Глоссарий

В данном разделе приведен глоссарий основных терминов, которые присутствуют в документации.

Аутентификация в StarVault

Процесс, в ходе которого информация, предоставленная пользователем или машиной, проверяется на соответствие внутренней или внешней системе. StarVault поддерживает множество методов аутентификации, включая LDAP, AppRole и другие.

Брокер аудита (audit broker)

Используется ядром для регистрации запросов и ответов, а также распространения информации между устройствами аудита.

Бэкенд хранилища (storage backend)

Компонент, обеспечивающий устойчивое и надежное хранение секретов.

Ключ распечатки

Используется для расшифровки корневого ключа. С помощью алгоритма разделения секрета Шамира делится на фрагменты.

Ключ шифрования (encryption key)

Используется для защиты всех данных StarVault. Зашифрован с помощью корневого ключа.

Корневой ключ (root key)

Используется для защиты ключа шифрования. Зашифрован с использованием ключа распечатки.

Политики доступа (access policies)

Представляют собой именованные наборы правил контроля доступа (ACL) к определенным путям в системе, ограничивая или разрешая клиенту выполнять конкретные действия в рамках этих путей.

Порог ключа (key threshhold)

Количество фрагментов ключа распечатки, достаточное для расшифровки корневого ключа.

Секрет

Конфиденциальные данные, такие как токены, API-ключи, пароли, ключи шифрования и сертификаты, доступ к которым должен быть строго ограничен.

Сервер StarVault

Основной компонент StarVault, который обрабатывает запросы от клиентов, управляет хранилищем секретов и принимает решения по аутентификации и авторизации.

Механизм управления секретами (secrets engine)

Компонент, отвечающий за управление, хранение и шифрование данных.

Устройства аудита (audit devices)

Механизм, отслеживающий операции в системе

Хранилище политик (policy store)

Компонент StarVault, обеспечивающий централизованное хранение и управление политиками.

Хранилище токенов (token store)

Компонент StarVault, обеспечивающий централизованное хранение и управление клиентскими токенами.

Доля ключа (key share)

Это отдельный фрагмент ключа распечатки, полученный в результате его разделения методом разделения секрета Шамира.

Отказоустойчивость

Для достижения отказоустойчивости StarVault работает в режиме высокой доступности (HA), запуская несколько серверов StarVault.

1. Обзор решения

Высокая доступность (HA) минимизирует время простоя, без ущерба для горизонтальной масштабируемости. StarVault ограничен лимитами ввода-вывода бэкенда хранения, а не требованиями к вычислительным ресурсам. Ограничение лимитами ввода-вывода упрощает подход к отказоустойчивости и координации.

Бэкенды хранения, такие как Integrated Storage, предоставляют дополнительные функции координации, позволяют StarVault работать в режиме высокой доступности. Если поддержан бэкенда хранения, то StarVault автоматически запускается в режиме высокой доступности без дополнительной настройки.

Узлы StarVault при работе в режиме высокой доступности находятся в двух состояниях: ожидание или активное. Для нескольких узлов StarVault, использующих общее хранилище, в любой момент времени активен только один узел. Узлы в состоянии ожидания помещаются в горячий резерв.

Только активный узел обрабатывает запросы; резервный узел перенаправляет запросы на активный узел StarVault.

В то же время, если активный узел запечатан, выходит из строя или теряет сетевое подключение, то один из резервных узлов StarVault становится активным.

Обратите внимание, что только распечатанные узлы StarVault действовуют как резервные. Если узел запечатан, то он не выступает в качестве резервного. Узлы в запечатанном состоянии не обрабатывают запросы, если активный узел выходит из строя.

2. Особенность работы в отказоустойчивом режиме

StarVault поддерживает многосерверный режим, который обеспечивает высокую доступность и защиту от сбоев. Режим высокой доступности включается автоматически при использовании хранилища данных, которое его поддерживает.

Чтобы узнать, поддерживает ли хранилище данных режим высокой доступности (HA), запустите сервер и посмотрите, отображается ли сообщение (HA available) рядом с

информацией о хранилище данных. Если да, то StarVault будет использовать режим автоматически. Эта информация также доступна на странице Конфигурирование.

Для поддержки высокой доступности один из серверных узлов StarVault выполняет блокировку хранилища данных. Такой серверный узел затем становится активным узлом, а остальные узлы – резервными. Если в этот момент резервные узлы получат запрос, то в зависимости от текущей конфигурации и состояния кластера либо переадресуют запрос, либо перенаправят клиента. Подробности см. в разделах ниже.

В силу такой архитектуры, HA не улучшает масштабируемость. Узкое место StarVault - само хранилище данных, а не ядро.

> Пример: чтобы повысить масштабируемость StarVault с Consul, обычно масштабируется Consul, а не StarVault.

Некоторые бэкенды хранения поддерживают режим высокой доступности, что позволяет им хранить не только значение блокировки HA, но и информацию StarVault. Однако StarVault также поддерживает режим "разделения данных/высокой доступности", в котором значение блокировки и остальные данные хранятся раздельно.

Для этого укажите в конфигурационном файле строкам конфигурации `storage` и `ha_storage` разные бэкенды. Например, кластер StarVault настроить на использование Consul в качестве `ha_storage` для управления блокировкой, а `file` в качестве storage для остальных сохраняемых данных.

В разделах ниже подробно описываются шаблоны взаимодействия с сервером и каждый тип обработки запросов. Для работы кластера высокой доступности должны выполнены минимальные требования к режиму перенаправления.

2.1. Взаимодействие сервер-сервер

Методы для взаимодействия сервер-сервер: перенаправления клиента, переадресации запросов серверам.

Оба метода обработки запросов основаны на том, что активный узел объявляет информацию о себе другим узлам. Это взаимодействие протекает не по сети, а выполняется внутри зашифрованного хранилища StarVault; активный узел записывает эту информацию, а незапечатанные резервные узлы StarVault могут ее прочитать.

В случае метода перенаправления клиента между серверами нет прямого взаимодействия, и только зашифрованные записи в хранилище данных используются для передачи состояния.

В случае метода переадресации запросов серверам необходимо прямое взаимодействие друг с другом. Чтобы сделать это безопасно, активный узел также объявляет через зашифрованную запись хранилища данных только что сгенерированный закрытый ключ (ECDSA-P521) и только что сгенерированный самоподписанный сертификат, предназначенный для аутентификации клиента и сервера. Каждый резервный узел использует закрытый ключ и сертификат для открытия взаимно аутентифицированного соединения TLS 1.2 с активным узлом через объявленный адрес кластера. Клиентских запросы при поступлении сериализуются, отправляются по защищенному TLS каналу связи и обрабатываются активным узлом. Затем активный узел возвращает ответ резервному узлу, который отправляет ответ обратно запрашивающему клиенту.

2.2. Переадресация запросов

Если переадресация запросов включена (по умолчанию включена), то при необходимости клиенты по-прежнему могут принудительно использовать более старую процедуру перенаправления как резервный вариант (см. ниже), установив заголовок `X-StarVault-No-Request-Forwarding` в любое непустое значение.

Для настройки кластера требуется несколько параметров конфигурации, хотя некоторые из них могут быть определены автоматически.

2.3. Перенаправление клиента

Если заголовок `X-StarVault-No-Request-Forwarding` в запросе установлен в непустое значение, то резервные узлы будут, используя код статуса `307`, перенаправлять клиента на адрес перенаправления активного узла.

Это тоже резервный метод, который используется, если переадресация запросов отключена или если при переадресации произошла ошибка. Таким образом, для настроек высокой доступности всегда требуется адрес перенаправления.

Некоторые драйверы хранилищ данных высокой доступности могут автоматически определять адрес перенаправления. Часто требуется настраивать адрес перенаправления вручную с помощью значения верхнего уровня в файле конфигурации. Ключ для этого значения — `api_addr`. Так же значение настраивается при помощи переменной окружения `VAULT_API_ADDR`. Переменная окружения `VAULT_API_ADDR` приоритетнее ключа `api_addr`.

Значение для `api_addr`, зависит от того, как настроен StarVault. Два частых сценария:

- серверы StarVault, к которым клиенты обращаются напрямую;
- серверы StarVault, обращение к которым происходит через балансировщик нагрузки.

В обоих случаях `api_addr` представляет полный URL-адрес, включая схему (`http` / `https`), а не просто IP-адрес и порт.

2.3.1. Прямой доступ

Когда клиенты обращаются к StarVault напрямую, `api_addr` для каждого узла представляет собой адрес этого узла. Например, есть два узла StarVault:

- **A**, доступный через `https://a.starvault.mycompany.com:8200`
- **B**, доступный через `https://b.starvault.mycompany.com:8200`

Тогда узел **A** установит свой `api_addr` в значение `https://a.starvault.mycompany.com:8200` , а узел **B** установит свой `api_addr` в значение `https://b.starvault.mycompany.com:8200` .

Когда узел **A** активный, то любые запросы, получаемые узлом **B**, будут перенаправлены на api_addr узла **A** по адресу `https://a.starvault.mycompany.com` , и наоборот.

2.3.2. Доступ через балансировщики нагрузки

Иногда клиенты используют балансировщики нагрузки в качестве первоначального метода доступа к одному из серверов StarVault, но при этом имеют прямой доступ к каждому узлу StarVault. В этом случае серверы StarVault настройте так же, как описано в предыдущем разделе, поскольку для целей перенаправления клиенты имеют прямой доступ.

Однако если единственный способ доступа к серверам StarVault – через балансировщик нагрузки, то на каждом узле должен быть настроен один и тот же `api_addr` : адрес балансировщика нагрузки. Клиенты, чьи запросы достигли резервного узла, будут перенаправлены обратно на балансировщик нагрузки. Если к этому моменту конфигурация балансировщика нагрузки обновится и адрес текущего ведущего узла станет известен, то будет создан замкнутый цикл перенаправления. Поэтому не рекомендуется использовать доступ через балансировщик нагрузки как единственный способ доступа к серверам StarVault.

2.3.3. Адреса обработчиков на каждом узле кластера

Каждый блок `listener` в конфигурационном файле StarVault содержит значение `address` , на котором StarVault прослушивает запросы. Аналогично, каждый блок `listener` может содержать `cluster_address` , на котором StarVault прослушивает запросы между серверами кластера. Если это значение не задано, то IP-адрес будет автоматически установлен в значение, равное значению `address` , а порт будет автоматически установлен в значение, равное значению `address` плюс один (по умолчанию – порт `8201`).

Обратите внимание, что только у активных узлов имеются активные обработчики. Когда узел становится активным, то запускает обработчики в кластере, а когда становится резервным, останавливает их.

2.3.4. Адрес каждого узла в кластере

Как и `api_addr`, `cluster_addr` – это значение, которое каждый активный узел объявляет резервным узлам, для использования во взаимодействии сервер-сервер. В конфигурационном файле `cluster_addr` - значение верхнего уровня.

На каждом узле должны быть имя хоста или IP-адрес, который резервный узел может использовать для связи с одним из значений `cluster_address` этого узла, установленных в блоках слушателей, включая порт. (Обратите внимание, что этот порт будет принудительно установлен на `https`, поскольку между серверами используются только TLS-соединения).

Это значение также можно указать с помощью переменной окружения `VAULT_CLUSTER_ADDR`, которая имеет приоритет.

2.4. Поддержка хранилища

Существует несколько бэкендов хранения, поддерживающих режим высокой доступности, включая встроенное хранилище и Consul. Время от времени они изменяются, поэтому обязательно приводите ссылка на страницу конфигурации.

При новом развертывании StarVault рекомендуется использовать встроенное хранилище StarVault в качестве бэкенда высокой доступности по умолчанию. Бэкенд хранения Consul также поддерживается и используется во многих продуктивных системах. Для выбора оптимального варианта см. таблицу сравнения.

Если вы хотите использовать другой бэкенд или добавить поддержку высокой доступности к другому бэкенду - обратитесь в поддержку StarVault.

Добавление поддержки высокой доступности требует внедрения интерфейса `physical.HABackend `для бэкенда хранения.

Устройство StarVault

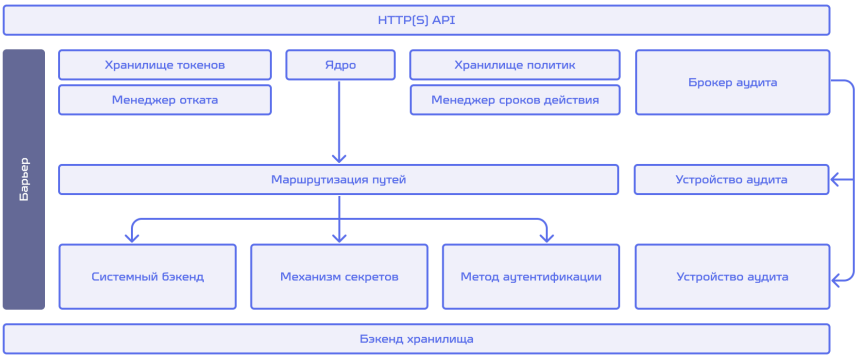
В этом разделе рассматриваются внутренние компоненты StarVault и объясняются технические детали функционирования StarVault, его архитектура и свойства безопасности.

Мы настоятельно советуем всем пользователям и администраторам внимательно изучить эту информацию до начала работы со StarVault, учитывая ее значимость для безопасности и эффективности рабочей среды.

1. Архитектура

StarVault - это сложная система, состоящая из множества различных компонентов. На этой странице описывается архитектура системы и предоставляется информация, которая поможет пользователям StarVault сформировать представление о системе, а также понять принципы её работы.

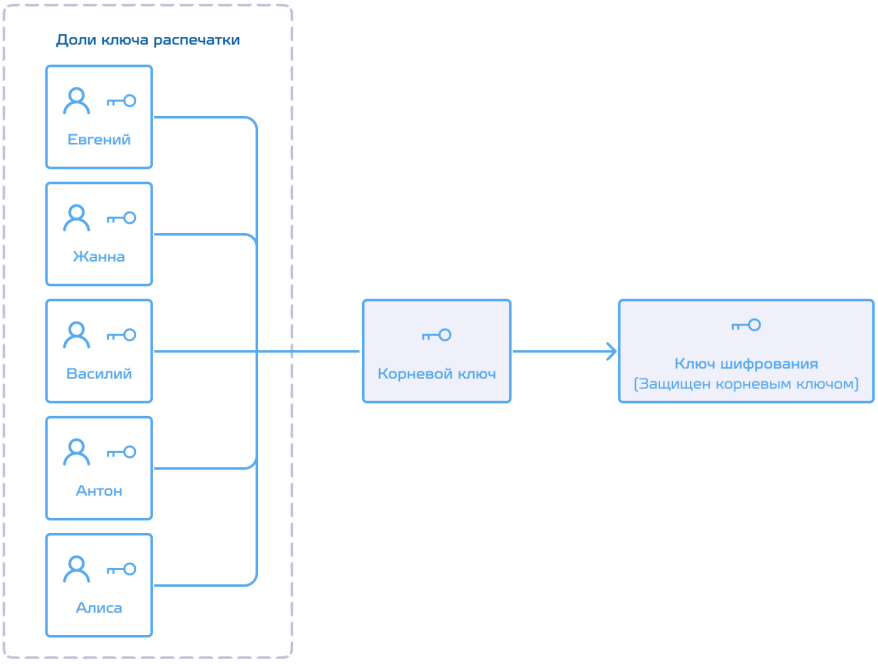
Приведенная ниже диаграмма наглядно демонстрирует структуру и многообразие компонентов системы StarVault.



Модуль шифрования StarVault, известный как **барьер**, отвечает за процесс шифрования и расшифровки данных в системе StarVauvlt. В момент запуска сервера StarVault все данные, записываемые во внутреннее хранилище, подлежат шифрованию. Так как бэкенд хранилища находится вне зоны доверия, то есть за **барьером**, StarVault применяет шифрование для защиты данных перед их передачей в хранилище. Этот подход обеспечивает безопасность данных даже в случае несанкционированного доступа к бэкенду хранилища, так как без расшифровки со стороны StarVault данные остаются недоступными для посторонних. Бэкенд хранилища служит для надежного долгосрочного хранения, гарантируя сохранность и доступность информации даже после перезагрузки сервера.

Когда сервер StarVault запускается, он начинает работу в запечатанном состоянии (**sealed state**). Прежде чем можно будет выполнить какую-либо операцию с StarVault, его необходимо распечатать (**unsealed**). Это делается путём предоставления ключей распечатки (**unseal key**). Во время инициализации StarVault генерирует ключ шифрования (**encryption key**), который используется для защиты всех данных StarVault. Этот ключ защищен корневым ключом (**root key**), который хранится вместе со всеми другими данными StarVault, но шифруется другим механизмом: ключом распечатки.

По умолчанию StarVault использует метод разделения секрета Шамира для разделения ключа распечатки на заданное количество фрагментов (долей ключа). Для воссоздания ключа распечатки требуется точное количество фрагментов, которые затем используются для расшифровки корневого ключа StarVault.



Метод Шамира может быть отключен. В этом случае для распечатывания можно использовать непосредственно корневой ключ. Как только StarVault получает ключ шифрования, он расшифровывает данные в бэкенде хранилища и переходит в распечатанное состояние. В распечатанном состоянии StarVault инициирует загрузку предварительно настроенных устройств аудита, методов аутентификации и механизмов управления секретами.

Конфигурация устройств аудита, методов аутентификации и механизмов управления секретами является чувствительной с точки зрения безопасности и хранится в StarVault. Только пользователи, обладающие необходимыми правами, могут вносить изменения в эти конфигурации, причем модификация возможна исключительно в пределах барьера. Размещение конфигурации в StarVault гарантирует, что любые изменения защищены системой контроля доступа (ACL) и документируются в журналах аудита.

После распечатывания StarVault, система может начать обработку входящих запросов, поступающих через HTTP API, направляя их к ядру. Ядро системы координирует дальнейшую маршрутизацию запросов, осуществляет контроль доступа с использованием списков контроля доступа (ACL) и ведёт журнал аудита для обеспечения прозрачности и отслеживания всех операций.

Перед началом работы с StarVault клиент должен пройти процесс аутентификации. StarVault поддерживает широкий спектр настраиваемых методов аутентификации, что позволяет выбрать наиболее подходящий механизм в зависимости от типа клиента. Так, для операторов доступны методы аутентификации через имя пользователя и пароль, в то время как приложения могут аутентифицироваться с помощью пары открытый/закрытый ключ или с использованием токенов. В процессе аутентификации запрос проходит через ядро системы и обрабатывается выбранным методом аутентификации, который проверяет его валидность и, в случае успеха, предоставляет список политик, связанных с аутентифицированным клиентом.

Политики в StarVault представляют собой именованные наборы правил контроля доступа (ACL). К примеру, встроенная политика "root" предоставляет неограниченный доступ ко всем операциям и ресурсам. Пользователи могут создавать множество именованных политик, настраивая детализированный контроль доступа к определенным путям в системе. StarVault функционирует по принципу явного разрешения: действие считается запрещенным до тех пор, пока не будет выдано явное разрешение через соответствующую политику. Если пользователю присвоено несколько политик, действие разрешается, если хотя бы одна из политик это допускает. Все политики централизованно хранятся и управляются через внутреннее хранилище политик StarVault. Доступ к этому хранилищу осуществляется через системный бэкэнд, который всегда монтируется по адресу **sys/**.

После прохождения аутентификации и получения набора соответствующих политик, генерируется новый клиентский токен, который управляется хранилищем токенов. Этот клиентский токен используется для выполнения последующих запросов. Метод использования токена аналогичен отправке cookie веб-сайтом при входе пользователя в систему. В зависимости от конфигурации метода аутентификации, клиентский токен может иметь связанный с ним срок действия (lease), и его может потребоваться периодически обновлять, чтобы избежать аннулирования.

После аутентификации запросы выполняются с предоставлением клиентского токена. Клиентский токен используется для верификации клиента, обеспечивая его авторизацию и загрузку соответствующих политик. Эти политики применяются для авторизации клиентского запроса. Затем запрос направляется к механизму управления секретами, где он обрабатывается в соответствии с его типом. Когда механизм секретов возвращает секрет, ядро системы регистрирует его в менеджере сроков действия и присваивает идентификатор аренды (lease ID). Клиенты используют идентификатор аренды для продления или отзыва своего секрета. Если клиент не продлевает аренду и срок её действия истекает, менеджер сроков действия автоматически отзывает секрет.

Ядро регистрирует запросы и ответы в брокере аудита, который, в свою очередь, распространяет информацию между всеми настроенным устройствам аудита. В дополнение к обработке запросов, ядро выполняет ряд фоновых операций, среди которых управление арендой занимает ключевое место. Это управление позволяет системе автоматически аннулировать клиентские токены и секреты, срок действия которых истек. StarVault также обеспечивает надежность системы при частичных сбоях, используя специальные механизмы, такие как журналирование с упреждающей записью и менеджер отката. Все эти процессы управления скрыты от пользователя и работают незаметно в фоновом режиме.

2. Высокая доступность

StarVault может функционировать в режиме высокой доступности (High Availability, HA) для защиты от сбоев путем запуска нескольких серверов StarVault.

Основная цель StarVault Highly Available (HA) - минимизировать время простоя системы без потери возможностей для ее масштабирования. Производительность StarVault ограничена скоростью операций ввода-вывода используемого бэкенда хранилища, а не потребностями в вычислительных ресурсах.

Бэкенды хранения, например Интегрированное хранилище (Integrated Storage), включают в себя дополнительные механизмы координации, которые позволяют StarVault функционировать в HA-конфигурации. Когда StarVault настроен на использование такого бэкенда, он автоматически переходит в режим высокой доступности, не требуя от администратора внесения дополнительных настроек.

В режиме высокой доступности (HA) серверы StarVault могут находиться в одном из двух состояний: активном или резервном. В конфигурации с несколькими серверами, использующими общий бэкенд хранилища, одновременно активным может быть только один сервер. Остальные серверы находятся в состоянии готовности к немедленному перехвату задач (горячее резервирование).

Запросы обрабатываются исключительно активным сервером, в то время как резервные серверы перенаправляют все входящие запросы к нему.

В случае блокировки, сбоя или потери сетевого соединения активным сервером, один из резервных серверов автоматически переключается в активное состояние, обеспечивая непрерывность работы системы.

Только серверы StarVault в распечатанном состоянии могут функционировать как резервные. Серверы в запечатанном состоянии не способны принять на себя роль активного сервера и не могут обрабатывать запросы в случае отказа активного сервера.

3. Бэкенды хранилища

3.1. Интегрированное хранилище Raft

3.1.1. Общие сведения

StarVault поддерживает несколько вариантов долговременного хранения информации. Каждый вариант имеет свои плюсы, минусы, преимущества и компромиссы. Например, некоторые варианты поддерживают высокую доступность, а другие обеспечивают более надежный процесс резервного копирования и восстановления. **Интегрированное хранилище** (**Integrated Storage**) - это "встроенный" вариант хранения, который поддерживает рабочие процессы резервного копирования/восстановления, высокую доступность и функции корпоративной репликации без использования систем сторонних производителей.

Хранилище **Raft** использует протокол консенсуса, основанный на **Paxos** и работах, описанных в статье Raft: В поисках понятного алгоритма консенсуса", для обеспечения согласованности в соответствии с теоремой CAP.

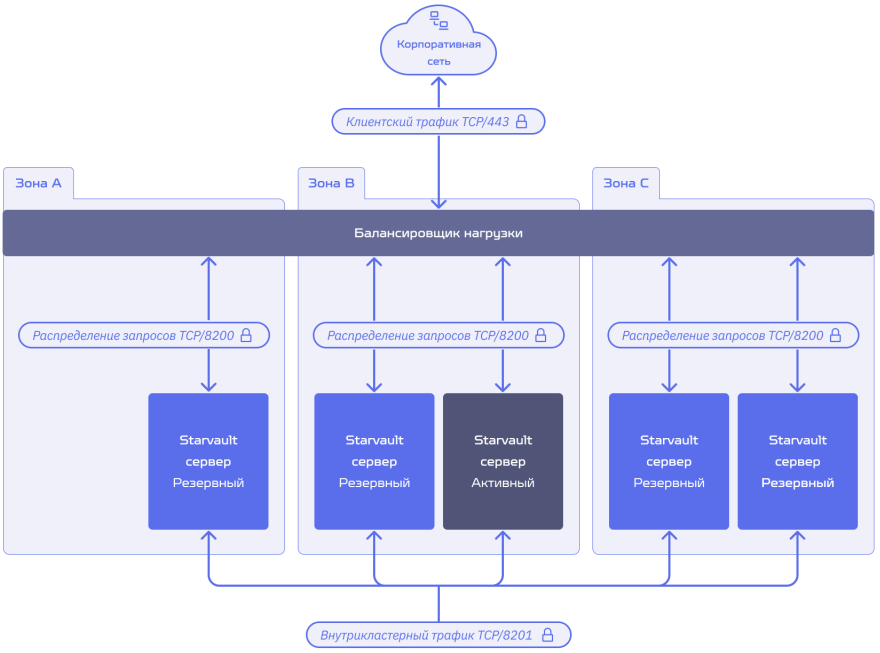
Производительность Raft ограничена операциями ввода-вывода на диске и сетевой задержкой, и сопоставима с **Paxos**. При стабильном лидерстве для фиксации записи в журнале требуется один полный цикл обмена данными с половиной узлов кластера. В сравнении с **Paxos**, **Raft** разработан таким образом, чтобы иметь меньше состояний и более простой, понятный алгоритм, который зависит от следующих элементов:

- **Журнал** (**Log**) — упорядоченная последовательность записей (реплицированный журнал), отслеживающая изменения в кластере. Например, операция записи данных является новым событием, создающим соответствующую запись в журнале.
- **Набор узлов** (**Peer set**) — множество всех участников, участвующих в репликации журнала. Все серверные узлы входят в набор узлов локального кластера.
- **Лидер** (**Leader**) — в любой момент времени набор узлов выбирает один узел в качестве лидера. Лидеры принимают новые записи журнала, реплицируют журнал на ведомые узлы и управляют моментом фиксации записи. Лидеры контролируют репликацию журнала. Несоответствия в реплицированных записях журнала могут указывать на проблемы с лидером.
- **Кворум** (**Quorum**) — большинство участников из набора узлов. Для набора узлов размером N требуется кворум, состоящий как минимум из `ceil((N + 1)/2)` участников. Например, для набора узлов из 5 членов требуется 3 узла. Если кластер не может достичь кворума, он становится недоступным и не может фиксировать новые записи в журнале.
- **Фиксированная запись** (**Committed entry**) — запись журнала, реплицированная на кворум узлов. Записи журнала применяются только после их фиксации.

- **Детерминированная машина конечных состояний** (**DFSM**) — набор известных состояний с предсказуемыми переходами между ними. В **Raft** DFSM переходит между состояниями при применении новых записей журнала. Согласно правилам DFSM, многократное применение одной и той же последовательности журналов всегда приводит к одному и тому же конечному состоянию.

3.1.2. Рекомендуемая архитектура

На следующей схеме показана рекомендуемая архитектура для развертывания одного кластера StarVault с максимальной отказоустойчивостью.



Архитектура StarVault, включающая пять узлов, распределенных по трем зонам доступности, обеспечивает устойчивость к отказу до двух узлов внутри кластера или к полной потере одной зоны доступности.

В ситуациях, когда развертывание в трех зонах доступности не представляется возможным, аналогичная архитектура может быть реализована в двух или даже одной зоне доступности, однако это существенно увеличивает риски для надежности системы в случае сбоя зоны доступности.

3.1.3. Системные требования

В этом разделе содержатся рекомендации по использованию аппаратного обеспечения, требования к сети и дополнительные соображения по инфраструктуре. Учитывая, что каждая хостинговая среда и профиль использования StarVault у каждого клиента уникальны, эти рекомендации должны служить лишь отправной точкой, на основании которой операционный персонал клиента может формировать собственные требования в соответствии с уникальными потребностями для каждого развертывания.

Все технические характеристики, изложенные в этом разделе, являются **минимальными рекомендациями** и не учитывают потребности в вертикальном масштабировании, избыточности или других требованиях инженерии надежности систем (SRE), а также не оценивают объемы пользователей или их сценарии использования во всех возможных случаях. Все требования к ресурсам прямо пропорциональны операциям, выполняемым кластером StarVault, а также использованию системы конечными пользователями.

Чтобы соответствовать вашим требованиям и обеспечить максимальную стабильность экземпляров StarVault, важно проводить нагрузочные тесты и следить за использованием ресурсов, а также за всеми данными телеметрии StarVault.

3.1.3.1. Требования к оборудованию для серверов Starvault

Требования к оборудованию для серверов Starvault зависят от условий эксплуатации кластера:

- **Минимальная конфигурация**: предназначена для тестовых кластеров, а также для производственных кластеров в средах с невысокой нагрузкой;
- **Рекомендуемая конфигурация**: используется для производственных кластеров, работающих в условиях высокой нагрузки (например, при большом числе транзакций, большом объёме секретов или их комбинации).

Ниже в таблице приведены требования для одного узла.

Конфигурация	ЦП	Память	Емкость диска	IOPS диска	Пропускная способность диска
Минимальная	2-4 ядра	8-16 GB RAM	100+ GB	3000+ IOPS	75+ MB/s
Рекомендуемая	4-8 ядра	32-64 GB RA	200+ GB	10000+ IOPS	250+ MB/s

Внутренняя база данных, которую использует StarVault, оптимизирована для современных SSD-накопителей. Запуск StarVault на HDD приведет к значительному снижению производительности.

3.1.3.2. Рекомендации по оборудованию

В целом требования к производительности ЦП и хранилища будут зависеть от конкретного профиля использования клиента (например, типов запросов, средней частоты запросов и пиковой частоты запросов). Требования к памяти зависят от общего размера данных, хранящихся в памяти, и их размер должен определяться в соответствии с этими данными.

При использовании интегрированного хранилища серверы StarVault должны иметь относительно высокопроизводительную систему хранения. Если создается или часто обновляется множество секретов, эта информация будет часто записываться на диск, и

использование более медленных систем хранения значительно скажется на производительности.

Кроме того, настоятельно рекомендуется настроить StarVault с включенным журналом аудита. Влияние дополнительных операций ввода-вывода хранилища при ведении журнала аудита будет зависеть от конкретного шаблона запросов. Для обеспечения максимальной производительности журналы аудита следует записывать на отдельный диск.

3.1.3.3. Задержка сети и пропускная способность

Чтобы члены кластера правильно синхронизировались, сетевая задержка между зонами доступности должна быть меньше восьми миллисекунд (8 мс).

Объем пропускной способности сети, используемой StarVault, полностью зависит от особенностей использования конкретного клиента. Во многих случаях даже большой объем запросов не приведет к большому потреблению пропускной способности сети. Однако все данные, записанные в StarVault, будут реплицированы на все члены кластера. Также важно учитывать требования к пропускной способности для других внешних систем, таких как коллекторы мониторинга и журналирования. И наконец, многокластерная система StarVault потребует передачи наборов данных StarVault между кластерами для обеспечения производительности и репликации в целях DR.

3.1.3.4. Сетевые подключения

В следующей таблице приведены требования к сетевым подключениям для узлов кластера StarVault. Если общий выход в сеть ограничен, особое внимание следует уделить предоставлению исходящего доступа с серверов StarVault любым внешним провайдерам интеграции (например, бэкендам провайдеров аутентификации и секретов), а также внешним обработчикам журналов, провайдерам сбора метрик, управления безопасностью и конфигурацией, а также системам резервного копирования и восстановления.

Источник	**Назначение**	**Порт**	**Протокол**	**Направление трафика**	**Назначение**
Клиентские машины	Балансировщик нагрузки	443	tcp	Входящий	Распределение запросов
Балансировщик нагрузки	Серверы StarVault	8200	tcp	Входящий	StarVault API
Серверы StarVault	Серверы StarVault	8200	tcp	Двунаправленный	Загрузка кластера
Серверы StarVault	Серверы StarVault	8201	tcp	Двунаправленный	Raft, репликация, пересылка запросов

Источник	Назначение	Порт	Протокол	Направление трафика	Назначение
Серверы StarVault	Внешние системы	различные	различные	различные	Внешние API

3.1.3.5. Шифрование сетевого трафика

Весь сетевой трафик, связанный со StarVault, должен быть зашифрован на каждом сегменте. От клиентских машин к балансировщику нагрузки и от балансировщика нагрузки к серверам StarVault можно использовать стандартное шифрование HTTPS TLS.

Для связи между серверами StarVault (порт 8201 по умолчанию), включая обмен информацией Raft, репликацию данных и пересылку запросов, StarVault автоматически согласовывает соединение mTLS через порт API адреса (по умолчанию 8200) при добавлении новых серверов к кластеру.

3.1.3.6. Рекомендации по масштабированию

В облачной среде рекомендуется использовать управляемый сервис масштабирования для поддержания работоспособности экземпляров в кластере StarVault. Однако, учитывая особенности бэкенда Интегрированного Хранилища, важно не заменять все экземпляры в управляемой группе масштабирования слишком быстро, чтобы избежать необходимости восстановления данных из снимков.

> Автоматическая очистка серверов не включена по умолчанию при использовании Интегрированного Хранилища. Эту функцию необходимо активировать после инициализации кластера через API Raft Autopilot.

Для масштабирования производительности кластера StarVault необходимо учитывать два фактора:

1. Добавление дополнительных узлов в кластер StarVault не увеличит производительность для любой активности, которая инициирует запись в бэкенд хранилища StarVault.
2. Для клиентов StarVault добавление **узлов резервной производительности** (**performance standby nodes**) может обеспечить горизонтальное масштабирование для запросов чтения внутри кластера StarVault.

3.1.3.7. Характеристики отказоустойчивости

При развертывании кластера StarVault важно учитывать и проектировать его с учетом специфических требований к различным сценариям отказов:

Отказ узла

Бэкэнд интегрированного хранилища для StarVault допускает отказ отдельных узлов, реплицируя все данные между каждым узлом кластера. Если ведущий узел выходит из

строя, оставшиеся члены кластера выбирают нового лидера, следуя протоколу Raft. Чтобы допустить отказ до двух узлов в кластере, идеальный размер кластера StarVault с использованием интегрированного хранилища - пять узлов.

Отказ зоны доступности

Благодаря развертыванию кластера StarVault в рекомендуемой архитектуре с тремя зонами доступности алгоритм консенсуса Raft должен поддерживать согласованность и доступность при отказе одной из зон доступности.

В тех случаях, когда развертывание в трех зонах невозможно, отказ одной из зон доступности может привести к тому, что кластер StarVault станет недоступным или не сможет выбрать лидера. Например, при развертывании с двумя зонами доступности отказ одной зоны доступности с вероятностью 50% приведет к тому, что кластер потеряет кворум Raft и не сможет обслуживать запросы.

Отказ региона или кластера

В случае отказа всего региона или кластера StarVault предоставляет функции репликации, которые помогают обеспечить отказоустойчивость благодаря использованию архитектуры с несколькими кластерами и/или регионами.

3.1.3.8. Внешнее хранилище токенов

Функция токенизации данных с помощью механизма преобразования секретов вводит дополнительные архитектурные соображения.

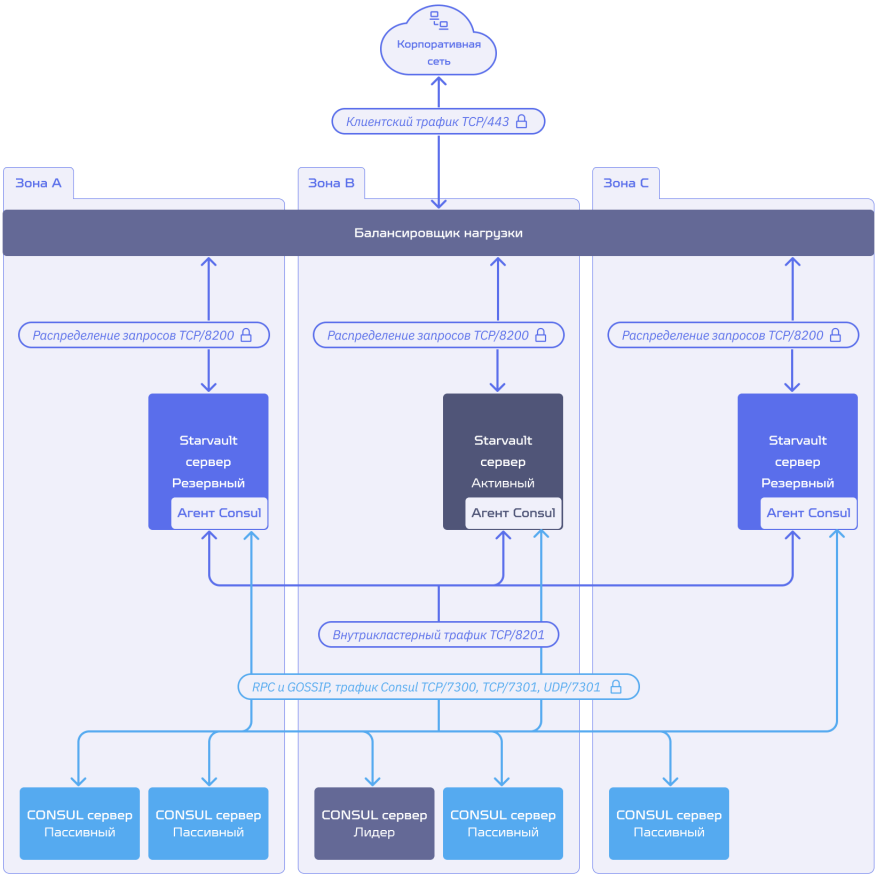
Функция токенизации требует внешнего хранилища данных для облегчения сопоставления токенов с криптографическими значениями. Убедитесь, что архитектура внешних хранилищ данных обеспечивает высокую доступность. По возможности важно следовать архитектурным моделям надежности и аварийного восстановления, которые отвечают тем же требованиям, что и для самого StarVault. Для обеспечения согласованности данных резервное копирование внешнего хранилища данных должно быть синхронизировано с резервным копированием StarVault.

3.2. Бэкенд хранилища Consul

В продуктивной среде рекомендуется использование интегрированного хранилища вместо Consul. Используйте Consul для хранения данных StarVault только при наличии четких причин.

3.2.1. Рекомендуемая архитектура

На следующей схеме показана рекомендуемая архитектура для развертывания одного кластера StarVault с использованием хранилища Consul.



В данной архитектуре основной риск доступности связан со слоем хранения. С пятью узлами в кластере Consul, распределенными между тремя зонами доступности, эта архитектура может выдержать потерю двух узлов внутри кластера или потерю целой зоны доступности и оставаться доступной. Поскольку StarVault использует только один активный узел, кластеру StarVault требуется всего три узла кластера, чтобы выдержать потерю двух узлов или целой зоны доступности.

В ситуациях, когда развертывание в трех зонах доступности не представляется возможным, аналогичная архитектура может быть реализована в двух или даже одной зоне доступности, однако это существенно увеличивает риски для надежности системы в случае сбоя зоны доступности.

Важно использовать выделенный кластер Consul для хранения данных StarVault, отдельно от любого кластера Consul, используемого в других целях, чтобы минимизировать конкуренцию за ресурсы на слое хранения. Это, скорее всего, потребует использования нестандартных портов для сетевого соединения Consul. В данной архитектуре вместо стандартных портов 8300 и 8301 используются порты 7300 и 7301.

3.2.2. Системные требования

В этом разделе содержатся рекомендации по использованию аппаратного обеспечения, требования к сети и дополнительные соображения по инфраструктуре. Учитывая, что каждая хостинговая среда и профиль использования StarVault у каждого клиента уникальны, эти рекомендации должны служить лишь отправной точкой, на основании

которой операционный персонал клиента может формировать собственные требования в соответствии с уникальными потребностями для каждого развертывания.

Все технические характеристики, изложенные в этом разделе, являются **минимальными рекомендациями** и не учитывают потребности в вертикальном масштабировании, избыточности или других требованиях инженерии надежности систем (SRE), а также не оценивают объемы пользователей или их сценарии использования во всех возможных случаях. Все требования к ресурсам прямо пропорциональны операциям, выполняемым кластером StarVault, а также использованию системы конечными пользователями.

Чтобы соответствовать вашим требованиям и обеспечить максимальную стабильность экземпляров StarVault, важно проводить нагрузочные тесты и следить за использованием ресурсов, а также за всеми данными телеметрии StarVault.

3.2.2.1. Требования к оборудованию для серверов StarVault

Рекомендации по размерам разделены на два типичных размера кластера.

Малые кластеры подходят для большинства первоначальных производственных развертываний или для сред разработки и тестирования.

Большие кластеры предназначены для производственных сред с постоянно высокой рабочей нагрузкой. Это может быть большое количество транзакций, большое количество секретов или их комбинация.

Размер кластера	ЦП	Память	Емкость диска	IOPS диска	Пропускная способность диска
Малый	2-4 ядра	8-16 GB RAM	100+ GB	3000+ IOPS	75+ MB/s
Большой	4-8 ядра	32-64 GB RA	200+ GB	10000+ IOPS	250+ MB/s

3.2.2.2. Требования к оборудованию для серверов Consul

Размер кластера	ЦП	Память	Емкость диска	IOPS диска	Пропускная способность диска
Малый	2-4 ядра	8-16 GB RAM	100+ GB	3000+ IOPS	75+ MB/s
Большой	4-8 ядра	32-64 GB RA	200+ GB	10000+ IOPS	250+ MB/s

3.2.2.3. Рекомендации по оборудованию

В целом требования к производительности ЦП и хранилища будут зависеть от конкретного профиля использования клиента (например, типов запросов, средней частоты запросов и

пиковой частоты запросов). Требования к памяти зависят от общего размера данных, хранящихся в памяти, и их размер должен определяться в соответствии с этими данными.

Настоятельно рекомендуется настроить StarVault с включенным журналом аудита. Влияние дополнительных операций ввода-вывода хранилища при ведении журнала аудита будет зависеть от конкретного шаблона запросов. Для обеспечения максимальной производительности журналы аудита следует записывать на отдельный диск.

3.2.2.4. Задержка сети и пропускная способность

Чтобы члены кластера правильно синхронизировались, сетевая задержка между зонами доступности должна быть меньше восьми миллисекунд (8 мс).

Объем пропускной способности сети, используемой StarVault и Consul, полностью зависит от особенностей использования конкретного клиента. Во многих случаях даже большой объем запросов не приведет к большому потреблению пропускной способности сети. Однако все данные, записанные в StarVault, будут реплицированы на все члены кластера Consul. Также важно учитывать требования к пропускной способности для других внешних систем, таких как коллекторы мониторинга и журналирования. И наконец, многокластерная система StarVault потребует передачи наборов данных StarVault между кластерами для обеспечения производительности и репликации в целях DR.

3.2.2.5. Сетевые подключения

В следующей таблице приведены требования к сетевым подключениям для узлов кластера StarVault при использовании хранилища Consul. Если общий выход в сеть ограничен, особое внимание следует уделить предоставлению исходящего доступа с серверов StarVault любым внешним провайдерам интеграции (например, бэкендам провайдеров аутентификации и секретов), а также внешним обработчикам журналов, провайдерам сбора метрик, управления безопасностью и конфигурацией, а также системам резервного копирования и восстановления.

Источник	**Назначение**	**Порт**	**Протокол**	**Направление трафика**	**Назначение**
Клиентские машины	Балансировщик нагрузки	443	tcp	Входящий	Распределение запросов
Балансировщик нагрузки	Серверы StarVault	8200	tcp	Входящий	StarVault API
Серверы StarVault	Серверы StarVault	8200	tcp	Двунаправленный	Загрузка кластера
Серверы StarVault	Серверы StarVault	8201	tcp	Двунаправленный	Raft, репликация, пересылка запросов

Источник	Назначение	Порт	Протокол	Направление трафика	Назначение
Серверы StarVault	Внешние системы	различные	различные	различные	Внешние API
Серверы StarVault и Consul	Серверы Consul	7300*	tcp	Входящий	RPC сервера Consul
Серверы StarVault и Consul	Серверы StarVault и Consul	7301*	tcp, udp	Двунаправленный	GOSSIP трафик Consul

Порты для трафика Consul RPC и GOSSIP отличаются от установленных по умолчанию в этой архитектуре.

3.2.2.6. Шифрование сетевого трафика

Весь сетевой трафик, связанный со StarVault, должен быть зашифрован на каждом сегменте. От клиентских машин к балансировщику нагрузки и от балансировщика нагрузки к серверам StarVault можно использовать стандартное шифрование HTTPS TLS.

Для связи между серверами StarVault (порт 8201 по умолчанию) с целью пересылки трафика запросов StarVault автоматически согласовывает соединение mTLS через порт API адреса (по умолчанию 8200) при добавлении новых серверов к кластеру. Для связи между агентами Consul на кластерах StarVault и Consul настоятельно рекомендуется настроить шифрование gossip.

3.2.2.7. Рекомендации по использованию балансировщика нагрузки

Для достижения максимального уровня надежности и стабильности настоятельно рекомендуется использовать технологию балансировки нагрузки для распределения запросов между узлами кластера StarVault. Каждая крупная облачная платформа предоставляет хорошие варианты управляемых балансировщиков нагрузки, кроме того, существует ряд самостоятельных вариантов, а также системы обнаружения сервисов, такие как Consul.

Если вы решите прервать TLS-соединение на балансировщике нагрузки, настоятельно рекомендуется использовать TLS и для соединения от балансировщика нагрузки к StarVault, чтобы свести к минимуму возможность утечки секретной информации в вашей сети.

Для мониторинга состояния узлов кластера StarVault, балансировщик нагрузки должен быть настроен на опрос API-эндпоинта **/v1/sys/health** для определения состояния узла и соответствующего направления трафика.

3.2.2.8. Рекомендации по масштабированию

В облачной среде рекомендуется использовать управляемый сервис масштабирования для поддержания работоспособности экземпляров в кластере StarVault и Consul. Однако, важно не заменять все экземпляры Consul в управляемой группе масштабирования слишком быстро, чтобы избежать потери данных.

Для масштабирования производительности кластера StarVault необходимо учитывать два фактора:

1. Добавление дополнительных узлов в кластер StarVault не увеличит производительность для любой активности, которая инициирует запись в бэкенд хранилища StarVault.
2. Для клиентов StarVault добавление **узлов резервной производительности** (**performance standby nodes**) может обеспечить горизонтальное масштабирование для запросов чтения внутри кластера StarVault.

3.2.2.9. Характеристики отказоустойчивости

При развертывании кластера StarVault важно учитывать и проектировать его с учетом специфических требований к различным сценариям отказов:

Отказ узла

В высокодоступном кластере StarVault, использующем хранилище Consul, все данные хранятся в кластере Consul, поэтому отказ узла StarVault не грозит потерей данных. Чтобы определить лидерство кластера StarVault, один из серверов StarVault получает блокировку в хранилище данных Consul и становится активным узлом StarVault.

Если в какой-то момент лидер будет потерян, другой узел StarVault займет его место в качестве лидера кластера. Чтобы предусмотреть возможность потери двух узлов StarVault, минимально рекомендуемый размер кластера StarVault составляет три узла.

В Consul репликация и лидерство достигаются за счет использования протоколов консенсуса и GOSSIP. В этих протоколах лидер избирается консенсусом, поэтому всегда должен существовать кворум активных серверов. Чтобы учесть потерю двух узлов из кластера Consul, минимальный рекомендуемый размер кластера Consul составляет пять узлов.

Отказ зоны доступности

Благодаря развертыванию кластеров StarVault и Consul в рекомендуемой архитектуре с тремя зонами доступности общая архитектура может выдержать потерю любой отдельной зоны доступности.

В тех случаях, когда развертывание в трех зонах невозможно, отказ одной из зон доступности может привести к тому, что кластер StarVault станет недоступным или кластер Consul не сможет выбрать лидера. Например, при развертывании с двумя зонами доступности отказ одной зоны доступности с вероятностью 50% приведет к тому, что кластер Consul потеряет кворум и не сможет обслуживать запросы.

Отказ региона или кластера

В случае отказа всего региона или кластера StarVault предоставляет функции репликации, которые помогают обеспечить отказоустойчивость благодаря использованию архитектуры с несколькими кластерами и/или регионами.

3.2.2.10. Внешнее хранилище токенов

Функция токенизации данных с помощью механизма преобразования секретов вводит дополнительные архитектурные соображения.

Функция токенизации требует внешнего хранилища данных для облегчения сопоставления токенов с криптографическими значениями. Убедитесь, что архитектура внешних хранилищ данных обеспечивает высокую доступность. По возможности важно следовать архитектурным моделям надежности и аварийного восстановления, которые отвечают тем же требованиям, что и для самого StarVault. Для обеспечения согласованности данных резервное копирование внешнего хранилища данных должно быть синхронизировано с резервным копированием StarVault.