. Защита от угроз безопасности с помощью Центра безопасности Azure....56

3.8. Хранение секретов и управление ими в Azure Key Vault 57

3.9.Глубинная защита 59

3.10.Защита виртуальных сетей с помощью Брандмауэра Azure 63

3.11.Сравнение затрат с помощью калькулятора совокупной стоимости владения 65

ЗАКЛЮЧЕНИЕ 68

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ 69

ПРИЛОЖЕНИЕ. Создание виртуальной сети.....70
ПРИЛОЖЕНИЕ. Создание базы данных SQL 74
ПРИЛОЖЕНИЕ. Создание хранилища ключей.....83

Введение

Учитывая высокую тенденцию развития информационных технологий и систем в современном мире и их внедрение в различные сферы деятельности, увеличивается предоставление различных услуг. Компаниям необходимо постоянно повышать свою эффективность в борьбе за конкурентоспособность.

Все больше компаний и университетов стремятся упростить работу с информацией. Одним из основных средств достижения этой цели является внедрение информационных систем и технологий. Внедрение таких комплексных систем позволяет облегчить работу, скорость работы по передаче и обработке информации, удобство ее обслуживания.

Актуальность темы исследования. Переход организаций на облачные решения в условиях пандемии

Целью исследование направлено на совершенствование бизнес-модели компании, защиту и обработку данных, а также разработку практических рекомендаций по формированию механизма реализации проекта.

Задачи исследования:

1. Изучить теоретические основы внедрения облачных технологий.
2. Изучить основные продукты Microsoft Azure.
3. Разработать рекомендации по внедрению выбранных продуктов на предприятии.

Объект исследования: РГГМУ

Предмет исследования: совершенствование IT структуры организации.

1.Теоретическая часть

1. 1.Информационные системы

1.1.1. Основные понятия и сущность информационных систем

Существует множество определений термина «система». Например, система воспринимается как совокупность взаимосвязанных элементов (объектов), объединенных для достижения общей цели, изолированных от внешней среды, взаимодействующих с ней как единое целое и проявляющих системные свойства. В более широком смысле система поясняется словарем терминов автоматизации, информатики и вычислительной техники: система - это совокупность взаимосвязанных объектов, подчиненных определенной общей цели с учетом условий внешней среды [1]. Организованный набор элементов системы и их отношения друг с другом представляют собой структуру системы. Системы существенно отличаются друг от друга по составу и основным целям.

Проанализировав понятие структуры и существующие определения системы, можно выделить следующие еѐ основные составляющие:

система – это упорядоченная совокупность элементов;

элементы системы взаимосвязаны и взаимодействуют в рамках данной системы, являясь еѐ подсистемами;

система как целое выполняет установленную ей функцию, которая не может быть сведена к функции отдельного элемента;

элементы системы могут взаимодействовать друг с другом в рамках системы, а также самостоятельно с внешней средой и изменять при этом своѐ содержание или внутреннее строение.

Добавление слова «информация» к понятию «система» отражает цель ее создания и функционирования. Информационные системы обеспечивают сбор, хранение, обработку, поиск и выдачу информации, необходимой в процессе принятия решений по задачам из любой области. Они помогают анализировать проблемы и создавать новые продукты.

Основная цель информационной системы – организация хранения, обработки и передачи итоговой информации, необходимой для принятия решения. Информационная система представляет собой систему обработки информации, как человеком, так и компьютером.

Современная информационная система – это набор информационных технологий, направленных на поддержку жизненного цикла информации и включающих три основные составляющие процесса: обработку данных, управление информацией и управление знаниями [2]. Любая информационная система состоит из трех компонентов, представленных на рисунке 1.

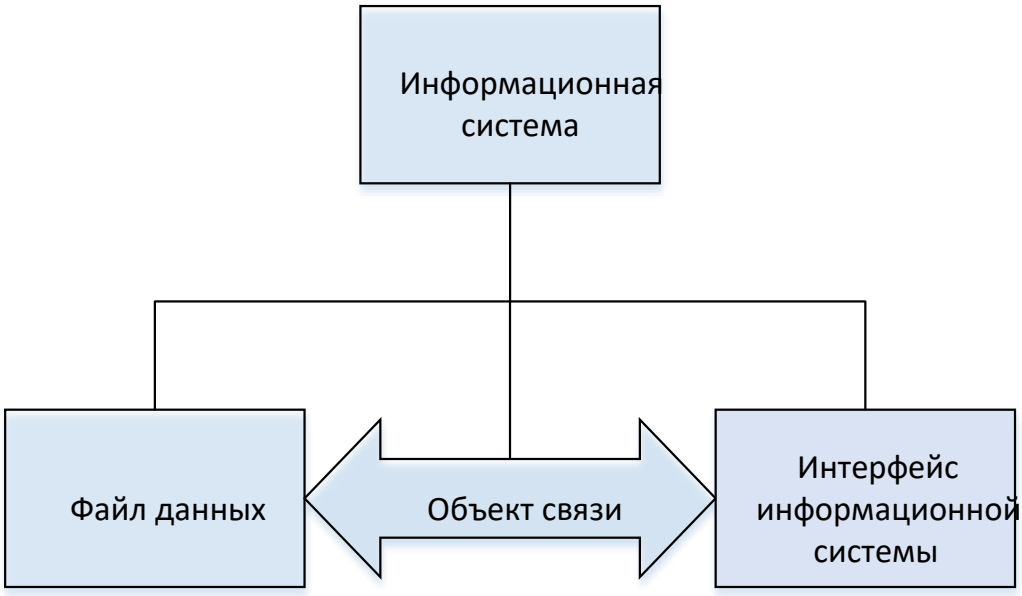


Рисунок 1 – Главные компоненты информационных систем

Файл данных – файл, находящийся на локальном компьютере или на сервере, который содержит внутри себя структуру данных. К структуре данных относятся таблицы, запросы и фильтры, а также хранимые процедуры, пользовательские функции, диаграммы, триггеры и т.д.

Объект связи – объект языка программирования, осуществляющий связь между файлом данных и интерфейсом информационной системы.

Интерфейс информационной системы – комплекс средств, осуществляющий взаимодействие системы с конечными пользователями. Он может находиться как на клиентском компьютере, так и на сервере.

Информационная система, как и любая другая система, обладает рядом свойств. Основные свойства информационных систем показаны на рисунке 2.

Современные системы любой природы, как правило, являются большими и сложными системами. Сложной системой называют систему, состоящую из большого числа взаимосвязанных и взаимодействующих между собой элементов и способную выполнять сложную функцию [3].

Весьма отличительным и важным свойством является подверженность информационных систем воздействию случайных факторов, причем не только, например, сбоев, отказов или ошибок технических устройств, персонала или пользователей, но и таким злонамеренным действиям.

Еще одним свойством является необходимость активного участия в информационных процессах человека. Это значит, что конечным пользователем информационных систем всегда являются сотрудники организации. Персонал организации имеет свои интересы и цели, которые необходимо учитывать при информационном обеспечении.

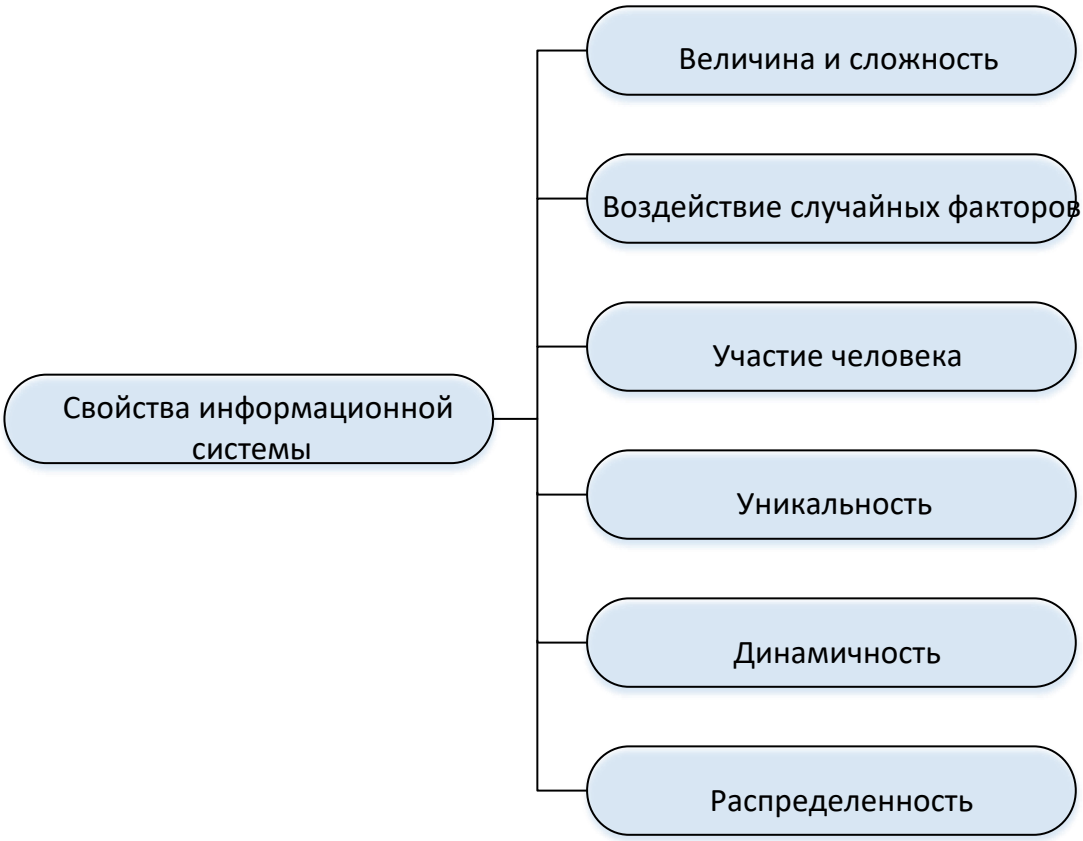


Рисунок 2 – Свойства информационных систем

Каждое состояние информационной системы уникально и требует учета всех ее особенностей.

Динамичность заключается в том, что информационные системы с течением времени сменяют свою структуру и состояние элементов. Распределенность – в пространственном расположении отдельных компонентов системы.

В деятельности организации информационная система рассматривается как программное обеспечение, реализующее деловую стратегию организации. При этом хорошей практикой является создание и развертывание единой корпоративной информационной системы, удовлетворяющей информационные потребности всех сотрудников, служб и подразделений организации [4]. Рассмотрим задачи информационных систем.

1.1.2 Основные задачи информационных систем

Конкретные задачи, которые должны решаться информационной системой, зависят от той прикладной области, для которой предназначена система. Области применения информационных приложений разнообразны: банковское дело, управление производством, медицина, транспорт, образование и т.д.

Ниже приведены основные задачи информационных систем.

Интерпретация данных**.** Под интерпретацией понимается процесс определения смысла данных, результаты которого должны быть согласованными и корректными. Обычно предусматривается многовариантный анализ данных.

Диагностика. Под диагностикой понимается процесс соотношения объекта с некоторым классом объектов и/или обнаружение неисправности в некоторой системе. Неисправность – это отклонение от нормы. Такая трактовка позволяет с единых теоретических позиций рассматривать и неисправность оборудования в технических системах, и заболевания живых организмов, и всевозможные природные аномалии.

Мониторинг. Основная задача мониторинга – непрерывная интерпретация данных в реальном времени и сигнализация о выходе тех или иных параметров за допустимые пределы.

Проектирование. Проектирование состоит в подготовке спецификаций на создание «объектов» с заранее определѐнными свойствами. Под спецификацией понимается весь набор необходимых документов – чертѐж, пояснительная записка и т.д. Основная проблема – получение чѐткого структурного описания знаний об объекте.

Прогнозирование. Прогнозирование позволяет предсказывать последствия некоторых событий или явлений на основании анализа имеющихся данных. Прогнозирующие системы логически выводят вероятные следствия из заданных ситуаций.

Планирование. Под планированием понимается нахождение планов действий, относящихся к объектам, способным выполнять некоторые функции. В таких электронных системах используются модели поведения реальных объектов с тем, чтобы логически вывести последствия планируемой деятельности.

Обучение. Под обучением понимается использование компьютера для обучения какой-то дисциплине или предмету. Системы обучения диагностируют ошибки при изучении какой-либо дисциплины с помощью ЭВМ и подсказывают правильные решения.

Управление**.** Под управлением понимается функция организованной системы, поддерживающая определенный режим деятельности. Такого рода электронные системы осуществляют управление поведением сложных систем в соответствии с заданными спецификациями.

Поддержка принятия решений. Поддержка принятия решения – это совокупность процедур, обеспечивающая лицо, принимающее решения, необходимой информацией и рекомендациями, облегчающие процесс принятия решения. Эти информационные системы помогают специалистам выбрать или сформировать нужную альтернативу среди множества выборов при принятии ответственных решений [8].

Основное отличие задач анализа от задач синтеза состоит в том, что если множество решений может быть включено в задачи анализа и включено в систему, то в задачах синтеза множество решений, скорее всего, будет неограниченным и строится из решений компоненты или подзадачи. Задачами анализа являются: интерпретация данных, диагностика, поддержка принятия решений. Задачи синтеза включают проектирование, планирование и контроль. Комбинированные задачи включают в себя обучение, мониторинг и прогнозирование.

1.1.3. Структура и классификация информационных систем

Структуру информационной системы составляет совокупность отдельных ее частей, называемых подсистемами.

Подсистема - это часть системы, выделенная по какому-либо признаку.

Общую структуру информационной системы, представленную на рисунке 3, можно рассматривать как совокупность подсистем независимо от сферы применения. В этом случае говорят о структурном признаке классификации, а подсистемы называют обеспечивающими. Таким образом, структура любой информационной системы может быть представлена совокупностью обеспечивающих подсистем [5].

Назначение подсистемы информационного обеспечения состоит в современном формировании и выдаче достоверной информации для принятия управленческих решений.

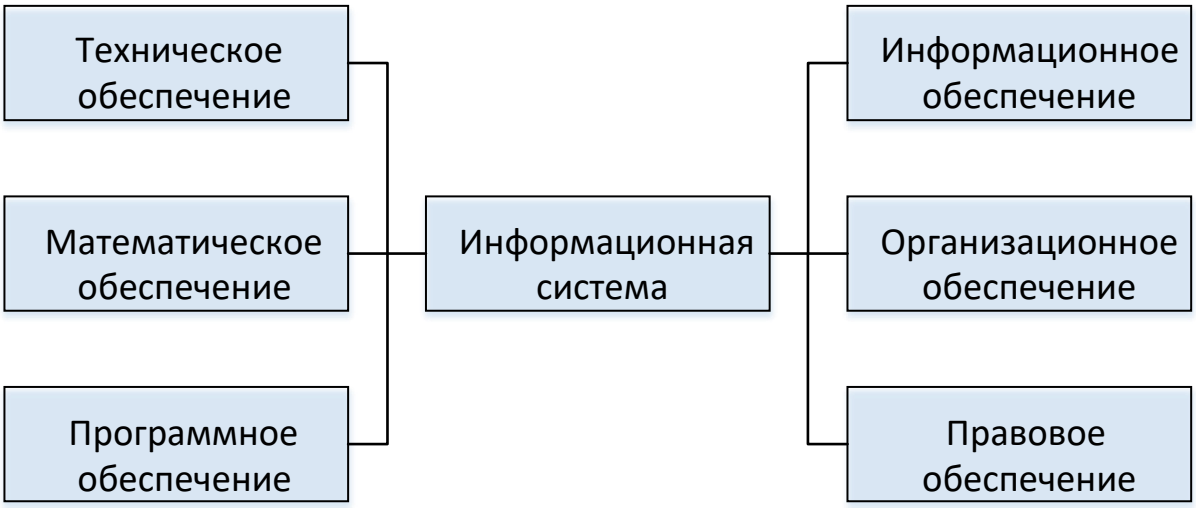


Рисунок 3 – Общая структура информационной системы

Информационное обеспечение – совокупность единой системы классификации и кодирования информации, унифицированных систем документации, схем информационных потоков, циркулирующих в организации, а также методология построения баз данных.

Техническое обеспечение – комплекс технических средств, предназначенных для работы информационной системы, а также соответствующая документация на эти средства и технологические процессы.

Математическое и программное обеспечение – совокупность математических методов, моделей, алгоритмов и программ для реализации целей и задач информационной системы, а также нормального функционирования комплекса технических средств.

Организационное обеспечение – это совокупность методов и средств, регламентирующих взаимодействие работников с техническими средствами и между собой в процессе разработки и эксплуатации ИС.

Правовое обеспечение – совокупность правовых норм, определяющих создание, юридический статус и функционирование информационных систем, регламентирующих порядок получения, преобразования и использования информации.

Классификация информационных систем управления способствует выявлению наиболее характерных черт, присущих информационным системам. Классификацию можно проводить по многим признакам [6]. Классификация по основным признаками информационных систем представлена на рисунке 4.

Классификация ИС по сфере применения:

корпоративные информационные системы используются для автоматизации всех функций организации и охватывают весь цикл работ от проектирования до сбыта продукции;

информационные системы организационного управления предназначены для автоматизации функций управленческого и оперативного контроля и регулирования, оперативного учета и анализа, перспективного и оперативного планирования, бухгалтерского учета, управления сбытом и снабжением и пр.;

информационные системы управления технологическими процессами (ТП) предназначены для автоматизации функций производственного персонала;

информационные системы автоматизированного проектирования (САПР) предназначены для автоматизации функций инженеровпроектировщиков, конструкторов, архитекторов дизайнеров для проведения инженерных расчетов, создания графической документации (чертежей, схем, планов), создания проектной документации, моделирования проектируемых объектов [7].

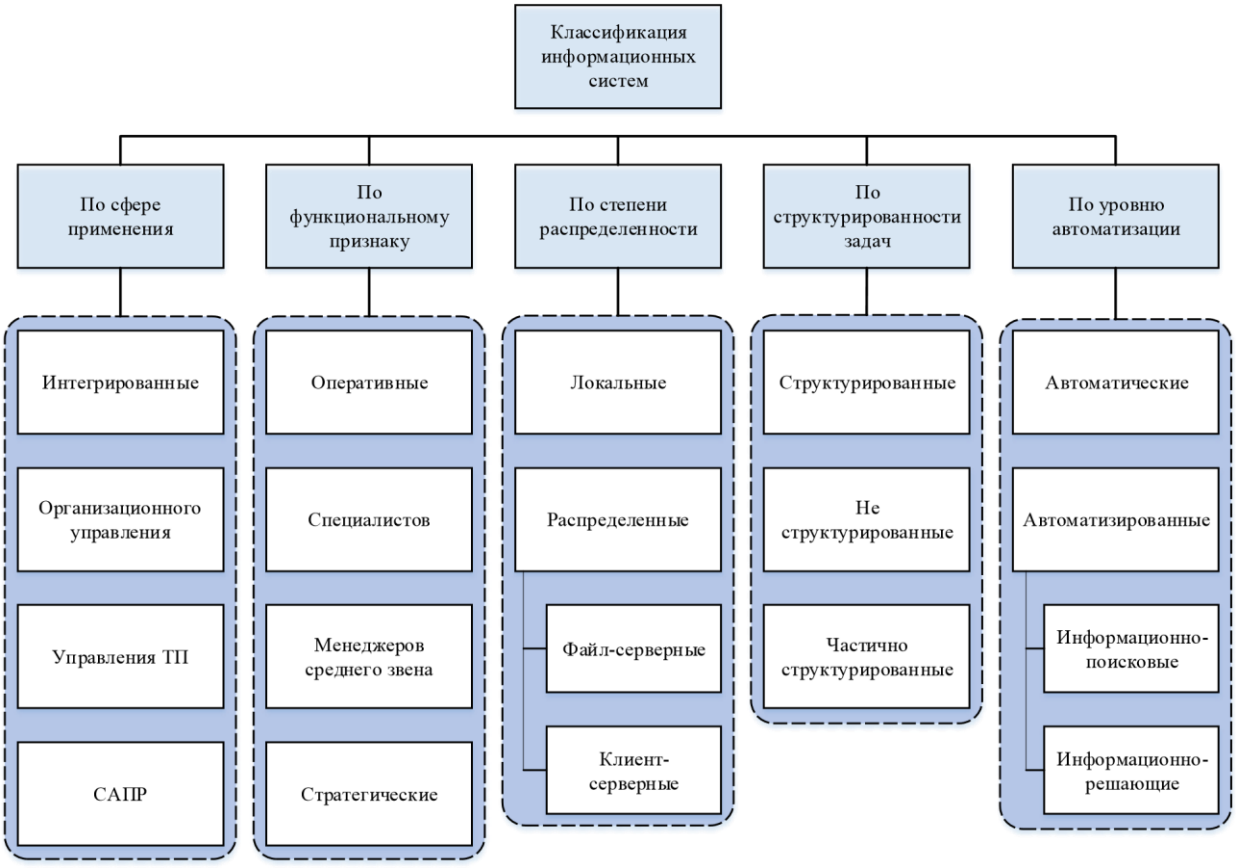


Рисунок 4 – Основная классификация информационных систем

По функциональному признаку:

информационные системы оперативного (операционного) уровня – (бухгалтерские, банковские, обработки заказов и пр.) поддерживают специалистов, обрабатывая данные о сделках и событиях (счета, накладные, зарплата, кредиты, поток сырья и материалов);

информационные системы специалистов – интеграция новых

сведений и помощь пользователям в обработке бумажных документов;

информационные системы для менеджеров среднего звена – используются для мониторинга, контроля, принятия решений и администрирования;

стратегические информационные системы – обеспечивают поддержку принятия решений по реализации стратегических перспективных целей развития организации и помогают высшему звену управленцев осуществлять долгосрочное планирование [9].

Классификация ИС по распределенности:

настольные (локальные) ИС, в которых все компоненты (БД, СУБД, клиентские приложения) находятся на одном компьютере;

распределѐнные ИС, в которых компоненты распределены по нескольким компьютерам. Такие ИС, в свою очередь, подразделяются на не сетевые (архитектура Файл-Сервер) и сетевые (архитектура Клиент-Сервер).

Классификация ИС по структурированности задач:

структурированные (формализуемые) задачи, где известны все ее элементы и взаимосвязи между ними;

неструктурированные (неформализуемые) задачи – задачи, в которых невозможно выделить элементы и установить между ними связи;

частично структурированные задачи – известна часть элементов и связей между ними. Данные информационные системы подразделяются еще на два вида. Первые создают управленческие отчеты и ориентированы главным образом на обработку данных. А вторые разрабатывают альтернативы решений, т.е. предоставляют пользователю математические, статистические, финансовые и другие модели, использование которых облегчает выработку и оценку альтернатив решения [7].

Классификация по степени автоматизации:

автоматические информационные системы – выполняют все опе-

рации по переработке информации без участия человека.

автоматизированные информационные системы (АИС) - предполагают участие в процессе обработки информации и человека, и технических средств, при этом главная роль отводится компьютеру. Данные системы, учитывая широкое использование в организациях, имеют различные модификации и также могут быть классифицированы по различным признакам (например, по характеру использования информации) [9].

По характеру использования информации:

информационно-поисковые системы производят ввод, систематизацию, хранение, выдачу информации по запросу пользователя без сложных преобразований данных;

информационно-решающие системы осуществляют все операции переработки информации по определенному алгоритму, выделяют управляющие и советующие системы [7].

Для понимания, какие информационные системы необходимы для внедрения в какую-либо организацию, необходимо ознакомиться с теорией по процессному подходу.

2. Описание и характеристики сервисов Azure.

2.1.Описание основных понятий Azure

Azure — это постоянно расширяемый набор облачных служб, которые помогают вашей организации решать текущие и будущие бизнес-задачи. Azure предоставляет возможность создания, развертывания приложений и управления ими в больших глобальных сетях с помощью ваших любимых средств и платформ.

Azure — это платформа облачных вычислений с постоянно расширяющимся набором служб, которая поможет вам создавать решения для ваших бизнес-задач. Службы Azure могут быть простыми веб-службами для размещения вашего бизнеса в облаке или полностью виртуализированными компьютерами для выполнения пользовательских программных решений. Azure предоставляет множество облачных служб, таких как удаленное хранилище, размещение баз данных и централизованное управление учетными записями. Azure также предлагает новые возможности, такие как ИИ и Интернет вещей.

Что предлагает Azure.

При использовании Azure вы получите все необходимое для создания очередного превосходного решения. В следующей таблице перечислены некоторые преимущества, предоставляемые Azure и позволяющие развиваться в правильном направлении.

Будьте готовы к будущему. Непрерывные инновации от корпорации Майкрософт поддерживают ваши разработки сегодня и ваши новые концепции на будущее.

Создавайте решения на своих условиях. У вас есть выбор. Имея доступ к инструментам с открытым кодом, любым языкам и платформам, вы можете работать как угодно и где угодно.

Эффективно управляйте гибридной средой. Мы поддержим ваши начинания где угодно — локально, в облаке, на границе сети. Интегрируйте свои среды и управляйте ими с помощью средств и служб, предназначенных для гибридного облака.

Доверяйте облаку. Создайте систему безопасности с нуля при поддержке группы экспертов и обеспечьте соответствие требованиям по самым высоким стандартам.

Что можно сделать с помощью Azure?

Azure предоставляет более 100 служб, позволяющих решать любые задачи: от запуска существующих приложений в виртуальных машинах до освоения новых парадигм программного обеспечения, таких как интеллектуальные боты и смешанная реальность.

Многие команды приступают к изучению облака, перемещая свои имеющиеся приложения на виртуальные машины, которые работают в Azure. Несмотря на то, что перенос имеющихся приложений в виртуальные машины — это оптимальный вариант, облако является не просто альтернативной средой для работы виртуальных машин.

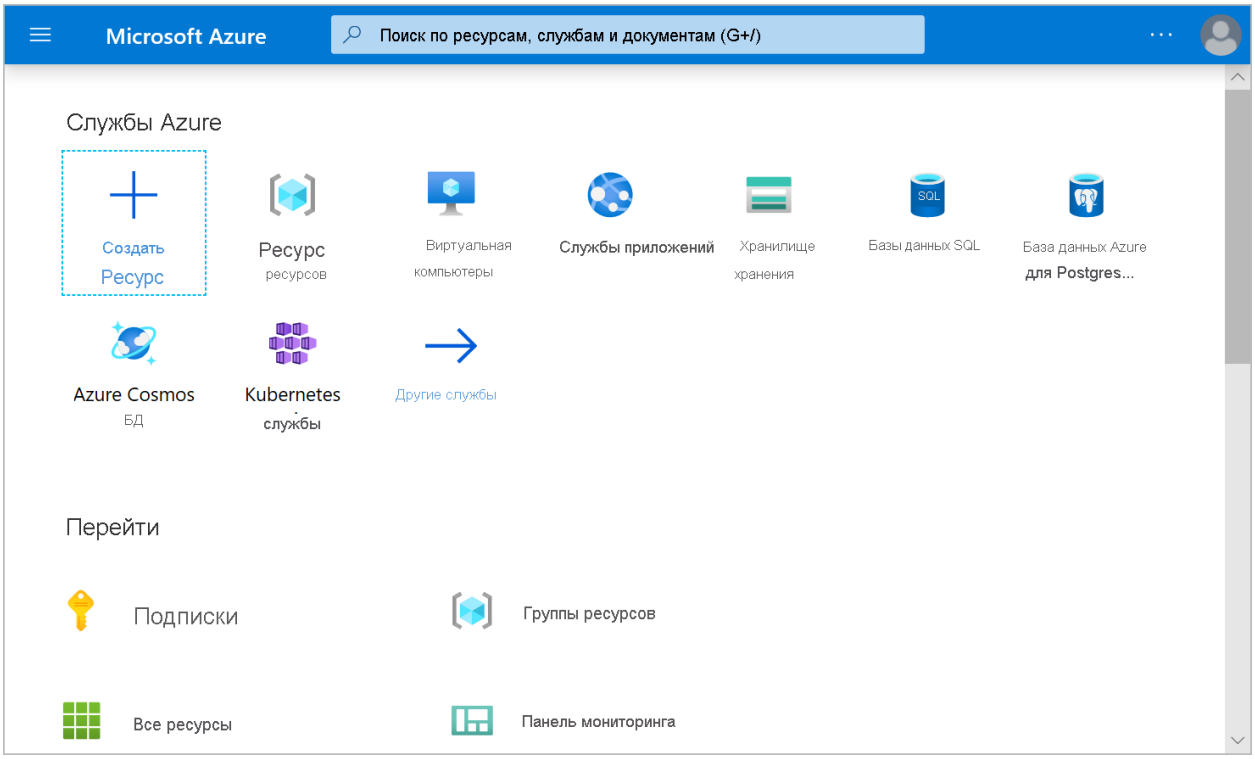
Например, платформа Azure предоставляет службы ИИ и машинного обучения, позволяющие вести естественное взаимодействие с пользователями посредством зрения, слуха и речи. Она также предоставляет решения для хранения, которые динамически увеличиваются для размещения больших объемов данных. Службы Azure реализуют решения, которые невозможны без облака.

Основные сведения о портале Azure

Портал Azure — это единая веб-консоль, которую можно использовать вместо средств командной строки. На портале Azure можно управлять подпиской Azure с помощью графического пользовательского интерфейса. Можно сделать следующее:

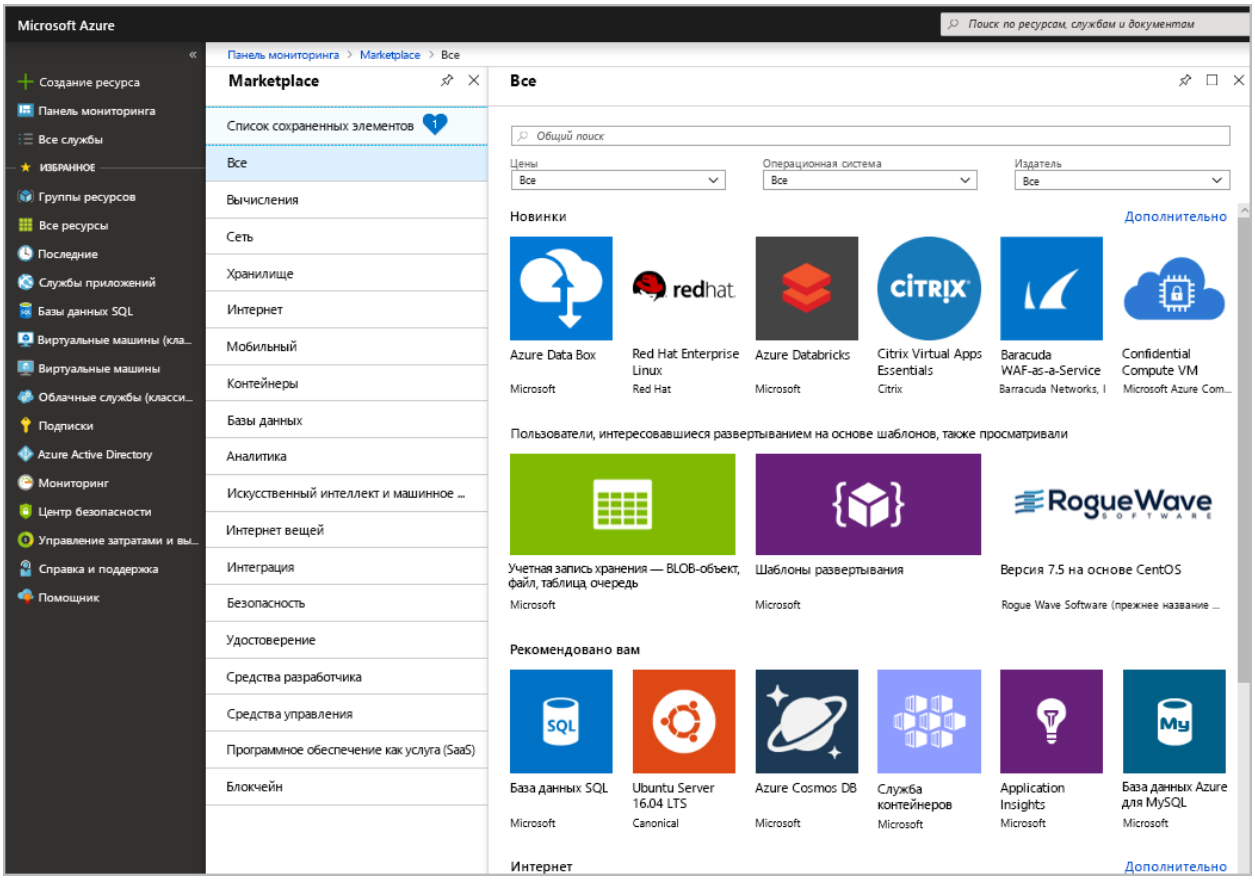
- Создавайте, администрируйте и отслеживайте все решения, начиная от простых веб-приложений и заканчивая сложными облачными развертываниями.
- Создавайте настраиваемые панели мониторинга для упорядоченного представления ресурсов.
- Настройте специальные возможности для оптимальной работы.

Портал Azure предназначен для обеспечения устойчивости и постоянной доступности. Он обеспечивает присутствие в каждом центре обработки данных Azure. Благодаря такой конфигурации портал Azure устойчив к сбоям отдельных центров обработки данных и позволяет избежать задержек в сети из-за близкого расположения к пользователям. Портал Azure постоянно обновляется и не отключается для выполнения обслуживания.



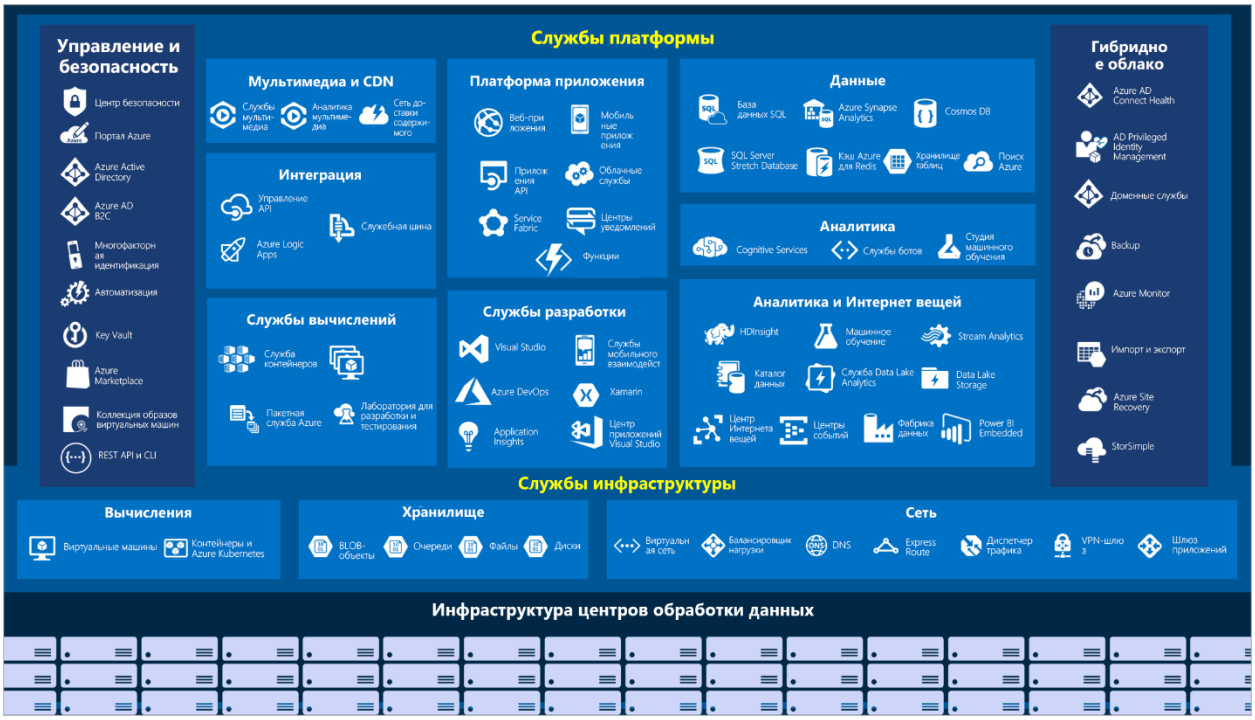
Что такое Azure Marketplace?

Azure Marketplace помогает конечным пользователям связываться с партнерами Майкрософт, независимыми поставщиками программного обеспечения и начинающими компаниями, которые предлагают свои решения, оптимизированные для работы в Azure. В Azure Marketplace клиенты могут найти, проверить в действии, приобрести и подготовить приложения и услуги, предлагаемые сотнями ведущих поставщиков услуг. Все решения и службы сертифицированы для работы в Azure.



2.2Службы Azure

Здесь приводится общее описание служб и возможностей, доступных в Azure.



Рассмотрим наиболее популярные категории более подробно.

- Вычисления
- Сеть
- Хранилище
- Мобильные приложения
- Базы данных
- Веб-службы
- Интернет вещей.
- Большие данные
- ИИ
- DevOps

Вычисления

Службы вычислений — это одна из основных причин того, что компании переходят на платформу Azure. Azure предоставляет широкий выбор вариантов для размещения приложений и служб. Ниже приведены некоторые примеры служб вычислений в Azure.

Виртуальные машины Azure

Виртуальные машины Windows или Linux, размещенные в Azure.

Масштабируемые наборы виртуальных машин Azure

Масштабирование виртуальных машин Windows или Linux, размещенных в Azure.

Служба Azure Kubernetes

Управление кластерами для виртуальных машин с контейнерными службами.

Azure Service Fabric

Платформа распределенных систем, работающая в Azure или локальной среде.

Пакетная служба Azure

Управляемая служба для параллельных и высокопроизводительных вычислительных приложений.

Экземпляры контейнеров Azure

Контейнерные приложения выполняются в Azure без подготовки серверов или виртуальных машин.

Функции Azure

Управляемая событиями служба бессерверных вычислений.

Сеть

Связывание вычислительных ресурсов и предоставление доступа к приложениям — это ключевая функция сетей Azure. Функции сетей в Azure включают в себя ряд вариантов для соединения внешнего мира со службами и компонентами в глобальных центрах обработки данных Azure.

Ниже приведены некоторые примеры сетевых служб в Azure.

Виртуальная сеть Azure

Подключает виртуальные машины к входящим подключениям виртуальной частной сети (VPN).

Azure Load Balancer

Балансирует входящие и исходящие подключения к приложениям или конечным точкам служб.

Шлюз приложений Azure

Оптимизирует доставку фермы серверов приложений и повышает безопасность приложений.

VPN-шлюз Azure

Позволяет получить доступ к виртуальным сетям Azure через высокопроизводительные VPN-шлюзы.

Azure DNS

Обеспечивает сверхвысокую скорость ответов DNS и доступность домена.

Сеть доставки содержимого Azure

Доставляет содержимое с высокой пропускной способностью клиентам по всему миру.

Защита от атак DDoS Azure

Защищает приложения, размещенные в Azure, от распределенных атак типа "отказ в обслуживании" (DDoS).

Диспетчер трафика Azure

Распределяет сетевой трафик между регионами Azure по всему миру.

Azure ExpressRoute

Подключается к Azure через выделенные безопасные соединения с высокой пропускной способностью.

Наблюдатель за сетями Azure

Проводит мониторинг и диагностику неполадок в сети с помощью анализа на основе сценариев.

Брандмауэр Azure

Реализует высокий уровень безопасности и доступности брандмауэра с неограниченной масштабируемостью.

Виртуальная глобальная сеть Azure (WAN)

Создает единую глобальную сеть (WAN), подключенную к локальным и удаленным сайтам.

Хранилище

Azure предоставляет четыре основных типа служб хранилища.

Хранилище BLOB-объектов Azure

Служба хранилища для очень больших объектов, например видеофайлов или растровых изображений.

Хранилище файлов Azure

Файловые ресурсы, к которым можно получать доступ как к файловому серверу и управлять как файловым сервером.

Хранилище очередей Azure

Хранилище данных для постановки сообщений в очередь и их надежной доставки между приложениями.

табличное хранилище Azure;

Хранилище таблиц — это служба для хранения нереляционных структурированных данных (также называются структурированными данными NoSQL) в облаке, предоставляющая бессхемное хранилище ключей и атрибутов.

Все эти службы имеют ряд общих характеристик:

- **Надежность** и высокая доступность с избыточностью и репликацией.
- **Защита** посредством автоматического шифрования и управления доступом на основе ролей.
- **Масштабируемость** с практически неограниченным хранилищем.
- **Управляемое** обслуживание и решение критических проблем без вашего участия.
- **Доступ** из любой точки мира по протоколу HTTP или HTTPS.

Мобильные приложения

Благодаря Azure разработчики могут быстро и легко создавать мобильные серверные службы для приложений iOS, Android и Windows. Функции, которые раньше отнимали много времени и повышали риски для проекта, например добавление корпоративного единого входа и подключение к локальным ресурсам, таким как SAP, Oracle, SQL Server и SharePoint, теперь легко использовать.

Другие функции этой службы:

- Синхронизация данных в автономном режиме.
- Подключение к локальным данным.

- Рассылка push-уведомлений.
- Автоматическое масштабирование в соответствии с потребностями бизнеса.

Базы данных

Azure предоставляет несколько служб базы данных для хранения разнообразных типов данных и томов. А с возможностями глобального соединения эти данные доступны пользователям моментально.

Azure Cosmos DB

Глобально распределенная база данных, которая поддерживает параметры NoSQL.

База данных SQL Azure

Полностью управляемая реляционная база данных с автоматическим масштабированием, интегральной аналитикой и надежной системой безопасности.

База данных Azure для MySQL

Полностью управляемая и масштабируемая реляционная база данных MySQL с высоким уровнем доступности и безопасности.

База данных Azure для PostgreSQL

Полностью управляемая и масштабируемая реляционная база данных PostgreSQL с высоким уровнем доступности и безопасности.

SQL Server в виртуальных машинах Azure

Служба, которая размещает корпоративные приложения SQL Server в облаке.

Azure Synapse Analytics

Полностью управляемое хранилище данных с интегрированной защитой для любых уровней масштабирования без дополнительных затрат.

Azure Database Migration Service

Служба, которая переносит базы данных в облако без изменения кода приложения.

Кэш Redis для Azure

Полностью управляемая служба, которая кэширует часто используемые и статические данные для снижения задержек в данных и приложениях.

База данных Azure для MariaDB

Полностью управляемая и масштабируемая реляционная база данных MariaDB с высоким уровнем доступности и безопасности.

Веб-службы

В современном мире для бизнеса критически важно быть достойно представленным в Интернете. Azure предлагает первоклассную поддержку для создания и размещения веб-приложений и веб-служб на базе HTTP. Следующие службы Azure ориентированы на размещение в Интернете.

Служба приложений Azure

Быстрое создание полнофункциональных облачных веб-приложений.

Центры уведомлений Azure

Отправка push-уведомлений из любой серверной части на любую платформу

Служба управления Azure API

Безопасная публикация API для разработчиков, партнеров и сотрудников в необходимом масштабе.

Когнитивный поиск Azure

Разверните этот полностью управляемый поиск в качестве службы.

Веб-приложения службы приложений Azure

Создание и развертывание критически важных веб-приложений с возможностью масштабирования

Служба Azure SignalR

Простое добавление функциональных возможностей в режиме реального времени.

Интернет вещей

Увеличение объема информации, доступного пользователям. Персональные цифровые помощники превратились в смартфоны, а теперь нам доступны умные часы, умные термостаты и даже умные холодильники. Повсеместное использование персональных компьютеров. Возможность доступа к ценной информации любых устройств, поддерживающих подключение к Интернету. Концепция Интернета вещей заключается в возможности сбора данных устройствами и их передачи для анализа.

В Azure существует много служб, которые помогут вам реализовать комплексные решения для Интернета вещей.

IoT Central

Полностью управляемое глобальное SaaS-решение (программное обеспечение как услуга), которое облегчает подключение и мониторинг ресурсов Интернета вещей, а также управление ими в любом масштабе.

Центр Интернета вещей Azure

Центр обмена сообщениями, который обеспечивает защищенный обмен данными между миллионами устройств Интернета вещей и их мониторинг.

IoT Edge

Полностью управляемая служба, которая позволяет отправлять модели анализа данных непосредственно на устройства Интернета вещей, чтобы они быстрее реагировали на изменения состояния без обращения к облачным моделям ИИ.

Большие данные

Данные могут иметь любой формат и размер. Под большими данными мы понимаем *большие* объемы данных. В метеорологических и коммуникационных системах, геномных исследованиях, на платформах визуализации и во многих других сценариях

могут генерироваться сотни гигабайтов данных. При таких объемах значительно усложняются процессы анализа данных и принятия решений. Зачастую объем данных настолько велик, что традиционные подходы к обработке и анализу попросту не работают.

Для сценариев с большими наборами данных были разработаны кластерные технологии с открытым исходным кодом. Azure предлагает широкий спектр технологий и услуг для обработки и анализа больших данных.

Azure Synapse Analytics

Облачное корпоративное хранилище данных для крупномасштабной аналитики, использующее массовую параллельную обработку для быстрого выполнения сложных запросов к данным объемом во множество петабайт.

Azure HDInsight

Управляемые кластеры Hadoop в облаке для обработки больших объемов данных.

Azure Databricks

Интегрируйте эту службу совместной аналитики на основе Apache Spark с другими службами больших данных в Azure.

ИИ

Возможности искусственного интеллекта в контексте облачных вычислений реализуются на базе широкого спектра служб, в основе которых лежат технологии машинного обучения. Машинное обучение — это способ обработки и анализа данных, который позволяет компьютерам использовать имеющиеся данные для прогнозирования будущего поведения, исходов и трендов. Используя машинное обучение, компьютеры учатся, не будучи явно запрограммированными.

Прогнозы машинного обучения позволяют сделать приложения и устройства эффективнее. Например, при покупках через Интернет машинное обучение помогает рекомендовать другие продукты, которые могут вам понравиться, на основе уже приобретенных вами товаров. Или при краже кредитной карты машинное обучение сравнивает транзакцию с базой данных транзакций и помогает обнаруживать мошенничество. Когда робот-пылесос убирает комнату, машинное обучение позволяет определить, когда этот процесс окончен.

Ниже описываются некоторые популярные службы искусственного интеллекта и машинного обучения Azure.

Служба машинного обучения Azure

Облачная среда, которую можно использовать для разработки, обучения, тестирования, развертывания и отслеживания моделей машинного обучения, а также управления такими моделями. Эта служба обеспечивает автоматическое создание моделей и их настройку. Она позволяет начать обучение на локальном компьютере, а затем развернуть его в облаке.

Студия машинного обучения Azure

Рабочее пространство с визуальным интерфейсом для совместной работы, в котором можно создавать, тестировать и развертывать решения машинного обучения, используя готовые алгоритмы машинного обучения и модули обработки данных.

Службы *Cognitive Services* включают в себя целый ряд тесно связанных друг с другом продуктов. Вы можете использовать эти готовые API в приложениях для решения различных сложных проблем.

Компьютерное зрение

Используйте интеллектуальные алгоритмы обработки изображений, позволяющие идентифицировать, индексировать и модерировать изображения и видеозаписи, а также добавлять к ним подписи.

Речь

Преобразование устной речи в текст, проверка подлинности по голосу или распознавание говорящего в приложении.

Сопоставление набора знаний

Сопоставление сложного набора сведений и данных для решения таких задач, как интеллектуальный подбор рекомендаций и семантический поиск.

Поиск Bing

API поиска Bing для приложений, позволяющие обрабатывать миллиарды веб-страниц, изображений, видеозаписей и новостей в рамках одного вызова API.

Обработка естественного языка

Позволяют реализовать в приложениях обработку естественного языка с использованием готовых скриптов, анализа тональности и обучения распознаванию пользовательских запросов.

DevOps

Концепция DevOps позволяет объединить людей, процессы, технологии и возможности автоматизации доставки ПО для обеспечения непрерывной поддержки пользователей. С помощью Azure DevOps вы можете создавать конвейеры *сборки* и *выпуска*, обеспечивающие непрерывную интеграцию, доставку и развертывание ваших приложений. Вы можете интегрировать тесты репозиториев и приложений, осуществлять мониторинг приложений и работать с артефактами сборки. Кроме того, вы можете работать с элементами невыполненной работы в целях отслеживания, автоматизировать развертывание инфраструктуры и осуществлять интеграцию с широким спектром сторонних средств и служб, таких как Jenkins и Chef. Все эти и многие другие функции тесно интегрируются с платформой Azure, обеспечивая согласованное регулярное развертывание приложений и, тем самым, оптимизацию процессов сборки и выпуска.

Azure DevOps

Используйте средства для совместной работы в области разработки, в том числе высокопроизводительные конвейеры, бесплатные частные репозитории Git, настраиваемые

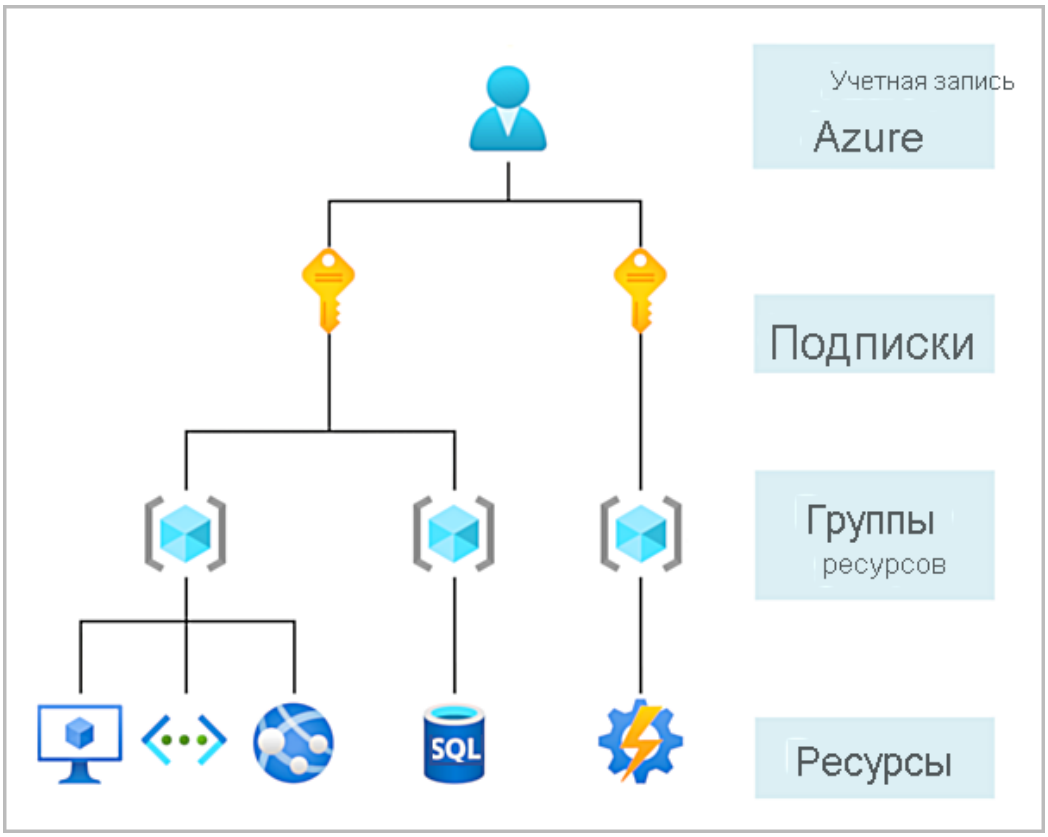
канбан-доски, а также автоматизированные и облачные инструменты для нагрузочного тестирования. Прежнее название — Visual Studio Team Services.

Azure DevTest Labs

Оптимизация процессов создания сред Windows и Linux по запросу для тестирования или демонстрационного запуска приложений непосредственно из конвейера развертывания.

2.3.Начало работы с учетными записями Azure

Чтобы создать и использовать службы Azure, вам потребуется подписка Azure. Когда вы работаете с модулями Learn, обычно для вас создается временная подписка, которая выполняется в среде песочницы Learn. При работе с собственными приложениями и бизнес-задачами вы должны создать учетную запись Azure, для которой будет создана подписка. После создания учетной записи Azure вы можете создавать дополнительные подписки. Например, ваша организация может использовать одну учетную запись Azure для вашего отдела, а также отдельные подписки для отделов разработки, маркетинга и продаж. После создания подписки Azure можно приступить к созданию ресурсов Azure в каждой подписке.



2.4.Обсуждение различных типов моделей облака

Существует три модели развертывания облачных вычислений: *общедоступное облако*, *частное облако* и *гибридное облако*. Каждая модель развертывания имеет различные аспекты, которые следует учитывать при миграции в облако.

Общедоступное облако

Службы предоставляются через общедоступный Интернет и доступны всем, кто хочет их купить. Облачные ресурсы, такие как серверы и хранилище, принадлежат стороннему поставщику облачных служб, и он же управляет этими ресурсами, а доступ к ним осуществляется через Интернет.

Частное облако

Частное облако представляет собой вычислительные ресурсы, которые используются сотрудниками исключительно из одной компании или организации. Частное облако может физически находиться в локальном центре обработки данных вашей организации или размещаться сторонним поставщиком услуг.

Гибридное облако

Гибридное облако — это вычислительная среда, сочетающая в себе общедоступное и частное облако и позволяющая переносить данные и приложения между ними.

Сравнение моделей облака

Общедоступное облако

- Нет капитальных средств для увеличения масштаба.
- Приложения можно быстро подготавливать и отзывать.
- Организации платят только за то, что они используют.

Частное облако

- Необходимо приобрести оборудование для запуска и обслуживания.
- Организации имеют полный контроль над ресурсами и безопасностью.
- Организации несут ответственность за обслуживание и модернизацию оборудования.

Гибридное облако

- Обеспечивает наибольшую гибкость.
- Организации сами определяют, где выполнять приложения.
- Организации контролируют безопасность, соответствие требованиям или юридические требования.

2.5.Описание преимуществ и особенностей облака

- **Высокая доступность**. В зависимости от выбранного соглашения об уровне обслуживания (SLA) облачные приложения могут обеспечить непрерывное взаимодействие с пользователем без видимого простоя даже в случае проблем.

- **Масштабируемость.** Приложения в облаке можно масштабировать *вертикально* и *горизонтально*:

    - Вертикальное масштабирование позволяет увеличить вычислительную мощность путем добавления ОЗУ или ЦП в виртуальную машину.

    - Горизонтальное масштабирование позволяет увеличить вычислительную мощность путем добавления экземпляров ресурсов, например добавляя в конфигурацию виртуальные машины.

- **Эластичность**. Облачные приложения можно настроить для использования преимуществ автомасштабирования, чтобы у приложений всегда были необходимые ресурсы.

- **Гибкость**. Облачные ресурсы можно развертывать и настраивать очень быстро по мере изменения требований приложения.

- **Географическое распределение**. Приложения и данные можно развернуть в региональных центрах обработки данных по всему миру, тем самым гарантируя, что клиенты всегда будут иметь лучшую производительность в своем регионе.

- **Аварийное восстановление**. Благодаря преимуществам облачных служб резервного копирования, репликации данных и географического распределения вы можете развертывать приложения и не сомневаться, что в случае аварии данные будут в безопасности.

Сравнение капитальных затрат и операционных расходов

Необходимо учитывать, что существует два разных типа расходов.

- **Капитальные затраты (CapEx)** — предварительные затраты на физическую инфраструктуру с последующим вычетом налогов через определенный период времени. Первоначальные капитальные затраты со временем обесцениваются.

- **Операционные расходы (OpEx)** — это расходы на услуги или продукты, счета за которые выставляются в настоящий момент. Эти расходы можно вычесть из налогов за этот же год. Здесь нет предварительных затрат, вы платите за услугу или продукт по мере использования.

Облачные вычисления — это модель на основе потребления ресурсов

Поставщики облачных услуг работают по *модели на основе потребления*. Это означает, что конечные пользователи платят только за те ресурсы, которые они используют. Что они используют, за то и платят.

Модель на основе потребления имеет много преимуществ, в том числе следующие.

- Никаких первоначальных затрат.
- Нет необходимости приобретать и поддерживать дорогостоящую инфраструктуру, все возможности которой могут не использоваться в полной мере.
- Возможность оплачивать дополнительные ресурсы только тогда, когда они необходимы.
- Возможность перестать оплачивать ресурсы, которые больше не требуются.

2.6.Описание различных облачных служб

Что такое модели облачных служб?

Эти модели определяют различные уровни ответственности поставщика облачных служб и облачного клиента.

IaaS

Инфраструктура как услуга

Эта модель облачных служб больше всего напоминает управление физическими серверами. Поставщик облачных служб отвечает за оборудование, а обслуживанием операционной системы и настройкой сети занимается облачный клиент. Например, виртуальные машины Azure — это полнофункциональные виртуальные вычислительные устройства, работающие в центрах обработки данных Майкрософт. Преимуществом этой модели облачных служб является быстрое развертывание новых вычислительных устройств. Настроить новую виртуальную машину будет значительно быстрее, чем купить, установить и настроить физический сервер.

PaaS

Платформа как услуга

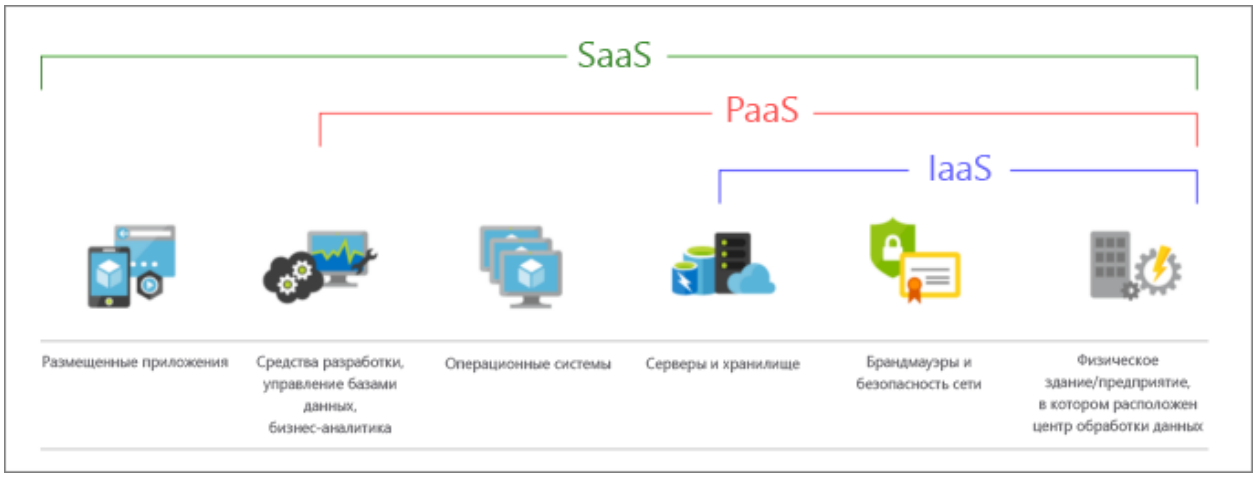
Эта модель облачной службы является управляемой средой размещения. Поставщик облачных служб управляет виртуальными машинами и сетевыми ресурсами, а облачный клиент развертывает свои приложения в управляемой среде размещения. Например, Службы приложений Azure предоставляют управляемую среду размещения, в которой разработчики могут отправлять свои веб-приложения, не заботясь о требованиях к физическому оборудованию и программному обеспечению.

SaaS

Программное обеспечение как услуга

В этой модели поставщик облачных служб управляет всеми аспектами среды приложений, такими как виртуальные машины, сетевые ресурсы, хранилище данных и приложения. Облачному клиенту необходимо только предоставить свои данные приложению, которое управляется поставщиком облачных служб. Например, Microsoft Office 365 предоставляет полностью работоспособную версию Microsoft Office, которая работает в облаке. Все, что вам нужно сделать, — это создать содержимое, а Office 365 позаботится обо всем остальном.

На следующем рисунке показаны службы, которые могут выполняться в каждой из моделей.



Мы подробно сравним эти три модели в следующих разделах.

IaaS

IaaS — самая гибкая категория облачных служб. Ее цель — предоставить вам полный контроль над оборудованием, на котором выполняется приложение. При использовании модели IaaS вам не нужно приобретать оборудование — вы просто арендуете его.

Преимущества

Нет капитальных затрат. Начальные капиталовложения отсутствуют.

Гибкость. Приложения можно быстро делать доступными и отзывать при необходимости.

Управление. Применяется модель солидарной ответственности; пользователь управляет предоставленными службами и поддерживает их, а поставщик облачных служб управляет облачной инфраструктурой и обслуживает ее.

Модель на основе потребления. Организации платят только за то, что используют, и работают по модели операционных расходов.

Навыки. Для развертывания, использования общедоступного облака и получения его преимуществ не требуется серьезный уровень технической подготовки. Организации могут пользоваться навыками и умениями поставщика облачных служб для обеспечения защиты, безопасности и высокой доступности рабочих нагрузок.

Преимущества облака. Организации могут пользоваться навыками и умениями поставщика облачных служб для обеспечения безопасности и высокой доступности рабочих нагрузок.

Гибкость. IaaS — это наиболее гибкая облачная служба, так как вы можете настраивать оборудование, на котором работает ваше приложение, и управлять им.

PaaS

PaaS обладает теми же преимуществами и характеристиками, что и IaaS, и также имеет дополнительные плюсы.

Преимущества

Нет капитальных затрат. Начальные капиталовложения отсутствуют.

Гибкость. Модель PaaS более гибкая, чем IaaS, и пользователям не нужно настраивать серверы для запуска приложений.

Модель на основе потребления. Пользователи платят только за то, что используют, и работают по модели операционных расходов.

Навыки. Для развертывания, использования и получения преимуществ PaaS не требуется серьезный уровень технической подготовки.

Преимущества облака. Пользователи могут задействовать навыки и умения поставщика облачных служб для обеспечения безопасности и высокой доступности своих рабочих нагрузок. Кроме того, пользователи могут получать доступ к более инновационным инструментам разработки, чтобы применять их на протяжении всего жизненного цикла приложения.

Производительность. Пользователи могут сосредоточиться только на разработке приложений, так как управление платформой осуществляется поставщиком облачных служб. Работать с распределенными командами как со службами проще, поскольку доступ к платформе осуществляется через Интернет. Эту платформу проще сделать глобально доступной.

Недостаток

Ограничения платформы. У облачной платформы могут быть некоторые ограничения, которые могут повлиять на способ работы приложений. При подборе платформы PaaS для вашей рабочей нагрузки учитывайте все ограничения в этой области.

SaaS

SaaS — это централизованно размещенное и управляемое программное обеспечение для пользователей или клиентов. Обычно для всех клиентов используется одна версия приложения, которая лицензируется путем месячной или годовой подписки.

SaaS обеспечивает те же преимущества, что и IaaS, но имеет и дополнительные плюсы.

Преимущества

Нет капитальных затрат. Начальные капиталовложения отсутствуют.

Гибкость. Организации могут быстро и просто предоставлять своему персоналу доступ к новейшему программному обеспечению.

Модель ценообразования с оплатой по мере использования. Пользователи платят за используемое программное обеспечение по модели подписки, обычно месячной или годовой, независимо от того, в каких объемах они используют это программное обеспечение.

Навыки. Для развертывания, использования и получения преимуществ SaaS не требуется серьезный уровень технической подготовки.

Гибкость. Пользователи могут получать доступ к одним и тем же данным приложения откуда угодно.

Недостаток

Программные ограничения. Для программных приложений могут существовать некоторые ограничения, влияющие на способ работы пользователей. Так как вы используете программное обеспечение "как есть", у вас нет прямого контроля над функциями. При подборе платформы SaaS для вашей рабочей нагрузки учитывайте потребности бизнеса и ограничения программного обеспечения.

Сравнение моделей облачных служб

IaaS

Самая гибкая облачная служба.

Вы настраиваете оборудование для приложения и управляете им.

PaaS

Сосредоточьтесь на разработке приложений.

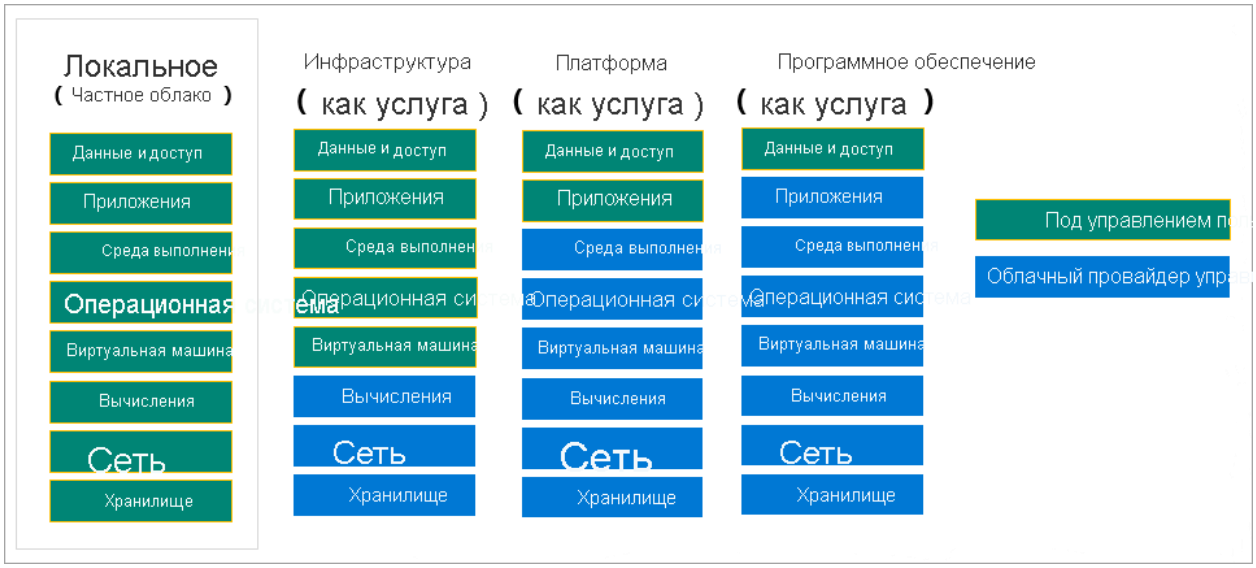
Управление платформой осуществляется поставщиком облачных служб.

SaaS

Модель ценообразования с оплатой по мере использования.

Пользователи платят за программное обеспечение, которое они используют по модели подписки.

На следующей схеме показаны разные уровни ответственности, разделяемой между поставщиком облачных служб и облачным арендатором.



Что такое бессерверные вычисления?

Как и PaaS, *бессерверные вычисления* позволяют разработчикам быстрее создавать приложения, поскольку берут на себя управление инфраструктурой. В модели

бессерверных приложений поставщик облачных служб автоматически подготавливает и масштабирует базовую инфраструктуру, необходимую для выполнения кода, а также управляет ею. Бессерверные архитектуры легко масштабируются и управляются событиями, при этом ресурсы используются только при срабатывании определенной функции или триггера.

Важно отметить, что для запуска кода все же используются серверы. Просто задачи, связанные с подготовкой инфраструктуры и управлением ею, невидимы для разработчика. Этот подход позволяет разработчикам уделять больше внимания бизнес-логике и основному направлению деятельности. Бессерверные вычисления помогают сотрудникам повысить производительность и ускорить вывод продуктов на рынок, а также позволяют организациям оптимизировать ресурсы и сосредоточиться на инновациях.

3. Применение сервисов Azure для совершенствования процессов компании.

3.1.Ресурсы Azure и Azure Resource Manager

- **Ресурс**. Управляемый элемент, доступный в Azure. Примеры ресурсов — виртуальные машины, учетные записи хранения, веб-приложения, базы данных и виртуальные сети.

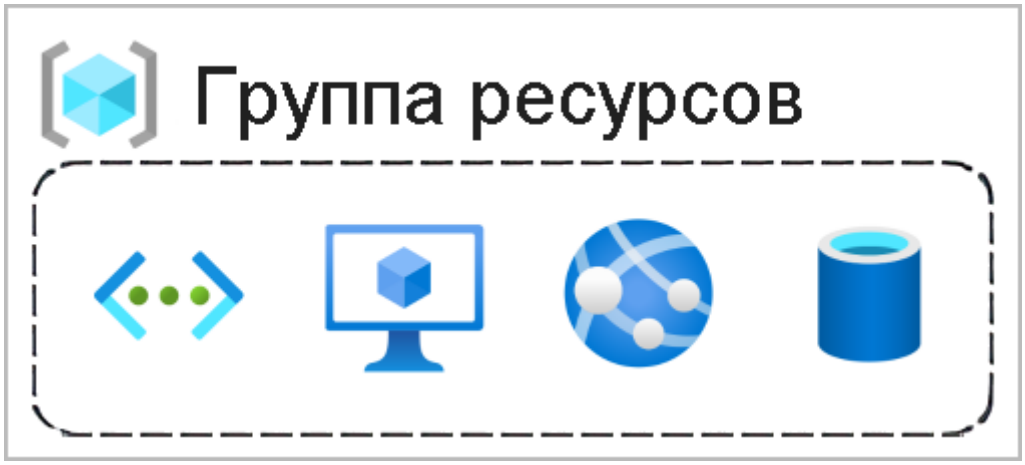
- **Группа ресурсов**: Контейнер, содержащий связанные ресурсы для решения Azure. Группа ресурсов содержит ресурсы, которыми вы хотите управлять как группой. Пользователи могут выбрать оптимальный для своей организации способ распределения ресурсов в группах ресурсов.

Группы ресурсов Azure

Группы ресурсов являются фундаментальным элементом платформы Azure. Группа ресурсов — это логический контейнер ресурсов, развернутых в Azure. Эти ресурсы — все, что вы создаете в подписке Azure: виртуальные машины, экземпляры Шлюза приложений Azure, экземпляры Azure Cosmos DB и т. д. Все ресурсы должны находиться в группах ресурсов, и ресурс может быть членом только одной группы ресурсов. Многие ресурсы можно перемещать между группами ресурсов, но у некоторых служб есть ограничения или требования для перемещения. Группы ресурсов не могут быть вложенными. Прежде чем можно будет подготовить какой-то ресурс, нужно поместить его в группу.

Логическое группирование

Группы ресурсов помогают контролировать и упорядочивать ваши ресурсы Azure. Размещая ресурсы по принципу схожего использования, типа или расположения в группе ресурсов, вы упорядочиваете ресурсы, создаваемые в Azure. Сейчас вас больше всего интересует логическое группирование, так как в наших ресурсах довольно много беспорядка.



Жизненный цикл

При удалении группы ресурсов все содержащиеся в ней ресурсы также будут удалены. Упорядочение ресурсов по жизненному циклу может быть полезно в непроизводственных средах, чтобы провести эксперименты, а затем просто удалить среду. Группы ресурсов позволяют легко удалить сразу ряд ресурсов.

Авторизация

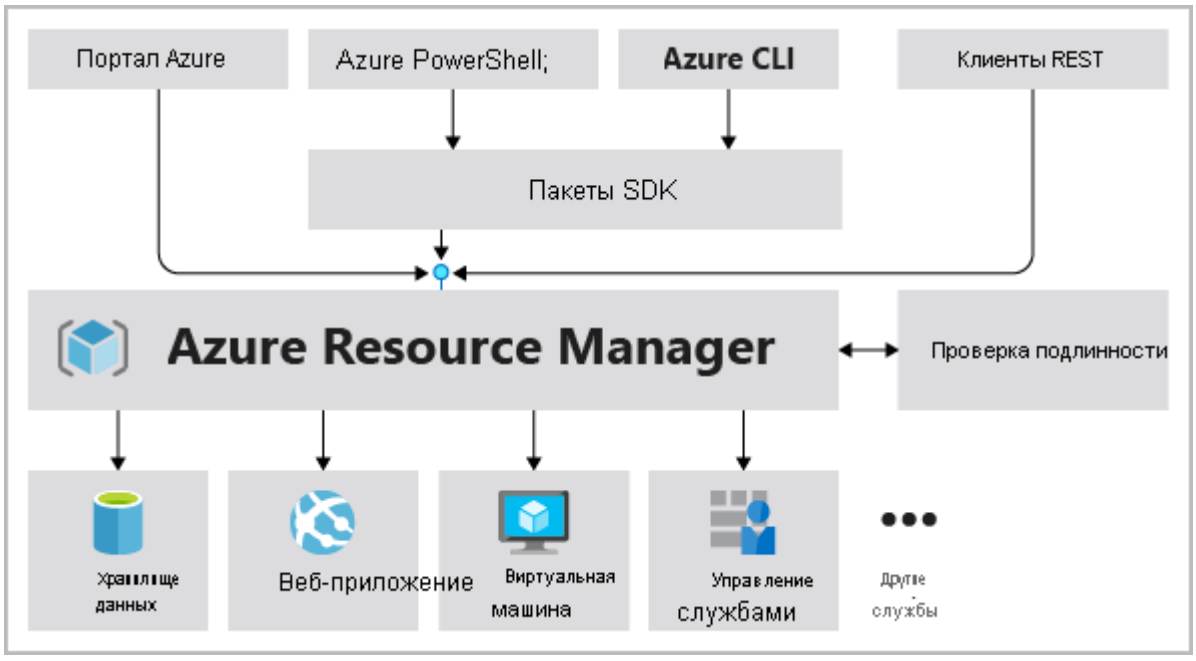
В группах ресурсов также можно применять разрешения управления доступом на основе ролей (RBAC). Применяя разрешения RBAC в группе ресурсов, вы можете упростить администрирование и ограничивать доступ, разрешая только то, что необходимо.

Azure Resource Manager

Azure Resource Manager — это служба развертывания и управления для Azure. Она обеспечивает уровень управления для создания, обновления и удаления ресурсов в учетной записи Azure. Для защиты и упорядочивания ресурсов после развертывания используются такие функции управления, как управление доступом, блокировки и теги.

Когда пользователь отправляет запрос из любого из средств Azure, API или пакетов SDK, он направляет к Resource Manager. Resource Manager выполняет аутентификацию и авторизацию запроса. Resource Manager отправляет запрос в службу Azure, которая принимает запрошенное действие. Так как все запросы обрабатываются через один API, результаты и возможности будут согласованы в различных средствах.

На следующем рисунке показана роль Resource Manager при обработке запросов Azure.



Все возможности, доступные на портале Azure, также доступны в PowerShell, Azure CLI, REST API и клиентских пакетах SDK. Функции, предоставленные через API, будут представлены на портале в течение 180 дней после выпуска.

Преимущества использования диспетчера ресурсов

С помощью Resource Manager можно:

- Управлять своей инфраструктурой с помощью декларативных шаблонов, а не сценариев. Шаблон Resource Manager — это JSON-файл, который определяет, что развернуть в Azure.

- Развертывать и отслеживать все ресурсы вашего решения, а также управлять ими как единой группой, а не работать с ними по отдельности.

- Повторно развертывайте решение на протяжении всего жизненного цикла разработки, чтобы гарантировать согласованность ресурсов.

- Определять зависимости между ресурсами, чтобы их развертывание выполнялось в правильном порядке.

- Применяйте управление доступом ко всем службам, так как RBAC изначально интегрирован в платформу управления.

- Применять теги в ресурсах для логического упорядочивания всех ресурсов в вашей подписке к ним.

- Контролируйте выставление счетов в организации, просматривая затраты для группы ресурсов с одним тегом.

3.2.Подписки и группы управления Azure

Подписки Azure

Для использования Azure требуется подписка Azure. Подписка предоставляет авторизованным и прошедшим проверку подлинности пользователям доступ к продуктам и службам Azure. Она также позволяет подготавливать ресурсы. Подписка Azure — это логическая единица служб Azure, связанная с учетной записью Azure. Она служит идентификатором в Azure Active Directory (Azure AD) или в каталоге, которому доверяет Azure AD.

В одной учетной записи может быть одна или несколько подписок с разными моделями выставления счетов, к которым применяются различные политики управления доступом. Подписки Azure можно использовать для определения границ для продуктов, служб и ресурсов Azure. Границы подписки бывают двух типов:

- **Границы выставления счетов**. Этот тип подписки определяет, как выставляются счета за использование Azure в учетной записи. Можно создать несколько подписок для различных типов требований к выставлению счетов. Azure создает отдельные отчеты о выставлении счетов и счета для каждой подписки, чтобы можно было организовывать затраты и управлять ими.

- **Границы управления доступом**. Azure применяет политики управления доступом на уровне подписки. Вы можете создавать отдельные подписки, соответствующие структуре вашей организации. Например, в компании

можно выделить отделы, к которым будут применяться особые политики по подпискам Azure. Эта модель выставления счетов позволит вам контролировать доступ к ресурсам, применяемым пользователями в соответствующих подписках.

Создание дополнительной подписки Azure

Возможно, потребуется создать дополнительные подписки для управления ресурсами или выставления счетов. Например, вы можете создать дополнительные подписки для разделения по следующим категориям:

- **Среды**. При управлении ресурсами вы можете создать подписки, чтобы настроить отдельные среды для разработки и тестирования, обеспечения безопасности или для изоляции данных по соображениям соответствия. Такая схема особенно полезна, поскольку управление доступом к ресурсам осуществляется на уровне подписки.

- **Организационные структуры**. Вы можете создавать подписки в соответствии со структурой организации. Например, можно ограничить какой-нибудь отдел низкозатратными ресурсами, а ИТ-отделу предоставить полный доступ. Такой подход позволяет вам контролировать доступ к ресурсам, которые пользователи используют в каждой подписке.

- **Выставление счетов**. Вы также можете создать дополнительные подписки для выставления счетов. Так как затраты сначала суммируются на уровне подписки, вы можете создавать подписки для контроля и отслеживания затрат в зависимости от ваших потребностей. Например, вы можете создать одну подписку для производственных рабочих нагрузок и еще одну подписку для рабочих нагрузок разработки и тестирования.

Вам могут потребоваться дополнительные подписки по следующим причинам:

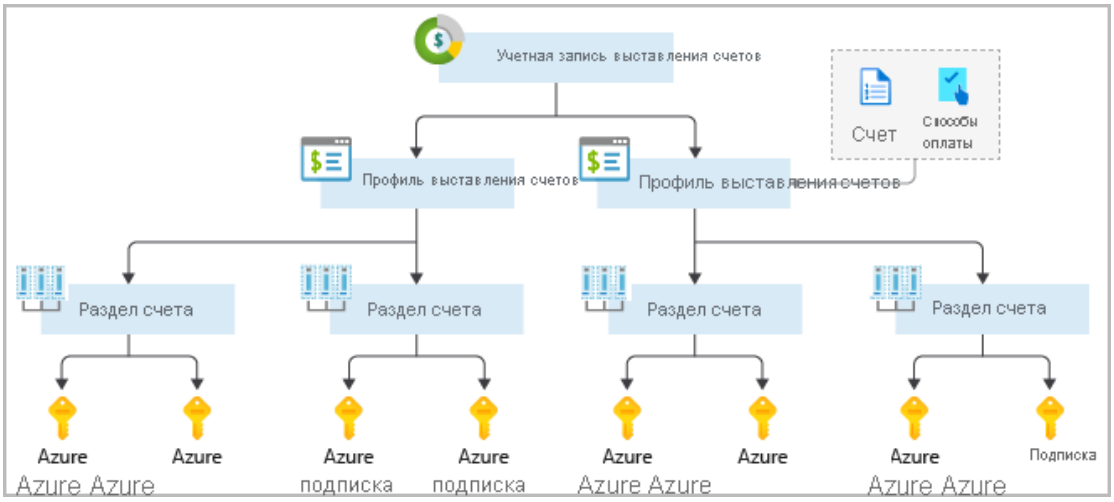
- **Ограничения подписки**. Подписки привязаны к некоторым аппаратным ограничениям. Например, максимальное количество каналов Azure ExpressRoute на одну подписку — 10. Эти ограничения необходимо учитывать при создании подписки в вашей учетной записи. Если в некоторых ситуациях вам необходимо обойти эти ограничения, можно добавить дополнительные подписки.

Настройка выставления счетов в соответствии с вашими потребностями

Если у вас несколько подписок, их можно объединить в разделы счета. Каждый раздел — это позиция в счете, которая показывает расходы за этот месяц. Например, вам может понадобиться один счет для организации, но вам будет необходимо упорядочить затраты по отделу, команде или проекту.

В зависимости от ваших потребностей можно настроить несколько счетов в одной учетной записи выставления счетов. Для этого создайте дополнительные профили выставления счетов. Каждый профиль выставления счетов включает собственный счет и методы оплаты.

На следующей схеме показана структура выставления счетов. Если вы ранее регистрировались в Azure или у вашей организации есть Соглашение Enterprise, выставление счетов может быть настроено по-другому.



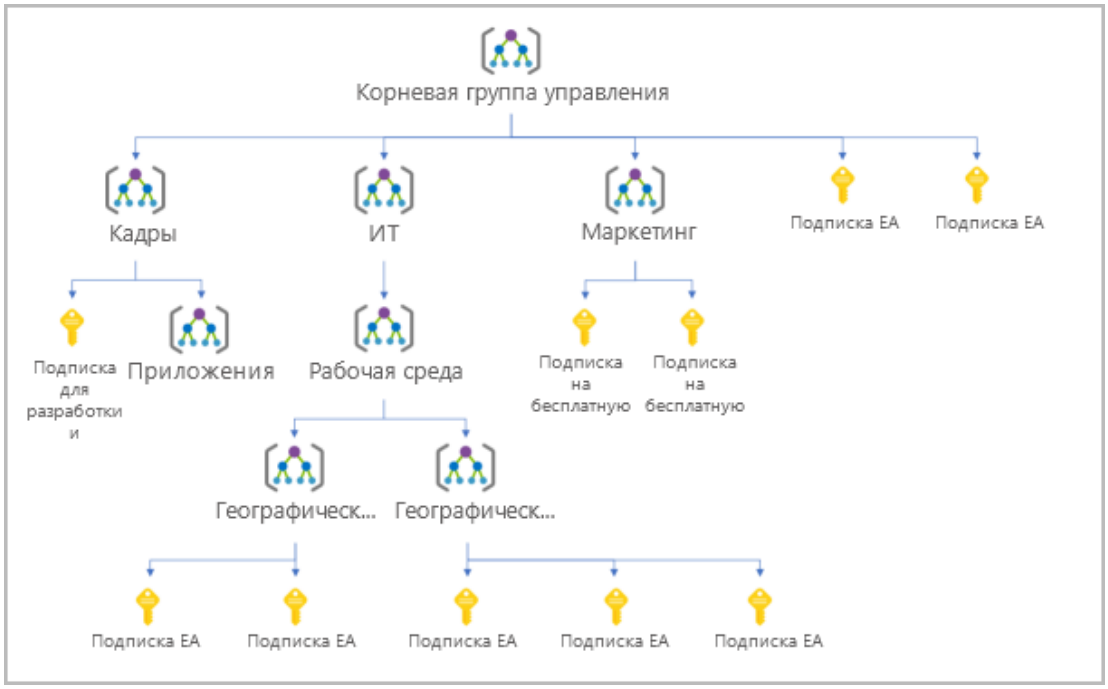
Группы управления Azure.

Если в организации много подписок, для эффективного управления доступом к ним, их политиками и соответствием требуется особый подход. Группы управления Azure представляют область действия уровнем выше, чем подписки. Вы объединяете подписки в контейнеры, которые называются группами управления, и применяете к ним условия системы управления. Все подписки в группе управления автоматически наследуют условия, применяемые к группе управления. Группы управления обеспечивают корпоративное управление в больших масштабах независимо от типа подписки. Все подписки в одной группе управления должны доверять одному и тому же клиенту Azure AD.

Например, можно применить политики к группе управления, которая ограничивает регионы, доступные для создания виртуальной машины. Эта политика будет применяться ко всем группам управления, подпискам и ресурсам в этой группе управления, разрешая создавать виртуальные машины только в этом регионе.

Иерархия групп управления и подписок

Вы можете создать гибкую структуру групп управления и подписок для упорядочивания своих ресурсов в иерархию для унифицированного управления политикой и доступом. На следующей схеме показано, как создать иерархию управления с использованием групп управления.



Вы можете создать иерархию, которая применяет политику. Например, можно ограничить расположения виртуальных машин западной частью США в группе с именем Production. Эта политика будет наследоваться во всех подписках Соглашения Enterprise, которые являются потомками этой группы управления, и применяться ко всем виртуальным машинам в этих подписках. Владелец ресурса или подписки не может изменить эту политику безопасности, что улучшает систему управления.

Еще один сценарий, в котором можно использовать группы управления, — предоставление пользователю доступа к нескольким подпискам. Перемещая несколько подписок в пределах одной группы управления, вы можете создать одно назначение RBAC (управление доступом на основе ролей) в этой группе управления, которая унаследует доступ ко всем нужным подпискам. Не нужно создавать скрипты назначений RBAC для разных подписок. Вместо этого вы можете разрешить пользователям доступ к необходимым ресурсам с помощью одного назначения в группе управления.

Важные сведения о группах управления

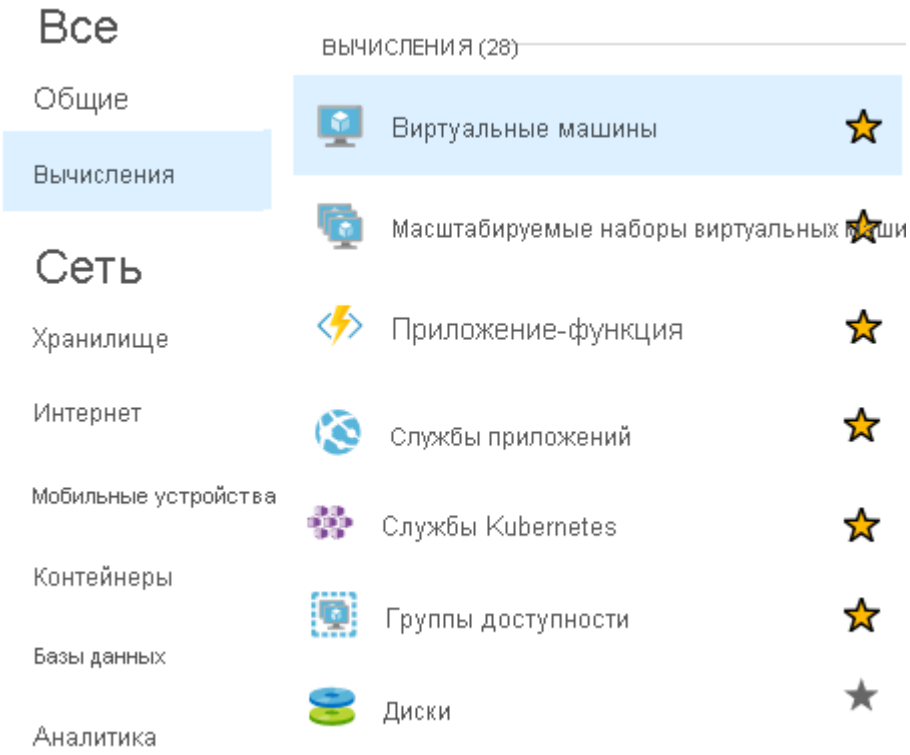
- Один каталог может поддерживать 10 000 групп управления.
- Дерево группы управления может поддерживать до шести уровней глубины. Данное ограничение не включает корневой уровень или уровень подписки.
- Каждая группа управления и подписка могут поддерживать только один родительский элемент.
- Каждая группа управления может содержать несколько дочерних групп.
- Все группы управления и подписки включены в иерархию в каждом каталоге.

3.3.Обзор вычислительных служб в Azure

Служба вычислений Azure — это предоставляемая по запросу служба вычислений для запуска облачных приложений. Она предоставляет вычислительные ресурсы, такие как диски, процессоры, память, сетевые подключения и операционные системы. Ресурсы доступны по запросу, обычно в течение нескольких минут или даже секунд. Вы платите только за используемые ресурсы и только за время их работы.

Azure поддерживает широкий спектр вычислительных решений для разработки и тестирования, выполнения приложений и расширения центра обработки данных, включая Linux, Windows Server, Microsoft SQL Server, Oracle, IBM и SAP. Azure также имеет множество служб, которые могут выполнять виртуальные машины. Каждая служба предоставляет различные параметры в зависимости от требований. Ниже перечислены некоторые из наиболее популярных служб.

- Виртуальные машины Azure
- Экземпляры контейнеров Azure
- Служба приложений Azure
- Функции Azure (или *бессерверные вычисления*)



Виртуальные машины

Виртуальные машины — это программная эмуляция физических компьютеров. У них есть виртуальный процессор, память, хранилище и сетевые ресурсы. В виртуальных машинах размещается операционная система, позволяя устанавливать и запускать программное обеспечение так же, как на физическом компьютере. Используя клиент удаленного рабочего стола, вы можете работать с виртуальной машиной и управлять ею, как если бы находились перед ней физически.

Благодаря виртуальным машинам Azure можно создавать и использовать виртуальные машины в облаке. Виртуальные машины предоставляют инфраструктуру как услугу (IaaS) и могут использоваться различными способами. Если вам нужен полный контроль над операционной системой и средой, виртуальные машины станут идеальным вариантом. Как и на физическом компьютере, вы сможете настраивать на виртуальной машине все запущенное программное обеспечение. Эта возможность полезна, если нужны нестандартные версии программного обеспечения или конфигурации размещения.

Масштабируемые наборы виртуальных машин

Масштабируемые наборы виртуальных машин — это вычислительный ресурс Azure для развертывания набора идентичных виртуальных машин и управления им. Так как все виртуальные машины настроены одинаково, масштабируемые наборы виртуальных машин позволяют выполнять действительно автоматическое масштабирование, ведь предварительная подготовка виртуальных машин не требуется. Это упрощает создание крупномасштабных служб, предназначенных для больших вычислений, больших данных и контейнерных рабочих нагрузок. По мере роста спроса можно добавить дополнительные экземпляры виртуальных машин. По мере снижения спроса экземпляры виртуальных машин можно удалить. Этот процесс может производиться вручную, автоматически или комбинированно.

Контейнеры и Kubernetes

Экземпляры контейнеров и Службы Azure Kubernetes — это ресурсы вычислений Azure, которые можно использовать для развертывания контейнеров и управления ими. Контейнеры — это упрощенные виртуализованные среды приложений. Они предназначены для быстрого создания, масштабирования и остановки динамическим образом. На одном хост-компьютере могут выполняться несколько экземпляров контейнерного приложения.

Служба приложений

С помощью Службы приложений Azure можно быстро создавать, развертывать и масштабировать веб-приложения, мобильные приложения и приложения API корпоративного уровня, работающие на любой платформе. Вы можете соблюдать строгие требования к производительности, масштабируемости, безопасности и соответствию, используя полностью управляемую платформу для обслуживания инфраструктуры. Служба приложений предлагается по модели "платформа как услуга" (PaaS).

Функции

Функции подходят в том случае, если для вас важен только код для службы, но не базовая платформа или инфраструктура. Они используются, когда в ответ на событие, например на запрос REST, таймер или сообщение от другой службы Azure, нужно выполнять простое и быстрое действие, которое завершается за несколько секунд или даже меньше.

Когда следует использовать Виртуальные машины Azure

Благодаря виртуальным машинам Azure можно создавать и использовать виртуальные машины в облаке. Они предоставляют инфраструктуру как услугу (IaaS) в форме виртуализованного сервера, и их можно использовать различными способами. Как и на физическом компьютере, вы сможете настраивать на виртуальной машине все

запущенное программное обеспечение. Виртуальные машины будут идеальным выбором, если вы хотите:

- Полный контроль над операционной системой (ОС).
- Возможность запускать пользовательское программное обеспечение.
- Использование настраиваемых конфигураций размещения.

Виртуальная машина Azure предоставляет гибкие возможности виртуализации без необходимости приобретать и обслуживать физическое оборудование, на котором она выполняется. Вам по-прежнему придется выполнять настройку, обновление и сопровождение выполняемого на виртуальной машине программного обеспечения.

3.4. Виртуальная сеть Azure

3.4.1. Основы виртуальной сети Azure

Виртуальные сети Azure позволяют ресурсам Azure, в том числе виртуальным машинам, веб-приложениям и базам данных, взаимодействовать друг с другом, с пользователями в Интернете и с локальными клиентскими компьютерами. Сеть Azure можно считать набором ресурсов, которые связывают другие ресурсы Azure.

Виртуальные сети Azure обеспечивают следующие основные сетевые возможности:

- изоляция и сегментирование;
- обмен данными через Интернет;
- обмен данными между ресурсами Azure;
- обмен данными с локальными ресурсами;
- маршрутизацию сетевого трафика;
- фильтрацию сетевого трафика;
- подключение виртуальных сетей.

Конфигурации сети для виртуальных машин

Изоляция и сегментирование

С помощью виртуальной сети можно создать несколько изолированных виртуальных сетей. Настраивая виртуальную сеть, вы определяете частный диапазон IP-адресов, используя общедоступные или частные диапазоны IP-адресов. Вы можете разделить этот диапазон IP-адресов на подсети и назначить каждой именованной подсети определенную часть диапазона адресов.

Для разрешения имен можно использовать службу разрешения имен, встроенную в Azure. Кроме того, вы можете настроить для виртуальной сети использование внутреннего или внешнего DNS-сервера.

Обмен данными через Интернет

Виртуальную машину в Azure можно подключить к Интернету по умолчанию. Можно разрешить входящие подключения из Интернета, определив общедоступный IP-адрес или общедоступную подсистему балансировки нагрузки. Для управления виртуальной машиной можно подключаться с помощью Azure CLI, протокола удаленного рабочего стола или Secure Shell.

Обмен данными между ресурсами Azure

Можно разрешить ресурсам Azure безопасно обмениваться данными друг с другом. Это можно сделать одним из двух способов.

- **Виртуальные сети**. Виртуальные сети могут соединять не только виртуальные машины, но и другие ресурсы Azure, такие как Среда службы приложений для Power Apps, Служба Azure Kubernetes и масштабируемые наборы виртуальных машин Azure.
- **Конечные точки службы** Конечные точки службы можно использовать для подключения к другим типам ресурсов Azure, таким как базы данных Azure SQL и учетные записи хранения. Такой подход позволяет связать несколько ресурсов Azure с виртуальными сетями, повышая уровень безопасности и обеспечивая оптимальную маршрутизацию между ресурсами.

Обмен данными через локальные ресурсы

С помощью виртуальных сетей Azure можно связывать ресурсы в локальной среде и в рамках подписки Azure. Фактически вы создаете сеть, которая охватывает и локальные, и облачные среды. Существует три механизма выполнения этого подключения.

- **Виртуальные частные сети типа "точка — сеть".** Типичный подход к подключению виртуальной частной сети (VPN) — с компьютера за пределами организации, обратно в корпоративную сеть. В этом случае клиентский компьютер инициирует зашифрованное VPN-соединение с Azure, чтобы подключиться к виртуальной сети Azure.
- **Виртуальные частные сети типа "сеть — сеть"**. Этот тип подключения связывает локальное устройство или шлюз VPN с VPN-шлюзом Azure в виртуальной сети. По сути, устройства в Azure могут отображаться как находящиеся в локальной сети. Подключение зашифровано и работает через Интернет.
- **Azure ExpressRoute** Azure ExpressRoute является лучшим подходом для сред, в которых требуется большая пропускная способность и даже более высокие уровни безопасности. ExpressRoute предоставляет выделенное частное соединение с Azure, которое не выходит в общедоступный Интернет. (Служба ExpressRoute будет рассмотрена подробнее в отдельном уроке далее в этом модуле.)

Маршрутизация сетевого трафика

По умолчанию Azure самостоятельно маршрутизирует трафик между подсетями во всех подключенных виртуальных сетях, локальных сетях и в Интернете. Но вы можете управлять маршрутизацией, переопределяя стандартные параметры, как описано ниже.

- **Таблицы маршрутов**. Таблица маршрутов позволяет задать правила направления трафика. Вы можете создать пользовательские таблицы маршрутов, которые управляют маршрутизацией пакетов между подсетями.
- **Протокол BGP**. Протокол BGP с помощью VPN-шлюзов Azure или Azure ExpressRoute распространяет локальные маршруты BGP в виртуальные сети Azure.

Фильтрация сетевого трафика

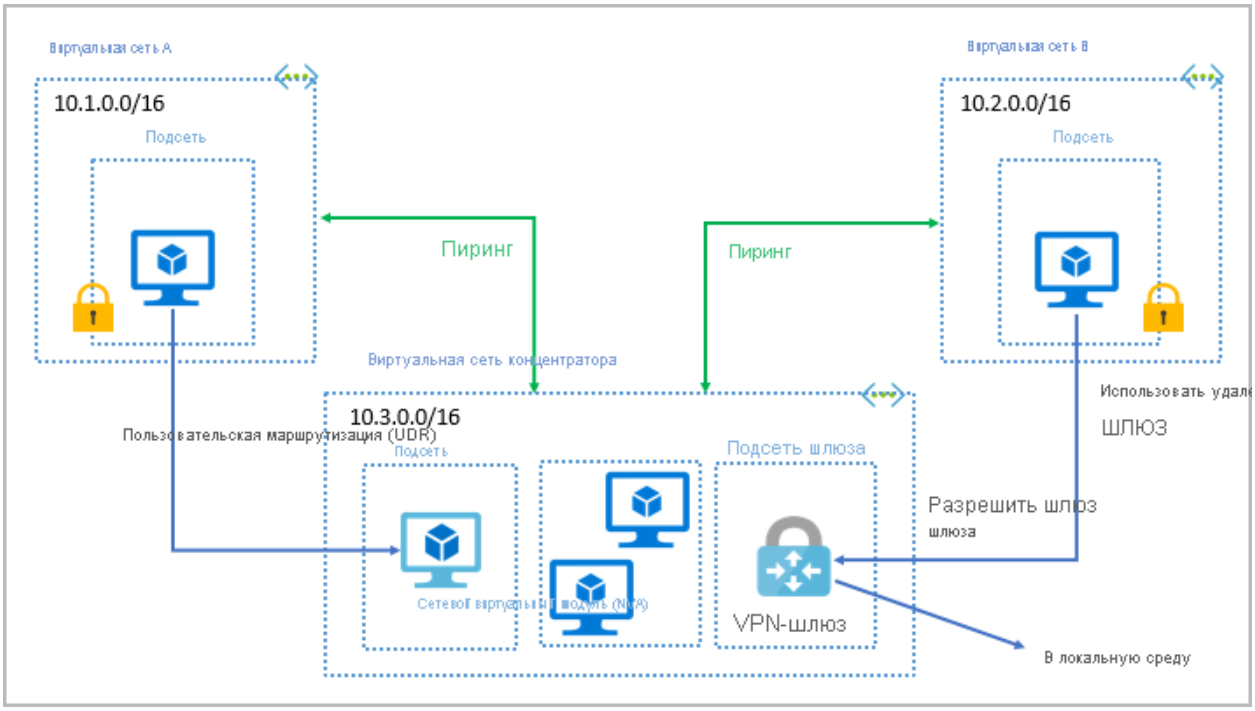
Виртуальные сети Azure позволяют фильтровать трафик между подсетями с помощью приведенных ниже подходов.

- **Группы безопасности сети** Группа безопасности сети — это ресурс Azure, который может содержать несколько правил безопасности относительно входящего и исходящего трафика. Эти правила для разрешения или блокировки трафика можно определить в зависимости от таких факторов, как исходный и конечный IP-адрес, порт и протокол.
- **Сетевые виртуальные модули** Сетевой виртуальный модуль — это специализированная виртуальная машина, которую можно сравнить с сетевым устройством с усиленной защитой. Сетевой виртуальный модуль выполняет определенную сетевую функцию, например роль брандмауэра или оптимизацию глобальной сети.

подключение виртуальных сетей.

Виртуальные сети можно связать с помощью *пиринга* виртуальной сети. Пиринг позволяет ресурсам в каждой виртуальной сети взаимодействовать друг с другом. Эти виртуальные сети могут располагаться в разных регионах, что позволяет создать глобальную взаимосвязанную сеть на основе Azure.

UDR — это определяемая пользователем маршрутизация. UDR является важным обновлением виртуальных сетей Azure, так как это позволяет сетевым администратором управлять таблицами маршрутизации между подсетями в виртуальной подсети, а также между виртуальными сетями, таким образом обеспечивая более высокую степень контроля потока сетевого трафика.



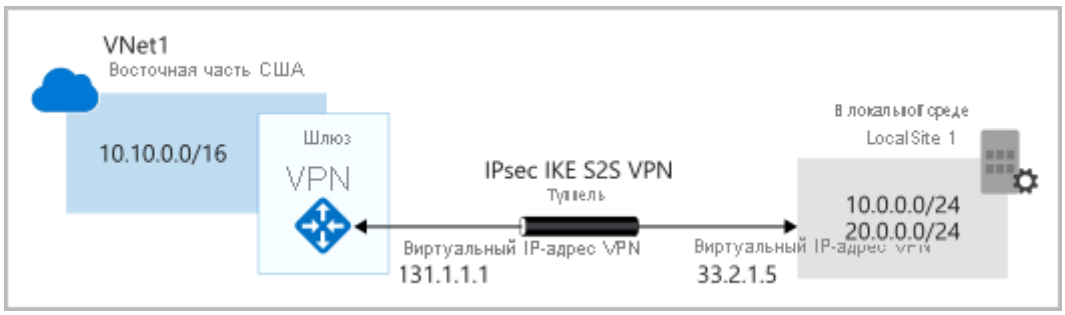
3.4.2. Основные сведения о VPN-шлюзе Azure

Эта частная сеть использует зашифрованный туннель внутри другой сети. Обычно они развертываются для соединения двух или более надежных частных сетей через ненадежную сеть (обычно с использованием общедоступного Интернета). Передаваемый по ненадежной сети трафик шифруется во избежание прослушивания или действия других атак.

VPN-шлюзы

VPN-шлюз — это тип шлюза виртуальной сети. Экземпляры VPN-шлюза Azure развертываются в виртуальных сетях Azure и обеспечивают следующие возможности соединения:

- из локальных центров обработки данных к виртуальным сетям с использованием подключения *сеть — сеть*;
- с отдельных устройств к виртуальным сетям с использованием подключения *точка —сеть*;
- из виртуальных сетей к виртуальным сетям с использованием подключения *сеть — сеть*.



Все передаваемые данные шифруются в закрытом туннеле, который проходит через Интернет. Вы можете развернуть только один VPN-шлюз в каждой виртуальной сети, но один шлюз можно использовать для подключения к нескольким расположениям, в том числе к другим виртуальным сетям или локальным центрам обработки данных.

При развертывании VPN-шлюза вам нужно указать тип VPN: *на основе политик* или *на основе маршрутов*. Основное различие между этими двумя типами VPN — способ указания шифруемого трафика. В Azure оба типа VPN-шлюзов используют общий ключ как единственный метод проверки подлинности. Оба типа также полагаются на протокол Internet Key Exchange (IKE) в версии 1 или версии 2 и Internet Protocol Security (IPSec). IKE используется для настройки сопоставления безопасности (соглашение шифрования) между двумя конечными точками. Это сопоставление затем передается в набор IPSec, который шифрует и расшифровывает пакеты данных, инкапсулированные в VPN-туннель.

VPN на основе политик

VPN-шлюзы на основе политик определяют статические IP-адреса пакетов, которые должны быть зашифрованы при прохождении через каждый туннель. Устройство этого типа оценивает каждый пакет данных на соответствие этим наборам IP-адресов, чтобы выбрать туннель, через который будет отправляться пакет.

Ключевые возможности VPN-шлюзов на основе политик в Azure:

- Поддержка только IKEv1.
- Использование *статической маршрутизации*, где комбинации префиксов адресов из обеих сетей управляют тем, как трафик, проходящий через туннель VPN, шифруется и расшифровывается. Источники и назначения туннельных сетей объявляются в политике. Их необязательно объявлять в таблицах маршрутизации.
- VPN на основе политик необходимо использовать в определенных сценариях, требующих, например, обеспечения совместимости с устаревшим локальным VPN-устройством.

VPN на основе маршрутов

Если определение IP-адресов за каждым туннелем является слишком трудоемкой задачей, можно использовать шлюзы на основе маршрутов. При использовании шлюзов на основе маршрутов туннели IPSec предоставляются как сетевой интерфейс или интерфейс виртуального туннеля. IP-маршрутизация (статические маршруты или протоколы динамической маршрутизации) определяет, какой из этих интерфейсов туннеля используется при отправке каждого пакета. VPN на основе маршрутов —

предпочтительный метод подключения локальных устройств. Они более устойчивы к изменениям топологии, например к созданию новых подсетей.

Если вам нужны какие-либо из следующих типов подключения, используйте VPN-шлюз на основе маршрутов:

- подключение между виртуальными сетями;
- подключения типа "точка — сеть";
- многосайтовые VPN-подключения;
- сосуществование со шлюзом Azure ExpressRoute.

Ключевые возможности VPN-шлюзов на основе маршрутов в Azure:

- поддержка IKEv2;
- использование селекторов трафика "любой к любому" (подстановочный знак);
- возможность использования *протоколов динамической маршрутизации*, в которых таблицы маршрутизации и перенаправления направляют трафик в разные туннели IPSec. В этом случае, исходная и целевая сети не определяются статически, как в VPN на основе политик или даже в VPN на основе маршрутов со статической маршрутизацией. Пакеты данных шифруются на основе таблиц сетевой маршрутизации, которые создаются динамически с помощью протоколов маршрутизации, например BGP.

Размеры VPN-шлюзов

Возможности VPN-шлюза зависят от номера SKU или развертываемого размера. В приведенной ниже таблице показаны основные возможности каждой доступной ценовой категории.

РАЗМЕРЫ VPN-ШЛЮЗОВ			
номер SKU	**Туннели типа "сеть — сеть"**	**Эталонная агрегированная пропускная способность**	**Протокол BGP**
Базовая [см. примечание]	Максимум: 10	100 Мбит/с	Не поддерживается
VpnGw1/Az	Максимум: 30	650 Мбит/с	Поддерживается
VpnGw2/Az	Максимум: 30	1 Гбит/с	Поддерживается
VpnGw3/Az	Максимум: 30	1,25 Гбит/с	Поддерживается

Развертывание VPN-шлюзов

Прежде чем можно будет развернуть VPN-шлюз, вам потребуются некоторые ресурсы Azure и локальные ресурсы.

Требуемые ресурсы Azure

Перед развертыванием рабочего VPN-шлюза вам понадобятся следующие ресурсы Azure.

- **Виртуальная сеть**. Разверните виртуальную сеть, задав достаточно большой диапазон адресов для дополнительной подсети, которая потребуется для VPN-шлюза. Адресное пространство этой виртуальной сети не должно перекрываться с локальной сетью, к которой вы будете подключаться. Вы можете развернуть только один VPN-шлюз в каждой виртуальной сети.

- **Подсеть шлюза**. Разверните подсеть с именем GatewaySubnet для VPN-шлюза. Используйте по меньшей мере маску адресов **/27**, чтобы предоставить достаточно IP-адресов в подсети для будущего расширения. Эту подсеть невозможно использовать для других служб.

- **Общедоступный IP-адрес**. В случае использования шлюза, не учитывающего зоны, создайте динамический общедоступный IP-адрес ценовой категории "Базовый". Этот адрес предоставляет общедоступный маршрутизируемый IP-адрес в качестве цели для локального VPN-устройства. Несмотря на то что этот IP-адрес является динамическим, он не изменится, если вы удалите и повторно создадите VPN-шлюз.

- **Шлюз локальной сети.** Создайте локальный сетевой шлюз для определения конфигурации локальной сети, в том числе места подключения и целевого объекта для VPN-шлюза. Эта конфигурация включает общедоступный IPv4-адрес локального VPN-устройства и маршрутизацию для локальных сетей. Эта информация используется VPN-шлюзом для маршрутизации пакетов, предназначенных для локальных сетей, через IPSec-туннель.

- **Шлюз виртуальной сети**. Создайте шлюз виртуальной сети для маршрутизации трафика между виртуальной сетью и локальным центром обработки данных или другими виртуальными сетями. Шлюзом виртуальной сети может быть VPN-шлюз или шлюз ExpressRoute, но в этом модуле мы рассматриваем только VPN-шлюзы виртуальной сети. (Служба ExpressRoute будет рассмотрена подробнее в отдельном уроке далее в этом модуле.)

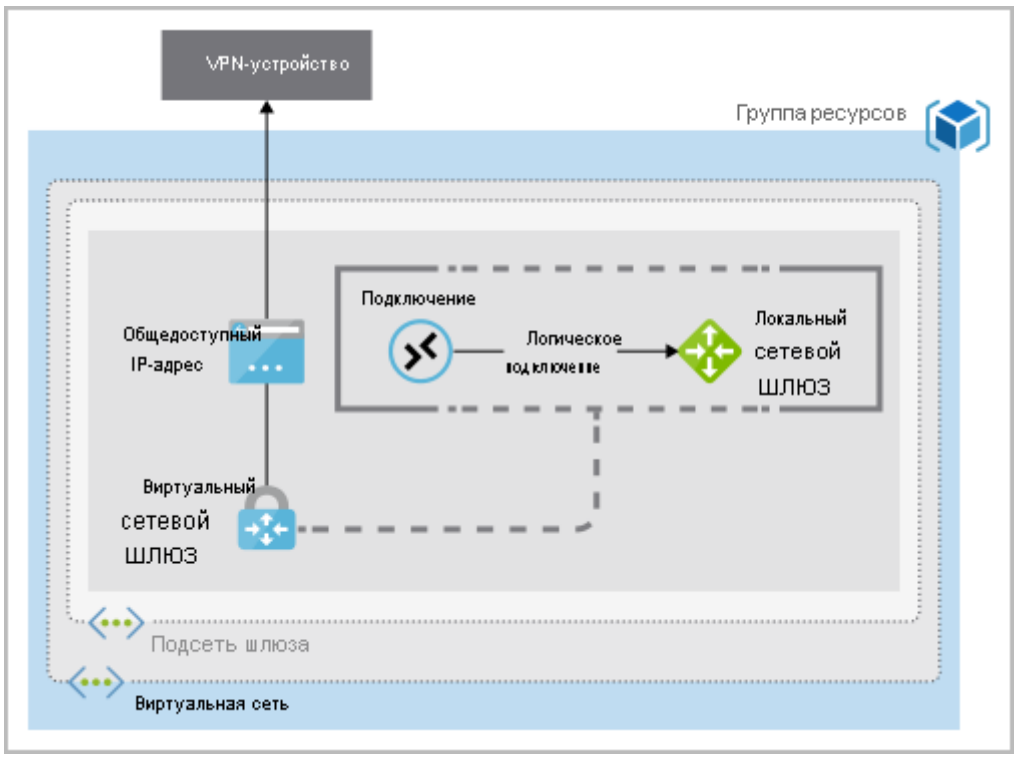
- **Подключение**. Создайте ресурс подключения для логического соединения между VPN-шлюзом и шлюзом локальной сети.

    - Соединение создается с IPv4-адресом локального VPN-устройства, определенным на локальном сетевом шлюзе.

    - Подключение создается от шлюза виртуальной сети и связанного с ним общедоступного IP-адреса.

Можно создать несколько подключений.

Приведенная ниже схема демонстрирует такое сочетание ресурсов и их отношений, чтобы вам было проще понять, что необходимо для развертывания VPN-шлюза.



Требования к локальным ресурсам

Для подключения центра обработки данных к VPN-шлюзу вам потребуются следующие локальные ресурсы.

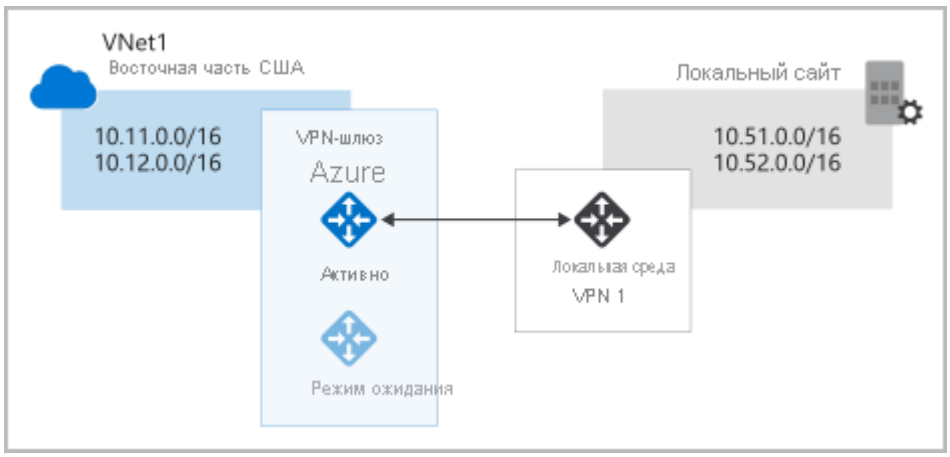
- VPN-устройство, которое поддерживает VPN-шлюзы на основе политик или на основе маршрутов.
- Общедоступный (интернет-маршрутизируемый) IPv4-адрес.

Сценарии с высоким уровнем доступности

Существует несколько вариантов, чтобы убедиться, что у вас отказоустойчивая конфигурация.

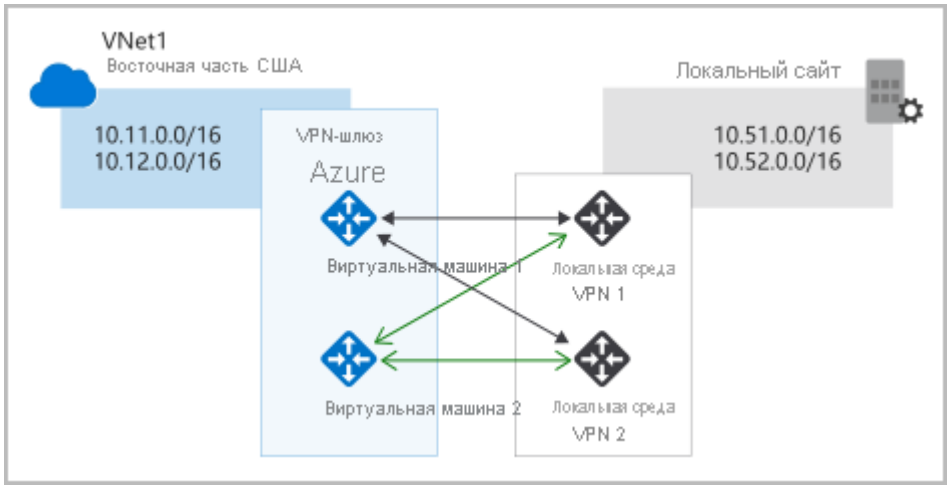
Активный — резервный

По умолчанию VPN-шлюзы развертываются в конфигурации из двух экземпляров (активного и резервного), даже если в Azure доступен только один ресурс VPN-шлюза. При плановом обслуживании или незапланированном простое, влияющем на активный экземпляр, ожидающий экземпляр автоматически принимает ответственность за соединения (вмешательство пользователя не требуется). Во время такой отработки отказа подключения прерываются, но обычно восстанавливаются через несколько секунд в ходе планового обслуживания и в течение 90 секунд в случае непредвиденных повреждений.



Активный — активный

С появлением поддержки протокола маршрутизации BGP можно развертывать VPN-шлюзы в конфигурации активный —активный. В этой конфигурации можно назначить уникальный общедоступный IP-адрес для каждого экземпляра. После этого можно создать отдельные туннели с локального устройства до каждого IP-адреса. Обеспечить высокую доступность можно путем развертывания дополнительного локального VPN-устройства.



Отработка отказа для ExpressRoute

Другой вариант для высокого уровня доступности — настройка VPN-шлюза как защищенного пути отработки отказа для подключений ExpressRoute. В каналы ExpressRoute встроен механизм обеспечения устойчивости. Но они не защищены от физических проблем с кабелями или сбоев, влияющих на все расположение ExpressRoute. В сценариях с высоким уровнем доступности, в которых есть риск отказа канала ExpressRoute, можно подготовить VPN-шлюз через Интернет в качестве альтернативного способа подключения. Так вы сможете гарантировать постоянное соединение с виртуальными сетями.

Шлюзы, избыточные между зонами

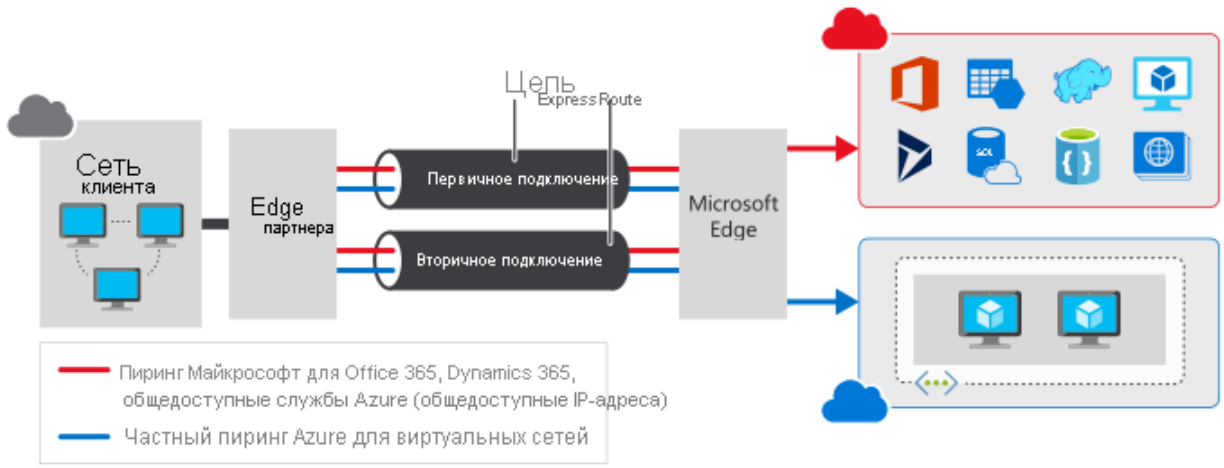
В регионах, поддерживающих зоны доступности, шлюзы VPN и шлюзы ExpressRoute можно развертывать в конфигурации с избыточностью между зонами. Такая конфигурация обеспечивает шлюзам виртуальной сети более высокие уровни устойчивости, масштабируемости и доступности. При развертывании в зонах доступности Azure происходит физическое и логическое разделение шлюзов в пределах региона с

одновременной защитой локального сетевого подключения к Azure от сбоев на уровне зоны. Для таких шлюзов требуются другие ценовые категории и используются общедоступные IP-адреса категории "Стандартный" вместо общедоступных IP-адресов категории "Базовый".

3.4.3. Основные сведения об Azure ExpressRoute

ExpressRoute позволяет переносить локальные сети в Microsoft Cloud по частному подключению, обеспечиваемому поставщиком услуг подключения. ExpressRoute позволяет устанавливать подключения к облачным службам Майкрософт, таким как Microsoft Azure и Microsoft 365.

Это может быть подключение типа "любой к любому" (IP VPN), подключение Ethernet типа "точка-точка" или виртуальное кросс-подключение через поставщика услуг подключения на совместно используемом сервере. Подключения ExpressRoute не проходят через общедоступный Интернет. Это обеспечивает повышенный уровень безопасности, надежности и быстродействия подключений ExpressRoute и сопоставимый уровень задержек по сравнению с типовыми подключениями через Интернет. Сведения о том, как подключить сеть к облаку Майкрософт с помощью ExpressRoute, см. в статье Модели подключения ExpressRoute.



Функции и преимущества ExpressRoute

Использование ExpressRoute в качестве службы подключения между Azure и локальными сетями дает сразу несколько преимуществ.

- Подключение третьего уровня между локальной сетью и облаком Майкрософт через поставщика услуг подключения. Это может быть подключение типа "любой к любому" (IP VPN), подключение Ethernet типа "точка-точка" или виртуальное кросс-подключение через Ethernet Exchange.
- Подключение к облачным службам Майкрософт во всех регионах геополитической области.
- Глобальное подключение к службам Майкрософт во всех регионах с помощью надстройки ExpressRoute Premium.

- Динамическая маршрутизация между вашей сетью и средой Майкрософт по протоколу BGP.
- Встроенная избыточность в каждом расположении пиринга для более высокой надежности.
- Соглашения об уровне обслуживания, обеспечивающие бесперебойное подключение.
- Поддержка QoS для Skype для бизнеса.

Подключение уровня 3

ExpressRoute обеспечивает подключение уровня 3 (на уровне адресов) между локальной сетью и облаком Майкрософт через партнеров по подключению. Эти подключения могут работать в сети в режиме "точка — точка" или "любой к любому". Также они могут выполнять роль виртуального перекрестного подключения через точку обмена трафиком.

Встроенная избыточность

Каждый поставщик услуг подключения использует избыточные устройства для обеспечения высокого уровня доступности подключений, установленных с Майкрософт. Вы можете настроить несколько цепей, чтобы дополнить эту функцию. Все избыточные подключения настраиваются на уровне 3, чтобы обеспечить соблюдение соглашений об уровне обслуживания.

Подключение к облачным службам Майкрософт

ExpressRoute обеспечивает прямой доступ к следующим службам во всех регионах:

- Microsoft Office 365
- Microsoft Dynamics 365
- Службы вычислений Azure, такие как виртуальные машины Azure
- Облачные службы Azure, такие как Azure Cosmos DB и служба хранилища Azure

Office 365 обеспечивает безопасный и надежный доступ через Интернет. Поэтому мы рекомендуем использовать ExpressRoute для конкретных сценариев. В разделе "Дополнительные сведения" в конце этого модуля содержится ссылка на статью об использовании ExpressRoute для доступа к Office 365.

Локальные подключения с помощью ExpressRoute Global Reach

Вы можете включить службу ExpressRoute Global Reach для обмена данными между локальными сайтами, подключившись к своим цепям ExpressRoute. Например, предположим, что у вас есть частный центр обработки данных в Калифорнии, подключенный к ExpressRoute в Кремниевой долине. У вас есть другой частный центр обработки данных в Техасе, подключенный к ExpressRoute в Далласе. С помощью ExpressRoute Global Reach можно подключать частные центры обработки данных через две цепи ExpressRoute. Трафик между центрами будет проходить через сеть Майкрософт.

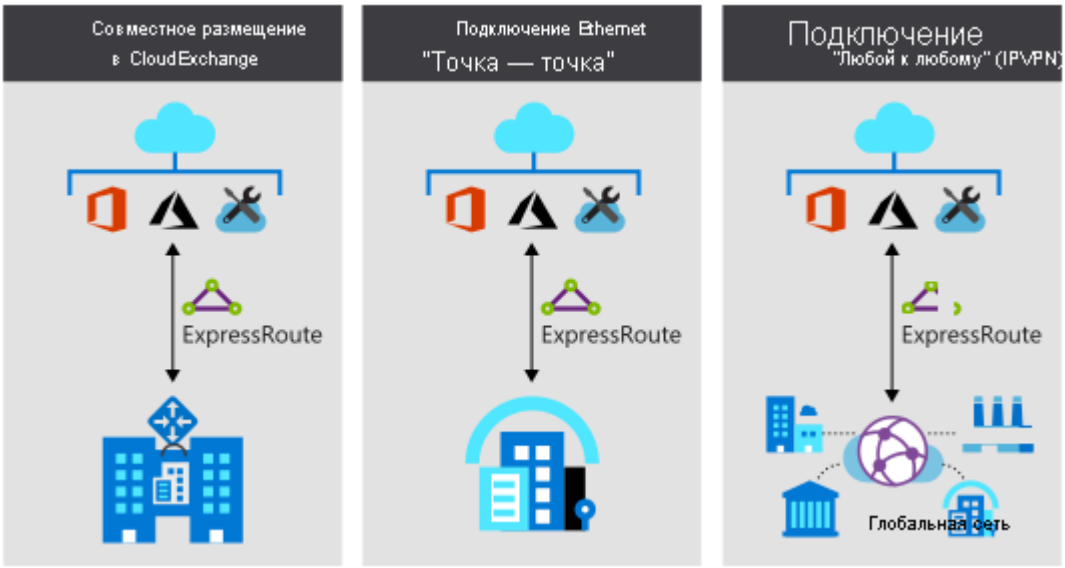
Динамическая маршрутизация

ExpressRoute использует протокол маршрутизации BGP. BGP используется для обмена маршрутами между локальными сетями и ресурсами, работающими в Azure. Этот протокол обеспечивает динамическую маршрутизацию между локальной сетью и службами, запущенными в облаке Майкрософт.

Модели подключения ExpressRoute

ExpressRoute поддерживает три модели, которые можно использовать для подключения между локальной сетью и облаком Майкрософт:

- совместное размещение в Cloud Exchange;
- Подключение Ethernet "точка-точка"
- Подключение типа "любой к любому"



Совместное размещение в Cloud Exchange

Поставщики услуг совместного размещения обычно предлагают подключения уровней 2 и 3 между вашей инфраструктурой, которая может располагаться на сервере совместного размещения, и облаком Майкрософт. Например, если ваш центр обработки данных размещен в точке обмена облачным трафиком, например в объекте поставщика услуг Интернета, вы можете отправить запрос на перекрестное подключение к облаку Майкрософт.

Подключение Ethernet "точка-точка"

Подключения типа "точка — точка" обеспечивают взаимодействие на уровнях 2 и 3 между локальным сайтом и сетью Azure. Вы можете подключить свои офисы или центры обработки данных к Azure с помощью каналов связи типа "точка-точка". Например, если у вас есть локальный центр обработки данных, для подключения к Майкрософт можно использовать канал связи типа "точка-точка".

Сети типа "любой к любому"

Подключение типа "любой к любому" позволяет интегрировать глобальную сеть (WAN) с Azure, обеспечивая подключение к корпоративным офисам и центрам обработки

данных. Azure интегрируется с подключением к глобальной сети и обеспечивает такое же взаимодействие, как между центром обработки данных и одним из филиалов.

При использовании подключений типа "любой к любому" все поставщики глобальной сети предлагают подключение на уровне 3. Например, если вы уже используете MPLS для подключения к филиалам или другим объектам организации, подключение ExpressRoute к Майкрософт будет работать так же, как и для другого расположения в вашей частной глобальной сети.

Вопросы безопасности

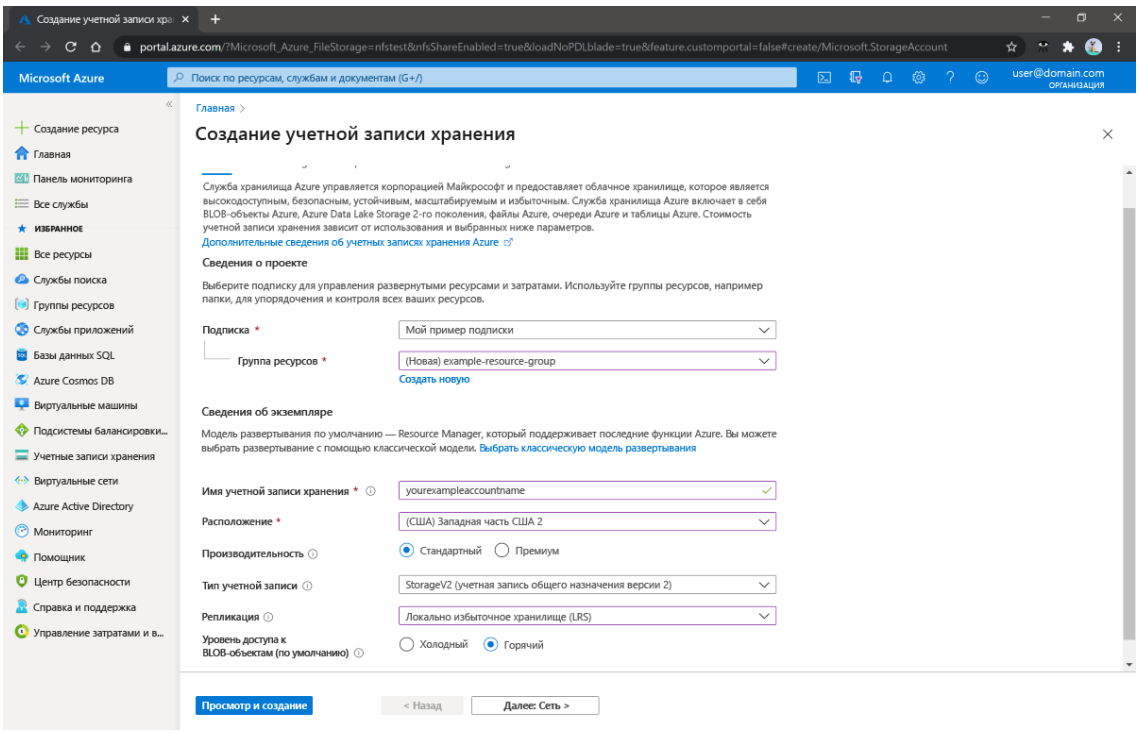
При использовании ExpressRoute ваши данные не передаются через общедоступный Интернет, поэтому они не подвержены потенциальным рискам, связанным с взаимодействием через Интернет. ExpressRoute — это частное подключение из локальной инфраструктуры к инфраструктуре Azure. Даже если у вас есть подключение ExpressRoute, запросы DNS, данные проверки списка отзыва сертификатов и запросы сети доставки содержимого Azure по-прежнему передаются через общедоступный Интернет.

3.5. Изучение служб хранилища Azure

3.5.1. Основные принципы учетной записи службы хранилища Azure

службу хранилища Azure, которую можно использовать для хранения файлов, сообщений, таблиц и других типов информации. Такие клиенты, как веб-сайты, мобильные приложения, классические приложения и многие другие типы пользовательских решений, могут считывать данные из службы хранилища Azure и записывать их в нее. Службу хранилища Azure также используют виртуальные машины IaaS (инфраструктура как услуга) и облачные службы PaaS (платформа как услуга).

Для использования службы хранилища Azure прежде всего нужно создать учетную запись службы хранилища Azure для хранения объектов данных. Учетную запись службы хранилища Azure можно создать с помощью портала Azure, PowerShell или интерфейса командной строки Azure.



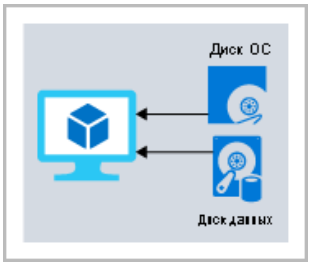
Учетная запись хранения предоставляет для данных службы хранилища Azure уникальное пространство имен, доступное из любой точки мира по протоколам HTTP или HTTPS. Данные в этой учетной записи хранения защищены, высокодоступны, надежны и масштабируемы.

3.5.2. Основные принципы хранилища дисков

Хранилище дисков предоставляет диски для виртуальных машин Azure. Приложения и другие службы могут по мере необходимости получать доступ к таким дискам и использовать их, как и в локальных сценариях. Хранилище дисков обеспечивает постоянное хранение данных на подключенном виртуальном жестком диске и доступ к ним.

Диски могут быть разных размеров и уровней производительности, начиная с твердотельных накопителей (SSD) и заканчивая традиционными вращающимися жесткими дисками (HDD) с разными показателями производительности. Вы можете использовать диски SSD и HDD цен. категории "Стандартный" для менее важных рабочих нагрузок, диски SSD цен. категории "Премиум" для критически важных рабочих приложений, а диски цен. категории "Ультра" для ресурсоемких рабочих нагрузок, таких как SAP HANA, базы данных верхнего уровня и рабочие нагрузки с большим объемом транзакций. Azure гарантирует согласованную надежность корпоративного уровня для дисков IaaS (инфраструктура как услуга) с ведущим в отрасли нулевым показателем сбоев в течение одного года.

На приведенном ниже рисунке показана виртуальная машина Azure, которая использует отдельные диски для хранения разных данных.



3.5.3. Основные принципы хранилища BLOB-объектов Azure

Хранилище BLOB-объектов Azure — это решение для хранения объектов в облаке. В нем можно хранить большие объемы данных, например текстовые или двоичные данные. Хранилище BLOB-объектов Azure является неструктурированным. Это означает, что оно может содержать любые виды данных. Хранилище BLOB-объектов может управлять тысячами параллельных загрузок, большими объемами видеоданных, постоянно растущими файлами журналов, кроме того, оно доступно повсеместно при условии наличия подключения к Интернету.

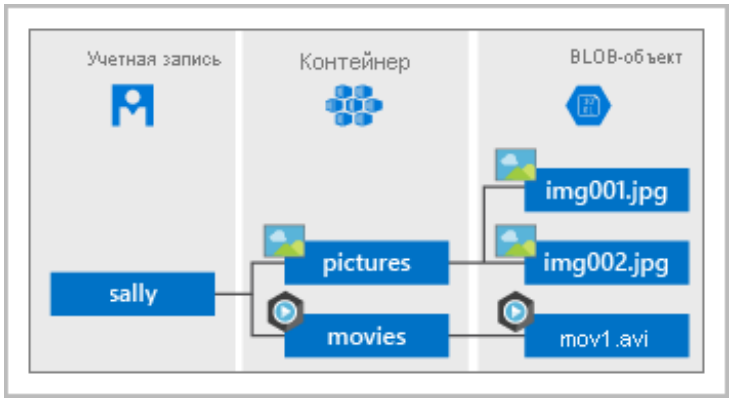
BLOB-объекты не ограничиваются распространенными форматами файлов. BLOB-объект может содержать гигабайты двоичных данных, передаваемых в потоковом режиме с прибора для научных исследований, зашифрованное сообщение для другого приложения или данные в пользовательском формате для разрабатываемого приложения. Одним из преимуществ хранилища BLOB-объектов по сравнению с дисковым является то, что разработчикам не требуется учитывать и контролировать диски. Данные загружаются в виде больших двоичных объектов, а за физическое хранилище отвечает Azure.

Хранилище BLOB-объектов идеально подходит для следующих целей:

- Обслуживание изображений или документов непосредственно в браузере.
- Хранение файлов для распределенного доступа.
- Потоковая передача видео и звука.
- Хранение резервных копий и восстановление данных, аварийное восстановление и архивация.
- Хранение данных для анализа локальной службой или службой, размещенной в Azure.
- Хранение до 8 ТБ данных для виртуальных машин.

Большие двоичные объекты хранятся в контейнерах, которые помогают упорядочить большие двоичные объекты так, как вам удобно для работы.

На приведенной ниже схеме показан пример использования учетных записей, контейнеров и больших двоичных объектов Azure.



3.5.4. Основы работы с файлами Azure

Служба Файлов Azure предоставляет полностью управляемые общие папки в облаке, доступ к которым можно получить с помощью стандартных отраслевых протоколов SMB и NFS (в предварительной версии). Общие ресурсы службы файлов Azure можно одновременно подключить к облачным или локальным развертываниям Windows, Linux и macOS. Приложения, работающие на виртуальных машинах Azure или в облачных службах, могут подключать ресурсы хранилищ файлов для доступа к данным файлов, так же как это бы делало настольное приложение при подключении обычного ресурса SMB. Любое количество виртуальных машин Azure может одновременно подключаться и получать доступ к ресурсам хранилища файлов. Типичные сценарии использования включают совместное использование файлов в любой точке мира, а также общий доступ к диагностическим данным или данным приложений.

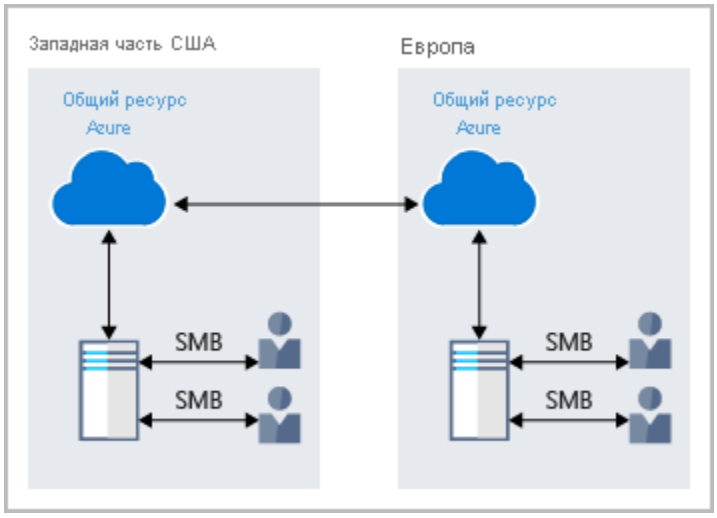
Используйте Файлы Azure в следующих ситуациях:

- Многие локальные приложения используют общие папки. Служба Файлов Azure упрощает перенос таких приложений, которые отправляют данные в Azure. Если вы подключите общую папку Azure к той же букве диска, которую использует локальное приложение, то весь механизм приложения, работающий с этой общей папкой, сможет работать с минимальными изменениями или без них.

- Файлы конфигурации хранятся в общей папке, а доступ к ним осуществляют несколько виртуальных машин. В этой папке также можно хранить средства и служебные программы, используемые несколькими разработчиками в группе. Это гарантирует, что любой пользователь может их найти, и что все они используют одинаковую версию.

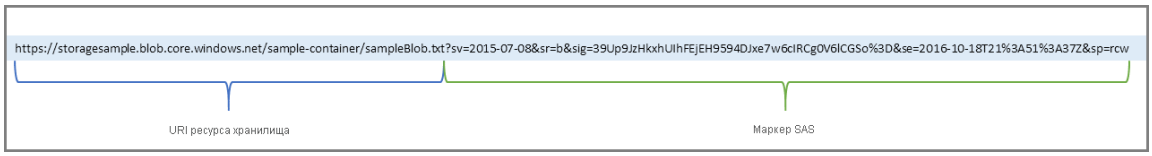
- Данные сохраняются в общей папке для последующей обработки или анализа. Например, это удобно для журналов диагностики, метрик и аварийных дампов.

Ниже показаны файлы Azure, которые используются для обмена данными между двумя географическими расположениями. Файлы Azure обеспечивают шифрование данных при хранении, а протокол SMB обеспечивает шифрование данных при передаче.



Одно из различий между Файлами Azure и файлами в корпоративной общей папке заключается в том, что вы можете получить доступ к файлам в Файлах Azure из любой точки мира, используя URL-адрес, указывающий на файл. Вы также можете использовать токены подписанного URL-адреса (SAS), чтобы разрешать доступ к частному ресурсу в течение определенного времени.

Ниже приведен пример URI SAS службы, в котором показаны URI ресурса и токен SAS.



3.5.5. Основные сведения об уровнях доступа к BLOB-объектам

Объем данных, хранящихся в облаке, может расти экспоненциально. Управления затратами при увеличении хранилища помогает организовать размещение данных по уровням в зависимости от таких атрибутов, как частота доступа и планируемый срок хранения. Данные, хранящиеся в облаке, могут быть разными в зависимости от способа их создания, обработки и доступа к ним в течение всего времени их существования. Одни данные активно используют и изменяют на протяжении всего жизненного цикла. Другие данные часто используются в начале цикла, но по мере их устаревания к ним обращаются все реже. Некоторые данные остаются неактивными в облаке, и к ним обращаются редко или не обращаются вообще. Чтобы удовлетворить эти разные потребности в доступе, Azure предоставляет несколько *уровней доступа*, которые можно использовать для поиска оптимального сочетания затрат на хранение и требований к доступу.

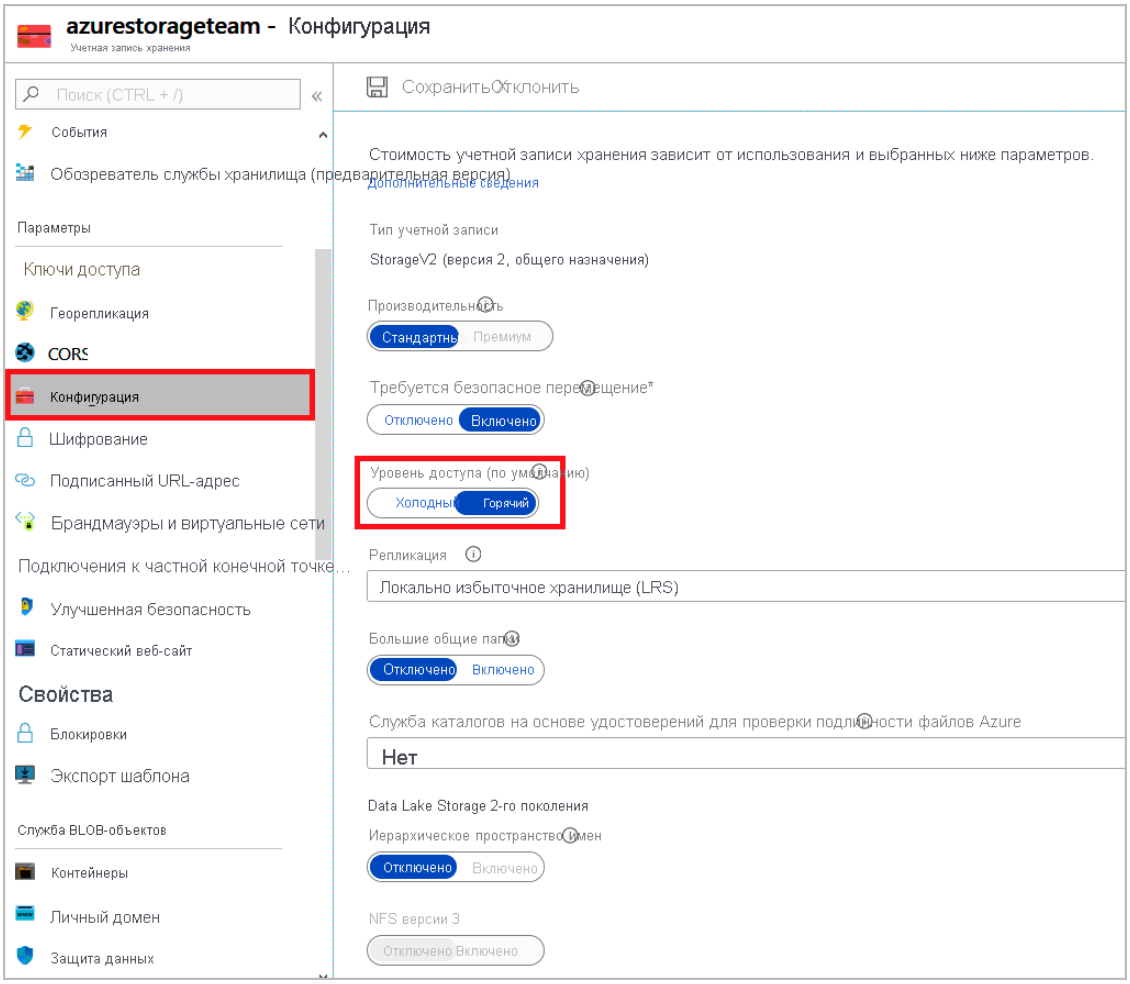
Служба хранилища Azure предлагает разные уровни доступа для хранилищ больших двоичных объектов, которые обеспечивают наиболее экономичное хранение объектов данных. Ниже перечислены возможные уровни доступа.

- **Горячий уровень хранилища**: Оптимизирован для хранения данных, к которым обращаются часто (например, изображения для веб-сайта).
- **Холодный уровень хранилища**: Оптимизирован для данных, которые используются редко и хранятся не менее 30 дней (например, счета для клиентов).
- **Архивный уровень хранилища**: Предназначен для данных, которые используются редко и хранятся не менее 180 дней с нестрогими требованиями к задержке (например, резервные копии для долгосрочного хранения).

Следующие факторы связаны с разными уровнями доступа.

- На уровне учетной записи можно задать только холодный и горячий уровни доступа. Архивный уровень доступа на уровне учетной записи недоступен.
- Горячий, холодный и архивный уровни доступа можно устанавливать на уровне большого двоичного объекта во время или после отправки данных.
- Для данных на холодном уровне допускается несколько меньший уровень доступности, но требуются те же показатели надежности, задержек при извлечении и пропускной способности, что и для данных на горячем уровне. Для холодных данных соглашение об уровне обслуживания (SLA) с несколько более низкой доступностью и более высокая стоимость доступа по сравнению с горячими данными являются приемлемым компромиссом с учетом более низких затрат на хранение.
- В архивных хранилищах данные хранятся без подключения к сети. Это обеспечивает наименьшую стоимость хранения, но зато влечет наибольшие затраты на восстановление данных и доступ к ним.

Приведенный ниже рисунок иллюстрирует выбор между горячим и холодным уровнями доступа для учетной записи хранения общего назначения.



3.6. Базы данных SQL Azure

База данных SQL Azure — это реляционная база данных на основе последней стабильной версии ядра СУБД Microsoft SQL Server. База данных SQL — это высокопроизводительная, надежная, полностью управляемая и безопасная база данных. С ее помощью можно создавать приложения и веб-сайты на основе данных, используя любой язык программирования, без необходимости управлять инфраструктурой.

Компоненты

Базы данных SQL Azure — это ядро СУБД по модели "платформа как услуга" (PaaS). Оно отвечает за работу большей части функций управления базами данных, таких как обновление, исправление, резервное копирование и мониторинг, без участия пользователя. База данных SQL обеспечивает доступность на уровне 99,99 %. Возможности PaaS, встроенные в Базу данных SQL, позволяют сосредоточиться на важных для бизнеса задачах

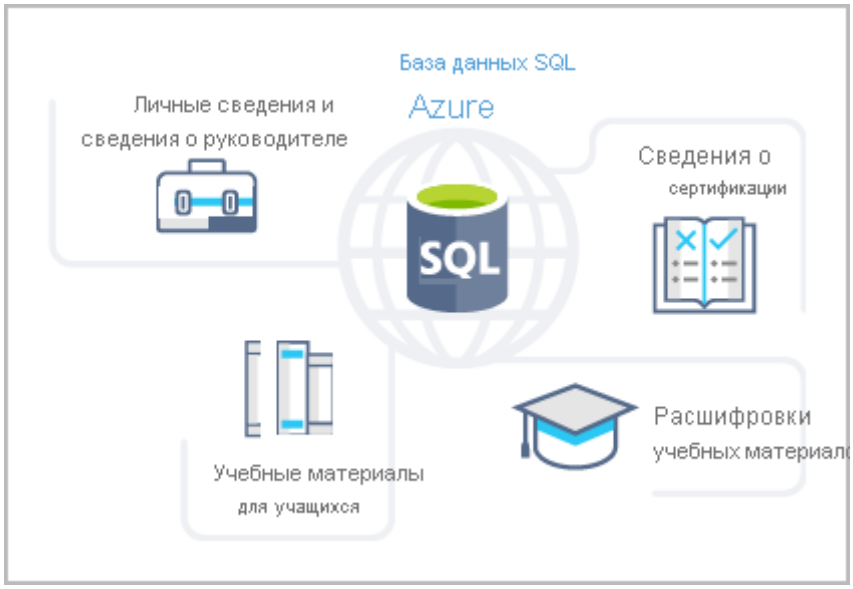
администрирования и оптимизации баз данных для конкретных областей. База данных SQL — это полностью управляемая служба со встроенными возможностями высокого уровня доступности, резервного копирования и других общих операций обслуживания. Корпорация Майкрософт обрабатывает все обновления кода SQL и операционной системы, так что вам не придется управлять базовой инфраструктурой самостоятельно.

Вы можете организовать высокодоступный и высокопроизводительный уровень хранения данных для приложений и решений в Azure. База данных SQL отлично подходит для различных современных облачных приложений, поскольку позволяет обрабатывать как реляционные данные, так и нереляционные структуры, такие как графы, JSON, пространственные объекты и XML.

Вы можете использовать расширенные функции обработки запросов, например технологии высокопроизводительных вычислений в памяти и интеллектуальную обработку запросов. На самом деле, новые возможности SQL Server выпускаются сначала для базы данных SQL и только потом для SQL Server. Вы получаете новейшие возможности SQL Server без дополнительных издержек на обновление или модернизацию, после тестирования на миллионах баз данных.

Миграция

На следующем рисунке показаны типы данных, которые ваша компания может хранить на веб-сайте образовательного портала в Базе данных SQL Azure.



3.7. Защита от угроз безопасности с помощью Центра безопасности Azure

Что такое Центр безопасности Azure?

Центр безопасности Azure — это служба мониторинга, позволяющая наблюдать за состоянием безопасности во всех ваших службах, как в Azure, так и в локальной среде. Термин *"состояние безопасности"* относится к элементам управления и политикам кибербезопасности, а также к тому, насколько хорошо вы можете прогнозировать угрозы безопасности, предотвращать их и реагировать на них.

Возможности центра безопасности:

- Мониторинг параметров безопасности для локальных и облачных рабочих нагрузок.
- Автоматическое применение необходимых настроек безопасности к новым ресурсам по мере их появления в сети.
- Предоставление рекомендаций по обеспечению безопасности на основе текущих конфигураций, ресурсов и сетей.
- Непрерывное отслеживание ваших ресурсов и выполнение автоматических оценок безопасности для определения потенциальных уязвимостей до того, как ими смогут воспользоваться злоумышленники.
- Использование машинного обучения для обнаружения и блокировки установки вредоносных программ на виртуальных машинах и других ресурсах. Можно с помощью *адаптивных элементов управления приложениями* определять правила, в которых перечислены разрешенные приложения, чтобы могли запускаться только приложения, которые вы разрешили.
- Обнаружение и анализ потенциальных входящих атак, а также исследование угроз и любых действий после нарушений, которые могут произойти.
- Обеспечение оперативного управления доступом к сетевым портам. Таким образом, сеть будет разрешать только необходимый трафик и тогда, когда он необходим, что позволяет сократить количество направлений атак.

3.8. Хранение секретов и управление ими в Azure Key Vault

Azure Key Vault — это облачная служба для хранения секретов приложений в одном центральном месте. Она обеспечивает безопасный доступ к конфиденциальной информации, предоставляя возможности управления доступом и ведения журнала.

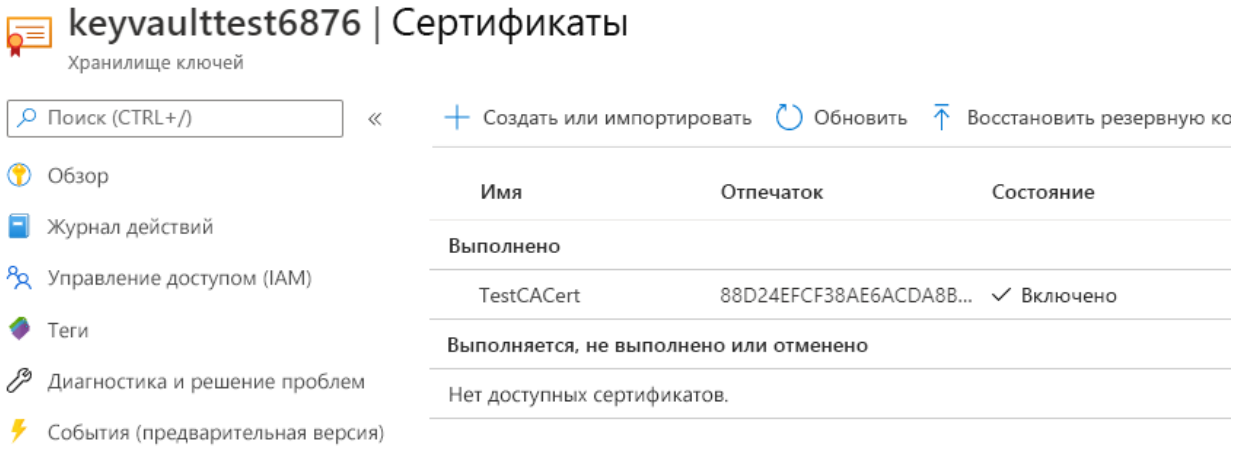
Возможности Azure Key Vault

Azure Key Vault предоставляет следующие возможности.

- **Управление секретами**. Azure Key Vault можно использовать для безопасного хранения токенов, паролей, сертификатов, ключей API и других секретов со строгим контролем доступа к ним.
- **Управление ключами шифрования**. Azure Key Vault можно использовать как решение для управления ключами. Эта служба позволяет легко создавать и контролировать ключи шифрования, используемые для шифрования данных.
- **Управление сертификатами SSL/TLS**. С помощью службы Azure Key Vault можно подготавливать, администрировать и развертывать общедоступные и закрытые сертификаты SSL и TLS для ресурсов Azure и внутренних ресурсов.

- **Хранение секретов с помощью аппаратных модулей безопасности (HSM)**. Хранение секретов, защищенных аппаратными модулями безопасности. Секреты и ключи могут быть защищены с помощью программного обеспечения или FIPS 140-2 уровня 2 с проверкой HSM.

В следующем примере показан сертификат, используемый для тестирования в Azure Key Vault.



Вы будете добавлять секрет в Azure Key Vault позднее в этом модуле.

Каковы преимущества Azure Key Vault?

Ниже перечислены основные преимущества использования Key Vault:

- **Централизация секретов приложений**. Централизованное хранение секретов приложений позволяет управлять их распространением и снижает вероятность случайной утечки.

- **Безопасное хранение секретов и ключей**. Azure использует стандартные отраслевые алгоритмы, длины ключей и модули HSM. Для доступа к Azure Key Vault требуется соответствующая проверка подлинности и авторизация.

- **Мониторинг доступа и управление доступом**. С помощью Azure Key Vault вы можете отслеживать доступ к секретам приложений и управлять им.

- **Упрощенное администрирование секретов приложений**. Key Vault упрощает регистрацию и обновление сертификатов из общедоступных центров сертификации (ЦС). Вы также можете масштабировать и реплицировать содержимое в пределах регионов и использовать стандартные инструменты управления сертификатами.

- **Интеграция с другими службами Azure**. Key Vault можно интегрировать с учетными записями хранения, реестрами контейнеров, концентраторами событий и многими другими службами Azure. Затем эти службы могут безопасно ссылаться на секреты, хранящиеся в Azure Key Vault.

-

3.9.Глубинная защита

Целью *глубинной защиты* является обеспечение безопасности информации и предотвращение кражи данных лицами, у которых нет разрешения на доступ к ним.

Стратегия глубинной защиты использует ряд механизмов для замедления атаки, направленной на получение несанкционированного доступа к данным.

Уровни глубинной защиты

Глубинную защиту можно представить в виде нескольких концентрических уровней, в центре которых находятся защищаемые данные.

Каждый уровень обеспечивает защиту, поэтому если злоумышленник преодолеет один уровень, следующий уровень помешает дальнейшему проникновению. Благодаря такому подходу вы избавляетесь от необходимости рассчитывать только на какой-либо один уровень защиты. Он замедляет атаку и обеспечивает телеметрию предупреждений, на основе которой группы обеспечения безопасности могут действовать, автоматически или вручную.

Ниже приводится краткий обзор роли каждого уровня.

- Уровень *физической безопасности* — это первая линия защиты компьютерного оборудования в центре обработки данных.
- Уровень *идентификации и доступа* контролирует доступ к инфраструктуре и управление изменениями.
- На уровне *периметра* используется защита от распределенных атак типа "отказ в обслуживании" (DDoS) для фильтрации крупномасштабных атак, прежде чем они приведут к отказу в обслуживании для пользователей.
- Уровень *сети* ограничивает взаимодействие между ресурсами посредством сегментации и управления доступом.
- Уровень *вычислений* защищает доступ к виртуальным машинам.
- Уровень *приложений* обеспечивает безопасность приложений и отсутствие уязвимостей.
- Уровень *данных* контролирует доступ к бизнес-данным и данным клиентов, которые вам необходимо защитить.

Эти уровни служат руководством, помогающим принимать решения о конфигурации системы безопасности на всех уровнях ваших приложений.

Azure предоставляет инструменты и функции безопасности на всех уровнях концепции глубинной защиты. Давайте подробнее рассмотрим каждый уровень.

Физическая безопасность

Физическая защита доступа к зданиям и контроль доступа к вычислительному оборудованию в центре обработки данных — это первая линия обороны.

Физическая безопасность предусматривает меры по ограничению физического доступа к ресурсам. Эти меры гарантируют, что злоумышленники не преодолеют остальные уровни, и защищают данные от потери и кражи. Майкрософт использует различные механизмы физической безопасности в своих облачных центрах обработки данных.

Удостоверение и доступ

На этом уровне:

- Управляйте доступом к инфраструктуре и изменениями.
- Используйте единый вход и многофакторную проверку подлинности.
- Проверяйте события и изменения.

Уровень идентификации и доступа обеспечивает безопасность удостоверений, предоставление доступа только лицам, которым он необходим, а также регистрацию событий входа и изменений.

Периметр

На этом уровне:

- Используйте защиту от атак DDoS для фильтрации крупномасштабных атак, прежде чем они повлияют на доступность системы для пользователей.

- Используйте брандмауэры по периметру, чтобы обнаруживать атаки на сеть и получать о них оповещения.

По периметру сети необходима защита от сетевых атак на ресурсы. Выявление атак, устранение их последствий и оповещение об атаках — это важные элементы обеспечения безопасности вашей сети.

Network

На этом уровне:

- Ограничьте обмен данными между ресурсами.
- Настройте запрет по умолчанию.
- Ограничьте входящий и исходящий интернет-трафик, где это имеет смысл.
- Реализуйте безопасное подключение к локальным сетям.

На этом уровне основное внимание уделяется ограничению сетевых подключений во всех ваших ресурсах, чтобы использовались только самые необходимые подключения. Ограничивая такие подключения, вы уменьшаете риск распространения атак на другие системы в вашей сети.

Среда выполнения приложений

На этом уровне:

- Защитите доступ к виртуальным машинам.
- Реализуйте защиту конечных точек на устройствах и своевременно устанавливайте все исправления.

Вредоносные программы, отсутствие исправлений и ненадлежащая защита систем делают вашу среду уязвимой для атак. Этот уровень нацелен на обеспечение безопасности ваших вычислительных ресурсов и реализацию соответствующих элементов управления для максимального сокращения проблем безопасности.

Приложение

На этом уровне:

- Убедитесь, что приложения защищены и не содержат уязвимостей.
- Храните конфиденциальные секреты приложений на защищенном носителе.
- Сделайте безопасность требованием к разработке всех приложений.

Интеграция безопасности в жизненный цикл разработки приложений позволяет сократить количество уязвимостей в коде. Каждая команда разработчиков должна обеспечивать безопасность своих приложений по умолчанию.

Данные

Практически всегда злоумышленники охотятся за данными:

- которые хранятся в базе данных;
- которые хранятся на диске на виртуальных машинах;
- которые хранятся в приложениях, предоставляемых в рамках предложения "Программное обеспечение как услуга" (SaaS), таких как Office 365;
- которые управляются через облачное хранилище.

Лица, ответственные за хранение данных и управление доступом к данным, обязаны обеспечить надлежащую защиту. Часто нормативные требования предписывают определенные меры контроля и процедуры для обеспечения конфиденциальности, целостности и доступности данных.

Состояние безопасности;

Ваше *состояние безопасности* — это способность вашей организации защищаться от угроз безопасности и реагировать на них. Общие принципы, которые используются для определения состояния безопасности, — *конфиденциальность*, *целостность* и *доступность*, известные под общим названием CIA (confidentiality, integrity, availability).

- **Конфиденциальность**

Принцип минимальных привилегий означает, что доступ к информации разрешается только лицам, которым он предоставлен явно, и только на том уровне, который им необходим для выполнения своей работы. Это включает защиту паролей пользователей, содержимого электронной почты и уровни доступа к приложениям и базовой инфраструктуре.

- **Целостность**

Предотвращение несанкционированного изменения информации:

  - Неактивной информации (когда она хранится).
  - Передаваемой информации (когда она передается из одного места в другое, в том числе с локального компьютера в облако).

Общий подход, используемый при передаче данных, заключается в том, что для отправителя создается уникальный отпечаток данных с использованием одностороннего хэш-алгоритма. Хэш отправляется получателю вместе с данными. Получатель повторно рассчитывает хэш данных и сравнивает его с оригиналом, чтобы данные не потерялись и не подверглись изменениям в процессе передачи.

- **Доступность**

Обеспечение функционирования служб и их доступности только авторизованным пользователям. *Атаки типа "отказ в обслуживании"* проводятся для снижения доступности системы, что оказывает воздействие на ее пользователей.

3.10.Защита виртуальных сетей с помощью Брандмауэра Azure

Брандмауэр — это устройство сетевой безопасности, которое отслеживает входящий и исходящий сетевой трафик и решает, блокировать или разрешить определенный трафик, на основе заданного набора правил безопасности. Вы можете создавать правила брандмауэра, определяющие диапазоны IP-адресов. Доступ к целевому серверу разрешается только клиентам, которым предоставлены IP-адреса из этих диапазонов. Правила брандмауэра также могут включать сведения о конкретных сетевых протоколах и портах.

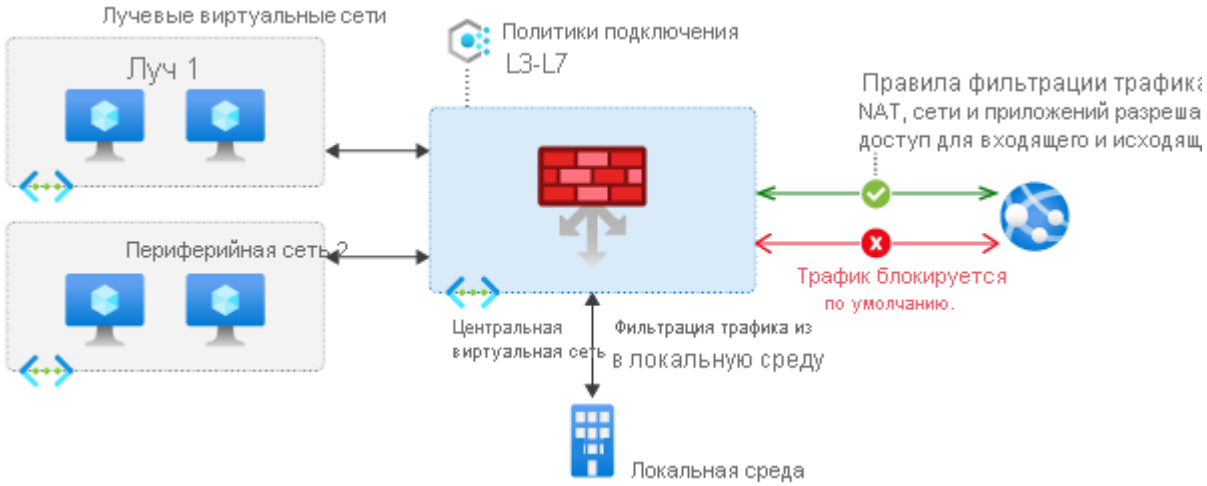
В этой части мы будем исследовать Брандмауэр Azure.

Что такое Брандмауэр Azure?

Брандмауэр Azure — это управляемая облачная служба сетевой безопасности, которая помогает защищать ресурсы в ваших виртуальных сетях Azure. Виртуальная сеть похожа на традиционную сеть, в которой вы бы работали в собственном центре обработки данных. Это ключевой компонент для построения вашей частной сети, в которой

виртуальные машины и другие вычислительные ресурсы могут безопасно взаимодействовать друг с другом, с Интернетом и локальными сетями.

Вот схема, на которой показана базовая реализация Брандмауэра Azure:



Брандмауэр Azure — это брандмауэр *с отслеживанием состояния*. Брандмауэр с отслеживанием состояния анализирует весь контекст сетевого подключения, а не только отдельный пакет сетевого трафика. Брандмауэр Azure обеспечивает высокую доступность и неограниченную облачную масштабируемость.

Брандмауэр Azure предоставляет центральное место для создания, применения и регистрации политик приложений и сетевых подключений в подписках и виртуальных сетях. Брандмауэр Azure использует статический (неизменяемый) общедоступный IP-адрес для виртуальных сетевых ресурсов, позволяя внешним брандмауэрам идентифицировать трафик из вашей виртуальной сети. Эта служба интегрирована с Azure Monitor, что обеспечивает ведение журнала и аналитику.

Брандмауэр Azure предоставляет множество функциональных возможностей, в том числе:

- высокий уровень доступности;
- неограниченную облачную масштабируемость;
- правила фильтрации входящего и исходящего трафика;
- поддержку внутреннего преобразования сетевых адресов назначения (DNAT).
- Ведение журнала Azure Monitor.

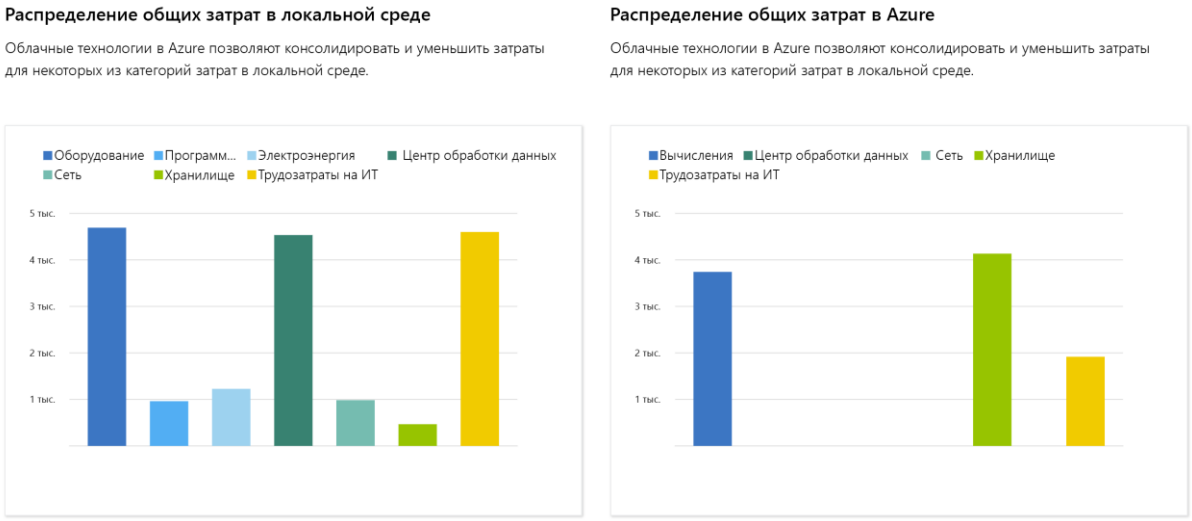
3.11.Сравнение затрат с помощью калькулятора совокупной стоимости владения

Калькулятор совокупной стоимости владения помогает рассчитать, сколько вы сэкономите в перспективе, если перенесете решение в Azure, а не продолжите использовать свой центр обработки данных.

Термин *совокупная стоимость владения* обычно используется в финансах. Иногда сложно увидеть все скрытые затраты, связанные с использованием технологии в локальной среде. Лицензии на программное обеспечение и оборудование — это дополнительные затраты.

В калькулятор совокупной стоимости владения вы вводите сведения о локальных рабочих нагрузках. Затем вы просматриваете предполагаемый размер связанных операционных расходов для отрасли (это значение можно изменить). Эти затраты включают электричество, обслуживание сети и трудовые затраты на ИТ. В результаты вы получаете параллельный отчет. С помощью отчета можно сравнить эти затраты с теми же рабочими нагрузками, которые выполняются в Azure.

На приведенном ниже рисунке показан пример.



Как работает калькулятор совокупной стоимости владения?

Работа с калькулятором совокупной стоимости владения состоит из трех этапов:

- Определите рабочие нагрузки.
- Скорректируйте предположительных значений.
- Просмотрите отчет.

Рассмотрим каждый шаг поподробнее.

Шаг 1. Определите рабочие нагрузки

Сначала вы вводите в калькулятор совокупной стоимости владения характеристики локальной инфраструктуры в следующих четырех категориях:

- **Серверы**

В эту категорию входят операционные системы, методы виртуализации, количество ядер ЦП и память (ОЗУ).

- **Базы данных**

В эту категорию входят типы баз данных, оборудование сервера и служба Azure, которую вы хотите использовать, включая ожидаемое максимальное число одновременных пользователей.

- **Память**

В эту категорию входят тип и емкость хранилища, включая все резервные или архивные хранилища.

- **Сеть**

В эту категорию входит пропускная способности сети, которую вы в настоящее время используете в локальной среде.

Шаг 2. Скорректируйте предположительные показатели

Затем вы указываете, зарегистрированы ли текущие локальные лицензии в Software Assurance, что позволит вам сэкономить, поскольку эти лицензии можно повторно использовать в Azure. Вы также указываете, нужно ли вам реплицировать хранилище в другой регион Azure для дополнительной избыточности.

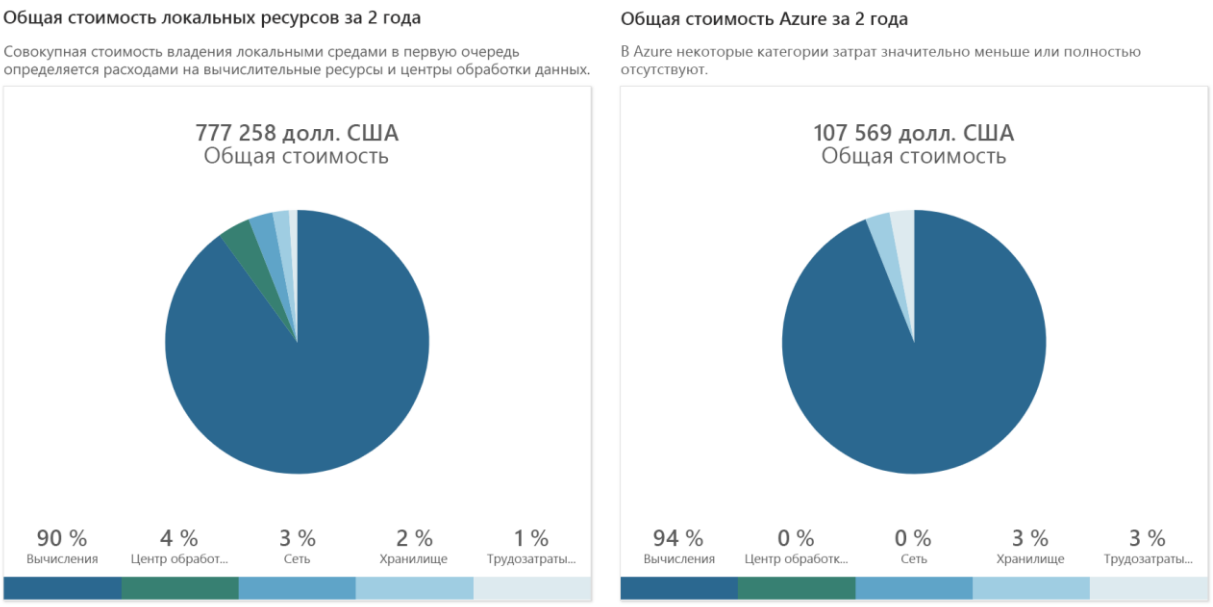
После этого вы увидите предположения о ключевых эксплуатационных затратах в нескольких разных областях — в разных отделах и организациях они могут отличаться. Эти затраты сертифицированы компанией Nucleus Research, независимой исследовательской организацией. Например, сюда входят:

- Стоимость электроэнергии за киловатт-час (кВт/ч).
- Почасовая оплата за ИТ–администрирование.
- Стоимость обслуживания сети в процентах от затрат на сетевое оборудование и программное обеспечение.

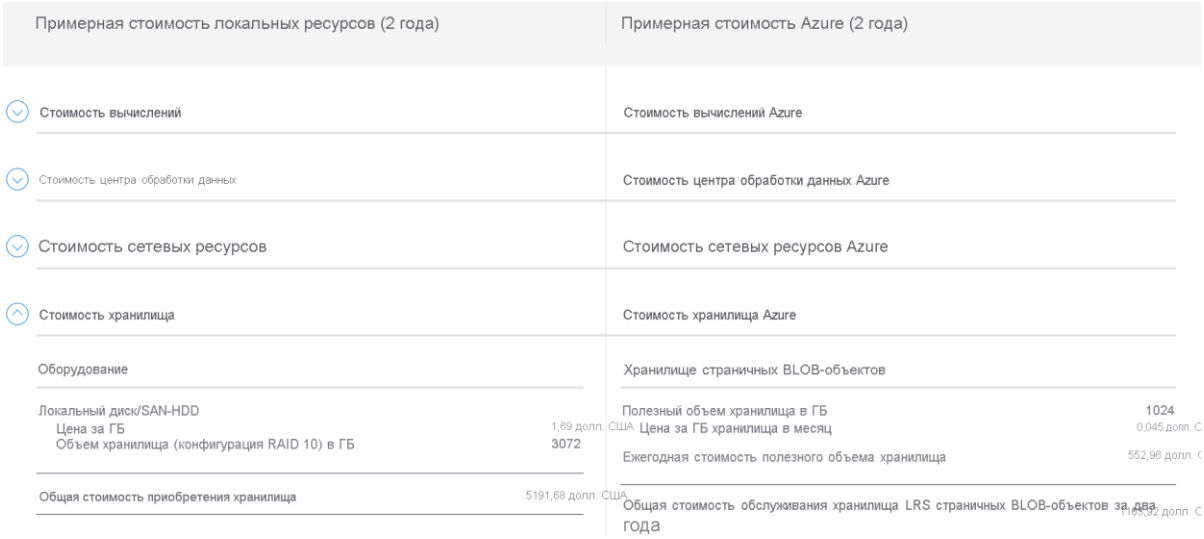
Чтобы повысить точность калькулятора совокупной стоимости владения, скорректируйте значения так, чтобы они соответствовали расходам на существующую локальную инфраструктуру.

Шаг 3. Просмотрите отчет

Выберите промежуток времени от одного до пяти лет. Калькулятор совокупной стоимости владения сформирует отчет на основе указанных данных. Пример:



В каждой категории (среда вычислений, центр обработки данных, сеть, хранилище и персонал) можно также сравнить детализацию затрат при выполнении рабочих нагрузок в локальной среде и в Azure. Пример:



ЗАКЛЮЧЕНИЕ

В данной бакалаврской работе изучалась предметная область, связанная с внедрением информационных систем и технологий Университета РГГМУ. В рамках темы определяются задачи и ставится цель.

Проведен анализ теоретического материала. Были рассмотрены, усовершенствованы и определены аспекты информационных систем и основы процессного подхода к управлению.

В данной работе Microsoft Azure использовалась для улучшения работы компании, за простоту и гибкость в работе, помимо наличия всех требований, сервисов и безопасности.

Описываются службы и функции Azure, а также упоминаются типы и функции облака.

Некоторые службы Azure были предложены для улучшения корпоративных операций:

- Ресурсы Azure и Azure Resource Manager
- Подписки и группы управления Azure
- вычислительных служб в Azure
- Виртуальная сеть Azure
- хранилища Azure
- Базы данных SQL Azure
- Защита от угроз безопасности с помощью Центра безопасности Azure
- Хранение секретов и управление ими в Azure Key Vault
- Глубинная защита
- Защита виртуальных сетей с помощью Брандмауэра Azure

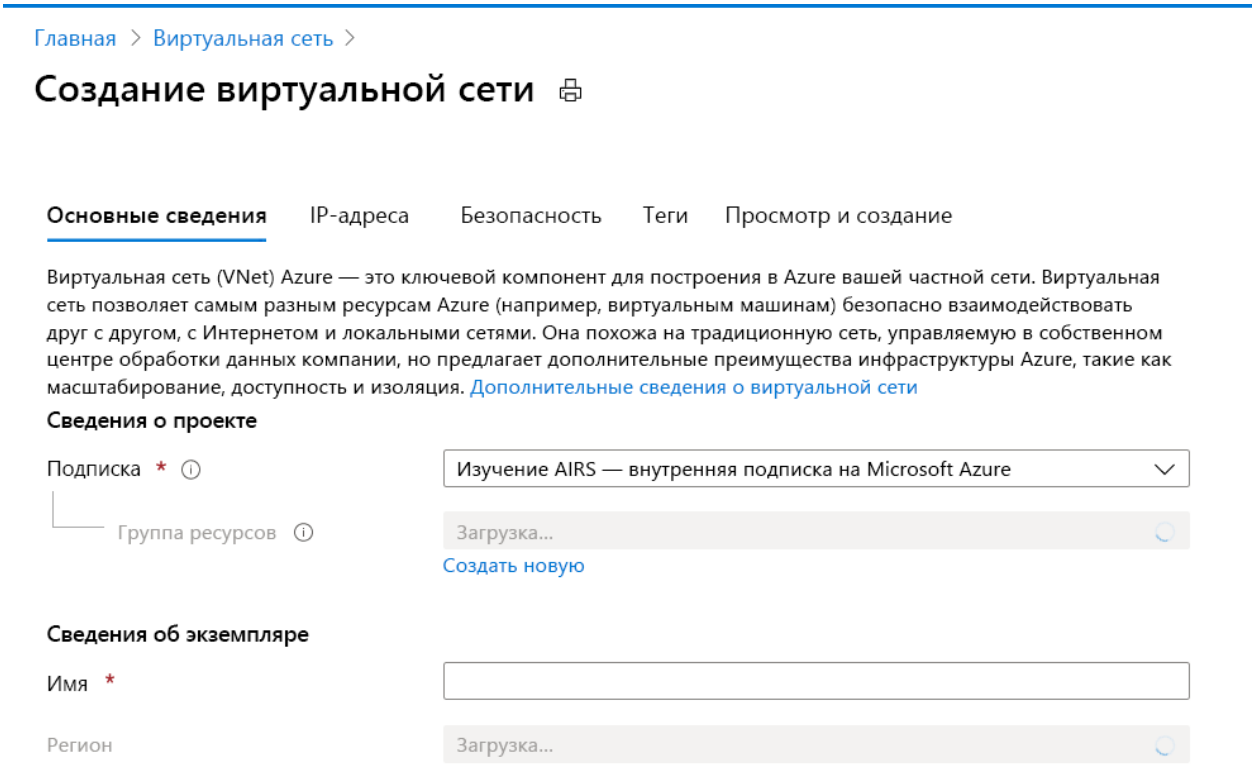
Подводя итог, можно сказать, что внедрение предложенных решений позволит компании улучшить свою работу и упростить управление, улучшится качество анализа информации, частично будет устранен человеческий фактор при работе с документами. Все задания бакалавриата выполнены, цель достигнута.

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

1) Петров, В. Н. Информационные системы: учебник для вузов / В. Н. Петров, М. А. Королев, Н. Г. Клешко, А. И. Мишенин. - Красноярск: СФУ, 2015. - 184 с.
2) Советов, Б. Я. Информационные технологии: учебник для вузов / Б. Я. Советов, В. В. Цехановский. - М.: Высшая школа, 2005. - 344 с.
3) Бурцева, Е. В. Информационные системы: учебное пособие / Е. В. Бурцева, И. П. Рак, А.В. Селезнев, А. В. Терехов, В. Н. Чернышов. - Тамбов: Изд-во Тамб. гос. техн. ун-та, 2009. - 128 с.
4) Надточий, А. И. Технические средства информатизации: учебное пособие / А. И. Надточий; под. ред. К. И. Курбакова. - М.: Кос-Инф, 2003. - 186 с.
5) Захаров, В. А. Влияние информационных технологий на развитие фирмы: учебник / В. Захаров. - М.: Инфра-М, 2005, - 113 с.
6) Петров, В. Н. Информационные системы: учебник / В. Н. Петров. - СПб.: BHV, 2002. - 358 с.
7) Шатунова, О. В. Информационные технологии: учебное пособие / О. В. Шатунова. - Елабуга: ЕГПУ, 2007. - 177 с.
8) Шнитман, В. З. Аппаратно-программные платформы корпоративных информационных систем: учебное пособие / В. З. Шнитман, С. Д. Кузнецов. - М.: МГУ, 2015. - 283 с.
9) AZ-900: Основы Microsoft Azure https://docs.microsoft.com/ru-ru/learn/certifications/exams/az-900.
10) DP-900: Основы работы с данными в Microsoft Azure https://docs.microsoft.com/ru-ru/learn/certifications/exams/dp-900.
11) Хаммер, М., Чампи, Дж. Реинжиринг корпорации: манифест революции в бизнесе / М. Хаммер, Д. Чампи; пер с англ. - СПб.: Издательство С.- Петербургского университета, 2015. - 332 с.
12) Юдина, Г .А. Аудит предприятия: учебное пособие для студентов / Г. А. Юдина. - Красноярск: СФУ, 2012. - 55 с.
13) Воронина, Л. И. Аудит информационных систем: учебное пособие / Л. И. Воронина. - СПб.: Омега-Л, 2012. - 675 с.
14) Изучение вычислительных служб Azure https://docs.microsoft.com/ru-ru/learn/modules/azure-compute-fundamentals/.
15) Изучение служб хранилища Azure https://docs.microsoft.com/ru-ru/learn/modules/azure-storage-fundamentals/.
16) Знакомство с базой данных Azure и службами аналитики https://docs.microsoft.com/ru-ru/learn/modules/azure-database-fundamentals/.
17) Защита от угроз безопасности в Azure https://docs.microsoft.com/ru-ru/learn/modules/protect-against-security-threats-azure/.
18) Защищенные сетевые подключения в Azure https://docs.microsoft.com/ru-ru/learn/modules/secure-network-connectivity-azure/.
19) Планирование и контроль затрат на Azure https://docs.microsoft.com/ru-ru/learn/modules/plan-manage-azure-costs/.

ПРИЛОЖЕНИЕ. Создание виртуальной сети

При создании виртуальной сети Azure можно настроить ряд основных параметров. У вас есть возможность настраивать такие дополнительные параметры, как несколько подсетей, защита от распределенных атак типа "отказ в обслуживании" (DDoS) и конечные точки службы.



Вы настроите следующие параметры для базовой виртуальной сети:

- **Имя сети.** Имя сети должно быть уникальным в пределах подписки, но не обязательно глобально уникальным. Задайте описательное имя, которое легко запомнить и отличить от имен других виртуальных сетей.

- **Адресное пространство** При настройке виртуальной сети внутреннее адресное пространство можно определить в формате бесклассовой междоменной маршрутизации (CIDR). Это адресное пространство должно быть уникальным в пределах вашей подписки и других сетях, к которым вы подключаетесь. Предположим, что для первой виртуальной сети вы выбрали диапазон адресов 10.0.0.0/24. Этот диапазон адресов определяет адреса от 10.0.0.1 до 10.0.0.254. Затем вы создаете вторую виртуальную сеть и выбираете адресное пространство 10.0.0.0/8. Этот диапазон адресов определяет адреса от 10.0.0.1 до 10.255.255.254. Некоторые адреса совпадают, а значит, такие диапазоны нельзя использовать для двух виртуальных сетей. Но вы можете использовать диапазон адресов 10.0.0.0/16, который определяет адреса от 10.0.0.1 до 10.0.255.254, и второй диапазон адресов 10.1.0.0/16, который определяет адреса от 10.1.0.1 до 10.1.255.254. Можно назначить эти диапазоны адресов виртуальным сетям, так как в них нет совпадающих адресов.

- **Подписка**. Этот параметр действует только в том случае, если у вас есть несколько подписок на выбор.

- **Группа ресурсов**. Как и любой другой ресурс Azure, виртуальная сеть должна существовать в группе ресурсов. Вы можете создать группу ресурсов или выбрать имеющуюся.

- **Расположение** Выберите расположение, в котором должна существовать виртуальная сеть.

- **Подсети** В каждом диапазоне адресов виртуальной сети можно создать одну или несколько подсетей, которые секционируют адресное пространство виртуальной сети. Маршрутизация между подсетями будет зависеть от маршрутов для трафика по умолчанию. Кроме того, вы можете определить пользовательские маршруты. Кроме того, можно определить одну подсеть, которая охватывает все диапазоны адресов виртуальных сетей.

Защита от атак DDoS Можно выбрать защиту от атак DDoS уровня "Базовый" или "Стандартный". Защита от атак DDoS категории "Стандартный" — это служба уровня "Премиум". Дополнительные сведения о защите от атак DDoS категории "Стандартный" см. в статье Защита от атак DDoS категории "Стандартный".

- **Конечные точки службы.** Здесь можно включить конечные точки служб. Затем вы можете выбрать из списка, какие конкретно конечные точки служб Azure нужно включить. Параметры включают Azure Cosmos DB, Служебную шину Azure, Azure Key Vault и т. д.

Завершив настройку этих параметров, щелкните элемент **Создать**.

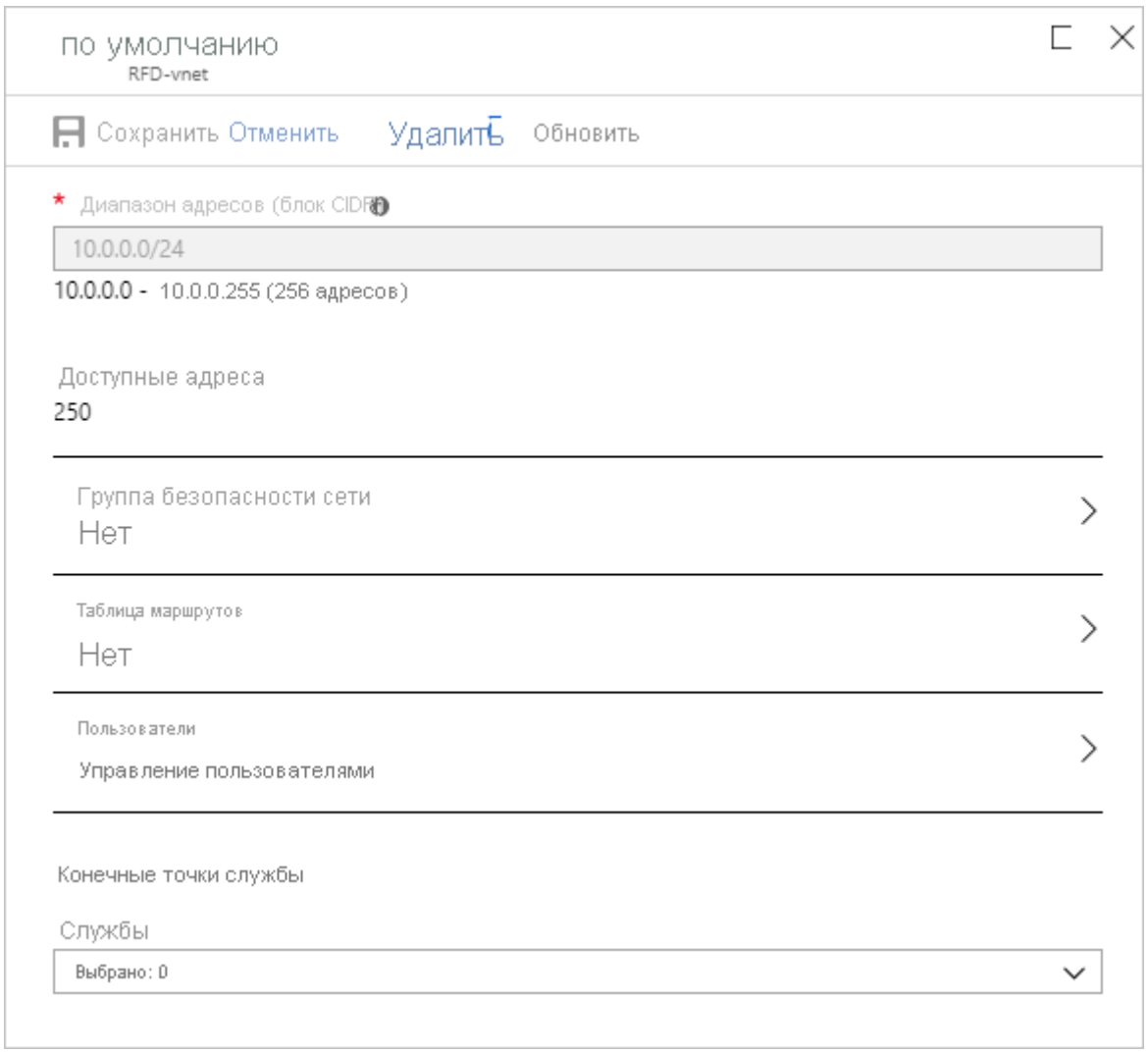
Дополнительные параметры

Завершив создание виртуальной сети, вы можете определить дополнительные параметры. приведенные ниже.

- **Группа безопасности сети** Группы безопасности содержат правила безопасности, позволяющие фильтровать тип сетевого трафика, который может направляться в подсети и сетевые интерфейсы виртуальной сети и из них. Группа безопасности сети создается отдельно. Затем вы можете сопоставить ее с виртуальной сетью.

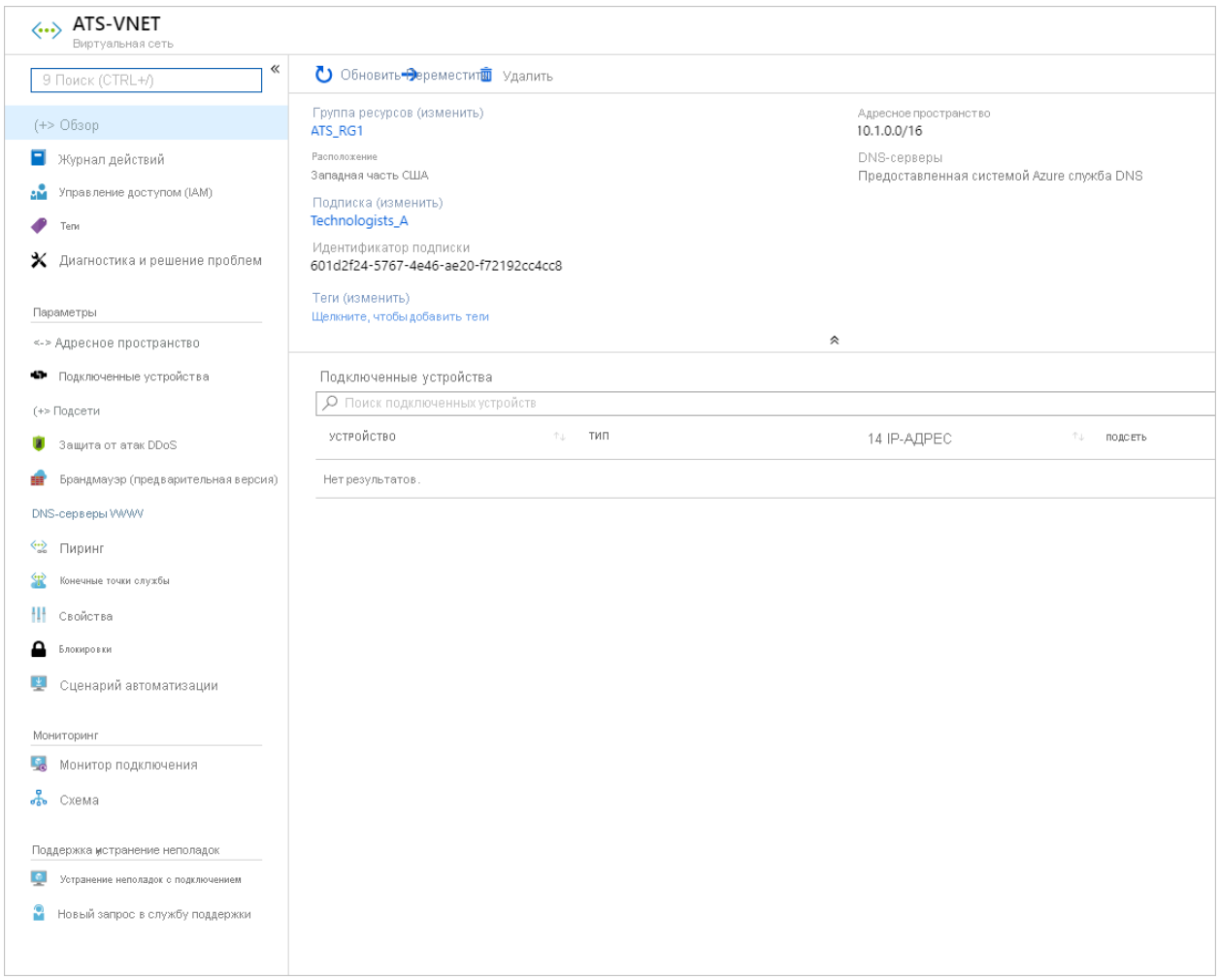
- **Таблица маршрутов** Azure автоматически создает таблицу маршрутов для каждой подсети в виртуальной сети Azure и добавляет в нее системные маршруты по умолчанию. Вы можете добавить пользовательские таблицы маршрутов для изменения трафика между виртуальными сетями.

Вы также можете изменить конечные точки службы.



Настройка виртуальных сетей

После создания виртуальной сети вы можете изменить любые ее параметры на панели **Виртуальная сеть** на портале Azure. Кроме того, для внесения изменений можно использовать команды PowerShell или Cloud Shell.



Параметры можно просмотреть и изменить на вложенных панелях. Эти параметры приведены ниже:

- **Адресные пространства**. Вы можете добавить дополнительные диапазоны адресов в начальное определение.
- **Подключенные устройства**. Используйте виртуальную сеть для подключения компьютеров.
- **Подсети**: Можно добавить дополнительные подсети.
- **Пиринг**. Соедините виртуальные сети с применением пиринга.

ПРИЛОЖЕНИЕ. Создание базы данных SQL

В этом упражнении вы создадите базу данных SQL в Azure, а затем запросите данные в этой базе данных.

Задача 1. Создание базы данных

В этой задаче мы создадим базу данных SQL на основе образца базы данных *AdventureWorksLT*.

1. Войдите на портал Azure.

2. Выберите **Создать ресурс** > **Базы данных** > **База данных SQL**. Появится панель **Создание Базы данных SQL**.

3. Введите указанные ниже значения для каждого параметра.

ТАБЛИЦА 1	
Параметр	**Значение**
Сведения о проекте	
Подписка	Центр подписки
Группа ресурсов	[имя группы ресурсов в песочнице]
Сведения о базе данных	
Имя базы данных	db1
Сервер	Выберите **Создать**.

Появится панель **Создание сервера Базы данных SQL**.

4. Введите указанные ниже значения для каждого параметра.

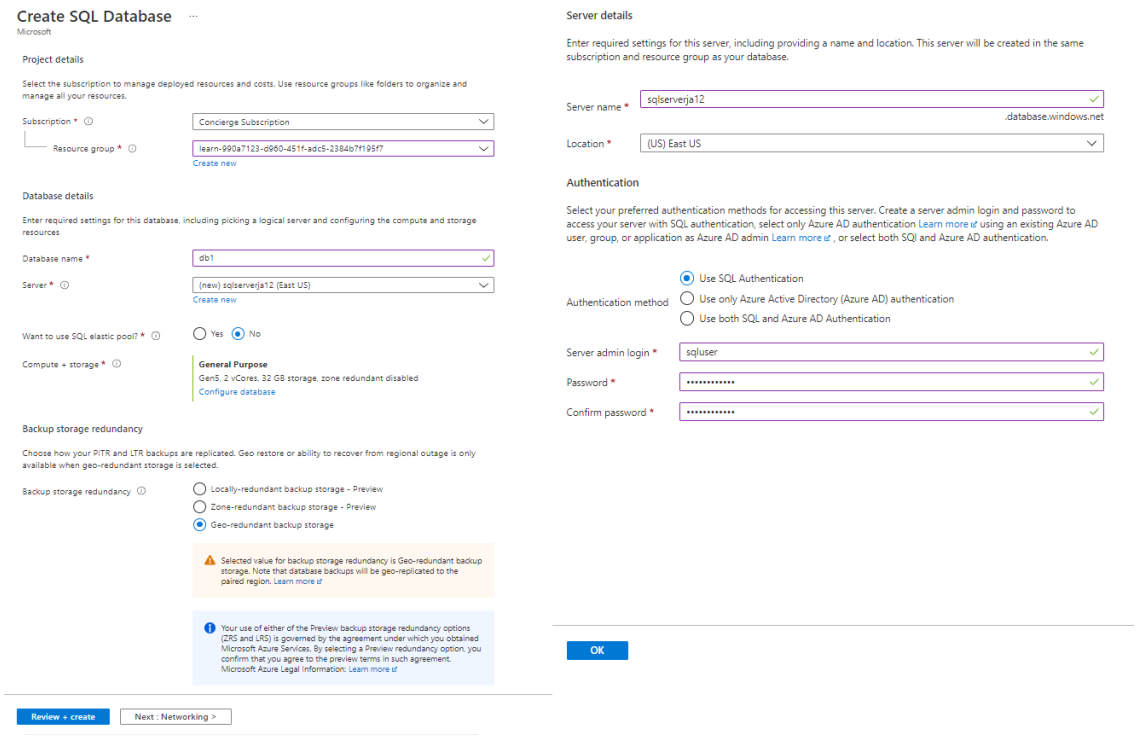
ТАБЛИЦА 2	
Параметр	**Значение**
Сведения о сервере	
Имя сервера	sqlservernnnn (замените **nnnn** на буквы и цифры, чтобы задать глобально уникальное имя)
Расположение	Восточная часть США (США)
Аутентификация	
Метод проверки подлинности	Использование аутентификации SQL
Имя для входа администратора сервера	sqluser
Пароль	Pa$$w0rd1234

5. Щелкните **ОК**.

6. Заполните остальные поля на странице **Создание базы данных SQL**, используя следующие значения.

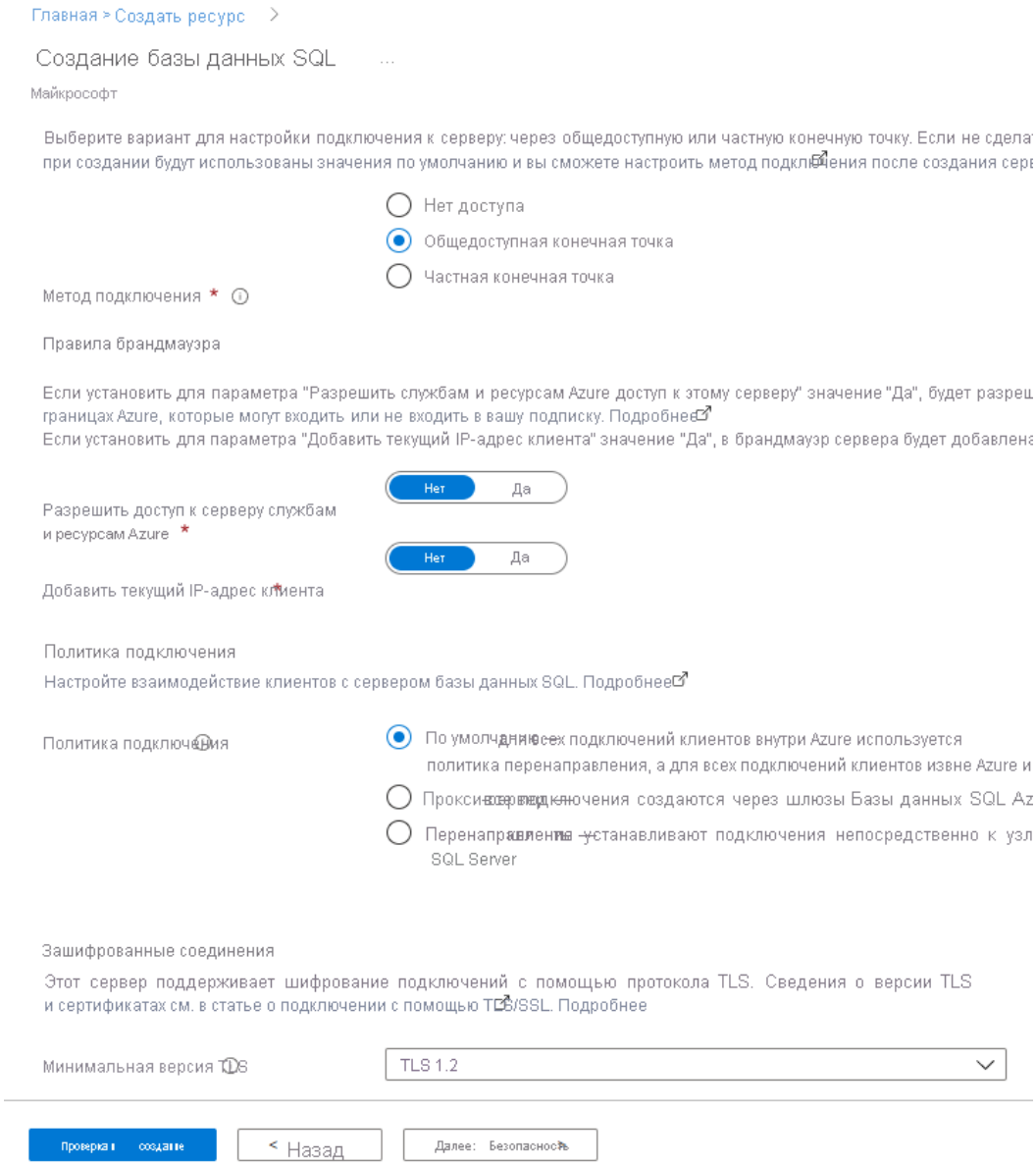
ТАБЛИЦА 3

Параметр	Значение
Хотите использовать эластичный пул SQL?	Нет (по умолчанию)
Вычисления и хранилище	Общего назначения (по умолчанию)
Избыточность хранилища резервных копий	
Избыточность хранилища резервных копий	Геоизбыточное хранилище резервных копий



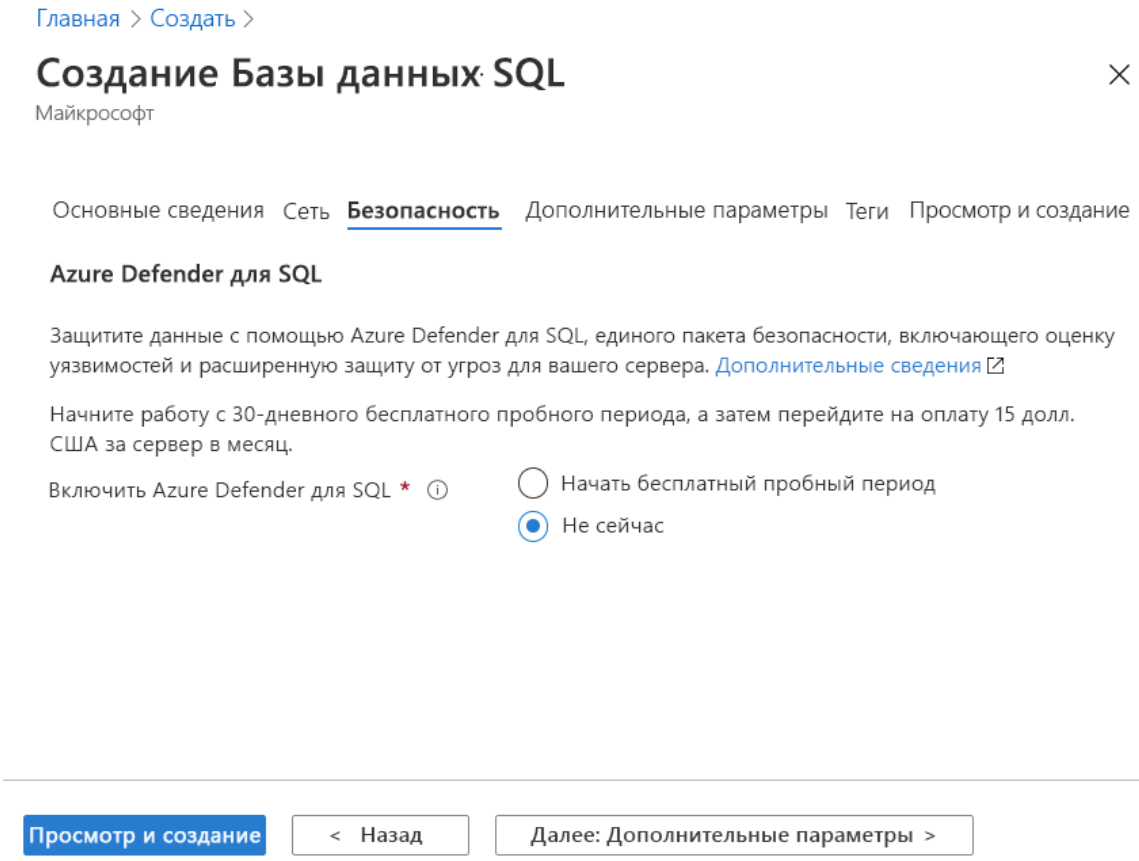
7. Выберите далее**: сеть** и настройте следующие параметры (оставьте значения по умолчанию в неуказанных полях).

ТАБЛИЦА 4	
Параметр	**Значение**
Сетевое подключение	
Метод подключения	Общедоступная конечная точка

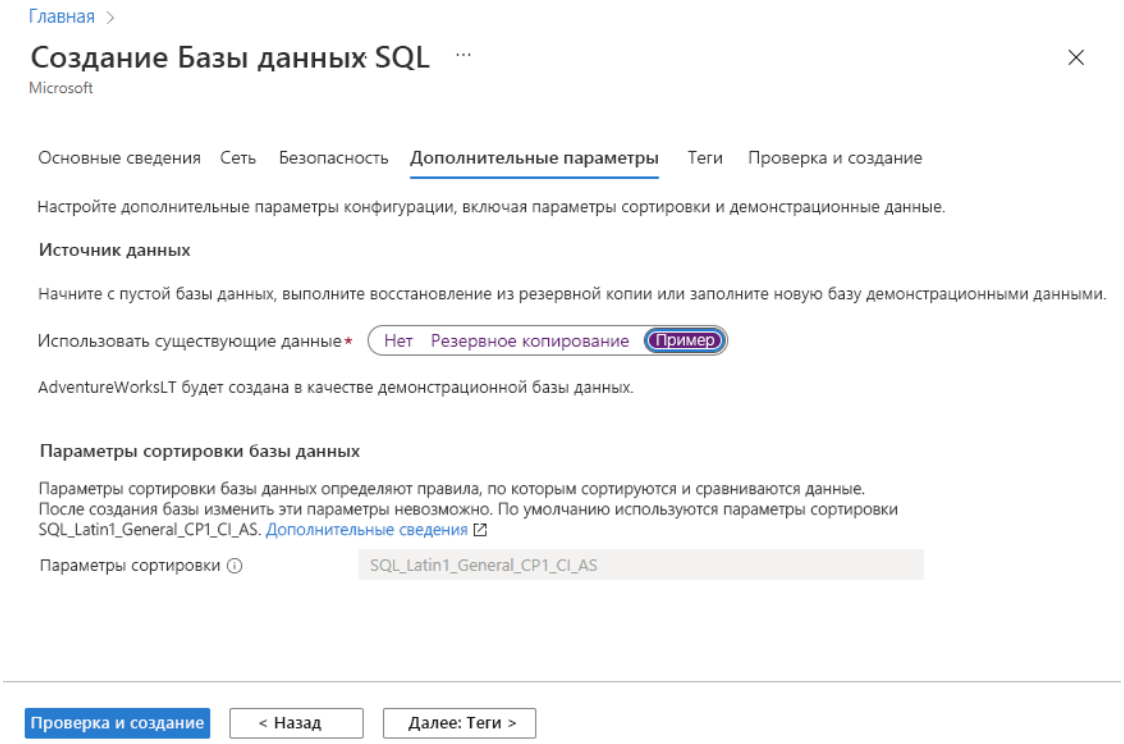


8. Нажмите кнопку **Далее: безопасность**, а затем для пункта **Включить Azure Defender для SQL** выберите **Не сейчас**. Для остальных параметров сохраните значения по умолчанию (не настроено).

ТАБЛИЦА 5	
Параметр	**Значение**
Источник данных	
Использование существующих данных	Образец
Параметры сортировки базы данных	
Параметры сортировки	SQL_Latin1_General_CP1_CI_AS (по умолчанию)



9. Выберите далее**:** **Дополнительные параметры** и настройте следующие параметры.



10. Выберите **Просмотр и создание**, чтобы подтвердить конфигурацию.

11. Нажмите **Создать**, чтобы развернуть сервер и базу данных. Создание сервера и развертывание образца базы данных может занять от двух до пяти минут. В области развертывания отображается состояние с обновлениями для каждого созданного ресурса.

12. По завершении развертывания выберите элемент **Перейти к ресурсу**. В области "Обзор" базы данных SQL db1 представлены основные компоненты только что развернутой базы данных.

13. В строке команд выберите **Настроить брандмауэр сервера**. Откроется страница **Параметры брандмауэра**.

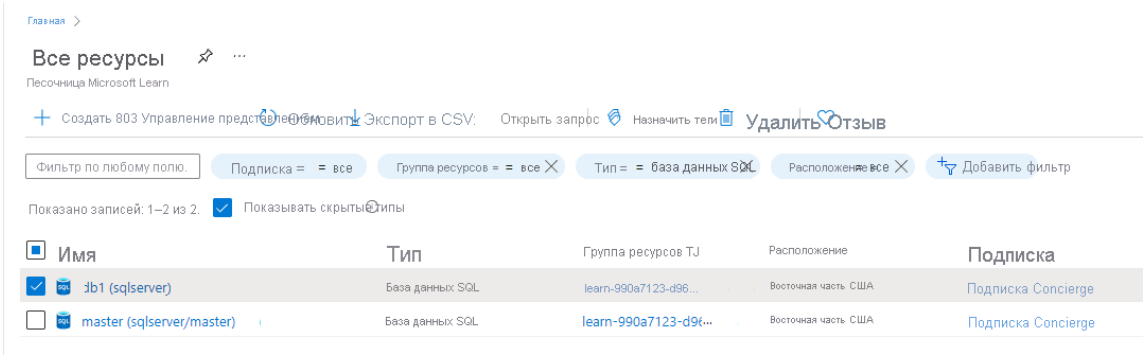
14. Установите для параметра **Разрешить доступ к серверу службам и ресурсам Azure** значение **Да**, а для остальных параметров оставьте значения по умолчанию.

15. В строке команд выберите **Сохранить**, чтобы обновить параметры брандмауэра, а затем закройте панель "Параметры брандмауэра".

Задача 2. Тестирование базы данных

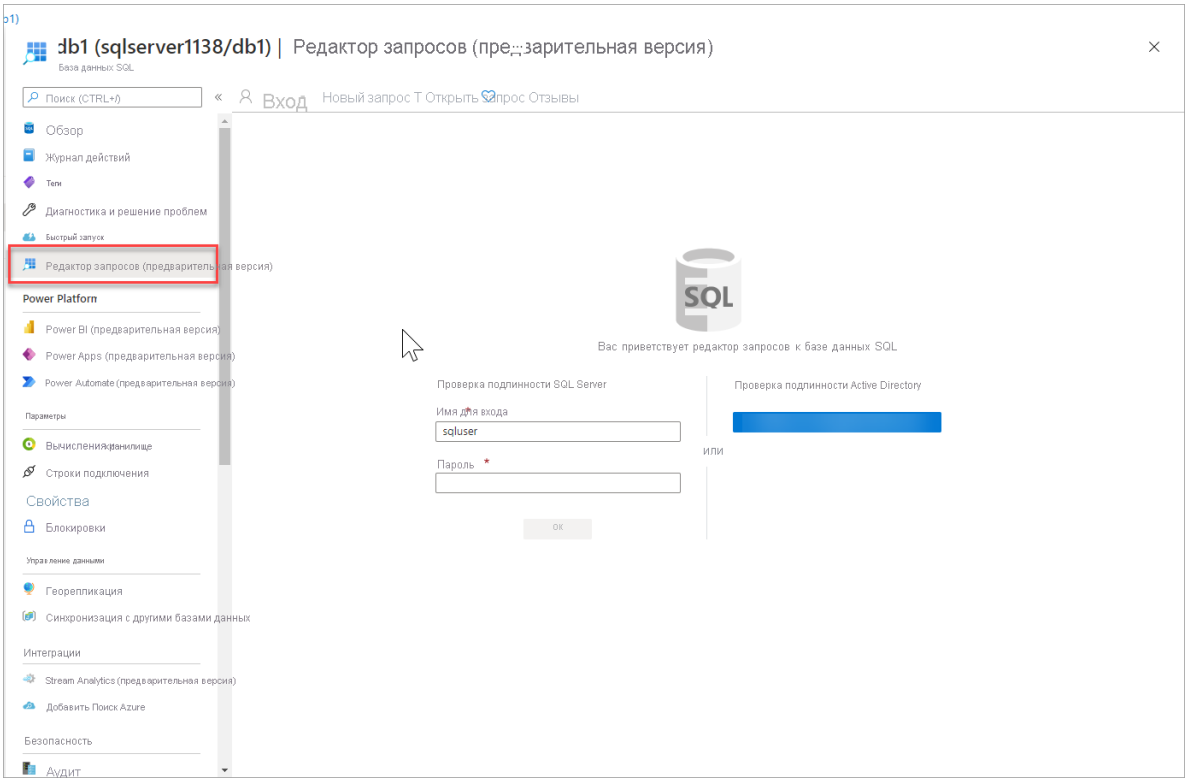
В этой задаче мы настроим сервер и выполним SQL-запрос.

1. В меню ресурсов Azure выберите **Все ресурсы**. Найдите и выберите тип ресурса **База данных SQL** и убедитесь, что новая база данных создана. Может потребоваться обновить содержимое страницы.



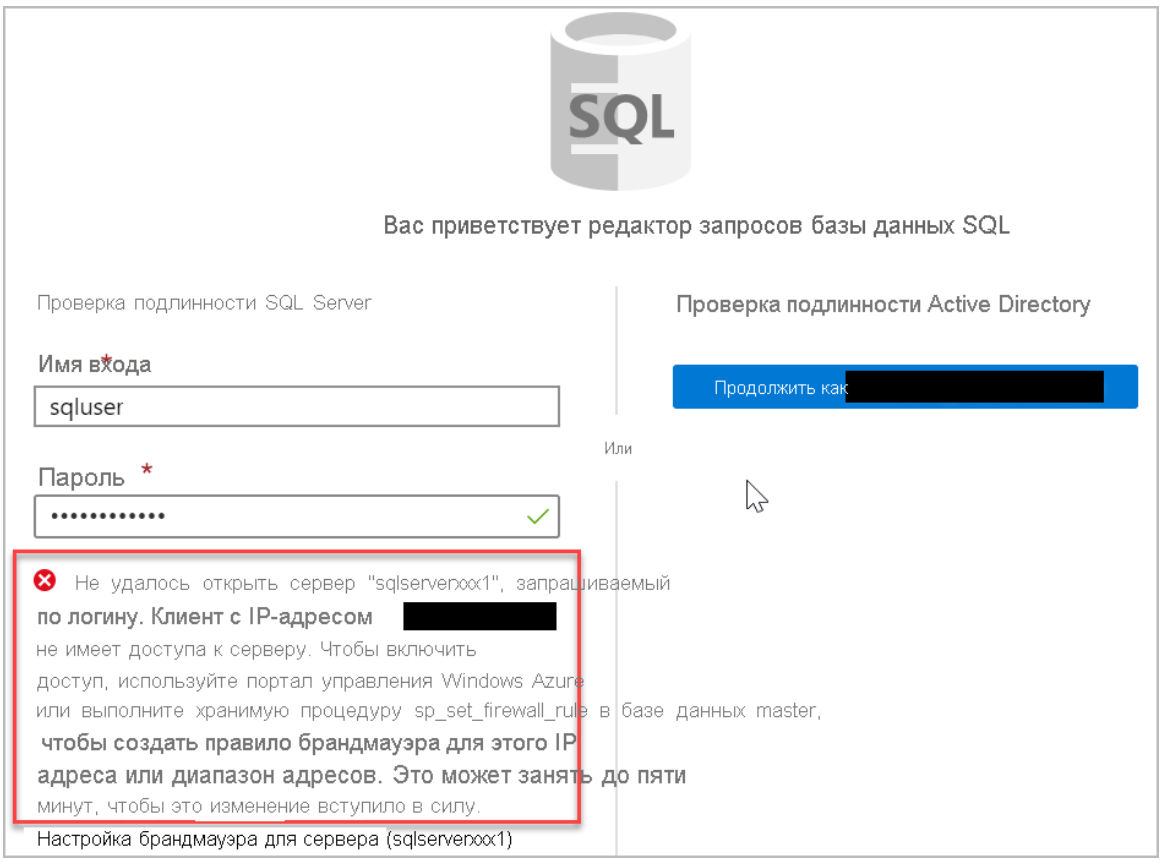
2. Выберите **db1**, базу данных SQL, которую вы создали.

3. В меню Базы данных SQL выберите **Редактор запросов (предварительная версия)**. Откроется область **предварительной версии редактора запросов**.



4. Войдите в систему как **sqluser** с паролем **Pa$$w0rd1234**.

Вы не сможете выполнить вход, так как ваш IP-адрес необходимо включить в правиле брандмауэра.

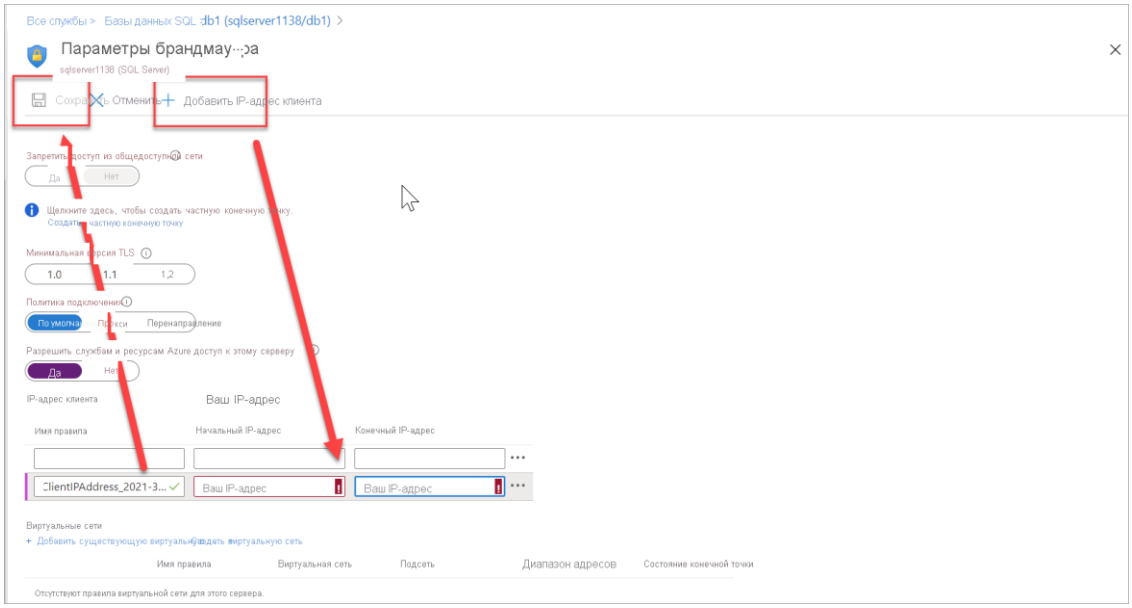


5. В меню редактора запросов выберите **Обзор** (изменения будут потеряны), а в строке команд выберите **Задать брандмауэр сервера**. Откроется страница **Параметры брандмауэра**.

6. В разделе **IP-адрес клиента** будет показан ваш IP-адрес (убедитесь, что он совпадает с IP-адресом клиента из ошибки, полученной на предыдущем шаге).

7. В командной строке выберите **Добавить IP-адрес клиента**. Будет добавлено **Имя правила**, содержащее ваш IP-адрес в полях **Начальный IP-адрес** и **Конечный IP-адрес**.

8. В командной строке выберите **Сохранить**, чтобы сохранить это правило брандмауэра.



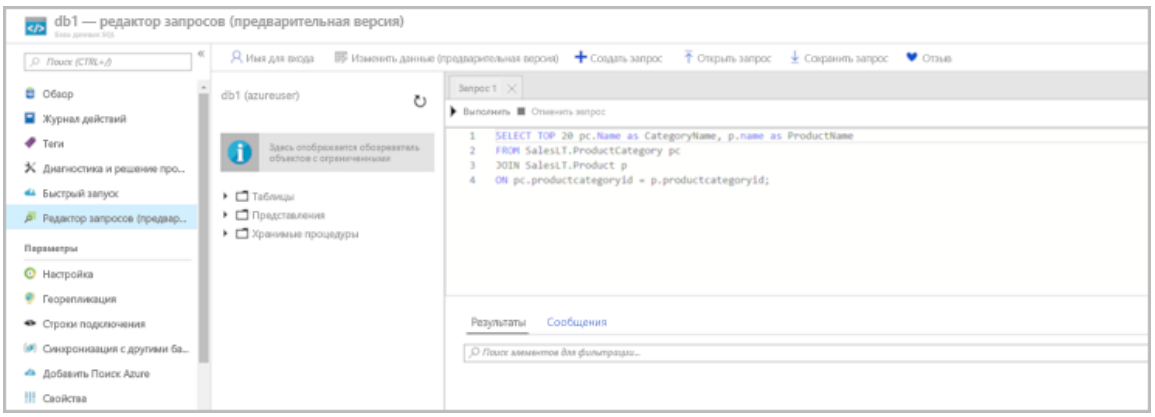
9. Выберите базу данных db1 в элементах навигации в верхней части страницы, чтобы вернуться к базе данных SQL, а затем в меню выберите **Редактор запросов (предварительная версия)**. страница входа.

10. Еще раз войдите в систему как **sqluser** с паролем **Pa$$w0rd1234**. На этот раз все должно получиться. Для развертывания нового правила брандмауэра может потребоваться несколько минут. Если вы продолжаете получать сообщение об ошибке, проверьте IP-адрес клиента в ошибке и вернитесь к разделу **Параметры брандмауэра**, чтобы добавить правильный IP-адрес клиента.

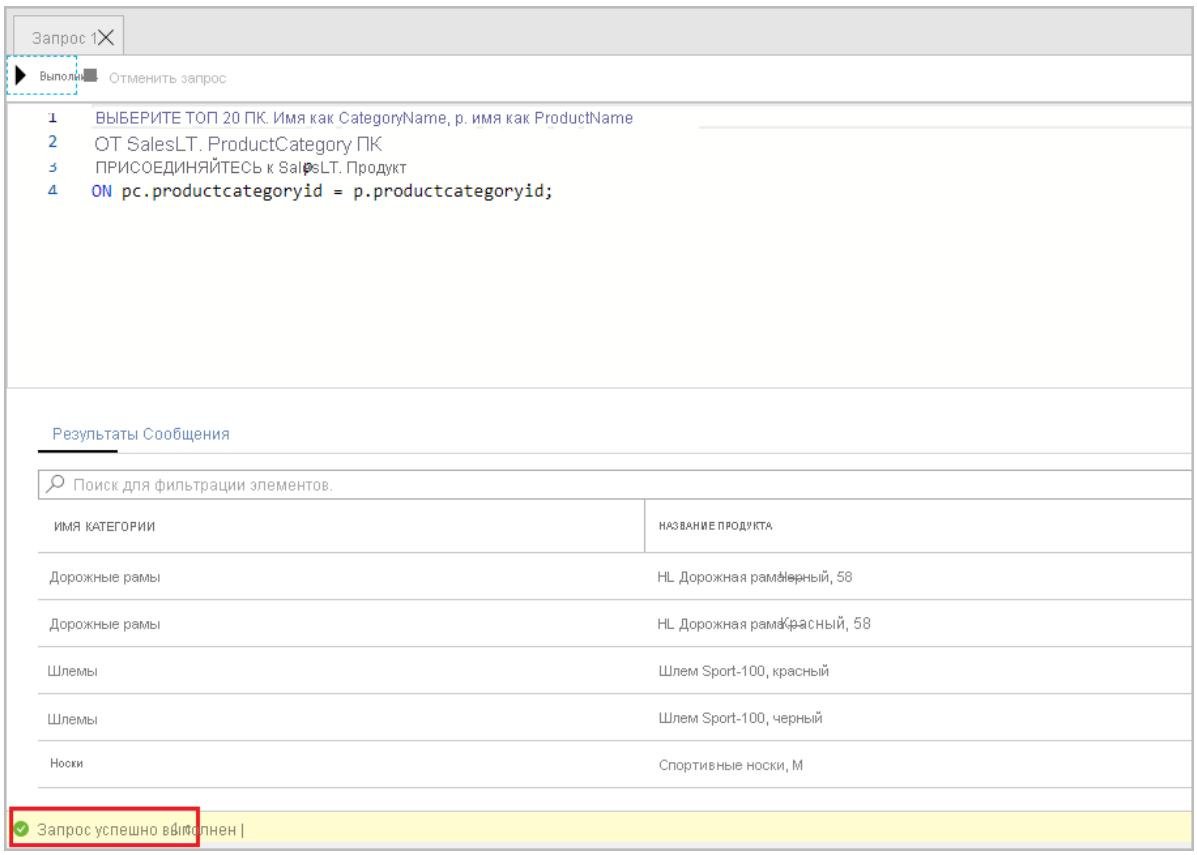
11. После успешного входа появится панель запросов. Введите в панели редактора приведенный ниже SQL-запрос.

SQLКопировать

```
SELECT TOP 20 pc.Name is CategoryName, p.name as ProductName
FROM SalesLT.ProductCategory pc
JOIN SalesLT.Product p
ON pc.productcategoryid = p.productcategoryid;
```



12. Щелкните **Выполнить** и просмотрите результаты запроса в области **Результаты**. Запрос должен выполниться успешно.


Запрос 1
Выполнить
Отменить запрос
1 ВЫБЕРИТЕ ТОП 20 ПК. Имя как CategoryName, p. имя как ProductName
2 ОТ SalesLT. ProductCategory ПК
3 ПРИСОЕДИНЯЙТЕСЬ к SalesLT. Продукт
4 ON pc.productcategoryid = p.productcategoryid;
Результаты Сообщения
Поиск для фильтрации элементов.
ИМЯ КАТЕГОРИИ
НАЗВАНИЕ ПРОДУКТА
Дорожные рамы
HL Дорожная рама, Черный, 58
Дорожные рамы
HL Дорожная рама, Красный, 58
Шлемы
Шлем Sport-100, красный
Шлемы
Шлем Sport-100, черный
Носки
Спортивные носки, M
Запрос успешно выполнен |

ПРИЛОЖЕНИЕ. Создание хранилища ключей

1. Перейдите на портал Microsoft Azure.

2. В меню портала Azure или на **домашней странице** в разделе **Службы Azure** выберите **Создать ресурс**. Откроется панель **Создание ресурса**.

3. В строке поиска введите *Key Vault*, а затем в результатах выберите **Key Vault**. Появится панель **Key Vault (Хранилище ключей)**.

4. Щелкните **Создать**. Откроется панель **Create key vault (Создать хранилище ключей)**.

5. На вкладке **Основные сведения** введите указанные ниже значения для каждого параметра.

Параметр	Значение
Сведения о проекте	
Подписка	**Подписка Concierge**
Группа ресурсов	[имя группы ресурсов в песочнице]
Сведения о базе данных	
Имя базы данных	**My-keyvault-NNN**, где NNN — уникальный идентификатор

Для остальных параметров примите значения по умолчанию.

6. Выберите **Проверка и создание**, а после завершения проверки нажмите **Создать**.
Дождитесь завершения развертывания.

7. Выберите **Перейти к ресурсу**.

8. Обратите внимание на некоторые сведения о вашем хранилище ключей.
Например, в поле **URI хранилища** отображается универсальный код ресурса (URI), который приложение может использовать для доступа к вашему хранилищу из REST API.
Ниже показан пример хранилища ключей с именем **my-keyvault-321**:

9. В качестве дополнительного действия на панели меню слева в разделе **Параметры** просмотрите некоторые другие функции.

Добавление пароля в хранилище ключей

1. На панели меню слева в разделе **Параметры** выберите **Секреты**. Появится панель хранилища ключей.

2. В верхней строке меню выберите элемент **Generate/Import** (Создать или импортировать). Откроется панель **Создание секрета**.

3. Задайте указанные ниже значения для каждого параметра.

Параметр	Значение
Параметры отправки	Вручную
Имя	MyPassword
Значение	hVFkk96

Для остальных параметров примите значения по умолчанию. Обратите внимание, что вы можете указать такие свойства, как дата активации и срок действия. Вы также можете отключить доступ к этому секрету.

4. Нажмите кнопку **Создать**.

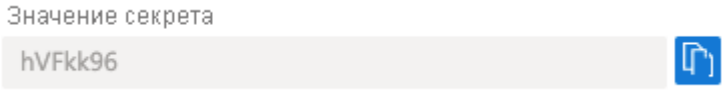
Отображение пароля

Теперь вам нужно дважды получить доступ к паролю из хранилища ключей. Сначала вы получите к нему доступ с портала Azure, а затем из Azure CLI.

1. На своей панели **Key Vault/Secrets** (Key Vault, секреты) выберите значение **MyPassword**. Появится панель **MyPassword/Versions** (MyPassword, версии). Вы увидите, что включена текущая версия.

2. Выберите текущую версию. Появится панель **Версия секрета**. В разделе **Идентификатор секрета** отображается URI, который теперь можно использовать в приложениях для доступа к секрету. Помните, что только авторизованные приложения могут получить доступ к этому секрету.

3. Нажмите **Показать значение секрета**. Отображается уникальное значение для этой версии пароля.



4. В Cloud Shell выполните следующую команду.

Azure CLI

```
az keyvault secret show \
  --name MyPassword \
  --vault-name my-keyvault-NNN \
  --query value \
  --output tsv
```

В выходных данных отобразится пароль.

Выходные данные

```
hVFkk96
```