Резервное копирование и восстановление с помощью AWS

Июнь 2016 г.

Уведомления

Этот документ предоставляется исключительно в информационных целях. В нем представлены текущие предложения продуктов и практики AWS, актуальные на дату публикации, которые могут меняться без предварительного уведомления. Клиентам необходимо провести собственную независимую оценку представленной в документе информации и возможности использования продуктов и услуг AWS любым способом. Указанные информация, продукты и услуги предоставляются «как есть», без какой-либо явной или подразумеваемой гарантии. Данный документ не создает никаких гарантий, контрактных обязательств и иных обязательств, условий или заверений от AWS, ее дочерних организаций, поставщиков или лицензиатов. Обязанности и финансовые обязательства AWS в отношении клиентов компании регулируются соглашениями AWS. Данный документ не является таким соглашением, а также не вносит изменения в какие-либо соглашения, заключенные между компанией AWS и ее клиентами.

Содержание

Резюме

Этот документ предназначен для специалистов по архитектуре корпоративных решений, систем резервного копирования и ИТ-администраторов, отвечающих за защиту данных в корпоративных средах. В нем описываются производственные рабочие нагрузки и архитектуры, которые можно реализовать с помощью AWS, чтобы дополнить или заменить систему резервного копирования и восстановления. Такой подход позволяет снизить расходы, улучшить масштабируемость и повысить надежность, в том числе добиться нужных показателей RTO (целевое время восстановления) и RPO (целевая точка восстановления), а также выполнить все нормативные требования.

Введение

Объем корпоративных данных стремительно растет, и защищать их становится все труднее. Часто возникают вопросы о надежности хранения и масштабировании различных методов резервного копирования, например: «Как облако может помочь с резервным копированием и архивированием?».

В этом документе рассматривается ряд архитектур резервного копирования (чистые облачные приложения, гибридные и локальные среды), а также соответствующие сервисы AWS, с помощью которых можно создавать масштабируемые и надежные решения для защиты данных.

Преимущества использования AWS в качестве платформы защиты данных

Amazon Web Services (AWS) – это безопасная, высокопроизводительная, гибкая, рентабельная и простая в использовании облачная платформа. Система AWS выполняет все самые сложные задачи, а также предоставляет инструменты и ресурсы для создания масштабируемых решений резервного копирования и восстановления.

Применяя AWS в качестве решения для защиты данных, вы получаете множество преимуществ.

- **Надежность хранения.** Amazon Simple Storage Service (Amazon S3) и Amazon Glacier гарантируют надежность хранения 99,999999999 % (11 девяток). Обе эти платформы предоставляют безопасные ресурсы для резервного копирования данных.
- **Безопасность.** Платформа AWS предоставляет ряд вариантов для управления доступом к данным и их шифрования при передаче и хранении.
- **Глобальная инфраструктура.** Сервисы AWS доступны во всем мире, поэтому вы сможете создавать резервные копии и хранить данные в том регионе, который соответствует вашим требованиям.
- **Соответствие требованиям.** Инфраструктура AWS сертифицирована по таким стандартам, как SOC, SSAE 16, ISO 27001, PCI DSS, HIPPA, SEC[1] и FedRAMP, поэтому вы легко сможете настроить данное решение резервного копирования в соответствии с существующей системой соблюдения требований.
- **Масштабируемость.** При использовании AWS вам не нужно будет волноваться о емкости систем. Вы сможете масштабировать ресурсы при изменении потребностей без административных расходов.
- **Снижение совокупной стоимости владения.** Масштабирование операций AWS снижает затраты на обслуживание и совокупную стоимость владения для систем хранения. Благодаря этому уменьшаются и цены на сервисы AWS для клиентов.
- **Оплата по мере использования.** Приобретайте сервисы AWS, когда они вам необходимы, и платите только за период, когда вы планируете их использовать. Никаких авансовых платежей, штрафов за прекращение использования или долгосрочных контрактов.

[1] https://aws.amazon.com/about-aws/whats-new/2015/09/amazon-glacier-receives-third-party-compliance-assessment-for-sec-rule-17a-4f-from-cohasset-associates-inc/

Сервисы хранения AWS для защиты данных

Amazon S3 и Amazon Glacier – это идеальные сервисы для резервного копирования и архивации. Это надежные и недорогие платформы хранения. Емкость систем не ограничена, а при увеличении объема данных вам не придется самостоятельно управлять томами или носителями. Благодаря модели оплаты по мере использования и низкой стоимости хранения эти сервисы станут прекрасным инструментом для защиты ваших данных.

Amazon S3

Amazon S3 – это безопасное и масштабируемое хранилище объектов.

Вы можете использовать Amazon S3 для хранения и извлечения любых объемов данных в любое время из любого места сети. В Amazon S3 данные хранятся как объекты в ресурсах, которые называют *корзинами*. AWS Storage Gateway и многие сторонние решения резервного копирования могут управлять объектами Amazon S3 от вашего имени. Вы можете хранить в корзине любое количество объектов, для которых возможны операции записи, чтения и удаления. Размер одного объекта может составлять до 5 ТБ.

Amazon S3 предоставляет широкий спектр классов хранилища для различного применения, в том числе:

- **Amazon S3 Standard** – хранилище часто используемых данных общего назначения;
- **Amazon S3 Standard – Infrequent Access** – для длительного хранения реже используемых данных;
- **Amazon Glacier** – архив для долгосрочного хранения.

Amazon S3 также предоставляет политики жизненного цикла, которые можно настроить для управления данными в течение их жизненного цикла. После настройки политики ваши данные будут перемещены в соответствующий класс хранилища, при этом изменять ваше приложение не нужно. Дополнительные сведения см. в разделе Классы хранилища S3.

Amazon Glacier

Amazon Glacier – это очень дешевый облачный сервис для безопасного и надежного хранения архивных данных с возможностью оперативного резервного копирования. Низкий уровень цен обеспечен тем, что хранилище Amazon Glacier оптимизировано для данных, доступ к которым осуществляется редко и для которых время выдачи в несколько часов является приемлемым. С помощью Amazon Glacier можно безопасно хранить большие и малые объемы данных по цене всего 0,007 USD за гигабайт в месяц, что намного выгоднее локальных решений. Amazon Glacier прекрасно подходит для длительного или бессрочного хранения резервных копий и долгосрочного архивирования данных. Дополнительные сведения см. в разделе Amazon Glacier.

AWS Storage Gateway

AWS Storage Gateway соединяет локальное программное обеспечение с облачным хранилищем для простой и безопасной интеграции вашей локальной ИТ-среды и инфраструктуры хранилища AWS. Дополнительные сведения см. в разделе AWS Storage Gateway.

Сервисы AWS для передачи данных

Помимо сторонних шлюзов и соединителей, вы можете использовать такие сервисы AWS, как AWS Direct Connect, AWS Snowball, AWS Storage Gateway и Amazon S3 Transfer Acceleration, чтобы быстро передавать данные. Дополнительные сведения см. в разделе Миграция данных в облако.

Проектирование решения для резервного копирования и восстановления

При разработке комплексной стратегии резервного копирования и восстановления данных сначала необходимо определить вероятные сбои или аварийные ситуации и оценить их возможное влияние на бизнес. В некоторых отраслях следует учитывать нормативные требования по обеспечению безопасности данных, конфиденциальности и хранения записей.

Вам необходимо реализовать процессы резервного копирования с соответствующим уровнем детализации для достижения показателей RTO и RPO, в том числе:

- восстановление на уровне файлов;
- восстановление на уровне томов;
- восстановление на уровне приложений (например, баз данных);
- восстановление на уровне образов.

В следующих разделах описываются подходы для резервного копирования, восстановления и архивации, основанные на организации вашей инфраструктуры. ИТ-инфраструктуру можно классифицировать как облачную, локальную и гибридную.

Чистая облачная инфраструктура

В этом сценарии описывается среда, которая полностью размещена в AWS. Как показано на следующем рисунке, она содержит веб-серверы, серверы приложений, серверы мониторинга, базы данных и каталог Active Directory.

Если все ваши сервисы размещены в AWS, вы можете использовать множество встроенных функций для защиты и восстановления данных.

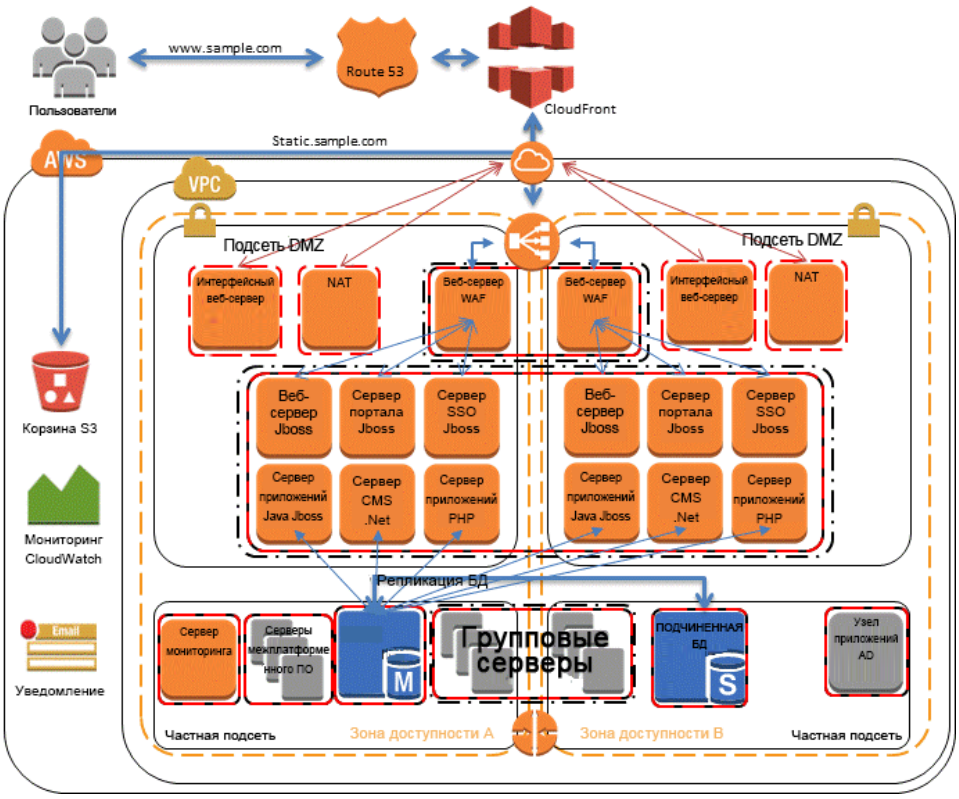

Рис. 1. Все сервисы находятся в AWS

Защита на основе снимков состояния EBS

Если сервисы работают в Amazon Elastic Compute Cloud[2] (Amazon EC2), вычислительные инстансы могут использовать тома Amazon Elastic Block Store (Amazon EBS) для хранения основных данных и доступа к ним. В этом блочном хранилище можно размещать структурированные данные, такие как базы данных, и неструктурированные данные, например файлы в файловой системе тома.

Amazon EBS позволяет создавать снимки состояния (резервные копии) любого тома Amazon EBS. Сервис создает копию тома и помещает его в Amazon S3, где она хранится с избыточностью в нескольких зонах доступности. Первый снимок – это полная копия тома, а в последующих снимках хранятся только инкрементные изменения на уровне блоков.

Это быстрый и надежный способ восстановления всех данных тома. Если вам нужно восстановить только часть данных, вы можете присоединить том к запущенному инстансу с другим именем устройства, подключить его и с помощью команд операционной системы скопировать данные из тома резервной копии на рабочий том.

Снимки состояния Amazon EBS также можно копировать между регионами AWS, используя функции копирования снимков Amazon EBS, доступные в консоли и в командной строке, как описано в руководстве пользователя Amazon Elastic Cloud Compute.[3] С помощью этой функции вы можете сохранить резервную копию в другом регионе, не настраивая базовые технологии репликации.

---

[2] http://aws.amazon.com/ec2/

[3] http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-copy-snapshot.html

Создание снимков состояния EBS

При создании снимков состояния вы защищаете свои данные, размещая их в надежном дисковом хранилище. Чтобы создать снимок состояния Amazon EBS, вы можете использовать консоль управления AWS, интерфейс командной строки (CLI) или API-интерфейсы.

В консоли Amazon EC2 на странице **Elastic Block Store Volumes** выберите **Create Snapshot** в меню **Actions**. В диалоговом окне **Create Snapshot** выберите **Create**, чтобы создать снимок, который будет сохранен в Amazon S3.

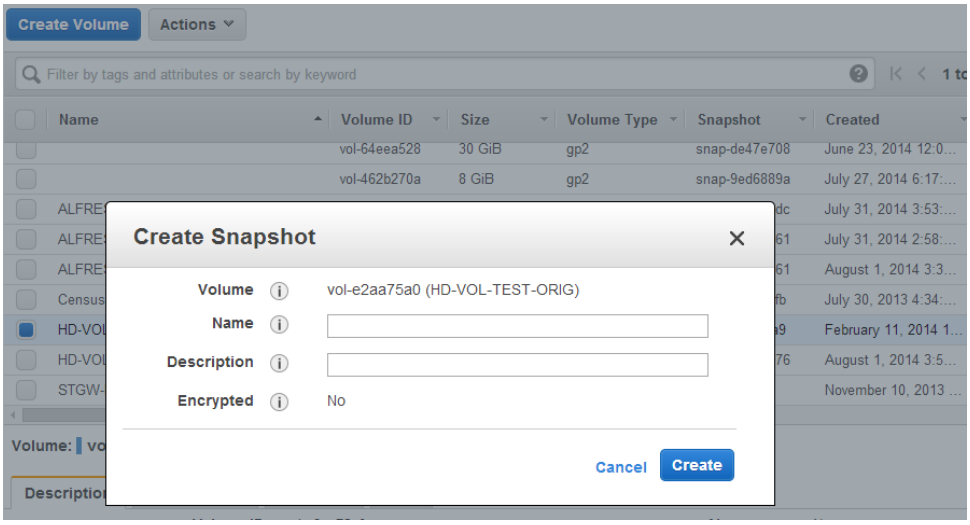

Рис. 2. Использование консоли EC2 для создания снимка состояния

Чтобы с помощью командной строки создать снимок состояния, выполните следующую команду:

```
➢  aws ec2 create-snapshot
```

Вы можете запланировать регулярное выполнение команд `aws ec2 create-snapshot` для создания резервных копий данных EBS. Низкая стоимость использования Amazon S3 позволяет хранить многие поколения данных. Так как снимки основаны на блоках, вы будете потреблять пространство только для данных, которые изменились после создания первого снимка состояния.

Восстановление данных из снимка состояния EBS

Чтобы восстановить данные из снимка состояния, вы можете использовать консоль управления AWS, интерфейс командной строки (CLI) или API-интерфейсы для создания тома на основе существующего снимка.

Например, выполните следующие действия, чтобы восстановить том из ранней резервной копии.

1. Выполните следующую команду, чтобы создать том из резервного снимка состояния:

```
➢ aws ec2 create-volume –region us-west-1b –snapshot-
  id mysnapshot-id
```

2. Отключите существующий том на инстансе Amazon EC2.

   В Linux используйте команду `umount`. В Windows воспользуйтесь диспетчером логических томов (LVM).

3. Выполните следующую команду, чтобы отсоединить существующий том от инстанса:

```
➢ aws ec2 detach-volume –volume-id oldvolume-id –
  instance-id myec2instance-id
```

4. Выполните следующую команду, чтобы присоединить том, созданный из снимка состояния:

```
➢ aws ec2 attach-volume –volume-id newvolume-id
  –instance-id myec2instance-id –device /dev/sdf
```

5. Повторно подключите том на запущенном инстансе.

Создание согласованных или «горячих» резервных копий

Во время резервного копирования не рекомендуется выполнять операции ввода-вывода. В идеальной ситуации машина вообще не должна принимать трафик, но это происходит все реже, так как ИТ-операции выполняются практически круглосуточно.

Поэтому для создания корректной резервной копии необходимо приостановить файловую систему или базу данных. То, как вы это сделаете, зависит от базы данных или файловой системы.

Для базы данных используется следующий процесс.

- Если возможно, переведите базу данных в режим горячего резервного копирования.
- Выполните команды Amazon EBS для создания снимка состояния.
- Выйдите из режима горячего резервного копирования или, если используется реплика чтения, завершите работу инстанса реплики чтения.

Для файловой системы применяется аналогичный процесс, но он зависит от операционной или файловой системы. Например, файловая система XFS может сбрасывать данные для получения согласованной резервной копии. Дополнительные сведения см. в разделе xfs_freeze.[4]

Если файловая система не поддерживает приостановку работы, отключите ее, выполните команду создания снимка состояния и повторно подключите файловую систему. Или же вы можете использовать диспетчер логических томов, который поддерживает заморозку ввода-вывода.

Так как процесс создания снимка продолжается в фоновом режиме и выполняется довольно быстро (записываются данные только определенной точки во времени), отсоединить тома нужно всего на несколько секунд. Поскольку окно резервного копирования небольшое, насколько это возможно, время простоя можно прогнозировать и планировать.

---

[4] https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Storage_Administration_Guide/xfsfreeze.html

Создание многотомных резервных копий

В некоторых случаях можно распределить данные по нескольким томам Amazon EBS с помощью диспетчера логических томов, чтобы повысить пропускную способность. При использовании диспетчера логических томов (например, mdadm или LVM) важно создать резервную копию на уровне диспетчера томов, а не на уровне томов EBS. При этом все метаданные и тома субкомпонентов будут согласованы.

Этого можно добиться несколькими способами. Например, можно использовать скрипт, созданный alestic.com[5]. Вам необходимо сбросить буферы памяти на диск, остановить ввод-вывод файловой системы на диск и одновременно создать снимок состояния для всех томов, из которых состоит набор RAID. После создания снимка для томов (обычно через одну или две секунды) файловая система может продолжить работу. Снимки состояния следует отметить, чтобы управлять ими коллективно во время восстановления.

Вы также можете выполнить резервное копирование на уровне диспетчера логических томов или файловой системы. В этом случае с помощью традиционного агента резервного копирования можно перемещать данные по сети. В Интернете и в AWS Marketplace доступно несколько решений резервного копирования на основе агентов.[6] Помните, что подобному программному обеспечению требуются согласованное имя и IP-адрес сервера. Поэтому использование этих инструментов с инстансами, развернутыми в виртуальном частном облаке (VPC)[7] Amazon – это лучший способ добиться надежности.

Альтернативный подход – создать реплику основных томов системы, которые размещены на одном большом томе. Это упрощает резервное копирование, поскольку нужно создать копию одного тома, а процесс происходит вне основной системы. Однако сначала следует определить, сможет ли этот том поддерживать достаточную производительность во время резервного копирования и подходит ли максимальный размер тома для приложения.

---

[5] https://github.com/alestic/ec2-consistent-snapshot

[6] https://aws.amazon.com/marketplace/

[7] http://aws.amazon.com/vpc/

Подходы для резервного копирования баз данных

Платформа AWS предоставляет множество возможностей для баз данных. Вы можете запустить собственную базу данных на инстансе EC2 или использовать один из управляемых сервисов баз данных Amazon Relational Database Service [8](Amazon RDS). Если база данных запущена на инстансе EC2, вы можете копировать данные в файлы с помощью собственных инструментов (например, MySQL[9], Oracle[10], MSSQL[11], PostgreSQL[12]) или можете создать снимок состояния томов, содержащих данные, с помощью одного из методов, описанных в разделе Защита на основе снимков состояния EBS.

Использование резервных копий реплик баз данных

Для баз данных, использующих RAID-наборы томов Amazon EBS, можно создать реплику для чтения, что позволит отказаться от резервного копирования основной базы данных. Это актуальная копия базы данных, которая работает на отдельном инстансе Amazon EC2. Инстанс базы данных реплики можно создать с использованием нескольких дисков, как у источника, или же данные можно объединить в одном томе EBS. Затем вы сможете воспользоваться одной из процедур, описанных в разделе «Защита на основе снимков состояния EBS» для создания снимков томов EBS. Такой подход часто используется для больших баз данных, которые должны быть доступны круглосуточно. В этом случае требуемое окно резервного копирования слишком длительное, а производственную базу данных попросту невозможно приостановить на такой период.

---

[8] https://aws.amazon.com/rds/

[9] http://dev.mysql.com/doc/refman/5.7/en/backup-and-recovery.html

[10] http://docs.oracle.com/cd/E11882_01/backup.112/e10642/rcmbckba.htm#BRADV8003

[11] http://msdn.microsoft.com/en-us/library/ms187510.aspx

[12] http://www.postgresql.org/docs/9.3/static/backup.html

Использование Amazon RDS для резервного копирования

Amazon RDS предоставляет функции для автоматизации резервного копирования баз данных. Amazon RDS создает снимок состояния тома хранилища для вашего инстанса базы данных, копируя весь инстанс, а не отдельные базы данных.

Amazon RDS предоставляет два разных метода резервного копирования и восстановления инстансов базы данных.

- **Автоматическое резервное копирование** дает возможность восстановления инстанса на момент времени. После создания инстанса базы данных автоматическое резервное копирование включено по умолчанию. Amazon RDS выполняет ежедневное резервное копирование данных во время, заданное при создании инстанса. Вы можете настроить период хранения автоматически созданных резервных копий (максимальное значение – 35 дней). Amazon RDS использует эти периодические резервные копии вместе с журналами транзакций, чтобы восстановить инстанс базы данных на любой момент периода хранения (с точностью до секунды) вплоть до значения параметра `LatestRestorableTime` (обычно это последние пять минут). Чтобы найти последний момент времени, доступный для восстановления инстансов, можно использовать вызов API `DescribeDBInstances` или вкладку **Description** базы данных в консоли управления AWS.

  После начала восстановления на момент времени журналы транзакций применяются к соответствующей ежедневной резервной копии, чтобы восстановить запрошенный инстанс базы данных.

- **Снимки состояния базы данных** – это резервные копии, инициируемые пользователем, позволяющие копировать инстанс базы данных в известном состоянии с любой частотой, а затем восстановить его в этом состоянии. Для создания снимков состояния базы данных можно использовать консоль управления AWS или вызов API `CreateDBSnapshot`. Эти снимки могут храниться бессрочно, пока вы не воспользуетесь консолью или вызовом API `DeleteDBSnapshot`, чтобы явно их удалить.

При восстановлении базы данных на момент времени или из снимка состояния, создается новый инстанс базы данных с новой конечной точкой. Таким образом можно создать несколько инстансов из определенного снимка состояния или для определенного момента времени.

Вы можете использовать консоль управления AWS или вызов API `DeleteDBInstance`, чтобы удалить старый инстанс базы данных.

Использование AMI для резервного копирования инстансов EC2

В AWS системные образы хранятся в Amazon Machine Images (AMI). Эти образы состоят из шаблона для корневого тома, необходимого для запуска инстанса. Чтобы создать резервную копию корневого тома в AMI, вы можете использовать консоль управления AWS или команду `aws ec2 create-image` CLI.

Рис. 3. Использование AMI для резервного копирования и запуска инстанса

При регистрации AMI образ хранится в вашем аккаунте с использованием снимков состояния Amazon EBS. Эти снимки размещаются в Amazon S3 с высоким уровнем надежности.

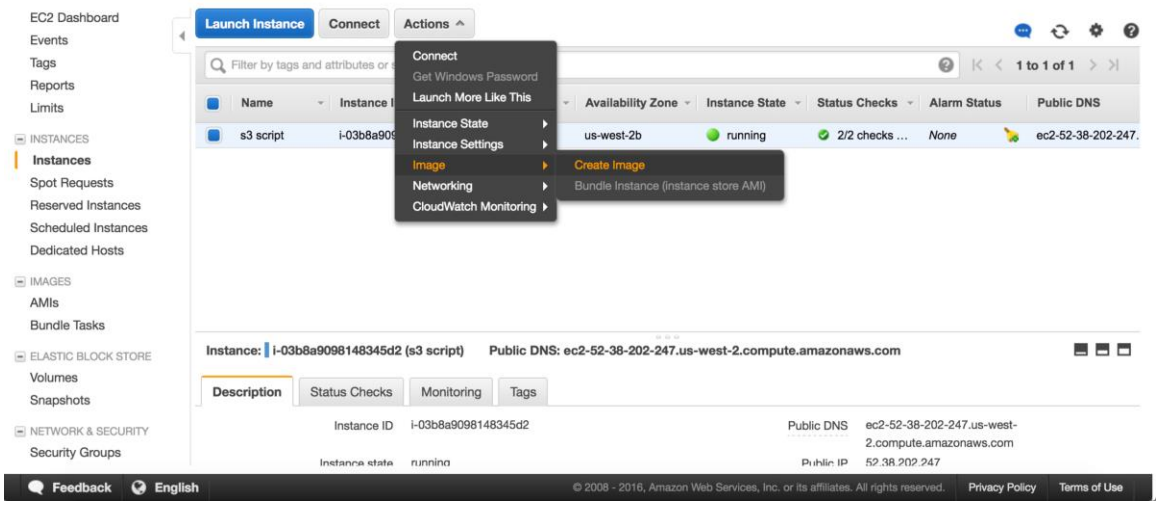

Рис. 4. Использование консоли EC2 для создания образа машины

После создания образа AMI для инстанса Amazon EC2 вы можете с помощью AMI повторно создать инстанс или запустить его дополнительные копии. Вы также можете скопировать образы AMI из одного региона в другой для переноса приложения или аварийного восстановления.

Локальная инфраструктура и AWS

В этом сценарии описывается среда, ни один компонент которой не находится в облаке. Все ресурсы, в том числе веб-серверы, серверы приложений, серверы мониторинга, базы данных, Active Directory и другие, размещаются в центре обработки данных клиента или в среде колокации.

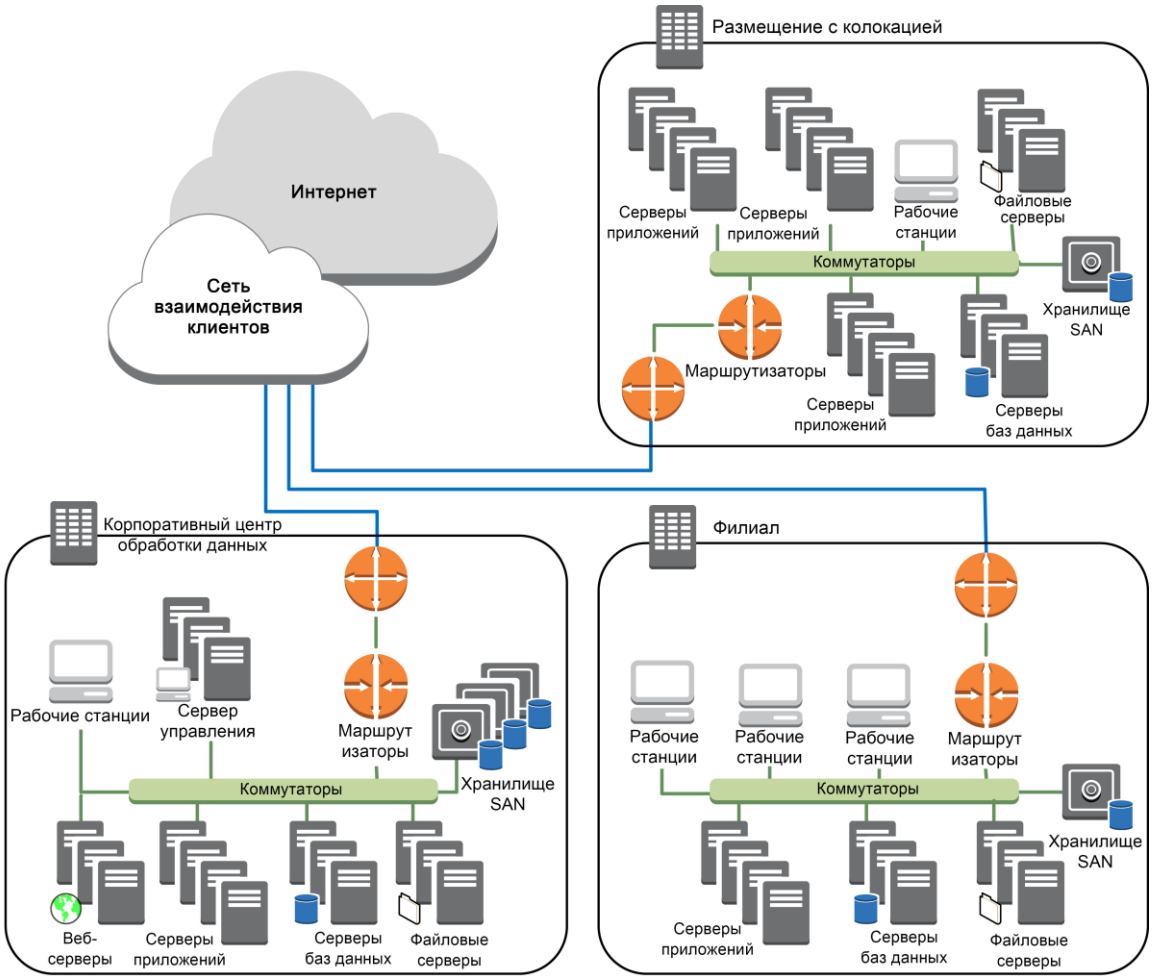

Рис. 5. Локальная среда

Используя сервисы хранения AWS в этом сценарии, вы можете сконцентрироваться на задачах резервного копирования и архивации. Вам не нужно будет переживать из-за масштабирования хранилища или емкости инфраструктуры для выполнения резервного копирования.

Amazon S3 и Amazon Glacier предоставляют нужные API-интерфейсы и доступны через Интернет. Это позволяет поставщикам программного обеспечения напрямую интегрировать свои приложения с решениями для хранения AWS, как показано на следующем рисунке.

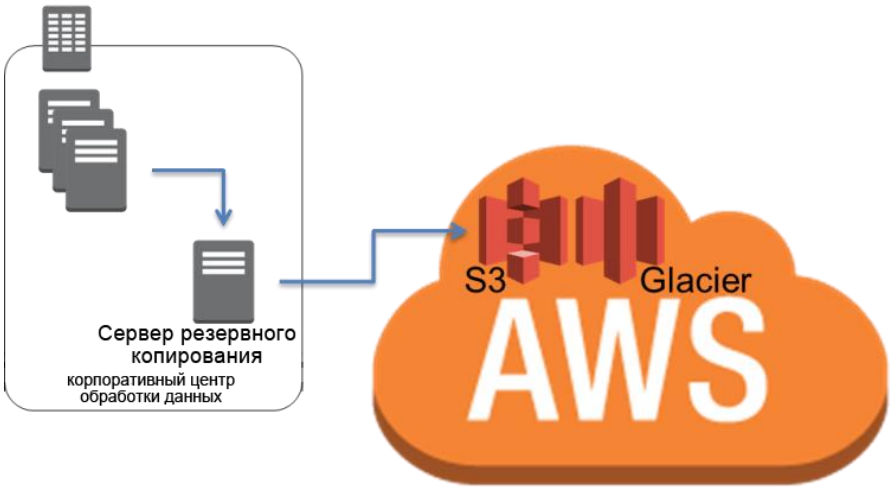

Рис. 6. Соединитель резервного копирования для Amazon S3 или Amazon Glacier

В этом сценарии решение резервного копирования и архивации напрямую взаимодействуют с AWS посредством API. Так как решение поддерживает AWS, оно скопирует данные с локальных серверов непосредственно в Amazon S3 или Amazon Glacier.

Если существующее программное обеспечение резервного копирования не поддерживает облако AWS, вы можете использовать AWS Storage Gateway. AWS Storage Gateway[13] – это виртуальное устройство для простой и безопасной интеграции вашего центра обработки данных и инфраструктуры хранилища AWS. Этот сервис позволяет безопасно хранить данные в облаке AWS, используя его как масштабируемое и рентабельное хранилище. Storage Gateway поддерживает общепринятые протоколы хранения, которые работают с существующими приложениями, а также надежно хранят все ваши данные в зашифрованном виде в Amazon S3 или Amazon Glacier.

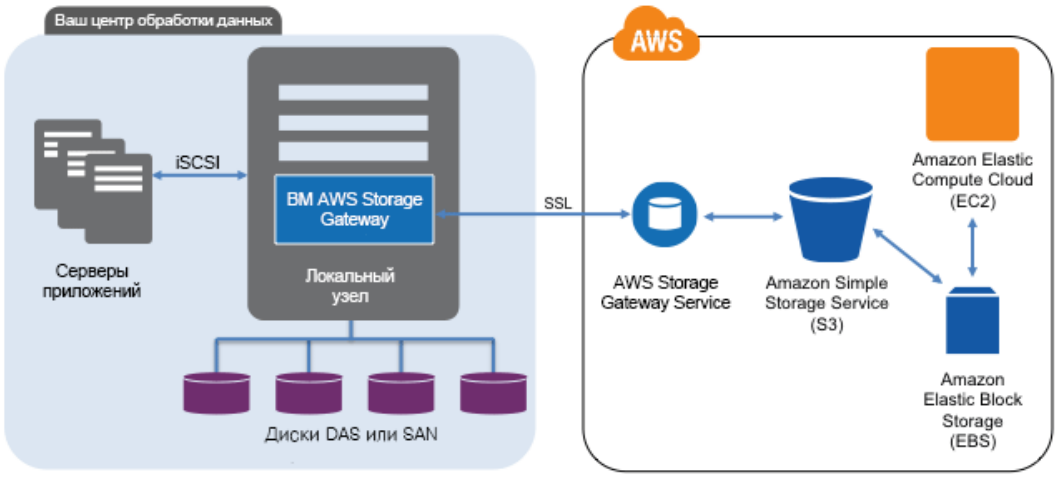

Рис. 7. Соединение локальной среды с хранилищем AWS Storage

AWS Storage Gateway поддерживает следующие конфигурации.

- **Шлюзы томов:** это тома с облачными резервными копиями, которые можно подключить как iSCSI-устройства с локальных серверов приложений. Шлюз поддерживает следующие конфигурации томов.

[13] http://aws.amazon.com/storagegateway/

  - **Тома с кэшем на шлюзе:** вы можете хранить основные данные в Amazon S3, а часто используемые данные – локально. Тома с кэшем на шлюзе позволяют существенно снизить расходы на первичное хранилище, свести к минимуму масштабирование хранилища в локальной среде и обеспечить низкую задержку при доступе к часто используемым данным.
  - **Тома, хранимые на шлюзе:** если вам необходим скоростной доступ ко всему набору данных, вы можете настроить локальный шлюз данных, чтобы хранить основные данные локально и асинхронно создавать резервные копии снимков состояния этих данных на момент времени в Amazon S3. Тома, хранимые на шлюзе – это надежные и недорогие внешние резервные копии, которые можно восстановить локально или из Amazon EC2.
- **Gateway-VTL:** это решение дает вам неограниченную коллекцию виртуальных лент. Каждую ленту можно хранить в библиотеке виртуальных лент с резервным копированием в Amazon S3 или на полке виртуальных лент с резервным копированием в Amazon Glacier. Библиотека виртуальных лент предоставляет стандартный интерфейс iSCSI, с помощью которого ваше приложение резервного копирования сможет получить доступ к виртуальным лентам. Если вам больше не требуется скоростной или частый доступ к данным на виртуальной ленте, вы можете использовать приложение резервного копирования, чтобы переместить их из библиотеки виртуальных лент на полку виртуальных лент и еще сильнее снизить расходы на хранение данных.

Эти шлюзы действуют как устройства Plug-and-Play с интерфейсом iSCSI, которые можно встроить в вашу систему резервного копирования или архивации. Вы можете использовать эти iSCSI-диски как пулы носителей для системы резервного копирования или как библиотеку gateway-VTL, чтобы перенести все задачи резервного копирования и архивации напрямую в Amazon S3 или Amazon Glacier.

При использовании этого метода резервные копии и архивы автоматически размещаются во внешней среде (для соответствия требованиям) и хранятся на надежном носителе, а вы избавляетесь от всех рисков безопасности, связанных с управлением внешними лентами.

Гибридные среды

Две описанные конфигурации инфраструктуры, чистая облачная и локальная, можно объединить в гибридной среде, в которой используются и локальные компоненты, и компоненты инфраструктуры AWS. Ресурсы, в том числе веб-серверы, серверы приложений, серверы мониторинга, базы данных, каталог Active Directory и т. д., размещаются в центре обработки данных клиента или в AWS. Приложения, работающие в облаке AWS, подключаются к приложениям, запущенным в локальной среде.

Такой сценарий все чаще применяется в корпоративных средах. Многие предприятия используют собственные центры обработки данных и AWS для увеличения объема ресурсов. Эти центры обработки данных клиентов зачастую подключены к сети AWS по высокоскоростным каналам. Например, с помощью AWS Direct Connect[14] можно установить частное подключение из локальной среды к AWS. При этом вы получите достаточную полосу пропускания и низкую задержку для передачи данных в облако. Также гарантируется их защита, высокий уровень производительности и малая задержка для гибридных рабочих нагрузок.

[14] http://aws.amazon.com/directconnect/

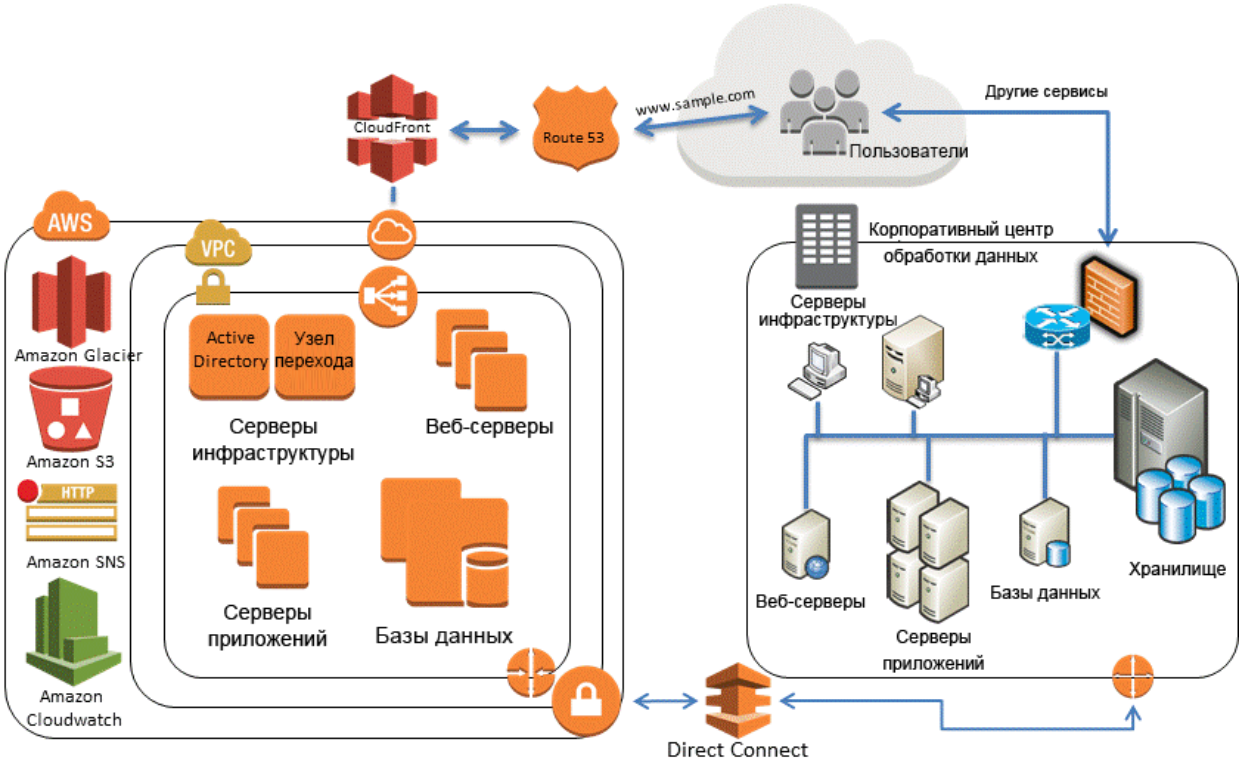

Рис. 8. Гибридная инфраструктура

Эффективно спроектированные решения защиты данных обычно используют комбинацию методов, описанных для облачных и локальных решений.

Резервное копирование приложений на основе AWS в центре обработки данных

Если вы уже используете платформу для резервного копирования локальных серверов, вы легко сможете подключить ее к ресурсам AWS с помощью VPN-подключения или AWS Direct Connect. Вы можете установить агент резервного копирования на инстансах Amazon EC2 и создавать их резервные копии в соответствии с политиками защиты данных.

Перенос задач управления резервным копированием в облако для повышения уровня доступности

В зависимости от архитектуры резервного копирования вы можете использовать основной сервер резервного копирования и один или несколько серверов мультимедиа или хранилища, размещенных в локальной среде с защищаемыми сервисами. В этом случае вы можете перенести основной сервер резервного копирования в инстанс Amazon EC2, чтобы защитить его от локальных аварий, и использовать высокодоступную инфраструктуру резервного копирования.

Для управления потоками данных резервного копирования также можно создать один или несколько серверов мультимедиа на инстансах Amazon EC2. Серверы мультимедиа на инстансах Amazon EC2 сэкономят вам деньги на передаче данных при резервном копировании в S3 или Amazon Glacier и повысят общую производительность резервного копирования и восстановления.

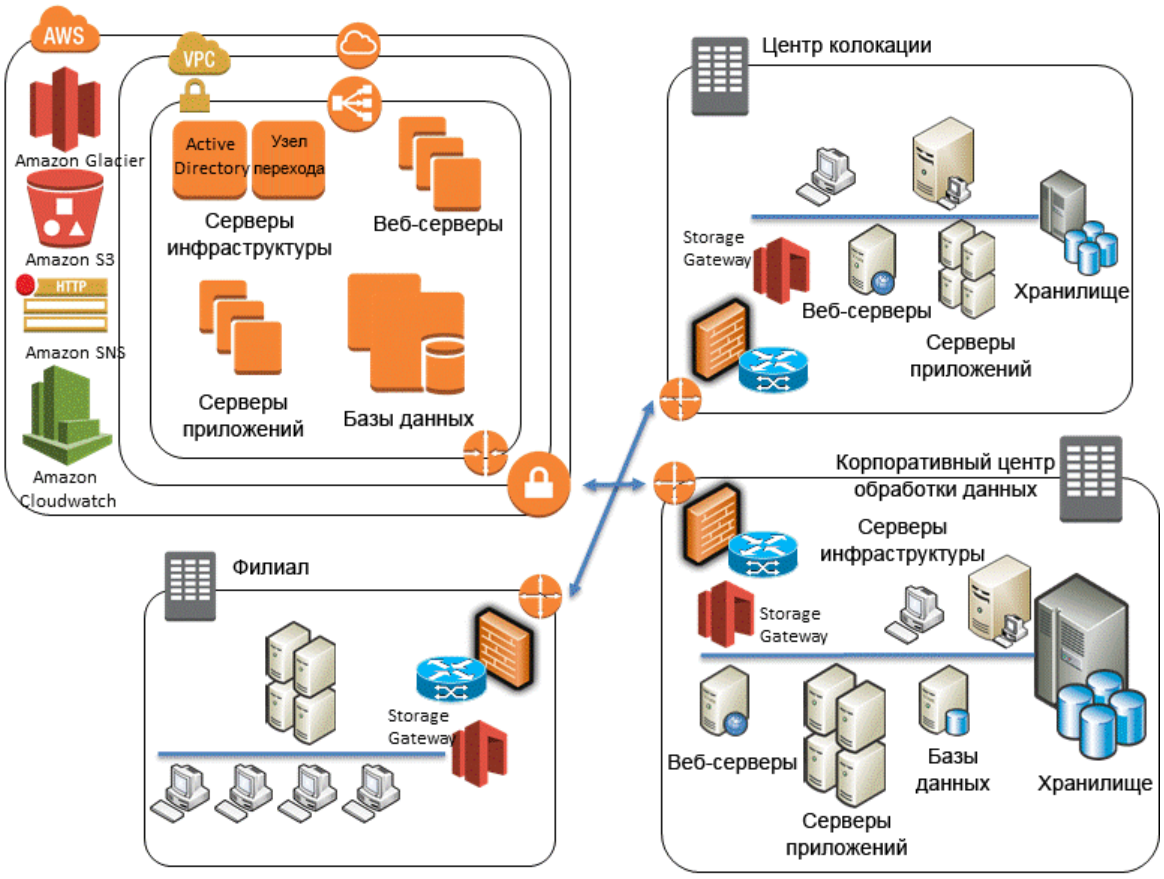

Рис. 9. Использование шлюзов в гибридном сценарии

Пример гибридного сценария

Предположим, что вы управляете средой, в которой создаются резервные копии инстансов Amazon EC2, автономных серверов, виртуальных машин и баз данных. В среде 1000 серверов, и вы создаете резервные копии операционной системы, файлов, образов виртуальных машин и баз данных. Всего необходимо создать копии 20 баз данных MySQL, Microsoft SQL Server и Oracle.

Ваше программное обеспечение резервного копирования использует агенты, которые создают копии операционной системы, файлов, образов виртуальных машин, томов данных, баз данных SQL Server и Oracle (с помощью RMAN). Для таких приложений, как MySQL, для которых агент отсутствует, можно использовать клиентскую программу mysqldump, чтобы создать дамп базы данных на диске, где стандартные агенты смогут защитить данные.

Для обеспечения безопасности этой среды стороннее решение резервного копирования, скорее всего, применяет глобальный сервер каталога или основной сервер, который управляет задачами резервного копирования, архивации и восстановления, а также несколько серверов мультимедиа, которые подключены к дисковому хранилищу, ленточным накопителям LTO и сервисам хранения AWS.

Самый простой способ дополнить решение резервного копирования сервисами хранения AWS – воспользоваться преимуществами поддержки Amazon S3 и Amazon Glacier со стороны поставщика вашего решения. Рекомендуется связаться с поставщиком и изучить доступные варианты интеграции и соединители. Список поставщиков программного обеспечения для резервного копирования, поддерживающих AWS, см. в каталоге партнеров[15].

Если существующее решение резервного копирования не поддерживает облачное хранилище, вы можете использовать устройство шлюза хранилища, например мост, между решением резервного копирования и Amazon S3 или Amazon Glacier.

Кроме того, существует множество сторонних шлюзов. Вы также можете воспользоваться виртуальными устройствами AWS Storage Gateway, так как в них применяются универсальные средства, например тома iSCSI и библиотеки виртуальных лент (VTL). Для такой конфигурации требуется поддерживаемый гипервизор (VMware или Microsoft Hyper-V) и локальное хранилище для размещения устройства.

---

[15] http://www.aws-partner-directory.com/PartnerDirectory/PartnerSearch?type=ISV

Архивация данных с помощью AWS

Если вам необходимо сохранить данные для соблюдения требований или по корпоративным причинам, вы их архивируете. В отличие от резервных копий, которые обычно создаются для хранения производственных данных в течение короткого времени и их восстановления в случае повреждения или потери, в архивах сохраняются все копии, пока не истечет период хранения.

Эффективный архив соответствует следующим критериям:

- надежное долгосрочное хранение данных;
- безопасность данных;
- простота восстановления;
- низкая стоимость.

В нормативных или отраслевых требованиях может быть указано, что необходимо использовать неизменяемые хранилища данных.

Amazon Glacier предоставляет недорогие архивы со встроенным шифрованием хранящихся данных, надежностью 99,999999999 % (11 девяток) и неограниченной емкостью.

Amazon S3 Standard – Infrequent Access станет хорошим выбором для ситуаций, в которых требуется быстро извлекать данные. Сервис Amazon Glacier оптимизирован для данных, доступ к которым осуществляется редко и для которых время выдачи в несколько часов является приемлемым.

Объекты могут размещаться в Amazon Glacier с использованием правил жизненного цикла в S3 или Amazon Glacier API. Функция Amazon Glacier Vault Lock позволяет легко развертывать и применять механизмы соблюдения требований для отдельных хранилищ Amazon Glacier с политикой блокировки. Вы можете указать механизмы управления, например «однократная запись, многократное чтение» (WORM), в политике блокировки, чтобы запретить ее изменение в будущем. Дополнительные сведения см. в разделе Amazon Glacier.

Защита данных резервного копирования в AWS

Безопасность данных – очень важный вопрос. В AWS к безопасности подходят очень серьезно, это основа каждого нашего сервиса. Хранилища, такие как Amazon S3, предоставляют мощные возможности управления доступом и шифрования данных в состоянии покоя и во время передачи. Все конечные точки API сервисов Amazon S3 и Amazon Glacier поддерживают SSL-шифрование передаваемых данных. Amazon Glacier по умолчанию шифрует все данные в состоянии покоя. При использовании Amazon S3 клиенты могут выбрать шифрование хранящихся объектов на стороне сервера, при этом AWS будет управлять ключами шифрования, а клиенты будут предоставлять собственные ключи при отправке объекта или использовать интеграцию AWS Key Management Service (AWS KMS) [16]для ключей шифрования. Кроме того, клиенты всегда могут шифровать свои данные перед их передачей в AWS. Дополнительные сведения см. в техническом описании Amazon Web Services: Overview of Security Processes.

Заключение

Компания Gartner называет AWS лидером в сфере сервисов хранения на основе общедоступного облака[17]. AWS помогает организациям перенести рабочие нагрузки в облачные платформы – следующее поколение систем резервного копирования. Платформа AWS предоставляет недорогие и масштабируемые решения резервного копирования и архивации. Эти сервисы хорошо интегрируются с технологиями, которые вы используете сегодня.

---

[16] http://docs.aws.amazon.com/AmazonS3/latest/dev/UsingKMSEncryption.html

[17] http://www.gartner.com/technology/reprints.do?id=1-1WWKTQ3&ct=140709&st=sb

Авторский коллектив

Данный документ был подготовлен при участии следующих лиц.

- Паван Агнихотри (Pawan Agnihotri), архитектор решений, Amazon Web Services
- Ли Кир (Lee Kear), архитектор решений, Amazon Web Services
- Питер Леветт (Peter Levett), архитектор решений, Amazon Web Services

Редакции документа

Обновлено в мае 2016 г.