Рекомендации по развертыванию Amazon WorkSpaces

Сетевой доступ, службы каталогов и безопасность

Июль 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 4
Введение 4
Требования WorkSpaces 5
Несколько слов о сетях 6
Проектирование VPC 7
Поток трафика 9
Пример типичной конфигурации 13
AWS Directory Service 17
Сценарии развертывания AD DS 18
Некоторые аспекты проектирования 27
Multi-Factor Authentication (MFA) 33
Безопасность 35
Шифрование данных во время передачи 35
Сетевые интерфейсы 37
Группа безопасности WorkSpaces 38
Зашифрованные данные WorkSpaces 39
Мониторинг и ведение журнала с использованием Amazon CloudWatch 41
Метрики WorkSpaces в Amazon CloudWatch 41
Устранение неполадок 43
AD Connector не удается подключиться к Active Directory 43
Проверка задержки до ближайшего региона AWS 45
Заключение 45
Авторский коллектив 46
Дополнительная литература 46

Резюме

Это техническое описание содержит ряд рекомендаций по развертыванию Amazon WorkSpaces. В этом документе рассматриваются вопросы, связанные с сетью, службами каталогов, аутентификацией пользователей, безопасностью, мониторингом и ведением журналов.

Для того чтобы нужную информацию было проще найти, документ разделен на 4 части. Техническое описание предназначено для инженеров по сетям, каталогам и безопасности.

Введение

Amazon WorkSpaces – это вычислительный сервис по предоставлению рабочих столов в облаке. Amazon WorkSpaces избавляет от необходимости приобретения и развертывания оборудования или установки сложного программного обеспечения и позволяет использовать клиент с функциями настольного ПК всего в несколько щелчков на консоли управления AWS, через интерфейс командной строки AWS или API. Благодаря Amazon WorkSpaces вы сможете всего за несколько минут запустить рабочий стол, быстро, надежно и безопасно подключиться к настольному ПО из локальной системы или внешней сети и приступить к работе с ним. Вы можете:

- использовать существующую локальную службу Microsoft Active Directory (AD) через AWS Directory Service: AD Connector;
- расширить свою службу каталогов ресурсами облака AWS;
- создать управляемый каталог в сервисе AWS Directory Service (Microsoft AD или Simple AD) для управления пользователями и сервисом WorkSpaces;

Кроме того, вы можете использовать свой локальный или размещенный в облаке сервис RADIUS с AD Connector для выполнения многофакторной аутентификации (MFA) в сервисе WorkSpaces.

С помощью интерфейса командной строки или API можно автоматизировать подготовку Amazon WorkSpaces, интегрируя Amazon WorkSpaces в существующие рабочие процессы подготовки ПО.

В целях безопасности в дополнение к интегрированному сетевому шифрованию, которое выполняется сервисом WorkSpaces, можно включить для WorkSpaces шифрование данных в состоянии покоя (см. подраздел Шифрование данных WorkSpaces в разделе «Безопасность»).

Развертывать приложения в WorkSpaces можно с использованием существующих локальных инструментов (например, диспетчера Microsoft System Center Configuration Manager (SCCM)) или Amazon WorkSpaces Application Manager (Amazon WAM).

В следующих разделах приводятся подробные сведения об Amazon WorkSpaces, принципах работы сервиса, требованиях к запуску сервиса и доступных параметрах и компонентах.

Требования WorkSpaces

Для успешного развертывания сервиса Amazon WorkSpaces требуется три компонента.

- **Клиентское приложение WorkSpaces**. Клиентское устройство с поддержкой Amazon WorkSpaces. Полный список доступен здесь: Поддерживаемые платформы и устройства.

  Кроме того, для подключения к WorkSpaces можно воспользоваться нулевыми клиентами PCoIP. Список доступных устройств см. в разделе Нулевые клиенты PCoIP для Amazon WorkSpaces.

- **Служба каталогов для аутентификации пользователей и предоставления доступа к сервису WorkSpace**. Amazon WorkSpaces в настоящее время работает с AWS Directory Service и Active Directory. Чтобы использовать существующие корпоративные данные для доступа пользователей в WorkSpaces, можно воспользоваться локальным сервером Active Directory с сервисом AWS Directory Service.

- **Облако Amazon Virtual Private Cloud (Amazon VPC), в котором запускается Amazon WorkSpaces**. Для развертывания WorkSpaces потребуется не менее двух подсетей, поскольку каждая конструкция AWS Directory Service требует двух подсетей в развертывании с несколькими зонами доступности.

Несколько слов о сетях

Каждый сервис WorkSpace связан с определенными конструкциями Amazon VPC и AWS Directory Service, использовавшимися для создания этого сервиса. Для работы любой конструкции AWS Directory Service (Simple AD, AD Connector и Microsoft AD) требуется две подсети, расположенных в разных зонах доступности. Подсети тесно связаны с конструкциями Directory Service, их невозможно изменить после создания AWS Directory Service. Следовательно, важно правильно определить размер подсети, прежде чем создавать конструкцию Directory Services. Прежде чем создавать подсети, внимательно ответьте на следующие вопросы:

- Сколько сервисов WorkSpaces вам потребуется в дальнейшем? Каковы прогнозируемые темпы роста?
- Потребности каких типов пользователей вам будет необходимо удовлетворить?
- Сколько доменов Active Directory будет подключено к системе?
- Где расположены корпоративные аккаунты пользователей в вашей системе?

Amazon рекомендует определять группы пользователей (так называемые «персоны») в процессе планирования с учетом типа доступа и требуемой аутентификации пользователей. Эти ответы окажутся полезными, если требуется ограничить доступ к определенным приложениям или ресурсам. После определения групп пользователей можно с помощью AWS Directory Service, сетевых списков контроля доступа, таблиц маршрутизации и групп безопасности VPC сегментировать и ограничивать доступ к системе. В каждой конструкции AWS Directory Service используется две подсети, и одни и те же настройки действуют для всех сервисов WorkSpaces, запускаемых из этой конструкции. Например, можно использовать группу безопасности, которая применяется ко всем сервисам WorkSpaces, подключенных к AD Connector, чтобы указать, нужна ли аутентификация MFA и может ли конечный пользователь иметь локальный доступ к своему сервису WorkSpace с правами администратора.

> **Примечание.** Каждый AD Connector подключается к одной организационной единице Microsoft Active Directory. Необходимо спроектировать сервис Directory Service так, чтобы использовать эту функцию с учетом особенностей и предпочтений пользователей.

В этом разделе приводятся рекомендации по определению оптимального размера VPC и подсетей, управлению потоком трафика и проектировании служб каталогов с учетом выбранных значений.

Проектирование VPC

При проектировании VPC, подсетей, групп безопасности, политик маршрутизации и сетевых списков контроля доступа для сервиса Amazon WorkSpaces необходимо учитывать несколько аспектов, чтобы получившаяся среда WorkSpaces была масштабируемой, безопасной и простой в управлении.

- **VPC**. Рекомендуется использовать отдельное VPC специально для развертывания WorkSpaces. При наличии отдельного VPC можно задать диапазоны допустимых значений параметров управления и безопасности для сервиса WorkSpace и обеспечить разделение трафика.
- **Сервисы Directory Services**. Для каждой конструкции AWS Directory Service требуется пара подсетей, обеспечивающих разделение службы каталогов высокой доступности между зонами доступности Amazon.
- **Размер подсети**. Развертывания WorkSpaces связаны с конструкцией каталога и расположены в тех же подсетях VPC, что и выбранный сервис AWS Directory Service. Несколько важных моментов:
  - Размер подсети является постоянным, изменить его невозможно, поэтому необходимо обеспечить достаточный запас для будущего роста.

— Можно указать группу безопасности по умолчанию для выбранного сервиса AWS Directory Service; эта группа безопасности будет действовать в отношении всех сервисов WorkSpaces, связанных с конкретной конструкцией AWS Directory Service.

— Несколько сервисов AWS Directory Services могут использовать одну и ту же подсеть.

Проектируя облако VPC, обязательно принимайте во внимание планы развития компании. Например, может потребоваться добавить компоненты управления, например антивирусный сервер, сервер управления исправлениями или сервер Active Directory или RADIUS MFA. Чтобы удовлетворить эти требования, целесообразно запланировать наличие в VPC дополнительных доступных IP-адресов.

Подробные описания и пошаговые инструкции по проектированию VPC и определению размера подсети см. в презентации **re:Invent** под названием Переход Amazon.com к Amazon WorkSpaces.

Сетевые интерфейсы

Каждый сервис WorkSpace имеет два эластичных сетевых интерфейса (ENI), сетевой интерфейс управления (eth0) и основной сетевой интерфейс (eth1). AWS использует сетевой интерфейс управления для управления WorkSpace; это интерфейс, где разъединяются ваши клиентские подключения. AWS использует для этого интерфейса диапазон частных IP-адресов. Нельзя использовать это частное пространство адресов в любой сети, из которой можно обмениваться данными с вашим облаком VPC в WorkSpaces. Только так можно обеспечить правильную сетевую маршрутизацию.

Список диапазонов частных IP-адресов, используемых нами в каждом регионе, см. в разделе Сведения об Amazon WorkSpaces.

Примечание. Amazon WorkSpaces и соответствующие сетевые интерфейсы управления не расположены в вашем VPC, и просмотреть сетевой интерфейс управления или ИД инстанса Amazon Elastic Compute Cloud (Amazon EC2) на консоли управления AWS невозможно (см. Рисунок 4, Рисунок 5 и Рисунок 6). Однако на консоли управления AWS можно просматривать и изменять настройки группы безопасности основного сетевого интерфейса (eth1). Кроме того, основные сетевые интерфейсы сервисов WorkSpace не влияют на лимит ресурсов ENI Amazon EC2. В крупных развертываниях WorkSpaces потребуется с помощью консоли управления AWS отправить в службу поддержки заявку на увеличение лимитов ENI.

Поток трафика

Трафик Amazon WorkSpaces можно разделить на два основных компонента:

- трафик между клиентским устройством и сервисом Amazon WorkSpace
- трафик между сервисом Amazon WorkSpace и сетью клиента

В следующем разделе мы рассмотрим оба этих компонента более подробно.

Подключение клиентского устройства к WorkSpace

Устройство, на котором выполняется клиент Amazon WorkSpaces, использует для подключения к сервису WorkSpaces те же два порта независимо от расположения (локальное или удаленное). Клиент использует протокол HTTPS в порту 443 для передачи всей информации об аутентификации и сеансах, а порт 4172 (PCoIP) с TCP и UDP – для потоковой передачи пикселей заданному сервису WorkSpace и проверок работоспособности сети. Трафик в обоих портах зашифрован. Трафик в порту 443 используется для передачи информации об аутентификации и сеансах, а для шифрования трафика используется протокол TLS. Для обмена данными между клиентом и интерфейсом eth0 сервиса WorkSpace используется 256-битное шифрование AES потокового трафика пикселей, а трафик передается через потоковый шлюз. Дополнительные сведения доступны в разделе Безопасность далее.

Мы публикуем диапазоны IP-адресов наших потоковых шлюзов PCoIP и URL сервера для проверки работоспособности сети для конкретных регионов. Чтобы ограничить исходящий трафик в порту 4172, передаваемый из вашей корпоративной сети в потоковый шлюз AWS и на URL сервера проверки работоспособности сети, нужно разрешить отправку исходящего трафика в порту 4172 только в определенные регионы AWS, где вы используете сервис Amazon WorkSpaces. Диапазоны IP-адресов и URL сервера проверки работоспособности сети указаны в разделе Диапазоны IP-адресов шлюзов PCoIP для Amazon WorkSpaces.

В клиенте Amazon WorkSpaces имеется встроенный механизм проверки состояния сети. Эта служебная программа показывает, возможно ли то или иное соединение в сети пользователя, отображая индикатор состояния в нижнем правом углу приложения. Чтобы получить более подробную информацию о состоянии сети, выберите **Сеть** в нижнем правом углу клиента, и откроется окно, показанное на рисунке 1.

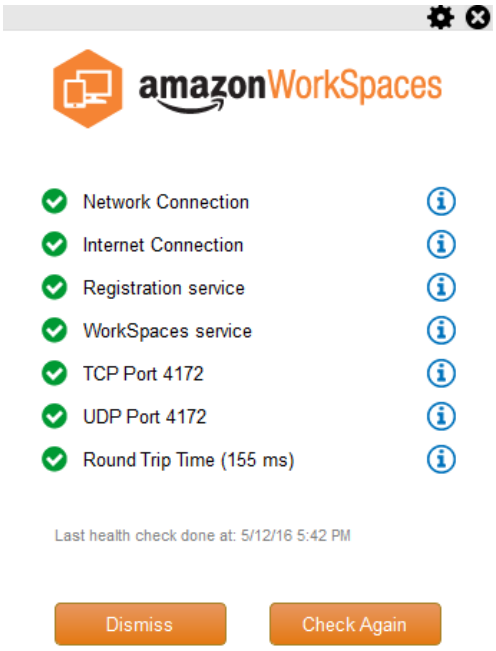

Рисунок 1. Клиент WorkSpaces – проверка состояния сети

Пользователь инициирует подключение из клиента к сервису WorkSpaces, указывая свои данные для входа в каталог, используемый в конструкции Directory Service (как правило, речь идет о корпоративном каталоге). Сведения для входа отправляются по протоколу HTTPS в шлюзы аутентификации Amazon WorkSpaces в регионе, где расположен сервис. Затем шлюз аутентификации сервиса Amazon WorkSpaces перенаправляет трафик в определенную конструкцию сервиса AWS Directory Service, связанную с вашим сервисом WorkSpace. Например, если используется AD Connector, он перенаправляет запрос аутентификации непосредственно в вашу службу Active Directory, которая может располагаться локально или в облаке VPC AWS (см. раздел Сценарии развертывания AD DS). AD Connector не хранит никакие сведения об аутентификации и функционирует в качестве прокси-сервера, не фиксирующего данные о запросах. Следовательно, очень важно обеспечить возможность подключения AD Connector к серверу Active Directory. AD Connector определяет сервер Active Directory, к которому выполняется подключение, используя серверы DNS, которые вы определяете при создании соединителя AD Connector.

Если используется соединитель AD Connector и в каталоге включена MFA, токен MFA будет проверен перед аутентификацией в службе каталогов. Если проверка токена MFA завершится ошибкой, информация пользователя для входа не будет перенаправлена в сервис AWS Directory Service.

После аутентификации пользователя начинается потоковая передача трафика сервису WorkSpace с использованием порта 4172 (PCoIP) через потоковый шлюз AWS. Обмен сведениями о сеансе на протяжении сеанса по-прежнему осуществляется через протокол HTTPS. Для передачи потокового трафика используется первый эластичный сетевой интерфейс WorkSpace (eth0 в WorkSpace), который не подключен к вашему облаку VPC. Управление сетевым подключением между потоковым шлюзом и эластичным сетевым интерфейсом осуществляет AWS. В случае сбоя подключения потоковых шлюзов к эластичному сетевому интерфейсу потоковой передачи WorkSpaces создается событие CloudWatch (см. раздел Мониторинг и ведение журнала с использованием Amazon CloudWatch этого технического описания).

Объем данных, которыми обмениваются сервис Amazon WorkSpaces и клиент, зависит от уровня активности пикселей. Чтобы обеспечить пользователям максимальное удобство, рекомендуется установить время приема-передачи (RTT) данных между клиентом WorkSpaces и регионом AWS, где находится ваш сервис WorkSpaces, менее 100 мс. Как правило, это означает, что клиент WorkSpaces находится менее, чем в 3200 км от региона, где размещен сервис WorkSpace. На странице Проверка состояния подключения можно определить оптимальный регион AWS для подключения при работе с сервисом Amazon WorkSpaces.

Подключение сервиса Amazon WorkSpaces к VPC

После успешной аутентификации подключения клиента к WorkSpace и запуска потокового трафика в клиенте WorkSpaces отобразится рабочий стол Windows (ваш WorkSpace), подключенный к VPC, а сеть должна показать, что подключение установлено. Основному интерфейсу ENI сервиса WorkSpace, обозначенному как eth1, службой DHCP будет назначен IP-адрес. Служба предоставляется облаком VPC, как правило, из тех же подсетей, что и сервис AWS Directory Service. Назначенный WorkSpace IP-адрес сохраняется на протяжении всего срока эксплуатации сервиса. Интерфейс ENI в облаке VPC имеет доступ к любому ресурсу VPC и к любой сети, подключенной к вашему облаку (через одноранговые соединения VPC, подключение AWS Direct Connect или VPN).

Доступ ENI к вашим сетевым ресурсам регулируется группой безопасности по умолчанию (см. более подробные сведения о группах безопасности здесь), которая настраивается сервисом AWS Directory Service для каждого WorkSpace, и любыми другими группами безопасности, назначенными ENI. При необходимости можно добавить группы безопасности в интерфейс ENI, обращенный к вашему VPC, с помощью консоли управления AWS или интерфейса командной строки. Помимо групп безопасности для ограничения сетевого доступа к ресурсам облака VPC в конкретном сервисе WorkSpace можно использовать серверный брандмауэр по вашему выбору.

Рисунок 4 в разделе Сценарии развертывания AD DS далее в этом техническом описании отображает поток трафика, описанный выше.

Пример типичной конфигурации

Рассмотрим сценарий, в котором имеется два типа пользователей, а AWS Directory Service использует для аутентификации пользователей централизованную службу Active Directory.

- **Сотрудники, которым требуется полный повсеместный доступ** (например, штатный персонал). Этим пользователям будет предоставлен полный доступ к Интернету и внутренней сети, и через брандмауэр они будут попадать из VPC в локальную сеть.
- **Сотрудники, которые должны иметь ограниченный доступ из корпоративной сети** (например, подрядчики и консультанты). Этим пользователям в VPC будет предоставлен ограниченный доступ к Интернету через прокси-сервер (к определенным веб-сайтам), они будут иметь ограниченный сетевой доступ в VPC и к локальной сети.

Целесообразно предоставить штатному персоналу возможность доступа к своим сервисам WorkSpace с правами локального администратора для установки программного обеспечения. Кроме того, необходимо реализовать принудительную двухфакторную аутентификацию с использованием механизмов MFA. Кроме того, необходимо обеспечить непрерывный доступ к Интернету из WorkSpace для штатного персонала.

Для подрядчиков, напротив, имеет смысл блокировать доступ с правами локального администратор, чтобы они могли пользоваться только определенными предустановленными приложениями. К этим WorkSpaces нужно применять весьма жесткие механизмы контроля сетевого доступа с использованием групп безопасности. Необходимо открыть порты 80 и 443 только для конкретных внутренних веб-сайтов и заблокировать доступ в Интернет.

В этом сценарии мы имеем дело с двумя совершенно разными группами пользователей с совершенно разными требованиями доступа к сетевым ресурсам и настольным приложениям. Рекомендуется настраивать такие WorkSpaces и управлять ими по отдельности. Для этого необходимо создать два соединителя AD Connector – по одному для каждой группы пользователей. Каждому AD Connector требуется две подсети, в которых должно быть достаточно IP-адресов, чтобы справиться с ростом использования WorkSpaces.

> **Примечание.** Каждая подсеть облака VPC AWS использует пять IP-адресов (четыре первых и последний IP-адрес) для управления, а каждый AD Connector использует по одному IP-адресу в каждой подсети, где он существует.

Кроме того, в этом сценарии необходимо учитывать следующее.

- Подсети облаков VPC в AWS должны представлять собой частные подсети, чтобы трафик (например, доступ к Интернету) можно было контролировать с помощью шлюза NAT или прокси-сервера NAT в облаке либо направлять трафик обратно через локальную систему управления трафиком.
- Брандмауэр должен использоваться для всего трафика VPC, который перемещается по локальной сети.
- Серверы Microsoft Active Directory и MFA RADIUS должны быть либо локальными (см. раздел Сценарий 1. Использование AD Connector для проксирования аутентификации в локальную службу AD DS), либо являться частью реализации облака AWS (см. сценарии 2 и 3 в разделе Сценарии развертывания AD DS).

Учитывая, что всем WorkSpaces в той или иной форме будет предоставлен доступ к Интернету и что они будут размещены в частной подсети, требуется также создать публичные подсети, которые могут осуществлять доступ к Интернету через интернет-шлюз. Для штатных сотрудников потребуется шлюз NAT, позволяющий осуществлять доступ к Интернету, а для консультантов и подрядчиков – прокси-сервер NAT, обеспечивающий ограниченный доступ к определенным внутренним веб-сайтам. Чтобы спланировать отработку отказа, обеспечить высокую доступность и свести к минимуму расходы на трафик между зонами доступности, два шлюза NAT и серверы NAT или прокси-серверы должны располагаться в двух разных подсетях в среде с несколькими зонами доступности. Две зоны доступности, выбранные вами в качестве публичных подсетей, буду соответствовать двум зонам доступности, используемым для подсетей WorkSpaces в регионах, где число зон доступности превышает 2. Весь трафик из каждой зоны доступности WorkSpaces можно направлять в соответствующую публичную подсеть, чтобы свести к минимуму расходы на трафик между зонами доступности и упростить управление. На рисунке 2 показана конфигурация VPC.

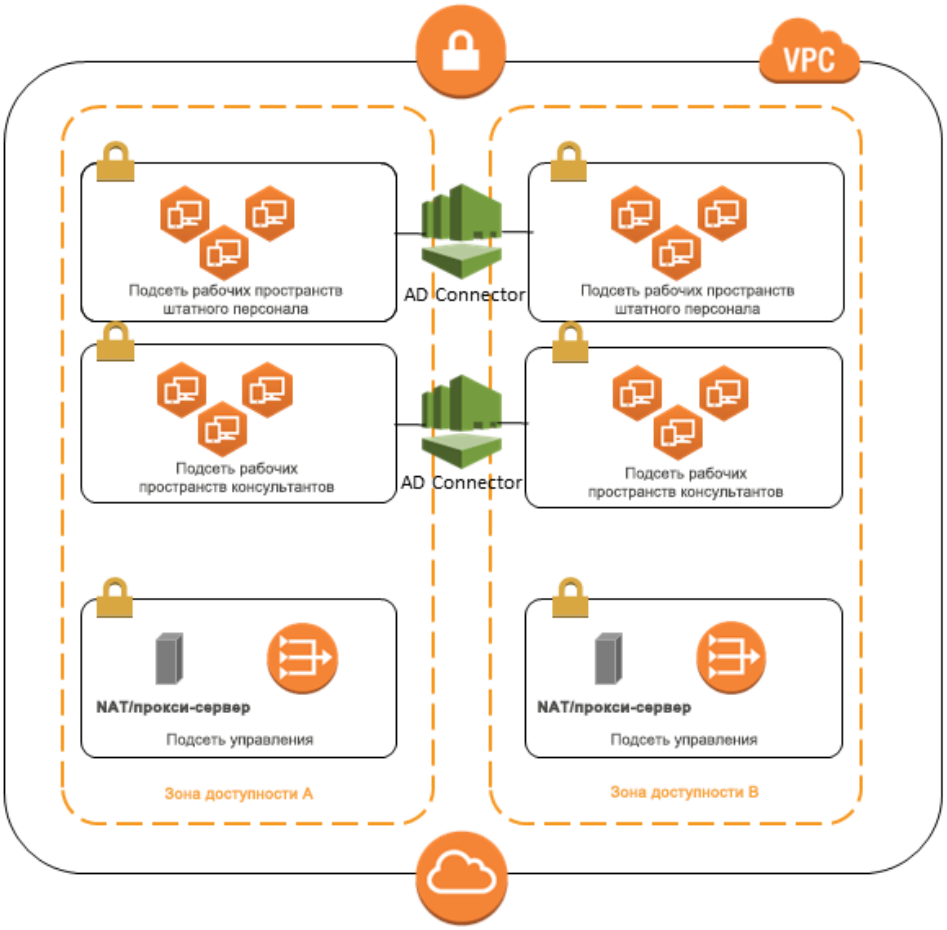

Рисунок 2. Общая схема структуры VPC

Далее описано, как настроить два вышеописанных типа WorkSpaces.

- **Штатный персонал**. На консоли управления Amazon WorkSpaces в строке меню выберите **Каталоги**, выберите каталог, в котором размещены ваши штатные сотрудники, и щелкните **Настройка локального администратора**. Если этот параметр включен, все создаваемые в дальнейшем сервисы WorkSpace будут обладать привилегиями локального администратора. Чтобы предоставить доступ к Интернету, требуется настроить трансляцию сетевых адресов (NAT) для исходящего доступа к Интернету из облака VPC. Чтобы включить MFA, необходимо указать сервер RADIUS, IP-адреса сервера, порты и предварительный ключ.

Входящий трафик в WorkSpaces штатных сотрудников будет ограничен протоколом RDP из подсети службы технической поддержки с использованием группы безопасности по умолчанию в настройках AD Connector.

- **Подрядчики и консультанты:** на консоли управления Amazon WorkSpaces отключите **Доступ к Интернету** и настройку **Локальный администратор**. Затем добавьте группу безопасности в раздел настроек **Группа безопасности**, чтобы использовать группу безопасности для всех новых инстансов WorkSpaces, создаваемых в этом каталоге.

  Для WorkSpaces консультантов исходящий и входящий трафик инстансов WorkSpaces требуется ограничить, применив группу безопасности по умолчанию в настройках AD Connector ко всем инстансам WorkSpaces, связанным с AD Connector. Группа безопасности позволит осуществлять исходящий доступ из WorkSpaces только к трафику HTTP и HTTPS, а входящий трафик будет ограничен RDP из подсети службы технической поддержки в локальной сети.

Примечание. Группа безопасности применяется только к интерфейсу ENI, который находится в VPC (eth1 в WorkSpace), а доступ к WorkSpace из клиента WorkSpaces не ограничен в результате применения группы безопасности. На рисунке 3 показана конечная структура VPC WorkSpaces, описанная ранее.

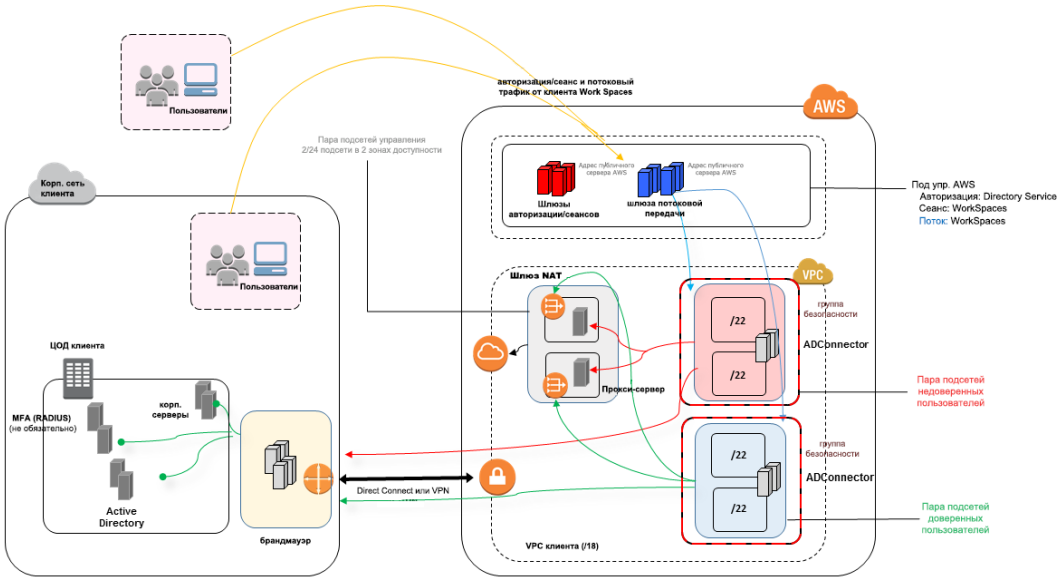

Рисунок 3. Структура WorkSpaces с группами пользователей

AWS Directory Service

Как упомянуто во введении, работа Amazon WorkSpaces обеспечивается сервисом AWS Directory Service. AWS Directory Service позволяет создавать три типа каталогов. Первые два размещаются в облаке AWS:

- AWS Directory Service для Microsoft Active Directory (корпоративный выпуск) или **Microsoft AD** – управляемая служба Microsoft Active Directory на базе Windows Server 2012 R2.
- **Simple AD** – автономный, совместимый с Microsoft Active Directory управляемый сервис каталогов на базе Samba 4.

Третий, **AD Connector,** представляет собой шлюз каталогов, который позволяет проксировать запросы аутентификации и поиски пользователей или групп в существующую локальную службу Microsoft Active Directory.

В следующем разделе описаны коммуникационные потоки аутентификации между брокерской службой Amazon WorkSpaces и сервисом AWS Directory Service, рекомендации по внедрению WorkSpaces с сервисом AWS Directory Service и некоторые сложные концепции, такие как MFA. Кроме того, обсуждаются некоторые аспекты инфраструктурной архитектуры для Amazon WorkSpaces в целом, требования к Amazon VPC и AWS Directory Service, включая интеграцию с локальными доменными службами Microsoft Active Directory (AD DS).

Сценарии развертывания AD DS

Функционирование Amazon WorkSpaces обеспечивается сервисом AWS Directory Service, поэтому грамотное проектирование и развертывание службы каталогов имеет критическое значение. В следующих трех сценариях выполняются инструкции из краткого руководства пользователя *доменных служб Microsoft Active Directory*, в котором даются подробные рекомендации по развертыванию AD DS, в частности для интеграции с WorkSpaces. В разделе *Некоторые аспекты проектирования* этой главы перечислены подробные требования и рекомендации по использованию AD Connector для WorkSpaces, поскольку соединитель является неотъемлемой частью общей структуры WorkSpaces.

- **Сценарий 1. Использование AD Connector для проксирования аутентификации в локальную службу AD DS.** В этом сценарии рассматривается сетевое соединение на стороне клиента (VPN/Direct Connect (DX)), а аутентификация через сервис AWS Directory Service (AD Connector) выполняется в локальной службе AD DS клиента.
- **Сценарий 2. Расширение локальной AD DS для AWS (реплика).** Этот сценарий аналогичен первому, однако здесь реплика службы AD DS клиента развертывается в AWS вместе с AD Connector, благодаря чему сокращается задержка при обработке запросов аутентификации и прочих запросов, адресованных AD DS и глобальному каталогу AD DS.

- **Сценарий 3. Автономное изолированное развертывание с использованием сервиса AWS Directory Service в облаке AWS.** Это изолированный сценарий, не включающий обратного подключения к клиенту с целью аутентификации. В этом подходе используются сервис AWS Directory Service (Microsoft AD) и AD Connector. Несмотря на то что в этом сценарии не выполняется подключение к системе клиента с целью аутентификации, все готово к обработке трафика приложения (если необходимо) по VPN или DX.

Сценарий 1. Использование AD Connector для проксирования аутентификации в локальную службу AD DS

Этот сценарий предназначен для клиентов, которые не хотят расширять свою локальную службу AD DS в облаке AWS или если возможность нового развертывания AD DS отсутствует. Рисунок 4. Подключение AD Connector к локальной службе Active Directory в общих чертах описывает каждый из компонентов и показывает процедуру аутентификации пользователей.

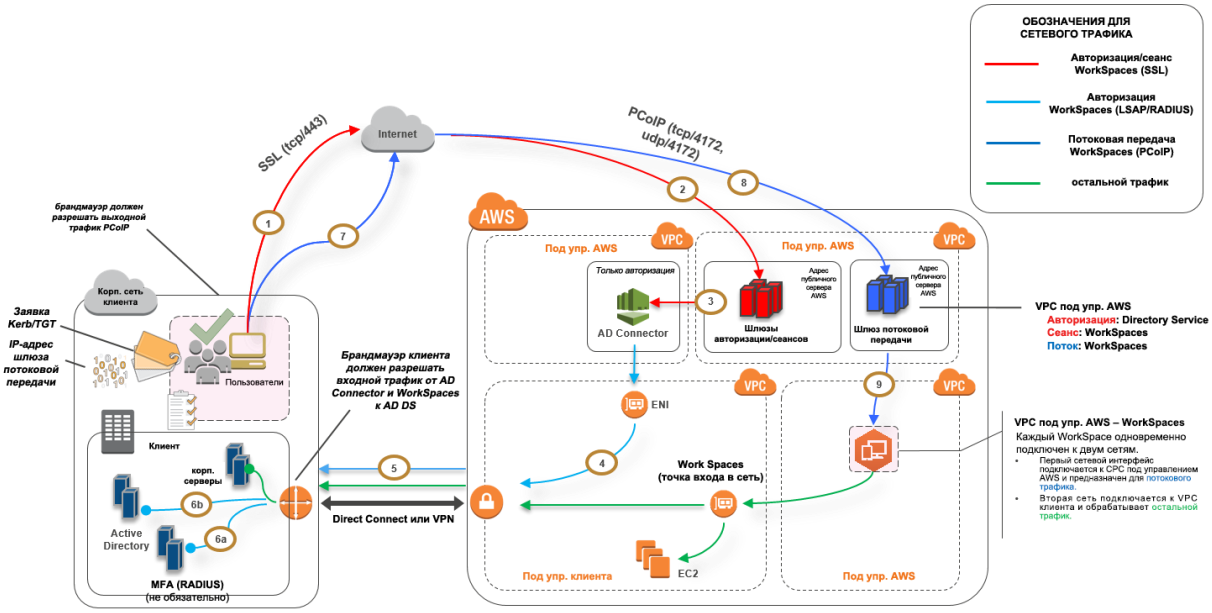

Рисунок 4. Подключение AD Connector к локальной службе Active Directory

В этом сценарии AWS Directory Service (AD Connector) используется для всех операций аутентификации пользователей или MFA, которая через AD Connector проксируется в локальную службу AD DS клиента (Рисунок 5). Сведения о протоколах и шифровании, используемых в процессе аутентификации, см. в разделе Безопасность этого технического описания.

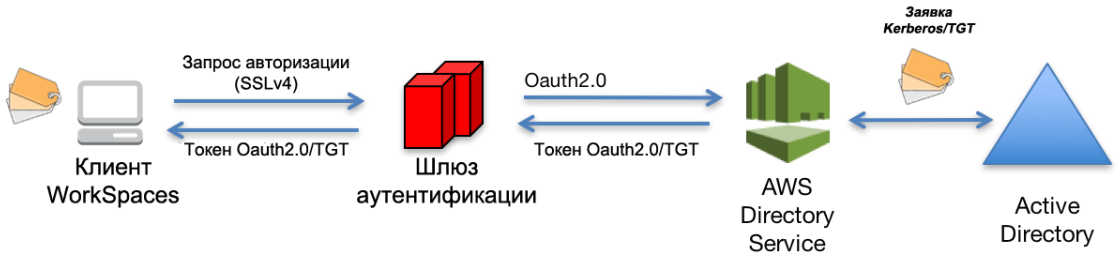

Рисунок 5. Аутентификация пользователей через шлюз аутентификации

В сценарии 1 показана гибридная архитектура, в которой у клиента, возможно, уже имеются ресурсы в AWS, а также ресурсы в локальном центре обработки данных, доступные через WorkSpaces. Клиент может использовать существующие локальные серверы AD DS и RADIUS для аутентификации пользователей и MFA.

В этой архитектуре используются следующие компоненты и конструкции.

Amazon Web Services:

- **Amazon VPC:** создание Amazon VPC с по меньшей мере двумя частными подсетями в двух зонах доступности.
- **Набор параметров DHCP:** создание набора параметров DHCP в Amazon VPC. Это позволяет определять заданные клиентом доменное имя и серверы доменных имен (DNS) (локальные службы). (Дополнительная информация доступна в разделе Набор параметров DHCP.)
- **Виртуальный частный шлюз Amazon:** включение возможности обмена данными с собственной сетью по тоннелю VPN IPsec или подключению AWS Direct Connect.
- **AWS Directory Service**: AD Connector развертывается в паре частных подсетей Amazon VPC.
- **Amazon WorkSpaces:** WorkSpaces развертываются в тех же частных подсетях, что и AD Connector (см. раздел Некоторые аспекты проектирования, AD Connector).

Клиент:

- **Сетевое подключение:** URL сервера корпоративной VPN или Direct Connect.
- **AD DS:** корпоративная служба AD DS.
- **MFA (не обязательно):** корпоративный сервер RADIUS.
- **Устройства конечных пользователей:** использование корпоративных устройств или личных устройств конечных пользователей (модель BYOL, устройства Windows, Mac, планшеты iPad или Android, нулевые клиенты, Chromebook) для доступа к сервису Amazon WorkSpaces (см. раздел Поддерживаемые платформы и устройства).

Это решение идеально подходит клиентам, которые не желают развертывать AD DS в облаке, однако имеет свои недостатки.

- **Зависимость от подключения:** если подключение к центру обработки данных разорвано, пользователь не сможет выполнить вход в соответствующие WorkSpaces, а существующие подключения останутся активными до конца жизненного цикла Kerberos/TGT.
- **Задержка:** если подключение выполняется с задержкой (это более актуально для VPN, нежели для DX), аутентификация WorkSpaces и все связанные с AD DS действия, например реализация групповых политик, будут выполняться медленнее.
- **Стоимость трафика:** все операции по аутентификации подразумевают перебор ссылок VPN или DX, поэтому стоимость зависит от типа подключения. Речь идет либо о переносе данных из Amazon EC2 в Интернет, либо о выносе данных (DX).

> **Примечание**. AD Connector – это прокси-сервис. Он не хранит и не кэширует данные для доступа пользователей. Все запросы аутентификации, поиска и управления обрабатываются Active Directory. В службе каталогов должна существовать учетная запись с правами делегирования и возможностью считывать всю информацию о пользователях и подключать компьютер к домену.

Сведения о настройке пользователя в каталоге для AD Connector см. в разделе Делегирование привилегий подключения.

В целом работа WorkSpaces во многом зависит от пункта 5, показанного на Рисунке 4.

Сценарий 2. Расширение локальной AD DS для AWS (реплика).

Этот сценарий аналогичен первому, однако здесь реплика службы AD DS клиента развертывается в AWS вместе с AD Connector, благодаря чему сокращается задержка при обработке запросов аутентификации и прочих запросов, адресованных AD DS и глобальному каталогу AD DS. Рисунок 6 показывает в общих чертах каждый из компонентов и процедуру аутентификации пользователей.

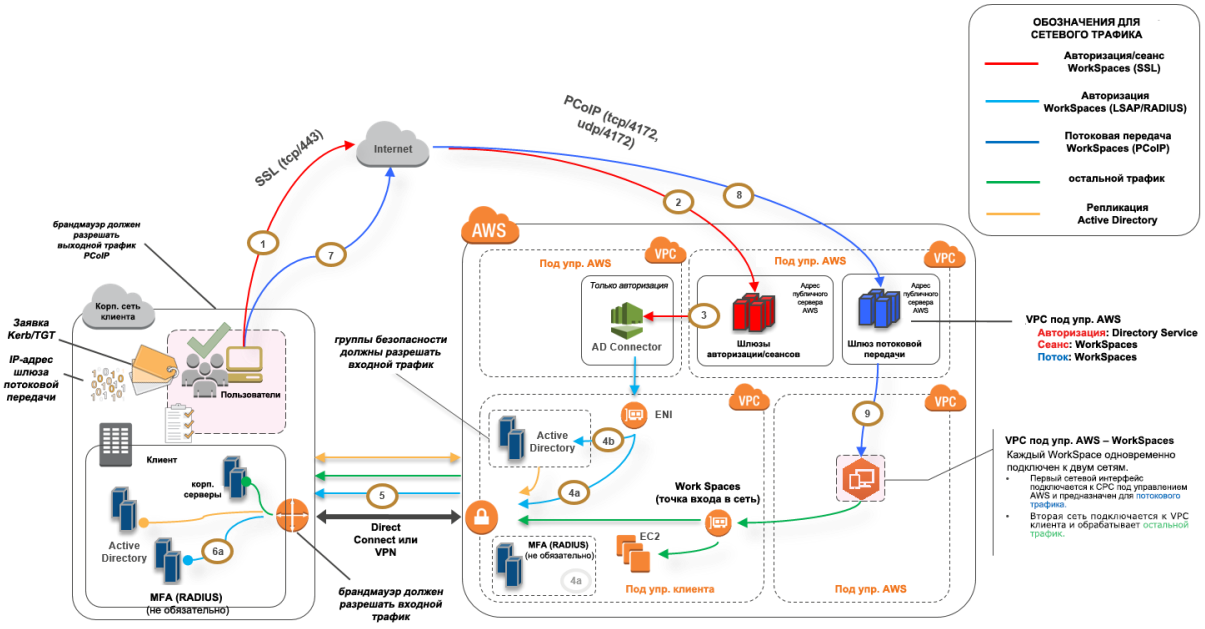

Рисунок 6. Расширение домена Active Directory клиента в облако

Как и в первом сценарии, AD Connector используется для всех операции аутентификации пользователей или MFA, которая проксируется в службу AD DS клиента (Рисунок 5). В сценарии 2 служба AD DS клиента развернута в зонах доступности в инстансах Amazon EC2, уровень которых был повышен до доменных контроллеров в локальном лесу Active Directory клиента, где выполняется облако AWS. Каждый доменный контроллер развернут в частных подсетях VPC, чтобы обеспечить высокую доступность AD DS в облаке AWS. Рекомендации по развертыванию AD DS в облаке AWS см. в разделе «Некоторые аспекты проектирования» далее в этом техническом описании.

Развернутые инстансы WorkSpaces получают доступ к облачным доменным контроллерам, а службы каталогов и DNS функционируют под защитой и с низкой задержкой. Безопасность всего сетевого трафика, включая обмен данными AD DS, запросы аутентификации и репликацию Active Directory, обеспечивается в частных подсетях или в тоннеле VPN или DX клиента.

В этой архитектуре используются следующие компоненты и конструкции.

Amazon Web Services:

- **Amazon VPC:** создание Amazon VPC с по меньшей мере четырьмя частными подсетями в двух зонах доступности (два для AD DS клиента и два для AD Connector или WorkSpaces).
- **Набор параметров DHCP:** создание набора параметров DHCP в Amazon VPC. Это позволяет определять заданные клиентом доменное имя и серверы доменных имен (DNS) (локальные службы AD DS). Дополнительная информация доступна в разделе Набор параметров DHCP.
- **Виртуальный частный шлюз Amazon:** включение возможности обмена данными с собственной сетью по тоннелю VPN IPsec или подключению AWS Direct Connect.
- **Amazon EC2:**
  - корпоративные доменные контроллеры AD DS клиента, развернутые в инстансах Amazon EC2 в выделенных частных подсетях VPC.
  - «Дополнительные» серверы RADIUS клиента для MFA.

- **AWS Directory Services**: AD Connector развертывается в паре частных подсетей Amazon VPC.
- **Amazon WorkSpaces:** WorkSpaces развертываются в тех же частных подсетях, что и AD Connector (см. раздел Некоторые аспекты проектирования, AD Connector).

Клиент:

- **Сетевое подключение:** URL сервера корпоративной VPN или AWS Direct Connect.
- **AD DS:** корпоративная AD DS (необходима для репликации).
- **MFA (не обязательно):** корпоративный сервер RADIUS.
- **Устройства конечных пользователей:** использование корпоративных устройств или личных устройств конечных пользователей (модель BYOL, устройства Windows, Mac, планшеты iPad или Android, нулевые клиенты, Chromebook) для доступа к сервису Amazon WorkSpaces (см. раздел Поддерживаемые платформы и устройства).

В отличие от сценария 1, это решение не имеет упомянутых недостатков. Следовательно, WorkSpaces и AWS Directory Service не зависят от наличия подключения.

- **Зависимость от подключения:** если подключение к центру обработки данных клиента разорвано, конечные пользователи могут продолжать работу, потому что аутентификация и необязательная MFA обрабатываются локально.
- **Задержка:** за исключением трафика репликации (см. раздел *Некоторые аспекты* проектирования. Сайты и службы AD DS), все процессы аутентификации выполняются на локальном уровне и с низкой задержкой.
- **Стоимость трафика:** в этом сценарии используется локальная аутентификация, поэтому перебор ссылок VPN или DX требуется только для репликации AD DS, что уменьшает объем переносимых данных.

В целом работа WorkSpaces оптимизирована и не настолько зависит от пункта 5, как показано на Рисунке 6. Это еще более актуально, если требуется масштабировать WorkSpaces и использовать сервис на тысячах рабочих столов. Особенно это касается запросов глобального каталога AD DS, поскольку трафик в среде WorkSpaces остается локальным.

Сценарий 3. Автономное изолированное развертывание с использованием сервиса AWS Directory Service в облаке AWS

В этом сценарии, показанном на Рисунке 7, AD DS развертывается в облаке AWS в автономной изолированной среде. AWS Directory Service используется исключительно в этом сценарии. Вместо того чтобы полностью управлять AD DS самостоятельно, вы делегируете AWS Directory Service такие задачи, как создание топологии каталогов высокой доступности, мониторинг доменных контроллеров и настройка резервных копий и снимков.

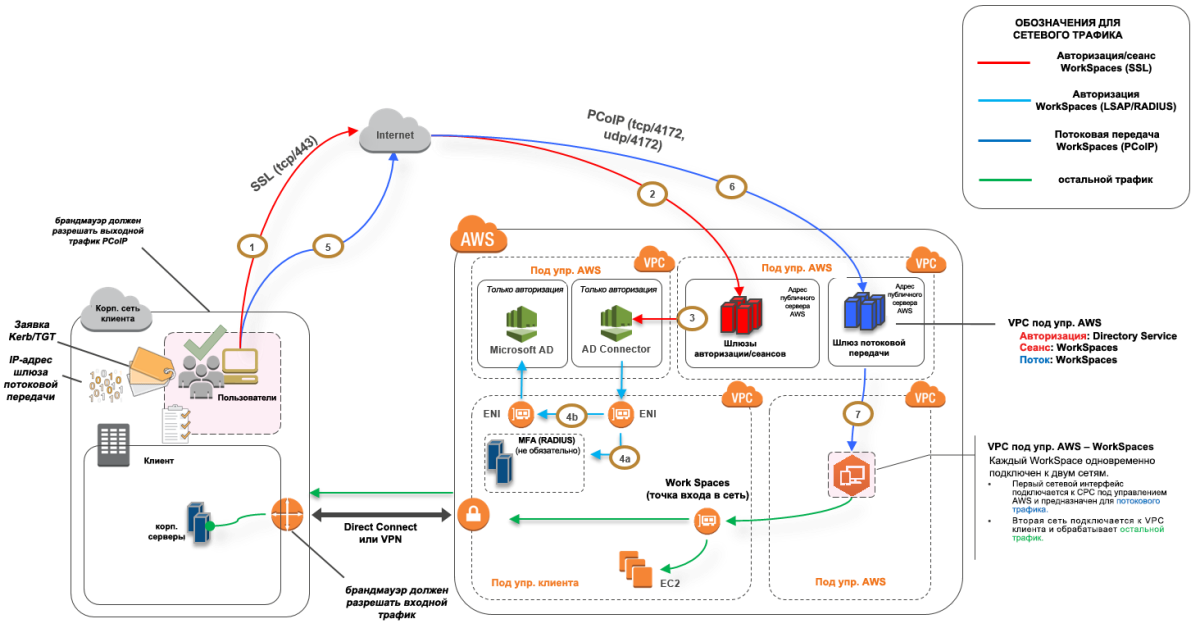

Рисунок 7. Только облако – AWS Directory Services (Microsoft AD)

Как и в сценарии 2, AD DS (Microsoft AD) развертывается в выделенной подсети, которая охватывает две зоны доступности, что обеспечивает высокую доступность AD DS в облаке AWS. В дополнение к Microsoft AD, AD Connector (во всех трех сценариях) развертывается для аутентификации WorkSpaces или MFA. Это обеспечивает разделение ролей и функций в Amazon VPC (что полностью соответствует общепринятым рекомендациям, см. раздел *Некоторые аспекты* проектирования. Разделение сети на разделы).

В сценарии 3 рассматривается стандартная универсальная конфигурация, которая подходит клиентам, которые желают делегировать AWS управление развертыванием, установкой исправлений, высокой доступностью, а также мониторинг AWS Directory Service. Благодаря изолированному режиму этот сценарий отлично подходит не только для продуктивной среды, но и для проверки концепций и лабораторных сред.

Рисунок 7 показывает не только расположение AWS Directory Service, но и поток трафика от пользователя в рабочее пространство и взаимодействие рабочего пространства с серверами AD и MFA.

В этой архитектуре используются следующие компоненты и конструкции.

Amazon Web Services:

- **Amazon VPC:** создание Amazon VPC с по меньшей мере четырьмя частными подсетями в двух зонах доступности (два для AD DS *Microsoft AD* клиента и два для AD Connector или WorkSpaces). «*Разделение ролей*»
- **Набор параметров DHCP:** создание набора параметров DHCP в Amazon VPC. Это позволяет определять заданные клиентом доменное имя и серверы доменных имен (DNS) (Microsoft AD). Дополнительная информация доступна в разделе Набор параметров DHCP.
- **(не обязательно) Виртуальный частный шлюз Amazon:** включение возможности обмена данными с собственной сетью по тоннелю VPN IPsec (VPN) или подключению AWS Direct Connect. Использование для доступа к локальным серверным системам.
- **AWS Directory Service:** Microsoft AD, развернутая в выделенной паре подсетей VPC (управляемая служба AD DS).

- **Amazon EC2:** «дополнительные» серверы RADIUS для MFA.
- **AWS Directory Services**: AD Connector развертывается в паре частных подсетей Amazon VPC.
- **Amazon WorkSpaces:** WorkSpaces развертываются в тех же частных подсетях, что и AD Connector (см. раздел Некоторые аспекты проектирования, AD Connector).

Клиент:

- **(не обязательно) Сетевое подключение:** URL сервера корпоративной VPN или AWS Direct Connect
- **Устройства конечных пользователей:** использование корпоративных устройств или личных устройств конечных пользователей (модель BYOL, устройства Windows, Mac, планшеты iPad или Android, нулевые клиенты, Chromebook) для доступа к сервису Amazon WorkSpaces (см. раздел Поддерживаемые платформы и устройства).

Как и в сценарии 2, здесь не возникает проблем с зависимостью от подключения к локальному ЦОД клиента, задержкой или затратами на исходящий трафик (за исключением случаев, когда доступ к Интернету для WorkSpaces обеспечивается в пределах VPC), поскольку по структуре это изолированный или подразумевающий использование только облачных компонентов сценарий.

Некоторые аспекты проектирования

Чтобы развернуть функциональную службу AD DS в облаке AWS, требуется хорошее понимание специфики Active Directory и конкретных сервисов AWS. В этом разделе рассматриваются основные аспекты проектирования, актуальные при развертывании AD DS для WorkSpaces, рекомендации по развертыванию VPC для AWS Directory Service, требования DHCP и DNS, специфика AD Connector и сайты и службы Active Directory.

Проектирование VPC

Как было сказано в разделе Несколько слов о сетях этого документа и выше, в описании сценариев 2 и 3, AD DS в облаке AWS нужно развертывать в выделенной паре частных подсетей, в двух зонах доступности и отдельно от подсетей AD Connector или WorkSpaces. Эта конструкция обеспечивает WorkSpaces доступ к службам AD DS с высокой доступностью и низкой задержкой. При этом соблюдаются стандартные рекомендации по разделению ролей и функций в Amazon VPC.

Рисунок 8 показывает разделение AD DS и AD Connector в выделенных частных подсетях (сценарий 3). В этом примере все сервисы расположены в одном облаке Amazon VPC.

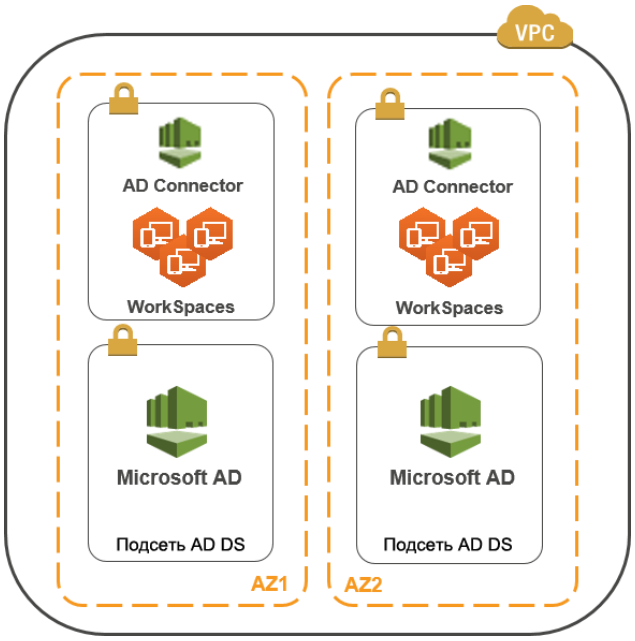

Рисунок 8. Сегрегация сети AD DS

На рисунке 9 показана структура, аналогичная сценарию 1, однако в этом сценарии локальные компоненты размещены в выделенном облаке Amazon VPC.

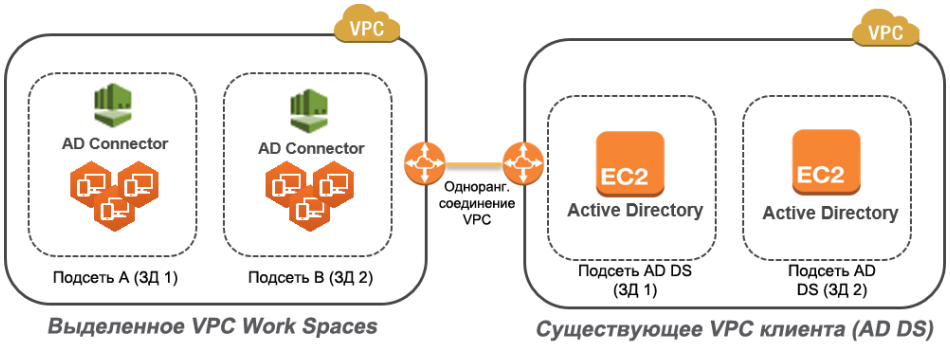

Рисунок 9. Выделенное VPC WorkSpaces

> **Примечание**. Клиентам, которые имеют существующее развертывание AWS, где используются службы AD DS, рекомендуется размещать WorkSpaces в выделенном VPC и использовать одноранговые соединения VPC для обмена данными AD DS.

Помимо создания выделенных частных подсетей для AD DS требуется несколько правил групп безопасности для доменных контроллеров и рядовых серверов – правил, регулирующих трафик сервисов, включая репликацию AD DS, аутентификацию пользователей, службу времени Windows и распределенную файловую систему (DFS).

> **Примечание**. Рекомендуется ограничить необходимые правила групп безопасности частными подсетями WorkSpaces и (как в случае со вторым сценарием) разрешить двунаправленный локальный обмен данными AD DS с облаком AWS, как показано в следующей таблице.

Протокол	Порт	Использование	Место назначения
tcp	53, 88, 135, 139, 389, 445, 464, 636	Авторизация (осн.)	Active Directory (частный центр обработки данных или EC2)*
tcp	49152 – 65535	Высокий диапазон портов RPC	Active Directory (частный центр обработки данных или EC2)**
tcp	3268-3269	Доверие	Active Directory (частный центр обработки данных или EC2)*
tcp	9389	Удаленный компонент Microsoft Windows PowerShell (не обязательно)	Active Directory (частный центр обработки данных или EC2)*
udp	53, 88, 123, 137, 138, 389, 445, 464	Авторизация (осн.)	Active Directory (частный центр обработки данных или EC2)*
udp	1812	Авторизация (MFA) (не обязательно)	RADIUS (частный центр обработки данных или EC2)*

* См. раздел Active Directory и доменные службы Active Directory: требования к портам

**См. раздел Обзор службы и требования к сетевым портам для Windows

Пошаговые инструкции по выполнению правил см. в разделе Добавление правил в группу безопасности *Руководства пользователя Amazon Elastic Compute Cloud*.

Проектирование VPC: DHCP и DNS

При использовании Amazon VPC сервисы DHCP для ваших инстансов предоставляются по умолчанию. По умолчанию каждое облако VPC предоставляет внутренний DNS-сервер, доступный с использованием метода бесклассовой адресации (CIDR) и два адресных пространства. VPC назначается всем инстансам через набор параметров DHCP по умолчанию.

Наборы параметров DHCP используются в Amazon VPC для определения параметров области, таких как доменное имя или серверы имен, которые должны быть переданы вашим инстансам через DHCP. Правильное функционирование служб Windows в VPC зависит от параметра области DHCP, поэтому его нужно задавать очень внимательно. В каждом из ранее определенных сценариев создаются и назначаются собственные области, определяющие ваше доменное имя и серверы имен. Это гарантирует, что подключенные к домену экземпляры Windows или WorkSpaces настроены для использования DNS Active Directory. В следующей таблице приводятся примеры задаваемых пользователем параметров области DHCP, корректные значения которых обеспечивают исправное функционирование WorkSpaces и AWS Directory Services.

Параметр	Значение
Метка имени	Создает метку с ключами = **name** и **value**, заданными для определенной строки Пример: exampleco.com
Доменное имя	exampleco.com
Серверы доменных имен	Адрес сервера DNS, разделяемый запятыми Пример: 10.0.0.10, 10.0.1.10
Серверы NTP	Оставьте это поле пустым
Серверы имен NetBIOS	Введите такие же IP-адреса (разделенные запятыми), что и для серверов доменных имен Пример: 10.0.0.10, 10.0.1.10
Тип узла NetBIOS	2

Подробные сведения о создании пользовательского набора параметров DHCP и связывании этого набора с Amazon VPC см. в разделе Работа с наборами параметров DHCP в *Руководстве пользователя Amazon Virtual Private Cloud*.

В сценарии 1 областью DHCP является локальная система DNS или AD DS. Однако в сценарии 2 или 3 это будет развернутая локально служба каталогов (AD DS в Amazon EC2 или AWS Directory Services: Microsoft AD). Рекомендуется сделать каждый доменный контроллер, размещенный в облаке AWS, глобальным каталогом или интегрированным в каталог DNS-сервером.

Active Directory: сайты и службы

В сценарии 2 сайты и службы имеют критическое значение для правильного функционирования AD DS. Топология сайтов контролирует репликацию Active Directory между доменными контроллерами в масштабах одного или нескольких сайтов. В сценарии 2 присутствует по меньшей мере два сайта: локальный и AWS WorkSpaces в облаке. Правильное определение топологии сайта обеспечивает сходство клиентов (то есть клиенты – в данном случае WorkSpaces – используют предпочтительный локальный доменный контроллер.

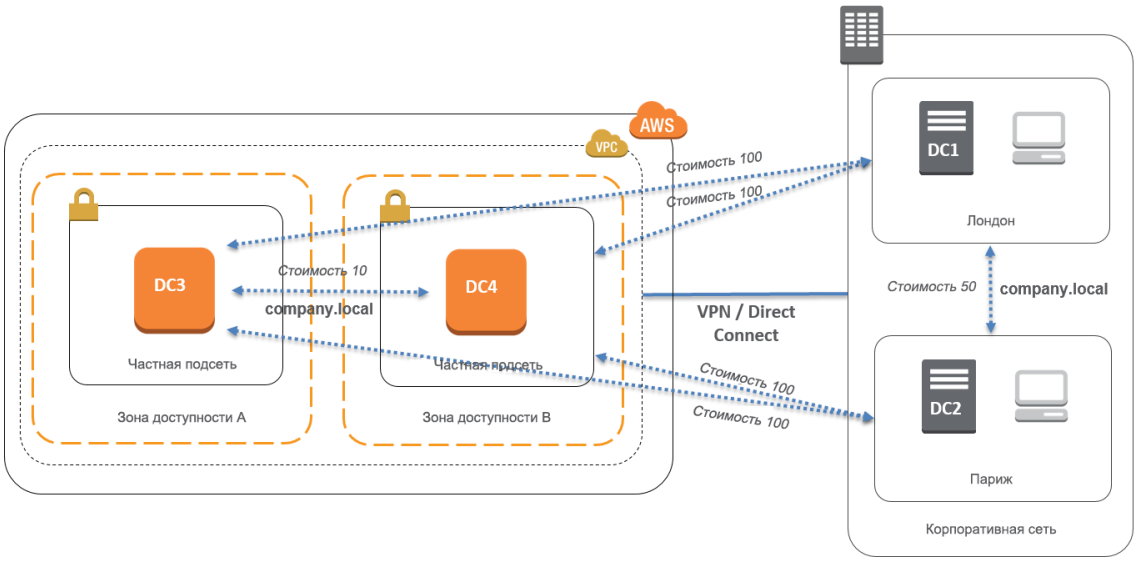

Рисунок 10. Сайты и службы Active Directory: сходство клиентов

Рекомендация. Определите, какие ссылки на сайты, связывающие вашу локальную службу AD DS и облако AWS, имеют наивысшую стоимость. Рисунок 10 содержит пример определения стоимости ссылок на сайты (в данном случае стоимость 100) так, чтобы обеспечить сходство клиентов независимо от сайта.

Эти связи помогают гарантировать перемещение данных (например, репликации AD DS и аутентификации клиента) по наиболее эффективному пути до доменного контроллера. В сценариях 2 и 3 это позволяет сократить задержку и уменьшить объем трафика между ссылками.

Multi-Factor Authentication (MFA)

Для реализации MFA необходимо, чтобы в инфраструктуре WorkSpaces AD Connector использовался в качестве сервиса AWS Directory Service и присутствовал сервер RADIUS. Несмотря на то что в этом документе не рассматривается развертывание сервера, в предыдущем разделе (Сценарии развертывания AD DS) подробно описано размещение RADIUS в каждом из сценариев.

MFA – двухфакторная аутентификация

Amazon WorkSpaces поддерживает MFA с использованием AWS Directory Service: AD Connector и *принадлежащего клиенту* сервера RADIUS. После включения MFA пользователи должны указать в клиенте WorkSpaces **имя пользователя**, **пароль** и **код MFA**, чтобы соответствующие рабочие столы WorkSpaces могли пройти аутентификацию.

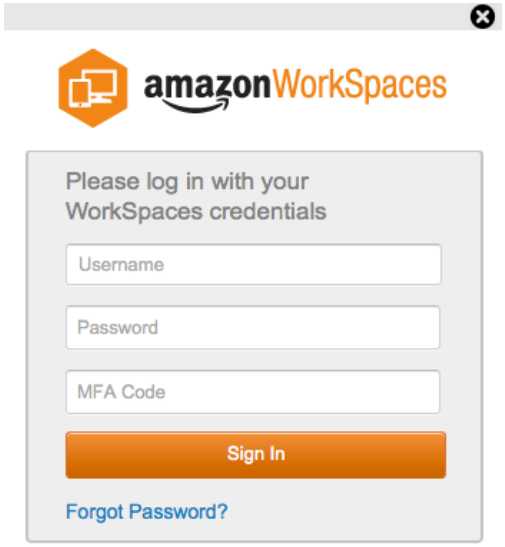

Рисунок 11. Клиент WorkSpaces с включенной MFA

Строгое правило. Для выполнения MFA требуется использовать AD Connector. AD Connector не поддерживает выборочную MFA отдельных пользователей, поскольку это глобальная настройка AD Connector. Если требуется выполнять выборочную MFA отдельных пользователей, необходимо разделить пользователей в AD Connector.

Реализация MFA WorkSpaces требует использования одного или нескольких серверов RADIUS. Как правило, можно использовать существующие решения (например, RSA) либо развернуть серверы в VPC (см. раздел Сценарии развертывания AD DS). Сегодня в отрасли доступно несколько вариантов развертывания нового решения RADIUS, включая FreeRADIUS, и облачные сервисы, такие как Duo Security.

Список обязательных требований для проведения MFA с использованием Amazon WorkSpaces см. в *Руководстве по администрированию Amazon WorkSpaces* и статье Подготовка сети к работе AD Connector Directory. Процедура настройки AD Connector для MFA описана в разделе «Управление AD Connector Directory. MFA» *Руководства по администрированию Amazon WorkSpaces*.

Безопасность

В этом разделе рассказано, как обеспечить безопасность данных с помощью шифрования при использовании сервисов Amazon WorkSpaces. В документе описано шифрование данных при передаче и в состоянии покоя, а также использование групп безопасности для защиты сетевого доступа к WorkSpaces. Дополнительные сведения об аутентификации (включая поддержку MFA) см. в разделе, посвященном AWS Directory Service.

Шифрование данных во время передачи

В Amazon WorkSpaces шифрование используется для обеспечения конфиденциальности на разных этапах обмена данными (в процессе переноса) и защиты данных в состоянии покоя (шифрование данных WorkSpaces). Процессы на каждом этапе шифрования передаваемых данных в Amazon WorkSpaces описаны в следующих разделах. Сведения о шифровании данных в состоянии покоя см. в разделе Шифрование данных WorkSpaces далее в этом техническом описании.

Регистрация и обновления

Для обмена данными между настольным клиентским приложением и Amazon в рамках обновлений и регистрации используется протокол HTTPS.

Этап аутентификации

Настольный клиент инициирует аутентификацию, отправляя данные для доступа в шлюз аутентификации. Для связи между настольным клиентом и шлюзом аутентификации используется протокол HTTPS. В конце этого этапа (если аутентификация пройдена успешно) шлюз аутентификации возвращает токен OAuth 2.0 настольному клиенту, используя то же подключение по протоколу HTTPS.

> **Примечание**. Настольное клиентское приложение поддерживает использование прокси-сервера для трафика через порт 443 (HTTPS), а также для обновлений, регистрации и аутентификации.

После получения от клиента данных для доступа шлюз аутентификации отправляет запрос аутентификации в AWS Directory Service. Обмен данными между шлюзом аутентификации и AWS Directory Service осуществляется по протоколу HTTPS, поэтому данные пользователей для доступа не передаются в виде обычного текста.

Аутентификация – AD Connector

AD Connector использует Kerberos, чтобы установить аутентифицированную связь с локальной службой AD, создать привязку к LDAP и выполнить последующие запросы LDAP. В настоящее время AWS Directory Service не поддерживает трафик LDAP с TLS (LDAPs). Однако данные для доступа пользователей в виде обычного текста никогда не передаются. В целях повышения безопасности можно подключить облако VPC WorkSpaces к локальной сети (где находится служба AD), используя подключение VPN. При использовании VPN-подключения с оборудованием AWS шифрование передаваемых данных настраивается с использованием стандартного протокола IPSEC (SA IKE и IPSEC) с ключами симметричного шифрования AES-128 или AES-256, SHA-1 или SHA-256 для хэша целостности и групп DH (2, 14–18, 22, 23 и 24 для этапа 1; 1, 2, 5, 14–18, 22, 23 и 24 для этапа 2) с PFS.

Этап брокера

После получения токена OAuth 2.0 (от шлюза аутентификации, если аутентификация прошла успешно), настольный клиент запрашивает службы Amazon WorkSpaces (диспетчер подключений к посреднику) по протоколу HTTPS. Настольный клиент проходит аутентификацию, отправляя токен OAuth 2.0, после чего клиент получает информацию о контактной точке потокового шлюза WorkSpaces.

Этап потоковой передачи

Настольный клиент запрашивает открытие сеанса PCoIP с потоковым шлюзом (используя токен OAuth 2.0). В сеансе используется шифрование aes256, а через порт PCoIP осуществляется контроль обмена данными (то есть 4172/tcp).

С помощью токена OAuth2.0 потоковый шлюз запрашивает сведения WorkSpaces о конкретном пользователе у сервиса WorkSpaces по протоколу HTTPS.

Потоковый шлюз также получает мандат TGT от клиента (зашифрованного с помощью пароля пользователя клиента) и, используя сквозную аутентификацию Kerberos с мандатом TGT, инициирует вход в систему в Windows в сервисе WorkSpace, уже с помощью извлеченного пользователем мандата TGT Kerberos.

Затем WorkSpace инициирует запрос аутентификации и направляет его в настроенный сервис AWS Directory Service, используя стандартную аутентификацию Kerberos.

После успешного входа в систему в сервисе WorkSpace начинается потоковая передача PCoIP. Подключение инициируется клиентом в порту tcp 4172 с обратным трафиком в порту udp 4172. Кроме того, первоначальное подключение между потоковым шлюзом и рабочим столом WorkSpaces через интерфейс управления устанавливается в порту UDP 55002. (См. документацию по Amazon Workspaces, Сведения об Amazon WorkSpaces. Первоначальный исходящий порт UDP имеет номер 55002.) Подключение для потоковой передачи данных (порты tcp и udp с номером 4172) шифруется с использованием 128- и 256-битных шифров AES, однако по умолчанию используется 128-битное шифрование. С помощью групповой политики Active Directory для PCoIP можно явным образом изменить эту настройку и установить 256-битное шифрование (pcoip.adm).

Сетевые интерфейсы

Каждый сервис Amazon WorkSpace имеет два сетевых интерфейса: основной сетевой интерфейс и сетевой интерфейс управления.

Основной сетевой интерфейс обеспечивает подключение к ресурсам внутри VPC, включая доступ к AWS Directory Service, Интернету и корпоративной сети. Можно прикрепить группы безопасности к основному сетевому интерфейсу (как к любому интерфейсу ENI). Концептуально мы различаем группы безопасности, прикрепляемые к этому интерфейсу ENI с учетом области развертывания: группа безопасности WorkSpaces и группы безопасности ENI.

Сетевой интерфейс управления

Невозможно контролировать сетевой интерфейс управления через группы безопасности, однако для блокирования портов и контроля доступа можно использовать серверный брандмауэр в WorkSpace. Не рекомендуется налагать ограничения на сетевой интерфейс управления. Если принято решение о добавлении правил серверного брандмауэра для управления этим интерфейсом, необходимо будет оставить несколько портов открытыми, чтобы сервис WorkSpaces мог управлять состоянием и доступностью системы, как определено в Руководстве по администрированию Amazon WorkSpaces.

Группа безопасности WorkSpaces

Группа безопасности по умолчанию создается для каждого сервиса AWS Directory Service и автоматически прикрепляется ко всем WorkSpaces, которые относятся к конкретному каталогу.

Как и в случае с любой другой группой безопасности, можно изменить правила группы безопасности WorkSpaces. Внесенные изменения вступают в силу немедленно.

Можно также изменить группу безопасности WorkSpaces по умолчанию, прикрепленную к AWS Directory Service, изменив связь групп безопасности WorkSpaces.

> **Примечание**. Вновь созданная группа безопасности будет прикреплена только к WorkSpaces, создаваемым или перестраиваемым после модификации.

Группы безопасности ENI

Поскольку основной сетевой интерфейс – это обычный интерфейс ENI, его настройкой можно управлять с использованием разных средств управления AWS (см. раздел Эластичные сетевые интерфейсы (ENI)). В частности, найдите IP-адрес WorkSpace (на странице WorkSpaces консоли Amazon WorkSpaces), а затем используйте этот IP-адрес в качестве фильтра, чтобы найти соответствующий интерфейс ENI (в разделе «Сетевые интерфейсы» на консоли Amazon EC2).

Найдя интерфейс ENI, можно управлять группами безопасности непосредственно из него. Если группы безопасности назначаются основному сетевому интерфейсу вручную, учитывайте требования портов Amazon WorkSpaces, указанные в разделе Сведения об Amazon WorkSpaces.

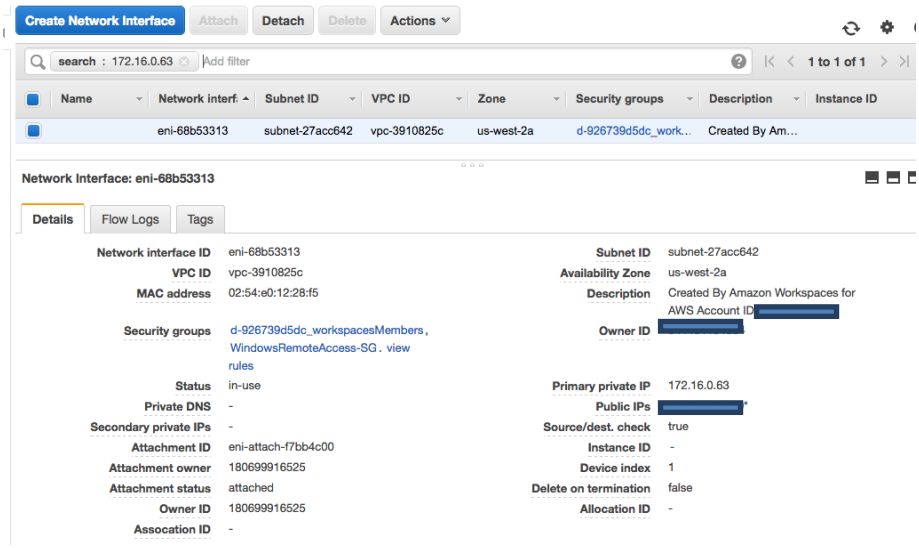

Рисунок 12. Управление связями групп безопасности

Зашифрованные данные WorkSpaces

В каждом Amazon WorkSpace подготовлен корневой том (диск C:) и том пользователя (диск D:). Функция шифрования данных WorkSpaces позволяет шифровать эти тома по отдельности или вместе.

Что шифруется?

Шифруются сохраненные данные в состоянии покоя, дисковые операции ввода-вывода в томе и снимки состояния зашифрованных томов.

Когда происходит шифрование?

Следует указать необходимость шифрования данных в WorkSpace во время запуска (создания) WorkSpace. Тома WorkSpaces можно зашифровать только на этапе запуска сервера: после этого изменить статус шифрования тома невозможно. Рисунок 13 показывает страницу консоли Amazon WorkSpaces, на которой можно выбрать режим шифрования при запуске нового WorkSpace.

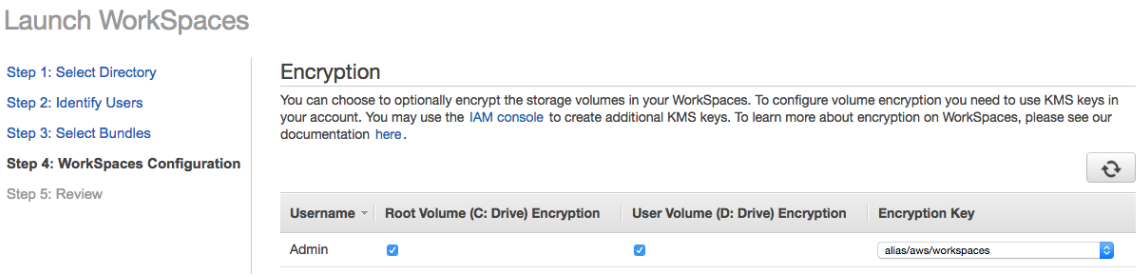

Рисунок 13. Шифрование томов WorkSpaces

Как шифруется новый сервис WorkSpace?

Шифрование данных WorkSpaces можно выбрать на консоли Amazon WorkSpaces, в интерфейсе командной строки AWS или с помощью API Amazon WorkSpaces в момент запуска нового WorkSpace.

Для шифрования томов Amazon WorkSpaces использует главный ключ клиента (CMK) из сервиса AWS Key Management Service (KMS). Главный ключ клиента AWS KMS по умолчанию создается при первом запуске WorkSpace в регионе (ключи клиента имеют область действия – регион AWS). Кроме того, можно создать управляемый клиентом ключ CMK и использовать его с зашифрованными WorkSpaces. Ключ CMK используется для шифрования ключей данных, с помощью которых сервис Amazon WorkSpaces шифрует тома (в строгом смысле тома шифруются сервисом Amazon Elastic Block Store (Amazon EBS)). Каждый ключ CMK можно использовать для шифрования ключей в нескольких (до 30) WorkSpaces.

> **Примечание**. Создание пользовательских изображений из зашифрованного WorkSpace в настоящее время не поддерживается. Кроме того, подготовка WorkSpaces, запущенного с включенным шифрованием корневого тома, может занимать до одного часа.

Подробное описание процесса шифрования WorkSpaces см. в разделе Обзор шифрования данных в Amazon WorkSpaces с использованием AWS KMS. Дополнительные сведения о главных ключах клиента AWS KMS и ключах данных см. в разделе Функционирование службы управления ключами AWS.

Мониторинг и ведение журнала с использованием Amazon CloudWatch

Мониторинг – неотъемлемая часть любой инфраструктуры (сети, серверов или журналов). Клиенты, развертывающие Amazon WorkSpaces, должны осуществлять мониторинг развертываний, в частности контролировать общее состояние и статус подключения отдельных WorkSpaces.

Метрики WorkSpaces в Amazon CloudWatch

Метрики WorkSpaces в CloudWatch предоставляют администраторам дополнительные сведения об общей работоспособности и состоянии подключения отдельных WorkSpaces. Доступны метрики как для отдельных сервисов WorkSpace, так и для всех сервисов WorkSpaces в организации в составе выбранного каталога (*AD Connector, см. раздел «Идентификация»*).

Эти метрики, как и все метрики CloudWatch, отображаются на консоли управления AWS (рисунок 13). Доступ к ним осуществляется через API, а мониторинг этих метрик – с использованием предупреждений CloudWatch и сторонних инструментов.

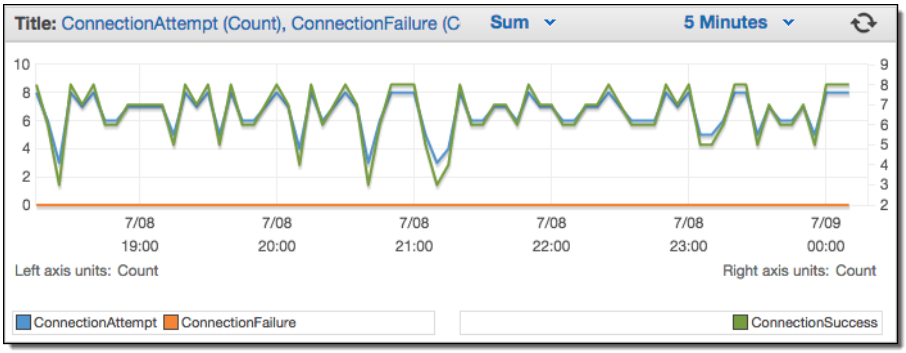

Рисунок 14. Метрики CloudWatch – ConnectionAttempt/ConnectionFailure

По умолчанию включены и доступны без дополнительной платы следующие метрики.

- **Доступно**: количество сервисов WorkSpaces, реагирующих на проверку состояния.
- **Неисправно**: количество сервисов WorkSpaces, которые не реагируют на эту проверку состояния.
- **ConnectionAttempt**: количество сделанных попыток подключения к WorkSpace.
- **ConnectionSuccess**: количество успешных попыток подключения.
- **ConnectionFailure**: количество неудачных попыток подключения.
- **SessionLaunchTime**: время, затраченное на запуск сеанса (по измерениям клиента WorkSpaces).
- **InSessionLatency**: время приема-передачи между клиентом WorkSpaces и сервисами WorkSpaces (по измерениям и данным клиента).
- **SessionDisconnect**: количество инициированных пользователем и автоматически закрытых сеансов.

Кроме того, как показано на рисунке 15, можно создавать и свои предупреждения.

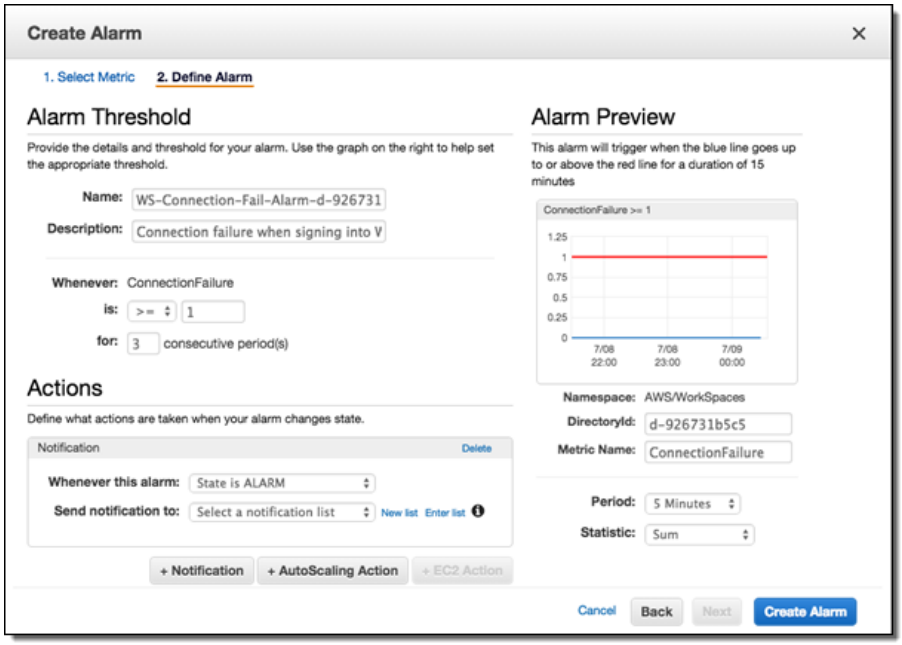

Рисунок 15. Создание предупреждения CloudWatch об ошибках подключения WorkSpaces

Устранение неполадок

Описание стандартных проблем администрирования и проблем, возникающих в клиентах, вроде «Я вижу следующее сообщение об ошибке: «Вашему устройству не удается подключиться к службе регистрации WorkSpaces» или «Невозможно подключиться к WorkSpace с интерактивным баннером входа» и т. д.» можно найти на страницах, посвященных устранению неполадок с клиентом и неполадок в администрировании, *Руководства по администрированию Amazon WorkSpaces*.

AD Connector не удается подключиться к Active Directory

Чтобы AD Connector мог подключиться к вашему локальному каталогу, в брандмауэре вашей локальной сети должны быть открыты определенные порты для бесклассовой адресации (CIDR) в обеих подсетях VPC (см. раздел AD Connector). Чтобы проверить выполнение этих условий, выполните следующие шаги.

Проверка подключения

1. Запустите экземпляр Windows в VPC и подключитесь к нему через RDP. Остальные шаги выполняются в инстансе VPC.
2. Загрузите и распакуйте пример приложения DirectoryServicePortTest. В пример приложения включены исходный код и файлы проекта Visual Studio, поэтому при необходимости в приложение можно внести изменения.
3. В командной строке Windows запустите пример приложения DirectoryServicePortTest со следующими параметрами.

```
DirectoryServicePortTest.exe -d <доменное_имя> -ip <IP-адрес_сервера> -tcp
"53,88,135,139,389,445,464,636,49152" -udp "53,88,123,137,138,389,445,464"
<доменное_имя>
```

<доменное_имя>

Полное доменное имя, использующееся для проверки функциональных уровней леса и домена. Если исключить доменное имя, функциональные уровни тестироваться не будут.

<IP-адрес_сервера>

IP-адрес контроллера вашего локального домена. Порты будут протестированы относительно этого IP-адреса. Если исключить IP-адрес, порты тестироваться не будут.

Это позволит определить, открыты ли необходимые порты в VPC для вашего домена. Пример приложения также проверяет минимальные функциональные уровни леса и домена.

Проверка задержки до ближайшего региона AWS

В октябре 2015 года Amazon WorkSpaces запустил веб-сайт для проверки состояния подключения. Этот веб-сайт быстро проверяет, доступны ли вам все необходимые сервисы для использования WorkSpaces. Кроме того, сайт выполняет проверку производительности каждого региона AWS, где работает WorkSpaces, и сообщает, в каком регионе сервис будет работать быстрее.

Заключение

По мере того как организации стремятся действовать более гибко, лучше защищать свои данные и способствовать повышению продуктивности своих сотрудников, мы наблюдаем стратегические изменения в вычислительных системах для конечных пользователей. Многие преимущества облачных вычислений актуальны и для вычислительных систем для конечных пользователей. Перенося рабочие столы в облако AWS с помощью Amazon WorkSpaces, организации могут быстро масштабировать свои системы, добавляя работников, повышать уровень безопасности, не храня данные на устройствах, и предоставлять своим специалистам портативные рабочие столы с повсеместным доступом с любого устройства по выбору пользователя.

Amazon WorkSpaces предусматривает интеграцию в существующие ИТ-системы и процессы, и в этом информационном документе вы найдете рекомендации по выполнению этой задачи. Следуя инструкциям в этом информационном описании, вы сможете с минимальными затратами развернуть облачные рабочие столы в глобальной инфраструктуре AWS и расширять систему по мере необходимости.

Авторский коллектив

Данный документ был подготовлен при участии следующих лиц.

- Джастин Брэдли (Justin Bradley), архитектор решений, Amazon Web Services
- Махди Саджадпур (Mahdi Sajjadpour), старший консультант, AWS Professional Services
- Маурицио Муноз (Mauricio Munoz), архитектор решений, Amazon Web Services

Дополнительная литература

См. дополнительные справочные сведения в следующих источниках:

- Устранение неполадок в администрировании AWS Directory Service
- Устранение неполадок в администрировании Amazon WorkSpaces
- Устранение неполадок с клиентом Amazon WorkSpaces
- Руководство по администрированию Amazon WorkSpaces
- Руководство разработчика Amazon WorkSpaces
- Поддерживаемые платформы и устройства
- Использования AWS KMS в Amazon WorkSpaces
- Справочник по командам интерфейса командной строки AWS – WorkSpaces
- Мониторинг метрик Amazon WorkSpaces