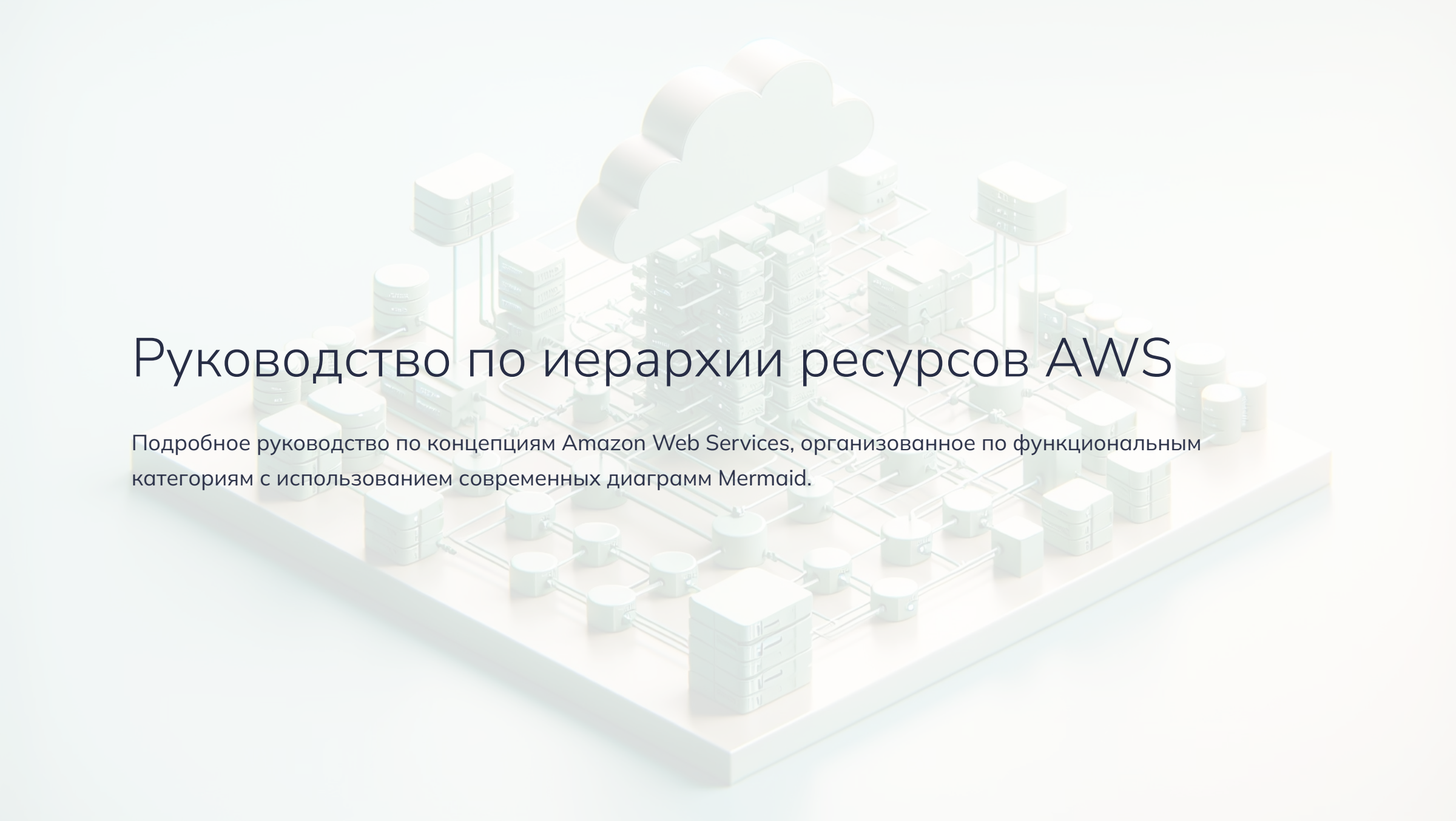


Руководство по иерархии ресурсов AWS

Подробное руководство по концепциям Amazon Web Services, организованное по функциональным категориям с использованием современных диаграмм Mermaid.

Базовая инфраструктура

Основные организационные и сетевые компоненты, лежащие в основе всех служб AWS.

Перед изучением услуг более высокого уровня необходимо понять базовую инфраструктуру AWS. Все в AWS работает в контексте учетных записей, регионов и зон доступности, образуя иерархическую структуру, которая обеспечивает как организационные границы, так и высокую доступность.

Организационная иерархия

AWS Organizations предоставляет централизованный способ управления несколькими учетными записями AWS.
Каждая учетная запись остаётся отдельной единицей с собственными настройками безопасности и биллингом, но Organizations позволяет объединить их в иерархическую структуру с общими правилами и консолидированным выставлением счетов.

Учетные записи можно группировать в **организационные подразделения (OU)** для удобства управления.
С помощью **политик контроля служб (SCP)** администратор может задавать общие ограничения — их нельзя обойти даже на уровне отдельной учетной записи.

Региональная и сетевая инфраструктура

Региональная и зональная структура AWS лежит в основе архитектур с высокой отказоустойчивостью. **Регионы** — это географически распределённые области, каждая из которых включает несколько **зон доступности (Availability Zones, AZ)**. Зоны доступности представляют собой изолированные центры обработки данных внутри региона, соединённые между собой высокоскоростными каналами.

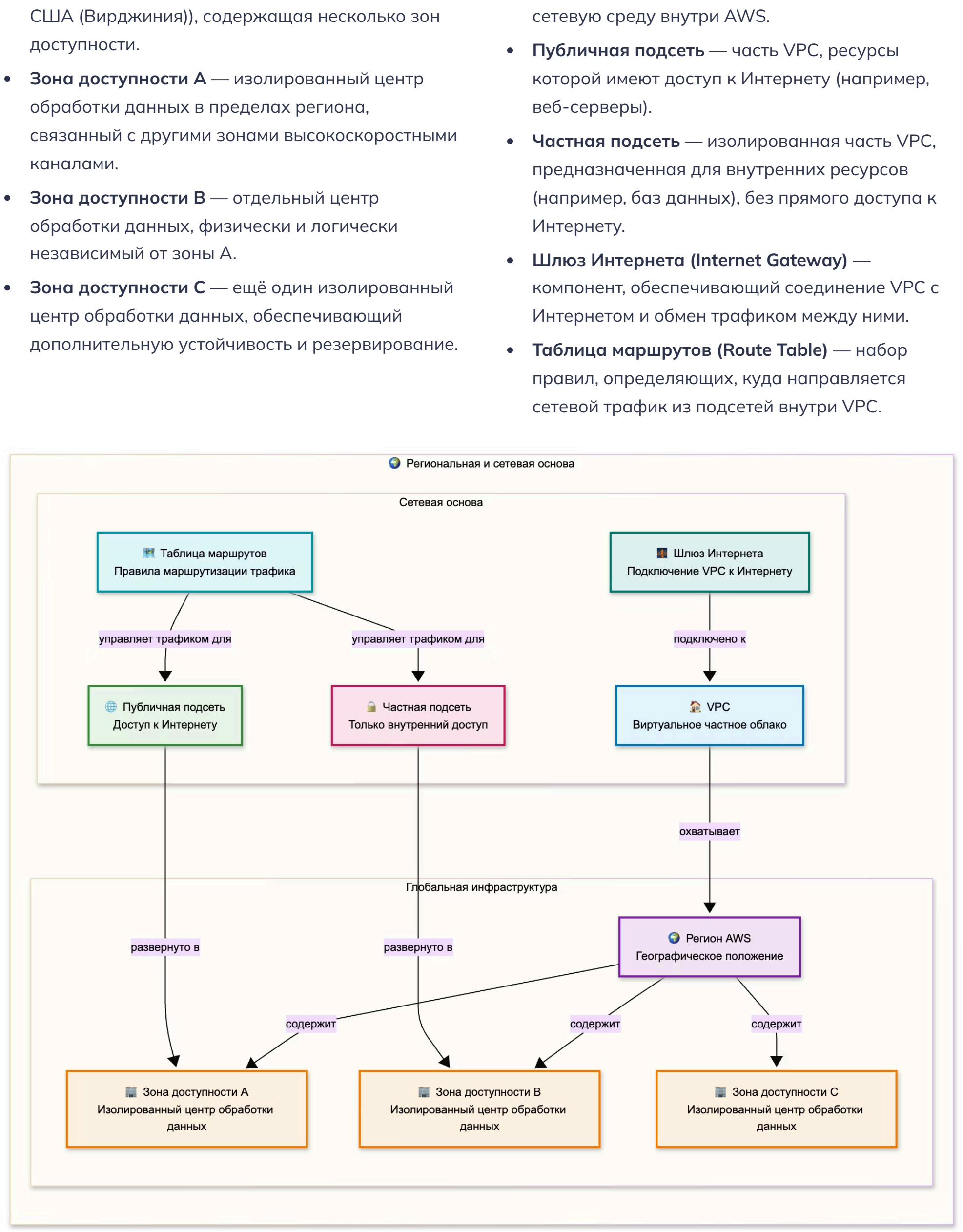
Внутри региона создаются **виртуальные частные облака (VPC)** — изолированные сетевые среды, где можно размещать ресурсы.
Подсети внутри VPC позволяют распределять ресурсы по зонам доступности и обеспечивать дополнительное разделение и контроль трафика.

Глобальная инфраструктура AWS

- **Регион AWS** — это географически определённая область (например, Европа (Франкфурт) или США (Вирджиния)), содержащая несколько зон доступности.
- **Зона доступности A** — изолированный центр обработки данных в пределах региона, связанный с другими зонами высокоскоростными каналами.
- **Зона доступности B** — отдельный центр обработки данных, физически и логически независимый от зоны A.
- **Зона доступности C** — ещё один изолированный центр обработки данных, обеспечивающий дополнительную устойчивость и резервирование.

Сетевая основа AWS

- **VPC (Virtual Private Cloud)** — виртуальное частное облако, создающее изолированную сетевую среду внутри AWS.
- **Публичная подсеть** — часть VPC, ресурсы которой имеют доступ к Интернету (например, веб-серверы).
- **Частная подсеть** — изолированная часть VPC, предназначенная для внутренних ресурсов (например, баз данных), без прямого доступа к Интернету.
- **Шлюз Интернета (Internet Gateway)** — компонент, обеспечивающий соединение VPC с Интернетом и обмен трафиком между ними.
- **Таблица маршрутов (Route Table)** — набор правил, определяющих, куда направляется сетевой трафик из подсетей внутри VPC.



Основы безопасности и идентификации

Безопасность в AWS строится вокруг управления идентификацией и доступом (**IAM — Identity and Access Management**), которое определяет, **кто** может получить доступ к ресурсам и **что** он может с ними делать.

IAM обеспечивает аутентификацию (подтверждение личности пользователя) и авторизацию (разрешение действий), формируя основу безопасности всех сервисов AWS.
Принцип **минимально необходимых прав** реализуется через гибкую систему политик — они могут применяться как к пользователям и ролям, так и напрямую к ресурсам, обеспечивая строгий контроль доступа на всех уровнях.

Основы IAM

Пользователи IAM — это индивидуальные учетные записи с постоянными идентификационными данными (например, логином и ключами доступа). Они предназначены для людей или систем, которым требуется постоянный доступ к AWS.

Роли IAM — это временные идентичности, которые можно "принимать на себя". Они используются для безопасного взаимодействия между службами AWS или при предоставлении доступа внешним пользователям без необходимости создавать отдельные учетные записи.

Группы IAM — объединяют пользователей, чтобы упростить управление разрешениями. Политики, назначенные группе, автоматически применяются ко всем её участникам.

Политики IAM — это документы в формате JSON, которые определяют, какие действия разрешены или запрещены для пользователей, групп или ролей.

Источники идентификации

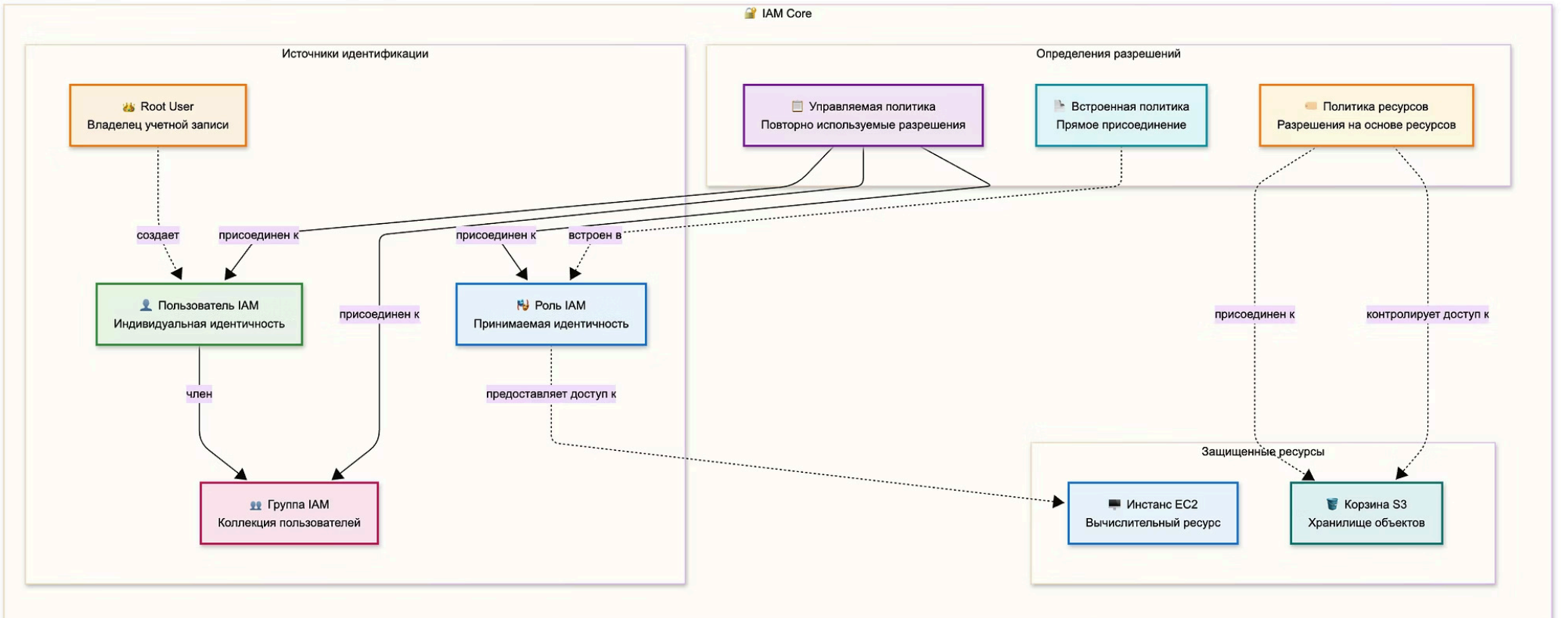
- Root User - владелец учетной записи
- Пользователь IAM - индивидуальная идентичность
- Группа IAM - коллекция пользователей
- Роль IAM - принимаемая идентичность

Определения разрешений

- Управляемая политика - повторно используемые разрешения
- Встроенная политика - прямое присоединение
- Политика ресурсов - разрешения на основе ресурсов

Защищенные ресурсы

- Корзина S3 - хранилище объектов
- Инстанс EC2 - вычислительный ресурс


IAM Core
Источники идентификации
Root User
Владелец учетной записи
Определения разрешений
Управляемая политика
Повторно используемые разрешения
Встроенная политика
Прямое присоединение
Политика ресурсов
Разрешения на основе ресурсов
создает
присоединен к
присоединен к
встроен в
Пользователь IAM
Индивидуальная идентичность
присоединен к
Роль IAM
Принимаемая идентичность
присоединен к
контролирует доступ к
член
предоставляет доступ к
Защищенные ресурсы
Группа IAM
Коллекция пользователей
Инстанс EC2
Вычислительный ресурс
Корзина S3
Хранилище объектов

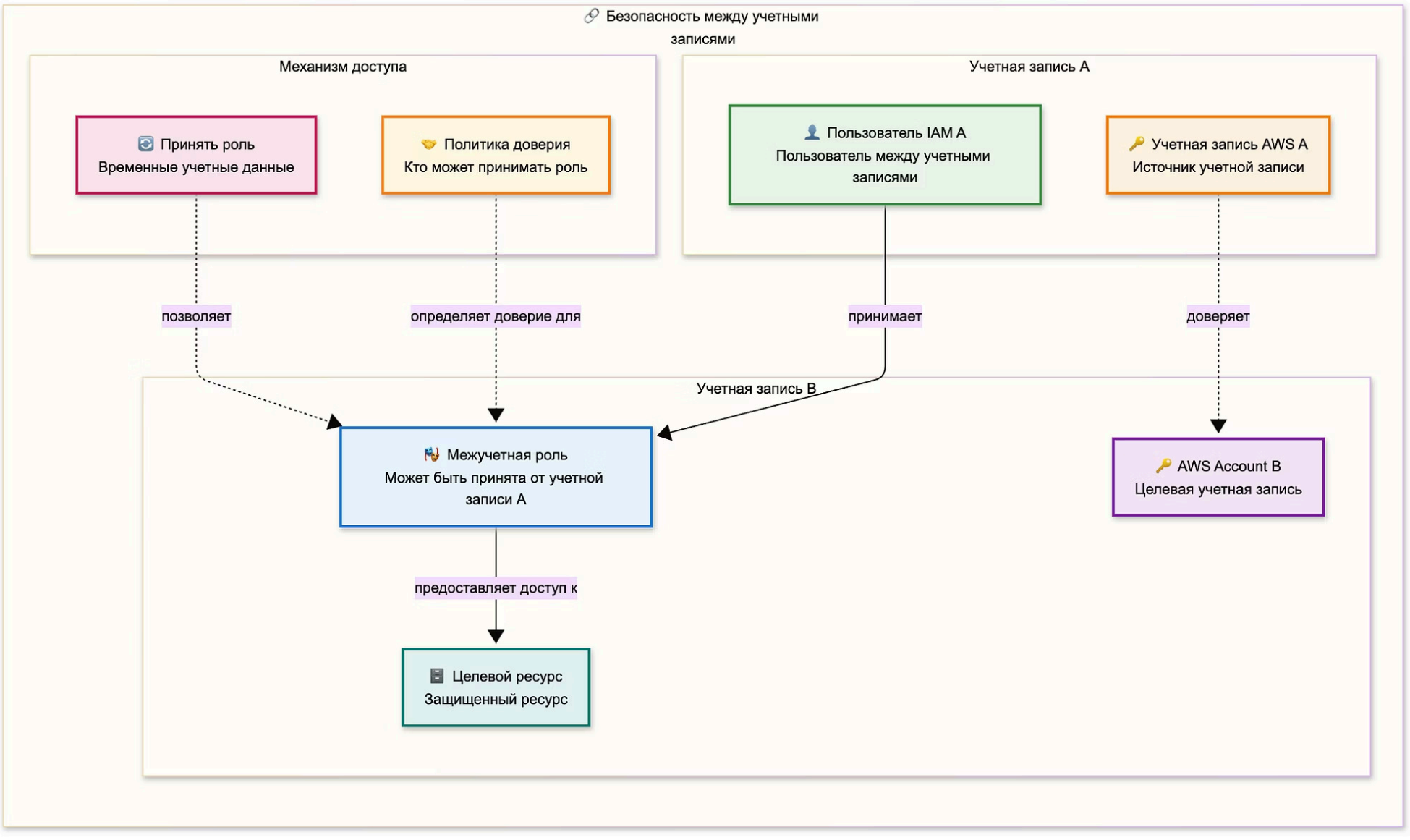
Безопасность между учетными записями

Доступ между учетными записями (Cross-Account Access)

Шаблоны доступа между учетными записями используют **роли IAM**, чтобы обеспечить безопасное взаимодействие между разными учетными записями AWS **без передачи долгосрочных учетных данных**.

Такой подход позволяет одной учетной записи временно “принимать” роль из другой, получая доступ только к тем ресурсам, которые явно разрешены политиками.
Эта модель особенно важна для:

- архитектур с **множеством учетных записей** (multi-account), где ресурсы и команды изолированы для безопасности;
- **интеграции со сторонними сервисами и приложениями**, которым требуется ограниченный доступ без компрометации учетных данных.



Вычислительные и контейнерные сервисы

Основная вычислительная инфраструктура AWS охватывает весь спектр — от полного контроля над серверами до полностью управляемых бессерверных решений.

В её основе лежит **Amazon EC2**, предоставляющий виртуальные машины с полным управлением операционной системой, конфигурацией и сетью. На другом конце спектра находится **AWS Lambda** — событийно-ориентированная платформа, где код запускается без управления инфраструктурой.

Между этими крайностями располагаются контейнерные решения:

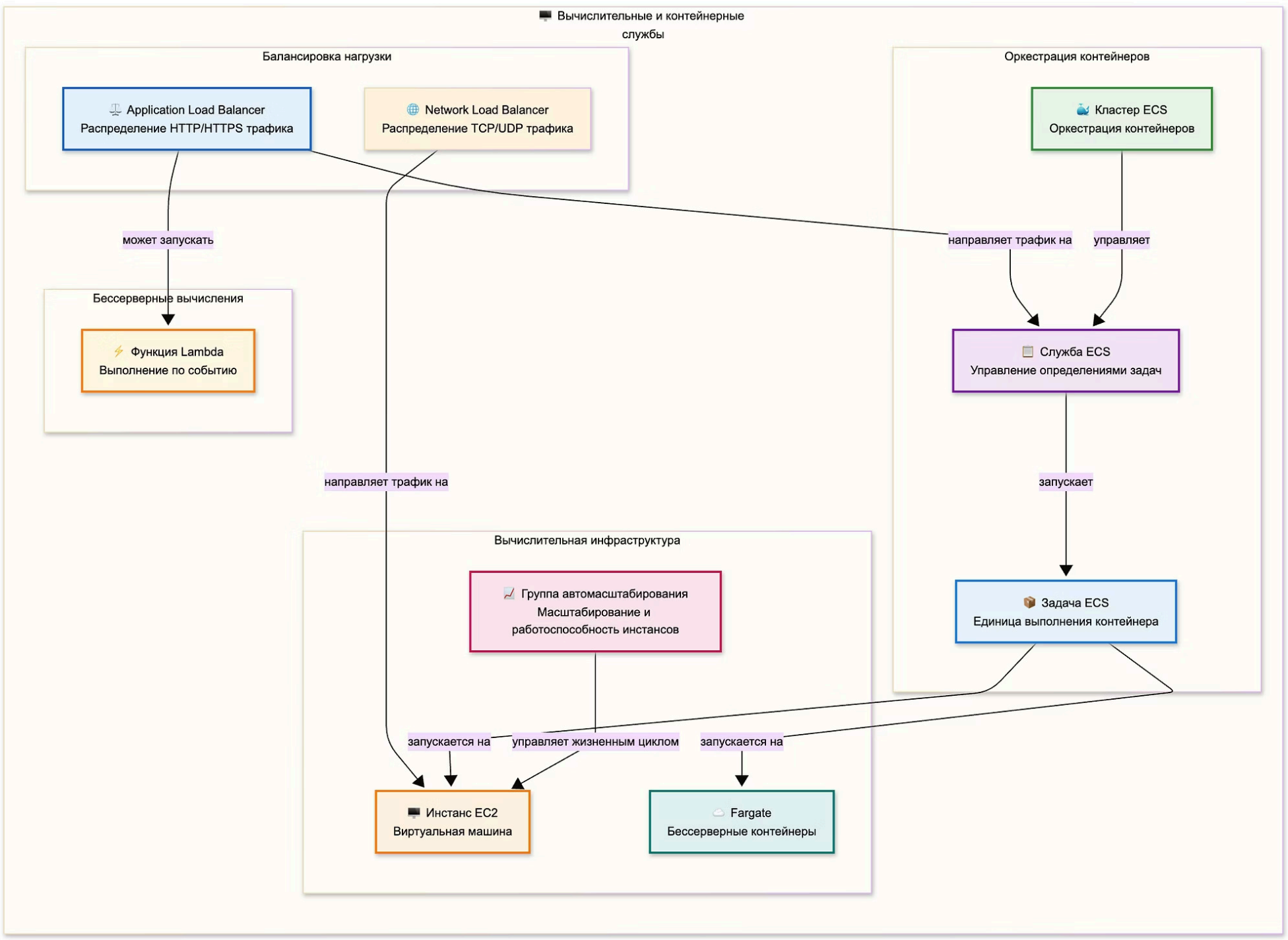
- **Amazon ECS (Elastic Container Service)** — сервис для оркестрации контейнеров с возможностью размещения на собственных EC2-инстансах.
- **AWS Fargate** — вариант запуска ECS или EKS без управления серверами, где AWS автоматически выделяет ресурсы под контейнеры.
- **Amazon EKS (Elastic Kubernetes Service)** — управляемый Kubernetes, обеспечивающий совместимость со стандартными инструментами экосистемы Kubernetes.

Группы авто-масштабирования (Auto Scaling Groups) повышают надежность и адаптивность систем, автоматически добавляя или заменяя инстансы в зависимости от нагрузки.
Балансировщики нагрузки (Application Load Balancers) равномерно распределяют входящий трафик между здоровыми инстансами, обеспечивая устойчивость и высокую доступность.

Понимание этой иерархии помогает выбирать оптимальный уровень абстракции:

- **EC2** — когда нужен полный контроль.
- **ECS** — для управляемой оркестрации контейнеров.
- **Fargate** — для контейнеров без серверов.
- **Lambda** — для событийных и краткосрочных рабочих нагрузок.

Каждый уровень представляет баланс между гибкостью и простотой эксплуатации.



Сеть и доставка контента

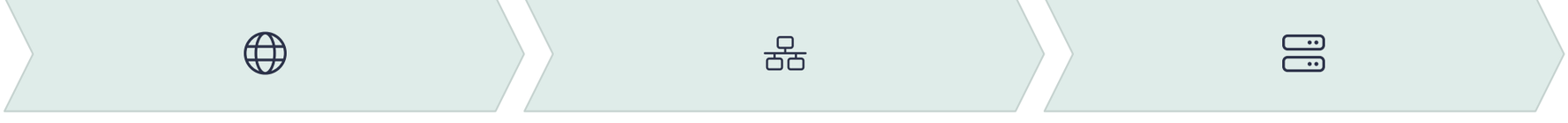
AWS объединяет **виртуальную частную облачную инфраструктуру (VPC)** и **глобальные сетевые службы**, обеспечивая безопасное подключение и быструю доставку контента по всему миру.

На **региональном уровне** действует **Amazon VPC (Virtual Private Cloud)** — изолированная сеть, в которой размещаются ресурсы, управляемые пользователем. Она предоставляет контроль над IP-диапазонами, маршрутизацией, подсетями и шлюзами.

На **глобальном уровне** работают службы, обеспечивающие связность и доставку данных:

- **Amazon CloudFront** — сеть доставки контента (CDN), ускоряющая распространение данных пользователям по всему миру.
- **AWS Global Accelerator** — улучшает производительность и доступность приложений, направляя трафик по оптимальным маршрутам глобальной сети AWS.
- **AWS Direct Connect** — предоставляет выделенное подключение к AWS из локальных дата-центров, повышая безопасность и стабильность каналов связи.
- **AWS Transit Gateway** — централизует маршрутизацию между несколькими VPC и локальными сетями.

Понимание различий между **глобальными службами** (например, CloudFront, Global Accelerator) и **региональной инфраструктурой VPC** помогает проектировать приложения, которые одновременно масштабируются глобально и остаются изолированными и безопасными внутри региона.



Глобальные службы

Route 53, CloudFront

Региональная сеть

VPC, подсети, шлюзы

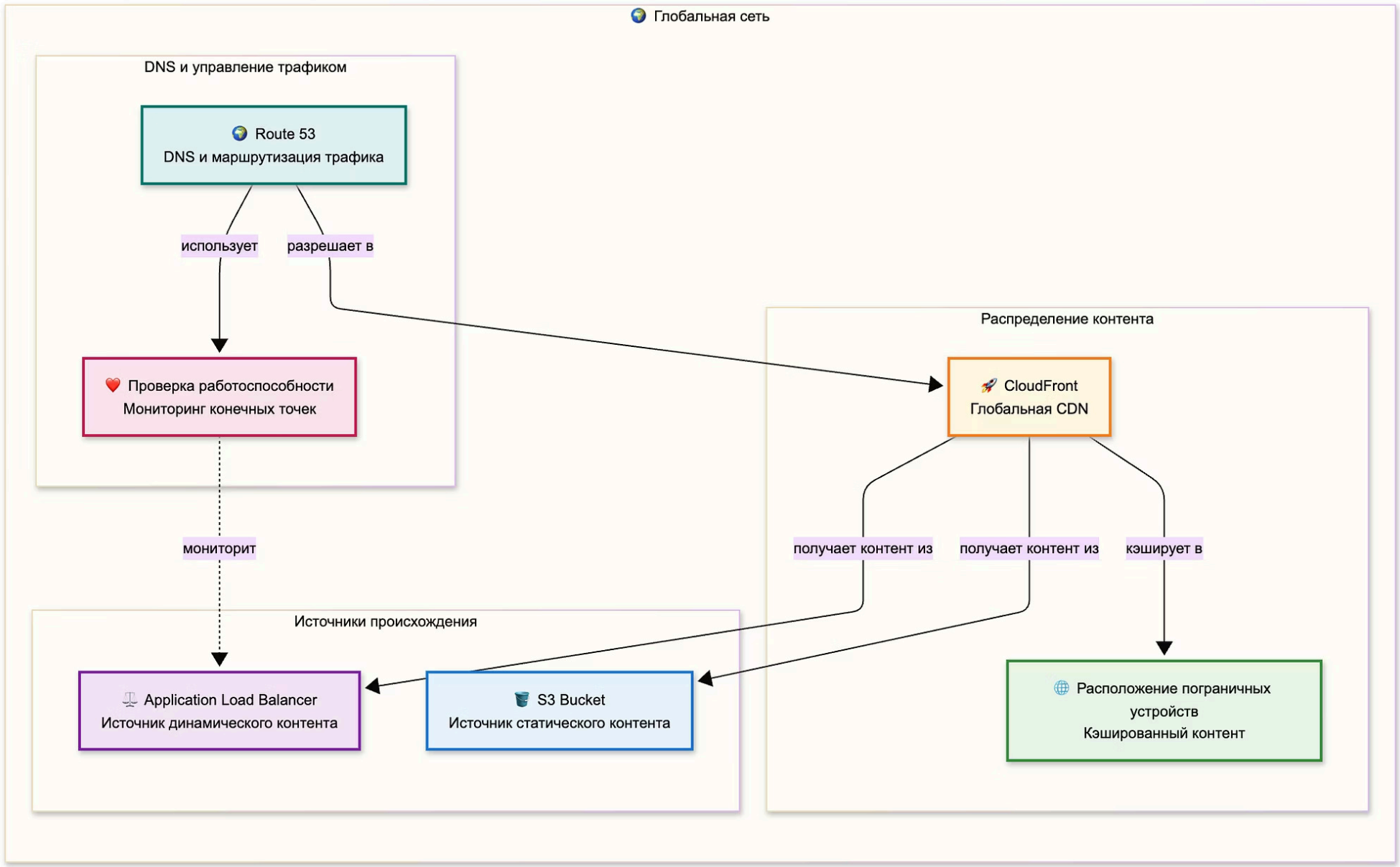
Локальные ресурсы

EC2, RDS, приложения

Глобальные сети

Amazon Route 53 предоставляет управляемые службы **DNS** с поддержкой интеллектуальной маршрутизации и проверки работоспособности ресурсов. Это позволяет направлять пользователей к ближайшим и наиболее доступным точкам приложения, обеспечивая отказоустойчивость и оптимальную производительность.

Amazon CloudFront — это **глобальная сеть доставки контента (CDN)**, которая кэширует данные на **пограничных узлах (edge locations)** по всему миру. Это сокращает задержки при загрузке и повышает скорость отклика приложений для пользователей независимо от их местоположения.



Сеть VPC

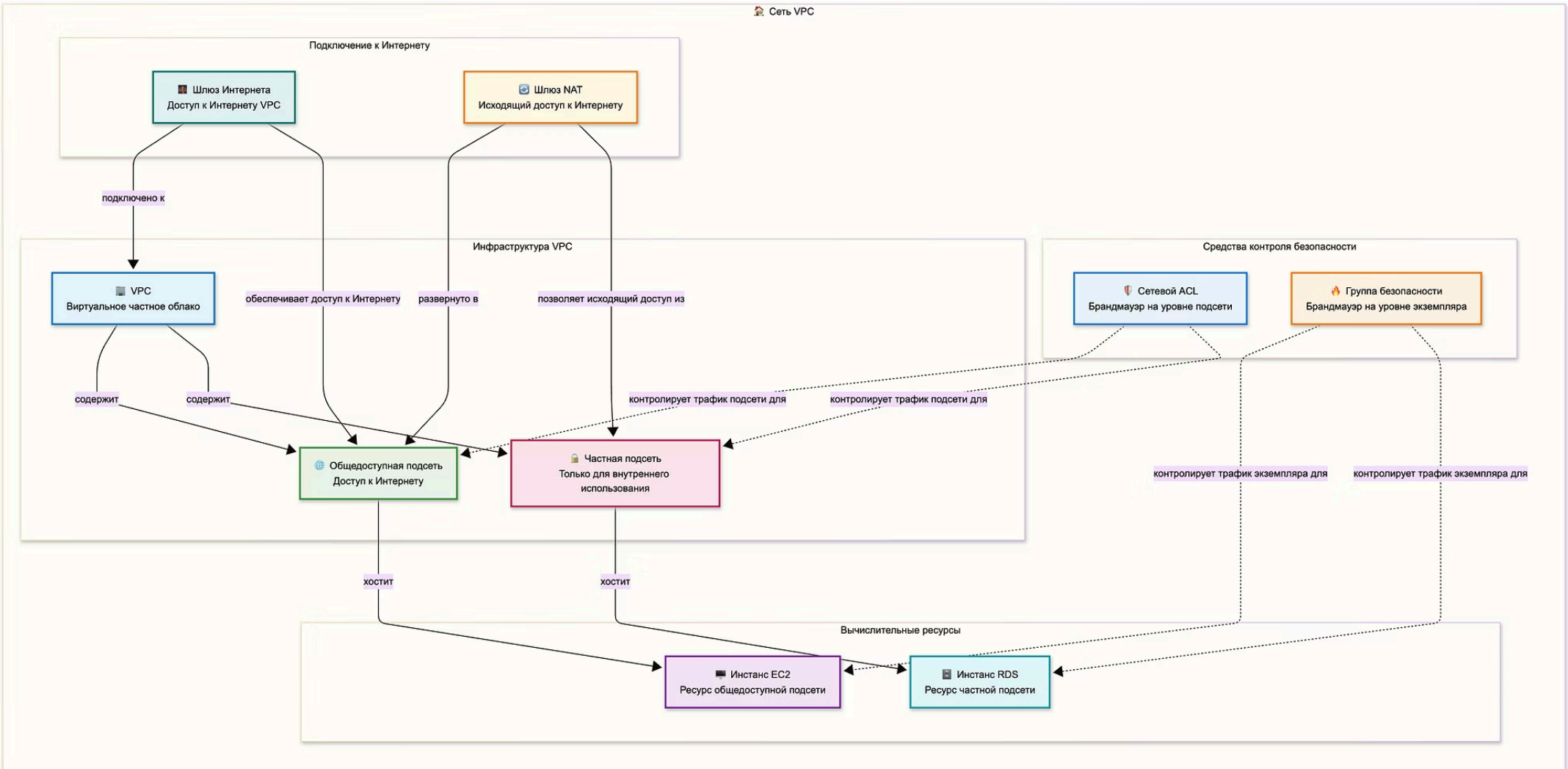
Сеть AWS построена на концепции **Virtual Private Cloud (VPC)** — виртуального частного облака, которое создаёт **изолированную сетевую среду** внутри региона AWS. В рамках VPC вы определяете диапазоны IP-адресов, создаёте подсети, маршруты и управляете подключением к Интернету.

Безопасность обеспечивается **многоуровневым контролем доступа**, включающим:

- **Security Groups** — правила для управления входящим и исходящим трафиком на уровне инстансов.
- **Network ACL (Access Control Lists)** — фильтрация трафика на уровне подсетей.
- **Route Tables** — определяют маршруты сетевого трафика внутри и за пределами VPC.

Подключение к Интернету организуется через разные механизмы:

- **Internet Gateway (IGW)** — обеспечивает выход публичных подсетей в Интернет.
- **NAT Gateway** — позволяет частным ресурсам инициировать исходящие подключения без прямого доступа из Интернета.
- **VPC Peering и Transit Gateway** — соединяют несколько VPC для безопасного обмена трафиком.


Сеть VPC
Подключение к Интернету
Шлюз Интернета
Доступ к Интернету VPC
Шлюз NAT
Исходящий доступ к Интернету
подключено к
Инфраструктура VPC
VPC
Виртуальное частное облако
обеспечивает доступ к Интернету
развернуто в
позволяет исходящий доступ из
Средства контроля безопасности
Сетевой ACL
Брандмауэр на уровне подсети
Группа безопасности
Брандмауэр на уровне экземпляра
содержит
содержит
контролирует трафик подсети для
контролирует трафик подсети для
Общедоступная подсеть
Доступ к Интернету
Частная подсеть
Только для внутреннего использования
контролирует трафик экземпляра для
контролирует трафик экземпляра для
хостит
хостит
Вычислительные ресурсы
Инстанс EC2
Ресурс общедоступной подсети
Инстанс RDS
Ресурс частной подсети

Хранение и база данных

AWS предоставляет широкий спектр сервисов для хранения данных и управления базами данных — от долговременного хранения объектов до высокопроизводительных управляемых СУБД.

Хранение данных

- **Amazon S3 (Simple Storage Service)** — объектное хранилище, обеспечивающее практически неограниченную масштабируемость и долговечность на уровне *99.999999999% (11 девяток)*. Поддерживает несколько классов хранения (Standard, Infrequent Access, Glacier), что позволяет оптимизировать стоимость под разные сценарии доступа.
- **Amazon EBS (Elastic Block Store)** — блочное хранилище для EC2-инстансов, обеспечивающее низкую задержку и высокую производительность. Подходит для баз данных, журналов транзакций и других приложений с частыми операциями чтения/записи.

Базы данных

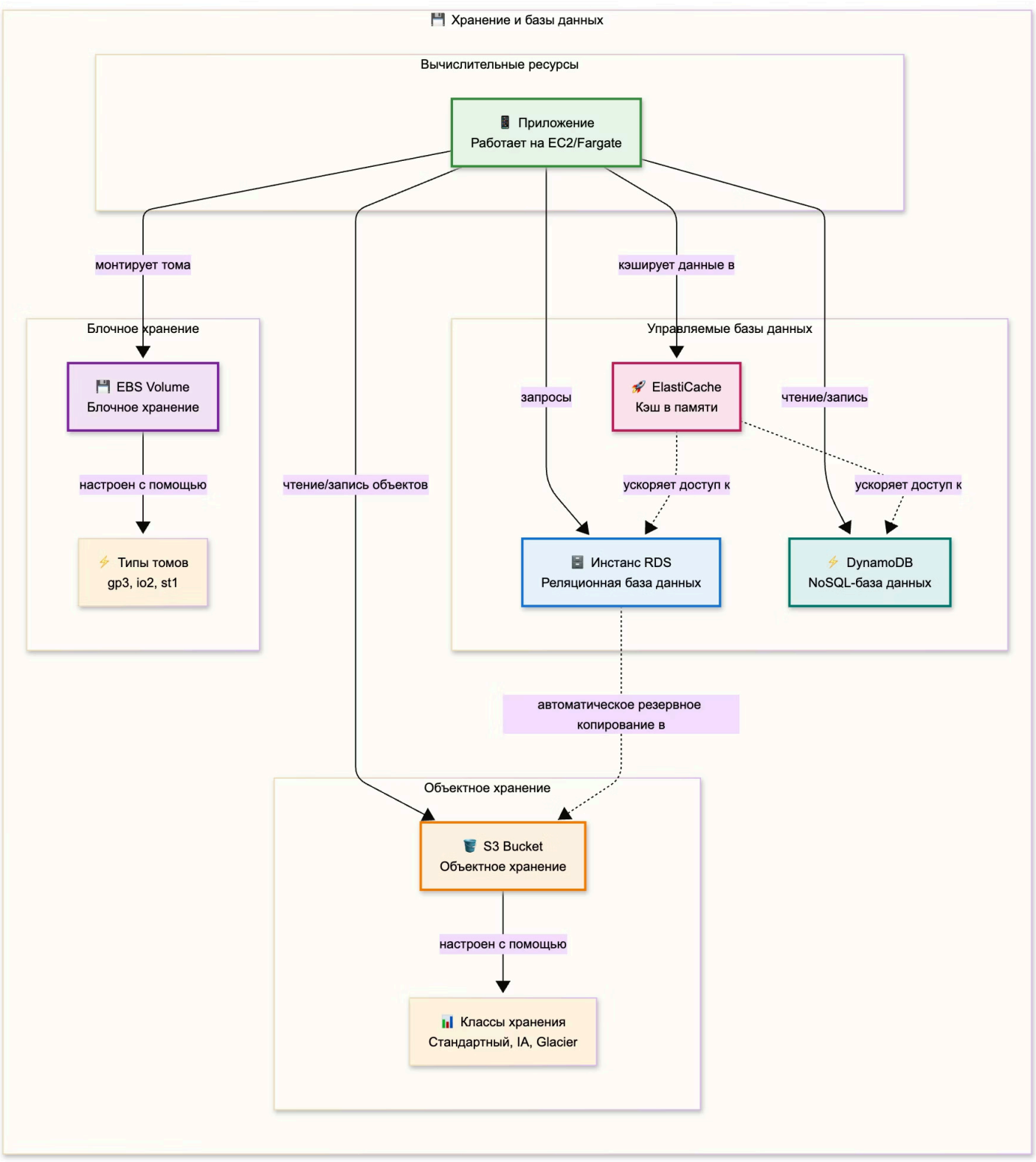
- **Amazon RDS (Relational Database Service)** — управляемая служба реляционных баз данных (MySQL, PostgreSQL, MariaDB, Oracle, SQL Server). Автоматизирует резервное копирование, патчи и масштабирование, снижая операционные затраты.
- **Amazon DynamoDB** — бессерверная NoSQL-база данных с автоматическим масштабированием и возможностью глобальной репликации для минимальной задержки доступа.
- **Amazon ElastiCache** — служба кэширования в памяти (Redis, Memcached), ускоряющая работу приложений за счёт хранения часто запрашиваемых данных в оперативной памяти.

Выбор уровня хранения

При проектировании систем хранения и баз данных важно учитывать баланс между:

- **долговечностью** (S3 — максимум надёжности для архивации и бэкапов),
- **производительностью** (EBS — высокая скорость ввода/вывода для активных данных),
- **операционными издержками** (RDS и DynamoDB — автоматизация и минимизация администрирования).

Такой подход позволяет строить гибкие и надёжные архитектуры, адаптированные под потребности приложений — от архивного хранения до высоконагруженных транзакционных систем.



Управление и администрирование

Современные распределённые системы требуют не только надёжной инфраструктуры, но и управляемости на уровне организации. **Службы управления AWS** формируют основу для этого, объединяя подходы **инфраструктуры как кода (Infrastructure as Code, IaC)**, **иерархического управления учетными записями** и **операционного контроля**.

AWS CloudFormation реализует декларативную модель управления инфраструктурой. С помощью шаблонов в формате YAML или JSON описываются ресурсы и их зависимости — от сетевых компонентов до баз данных и приложений. Такой подход обеспечивает воспроизводимость окружений, контроль версий, возможность автоматического отката и анализ изменений (drift detection). Инфраструктура становится кодом, поддающимся ревью и интеграции в CI/CD-процессы, что существенно повышает надёжность и согласованность развёртываний.

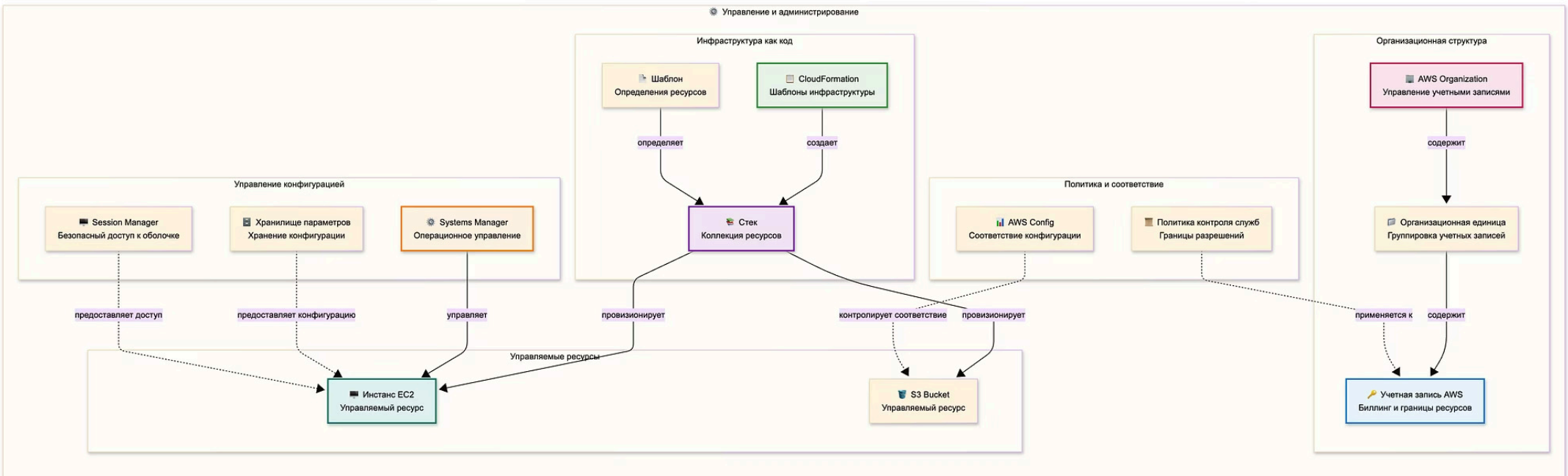
На уровне организации управление берёт на себя **AWS Organizations**. Этот сервис позволяет объединять несколько учётных записей в иерархическую структуру с консолидированным биллингом и наследованием политик. С помощью **Service Control Policies (SCP)** администраторы задают глобальные ограничения и правила безопасности, которые действуют во всех учетных записях, независимо от прав локальных администраторов. Это создаёт баланс между централизованным контролем и автономией отдельных команд.

Операционный слой реализуется через **AWS Systems Manager (SSM)** — универсальную платформу для обслуживания и контроля инфраструктуры. С её помощью можно управлять исправлениями, проверять соответствие конфигураций политикам безопасности и подключаться к инстансам через **Session Manager**, не открывая SSH-доступ. Компонент **Parameter Store** обеспечивает безопасное хранение конфигураций и секретов с возможностью интеграции в CloudFormation и другие сервисы AWS.

Таким образом, в AWS формируется трёхуровневая иерархия управления:

- **Организационный уровень (Organizations, SCP)** — стратегические границы и централизованные политики.
- **Инфраструктурный уровень (CloudFormation)** — создание и конфигурация ресурсов.
- **Операционный уровень (Systems Manager, Parameter Store)** — эксплуатация и контроль состояния.

Эта структура обеспечивает корпоративный масштаб управления инфраструктурой при сохранении гибкости и независимости отдельных команд. В системном дизайне она становится фундаментом для построения управляемых, согласованных и безопасных облачных сред.


Управление и администрирование
Инфраструктура как код
Шаблон
Определения ресурсов
CloudFormation
Шаблоны инфраструктуры
определяет
создает
Стек
Коллекция ресурсов
Организационная структура
AWS Organization
Управление учетными записями
содержит
Организационная единица
Группировка учетных записей
Управление конфигурацией
Session Manager
Безопасный доступ к оболочке
Хранилище параметров
Хранение конфигурации
Systems Manager
Операционное управление
Политика и соответствие
AWS Config
Соответствие конфигурации
Политика контроля служб
Границы разрешений
предоставляет доступ
предоставляет конфигурацию
управляет
провизионирует
контролирует соответствие
провизионирует
применяется к
содержит
Управляемые ресурсы
Инстанс EC2
Управляемый ресурс
S3 Bucket
Управляемый ресурс
Учетная запись AWS
Биллинг и границы ресурсов

Наблюдаемость и аналитика

Наблюдаемость (observability) — это ключевой элемент системного дизайна современных распределённых систем. В AWS она строится на сочетании **native-сервисов** и **сторонних решений**, которые вместе обеспечивают прозрачность, корреляцию событий и раннее обнаружение проблем.

Amazon CloudWatch является центральным компонентом экосистемы наблюдаемости. Он собирает метрики и логи со всех сервисов AWS, пользовательских приложений и системных агентов.

- **CloudWatch Metrics** — агрегирует метрики инфраструктуры (нагрузка, задержка, использование ресурсов).
- **CloudWatch Logs** — централизует журналы, позволяет выполнять поиск и строить визуализации на их основе.
- **CloudWatch Alarms и Dashboards** — обеспечивают автоматическое оповещение и визуальный контроль состояния системы.

Для глубокого анализа распределённых систем используется **AWS X-Ray**, который выполняет **трассировку запросов** через микросервисы, функции Lambda и API Gateway. Он помогает выявлять узкие места, неэффективные вызовы и ошибки в цепочке зависимостей. Интеграция X-Ray с CloudWatch создаёт сквозной контекст между метриками, логами и трассировками, что особенно ценно для корреляционного анализа.

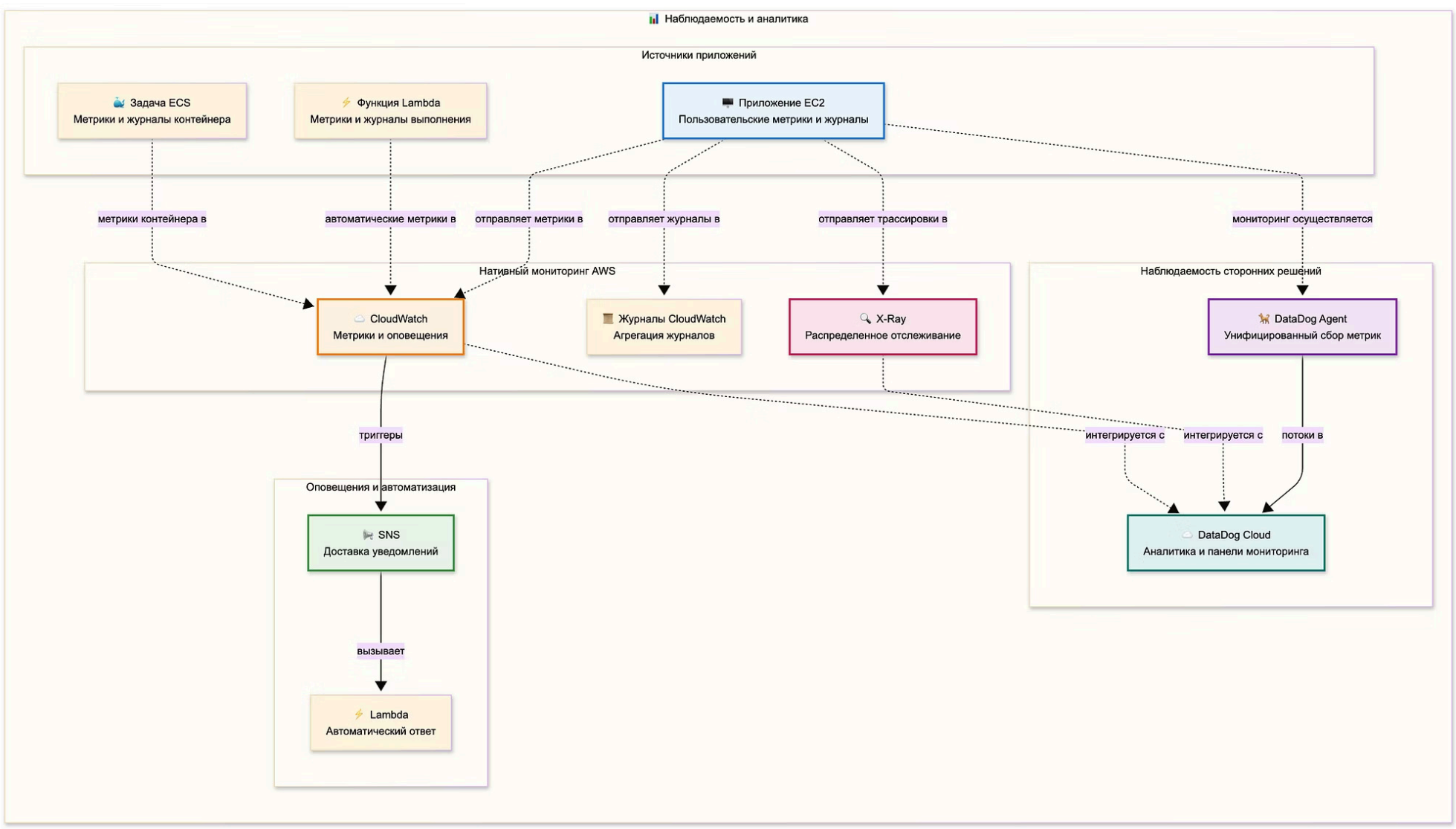
Помимо встроенных инструментов, AWS поддерживает интеграцию со сторонними платформами наблюдаемости, такими как **Datadog**, **New Relic** и **Grafana**.
В частности, **Datadog** расширяет функциональность CloudWatch за счёт:

- продвинутой аналитики метрик и логов,
- интеллектуальных оповещений,
- панелей мониторинга, объединяющих данные из AWS, приложений и сторонних систем.
  Агент Datadog собирает метрики с EC2, контейнеров, Lambda и сервисов AWS, обеспечивая **единую наблюдаемость** для гибридных и мультиоблачных архитектур.

Иерархия наблюдаемости AWS выглядит следующим образом:

1. **Сбор данных** — CloudWatch и агенты Datadog собирают метрики, логи и трассировки.
2. **Анализ и корреляция** — X-Ray и аналитические инструменты Datadog связывают данные между сервисами.
3. **Визуализация и оповещение** — CloudWatch Dashboards, Datadog и SNS уведомляют о событиях и предоставляют контекст.

Такой подход позволяет реализовать **проактивный мониторинг**: не просто фиксировать сбои, а прогнозировать проблемы до того, как они повлияют на пользователей, и использовать собранные данные для **непрерывной оптимизации производительности**.



Ключевые взаимосвязи

На приведенных выше диаграммах показано, как ресурсы AWS в каждой категории связаны друг с другом. Ниже приведены некоторые важные межкатегорийные взаимосвязи:

- **Вычислительные** службы работают в VPC **сетей** и используют ресурсы **хранения** для обеспечения постоянства
- **Политики и средства контроля безопасности** применяются ко всем категориям служб, а IAM обеспечивает основу для аутентификации
- **Службы управления**, такие как CloudFormation, предоставляют ресурсы во всех категориях с использованием инфраструктуры как кода
- Инструменты **наблюдаемости** отслеживают и собирают данные из ресурсов всех категорий служб.
- Службы **хранения** интегрированы со службами **безопасности** для шифрования и контроля доступа.
- **Сеть** обеспечивает основу для подключения, которая позволяет службам **вычислений** безопасно обмениваться данными.

Эта классификация помогает разработчикам понять, как службы AWS взаимодействуют друг с другом для создания безопасных, масштабируемых и наблюдаемых облачных приложений, сохраняя при этом операционную эффективность за счет автоматизации и управления.