Запечатывание/распечатывание хранилища

Сервер StarVault запускается в запечатанном состоянии. В этом состоянии StarVault знает, где и как получить доступ к физическому хранилищу, но не знает, как его расшифровать.

Распечатывание — это процесс получения (в незашифрованном виде) корневого ключа, без которого невозможно прочитать ключ дешифрования, расшифровать данные и получить доступ к StarVault.

До распечатывания невозможны почти никакие операции с StarVault, в том числе аутентификация или управление таблицами монтирования. Доступны только операции распечатывания StarVault и проверки статуса печати (status of the seal).

Данные, хранящиеся в StarVault, зашифрованы. Для расшифровки данных StarVault нужен *ключ шифрования*. Ключ шифрования также хранится вместе с данными (в *связке ключей*), но зашифрован другим *корневым ключом шифрования*.

Поэтому для расшифровки данных StarVault должен расшифровать ключ шифрования, для чего требуется корневой ключ. Распечатывание — процесс получения доступа к корневому ключу. Корневой ключ хранится вместе с другими данными StarVault, но зашифрован еще одним механизмом: ключом распечатывания.

Подведем итог: большинство данных StarVault зашифрованы ключом шифрования в связке ключей, связка ключей зашифрована корневым ключом, а корневой ключ зашифрован ключом распечатывания.

1. Схема Шамира

Конфигурация StarVault по умолчанию использует схему Шамира.

В алгоритме "Схема разделения секрета Шамира" ключ распечатывания разделяется на несколько частей. Оператору передается только часть ключа распечатывания. Для восстановления ключа распечатывания требуется некоторое установленное пороговое количество частей. Восстановленный ключ распечатывания затем используется для расшифровки корневого ключа.

Это и есть процесс распечатывания: части ключа распечатывания добавляются по одной за раз (в любом порядке) до тех пор, пока количество частей не станет достаточным для восстановления ключа и расшифровки корневого ключа.

2. Распечатывание

Чтобы запустить распечатывание, выполните starvault operator unseal или создайте API-запрос В процессе сохраняется состояния: каждый ключ распечатывания можно ввести с помощью нескольких механизмов и с нескольких клиентских машин. Поэтому каждую часть корневого ключа можно держать на отдельной клиентской машине, тем самым повысив безопасность.

Обратите внимание, что при использовании схемы Шамира с несколькими узлами каждый узел должен быть распечатан с помощью порогового количества частей ключа. Частичное распечатывание каждого узла не распространяется по кластеру.

Узел StarVault остается распечатанным, пока не произойдет одно из следующих событий:

1. Узел повторно запечатан через API (см. ниже).
2. Сервер перезапущен.
3. На уровне хранения StarVault возникнет неустранимая ошибка.

Распечатывание затрудняет автоматизацию установки StarVault. Автоматизированные инструменты позволяют легко установить, настроить и запустить StarVault, но распечатывание по схеме Шамира происходит вручную. Для большинства пользователей автоматическое распечатывание (Auto Unseal) – лучший вариант.

3. Запечатывание

Для запечатывания StarVault, в том числе есть API. В результате запечатывания корневой ключ в памяти будет сброшен, и, чтобы восстановить работоспособность StarVault, придется снова его распечатать. Для запечатывания требуется только один оператор с root-привилегиями.

Таким образом, при вторжении данные StarVault можно быстро заблокировать для минимизации ущерба. К ним нельзя будет получить доступ снова, пока нет доступа к частям корневого ключа.

4. Автоматическое распечатывание

Автоматическое распечатывание позволяет обезопасить ключ распечатывания гораздо меньшими усилиями. Эта функция делегирует защиту ключа распечатывания от пользователей к доверенному устройству или службе. При запуске StarVault подключится к устройству или службе запечатывания и запросит расшифровку корневого ключа из хранилища.

Помимо распечатывания, в StarVault есть и другие операции (например, создание корневого токена), требующие кворума пользователей. Если используется схема Шамира, то для авторизации этих операций должны быть предоставлены ключи распечатывания. Если же происходит автоматическое распечатывание, то для этих операций требуются ключи восстановления.

Так же, как процесс инициализации с использованием схемы Шамира дает ключи распечатывания, инициализация с автоматическим распечатыванием дает ключи восстановления.

По-прежнему можно запечатать узел StarVault с помощью API. В этом случае StarVault останется запечатанным до перезапуска или до использования API распечатывания. В случае автоматического распечатывания для API потребуются фрагменты ключа восстановления вместо фрагментов ключа распечатывания, которые предоставлялись при использовании схемы Шамира. Процесс же остается прежним.

Ключи восстановления не расшифровывают корневой ключ

Ключи восстановления не расшифровывают корневой ключ, и поэтому их недостаточно для распечатывания StarVault, если механизм автоматического распечатывания не работает. Они используются исключительно для авторизации. Автоматическое распечатывание создает строгую зависимость жизненного цикла StarVault от базового механизма запечатывания. Это означает, что если механизм запечатывания (например, ключ Cloud KMS) становится недоступным или удаляется до изменения способа запечатывания, то восстановить доступ к кластеру StarVault нельзя до тех пор, пока механизм не станет снова доступен. Если механизм запечатывания или его ключи будут удалены навсегда, то кластер StarVault не получится восстановить даже из резервных копий. Чтобы снизить этот риск, рекомендуем тщательно контролировать механизм запечатывания.

5. Ключ восстановления

Когда StarVault инициализируется с помощью KMS, вместо возврата ключей распечатывания оператору возвращаются ключи восстановления. Они генерируются из внутреннего ключа восстановления, который разделяется с помощью Схемы разделения секрета Шамира, так же как это происходит с ключами распечатывания при запуске StarVault без KMS.

Подробная информация об инициализации и пересоздании ключей приведена ниже. При выполнении операции, использующей ключи восстановления, например, `generate-root`, выбор соответствующих ключей восстановления, а не барьерных ключей распечатывания, происходит автоматически.

5.1. Инициализация

При инициализации разделение выполняется в соответствии со следующими флагами командной строки и их эквивалентами API в конечной точке `/sys/init`:

- `recovery-shares`: Количество частей, на которое следует разделить ключ восстановления. Эквивалентно значению `recovery_shares` в конечной точке API.
- `recovery-threshold`: Пороговое количество частей, необходимое для воссоздания ключа восстановления. Эквивалентно значению `recovery_threshold` в конечной точке API.
- `recovery-pgp-keys`: PGP-ключи, используемые для шифрования возвращаемых частей ключа восстановления. Эквивалентно значению `recovery_pgp_keys` в конечной точке API, хотя, как и в случае с `pgp_keys`, объект в конечной точке API является массивом, а не строкой.

Кроме того, StarVault не инициализируется, если генерация ключа параметром не была задана и никаких ключей не найдено. Дополнительную информацию см. в разделе «Конфигурация».

5.2. Пересоздание ключей

5.2.1. Ключ распечатывания

Ключ распечатывания в StarVault можно пересоздать с помощью обычной операции `starvault operator rekey` из командной строки или соответствующих вызовов по API. Операция пересоздания ключа разрешается, когда количество ключей восстановления достигает порогового значения. После пересоздания новый барьерный ключ хранится как предыдущий ключ. Новый барьерный ключ не возвращается пользователям, которые отправили свои ключи восстановления.

5.2.2. Ключ восстановления

Ключ восстановления можно пересоздать, чтобы изменить количество частей, пороговое значение или указать разных держателей ключей с помощью разных PGP-ключей. Для пересоздания в командной строке StarVault установите флаг `-target=recovery` команде `starvault operator rekey`.

Через API операция пересоздания выполняется с теми же параметрами, что и на обычной конечной точке `/sys/rekey`; однако для этой операции префикс API находится в `/sys/rekey-recovery-key`, а не в `/sys/rekey`.

6. Изменение способа запечатывания

Из-за технических особенностей реализации для изменения способа запечатывания придется на короткое время отключить весь кластер. Изменение способа запечатывания

происходит довольно редко, в отличие от других видов простоя.

ПРИМЕЧАНИЕ: Прежде чем менять способ запечатывания, сделайте резервную копию на случай, если что-то пойдет не так.

ПРИМЕЧАНИЕ: Для успешного изменения способа запечатывания, в ходе операции должны быть доступны как старый, так и новый способы запечатывания. Например, при переходе с автоматического распечатывания на схему Шамира служба, сопровождающая автоматическое распечатывание, должна быть доступна во время такого перехода.

Полный список метрик телеметрии StarVault

Ниже приведен полный список доступных метрик в алфавитном порядке по названиям:

1. Полный список метрик

Название метрики	Тип метрики	Единицы измерения	Описание	Примечание
database.Close	сводная	мс	Время, необходимое для закрытия хранилища секретов баз данных (по всем хранилищам секретов баз данных)	---
database.NewUser	сводная	мс	Время, необходимое для создания пользователя во всех хранилищах секретов баз данных	---
database.New-User.error	счетчик	число	Количество ошибок, возникших при создании пользователей во всех хранилищах секретов баз данных	---
database.Initialize	сводная	мс	Время, необходимое для инициализации хранилища секретов баз данных (по всем хранилищам секретов баз данных)	---
database.Initial-ize.error	счетчик	число	Количество ошибок, возникших при инициализации базы данных во всех хранилищах секретов баз данных.	---

Название метрики	Тип метрики	Единицы измерения	Описание	Примечание
database.{NAME}.Close	сводная	мс	Время, необходимое для закрытия хранилища секретов базы данных с именем {NAME}	---
database.{NAME}.NewUser	сводная	мс	Время, необходимое для создания пользователя в хранилище секретов базы данных с именем {NAME}	---
database.{NAME}.New-User.error	счетчик	число	Количество ошибок, возникших при создании пользователей в хранилище секретов базы данных с именем {NAME}	---
database.{NAME}.Initialize	сводная	мс	Время, необходимое для инициализации хранилища секретов базы данных для базы данных с именем {NAME}	---
database.{NAME}.Initialize.error	счетчик	число	Количество ошибок, возникших при инициализации базы данных в хранилище секретов с именем {NAME}	---
database.{NAME}.Update-User	сводная	мс	Время, необходимое для обновления пользователя в хранилище секретов базы данных с именем {NAME}	---
database.{NAME}.Update-User.error	счетчик	число	Количество ошибок, возникших при обновлении пользователей в хранилище секретов базы данных с именем {NAME}	---

Название метрики	Тип метрики	Единицы измерения	Описание	Примечание
database.{NAME}.DeleteUser	сводная	мс	Время, необходимое для аннулирования пользователя в хранилище секретов базы данных с именем {NAME}	---
database.{NAME}.Delete-User.error	счетчик	число	Количество ошибок, возникших при аннулировании пользователей в хранилище секретов базы данных с именем {NAME}	---
database.Update-User	сводная	мс	Время, необходимое для обновления пользователя во всех хранилищах секретов баз данных	---
database.Update-User.error	счетчик	число	Количество ошибок, возникших при обновлении пользователей во всех хранилищах секретов баз данных	---
database.Delete-User	сводная	мс	Время, необходимое для аннулирования пользователя во всех хранилищах секретов баз данных	---
database.Delete-User.error	счетчик	число	Количество ошибок, возникших при аннулировании пользователей во всех хранилищах секретов баз данных	---
secrets.p-ki.tidy.cert_s-tore_current_entry	датчик	число	Индекс текущей записи в хранилище сертификатов, проверяемой операцией очистки сертификатов	---

Название метрики	Тип метрики	Единицы измерения	Описание	Примечание
secrets.pki.tidy.cert_store_deleted_count	счетчик	число	Количество записей, удалённых из хранилища сертификатов	---
secrets.pki.tidy.cert_store_total_entries_remaining	датчик	число	Количество записей в хранилище сертификатов, проверенных, но не удалённых в ходе операции очистки сертификатов	---
secrets.pki.tidy.cert_store_total_entries	датчик	число	Количество записей в хранилище сертификатов, подлежащих проверке в ходе операции очистки сертификатов	---
secrets.pki.tidy.duration	сводная	мс	Время, необходимое для завершения операции очистки PKI	---
secrets.pki.tidy.revoked_cert_current_entry	датчик	число	Индекс текущей записи в хранилище отозванных сертификатов, проверяемой операцией очистки	---
secrets.pki.tidy.revoked_cert_deleted_count	счетчик	число	Количество записей, удалённых из хранилища для отозванных сертификатов	---
secrets.pki.tidy.revoked_cert_total_entries_fixed_issuers	датчик	число	Количество записей в хранилище сертификатов, у которых были обнаружены и исправлены некорректные данные об издателе в ходе операции очистки	---

Название метрики	Тип метрики	Единицы измерения	Описание	Примечание
secrets.pki.tidy.revoked_cert_total_entries_incorrect_issuers	датчик	число	Общее количество записей в хранилище сертификатов, у которых были обнаружены некорректные данные об издателе	---
secrets.pki.tidy.revoked_cert_total_entries_remaining	датчик	число	Количество отозванных сертификатов в хранилище, проверенных, но не удалённых в ходе операции очистки сертификатов	---
secrets.pki.tidy.revoked_cert_total_entries	датчик	число	Количество записей об отозванных сертификатах в хранилище, подлежащих проверке в ходе операции очистки сертификатов	---
secrets.pki.tidy.start_time_epoch	датчик	секунды	Время начала операции очистки PKI в формате эпохи (секунды с 1970-01-01)	Показатель времени начала будет равен 0, если операция очистки PKI не активна в данный момент.
secrets.pki.tidy.success	счетчик	число	Количество успешных завершений операции очистки PKI	---
vault.audit.{DEVICE}.log_request	сводная	мс	Время, необходимое для завершения всех запросов логов аудита на устройстве	---
vault.audit.{DEVICE}.log_response	сводная	мс	Время, необходимое для завершения всех ответов логов аудита на устройстве	---

Название метрики	Тип метрики	Единицы измерения	Описание	Примечание
vault.audit.log_request_failure	счетчик	число	Количество неудачных запросов логов аудита по всем устройствам	Количество неудачных запросов является **критически важной метрикой**. Ненулевое значение для vault.audit.`log_request_failure` указывает на то, что все ваши настроенные аудиторские устройства не смогли зарегистрировать запрос (или ответ). Если Starault не может правильно провести аудит запроса или ответа на него, исходный запрос завершится неудачей. Обратитесь к логам StarVault и любым специфичным для устройства метрикам для устранения неполадок в неработающем аудиторском лог-устройстве.
vault.audit.log_request	сводная	мс	Время, необходимое для завершения всех запросов логов аудита по всем устройствам для аудита логов	---
vault.audit.log_response_failure	счетчик	число	Количество неудачных запросов на логи аудита по всем устройствам	Количество неудачных запросов является **критически важной метрикой**. Ненулевое значение для `vault.audit.log_response_failure` указывает на то, что одно из настроенных устройств аудита не смогло ответить StarVault. Если StarVault не может правильно провести аудит запроса или ответа на него, исходный запрос завершится неудачей. Обратитесь к специфичным для устройства метрикам и логам для устранения неполадок в неработающем лог-устройстве аудита.
vault.audit.log_response	сводная	мс	Время, необходимое для завершения ответов на логи аудита по всем устройствам для аудита логов	---
vault.autopilot.failure_tolerance	датчик	узлы	Количество здоровых узлов, превышающих кворум	Допустимый уровень отказов указывает, сколько текущих здоровых узлов может выйти из строя без потери кворума.
vault.autopilot.healthy	датчик	логическое значение	Указывает, все ли узлы здоровы	• Значение 1 на датчике означает, что Autopilot считает все узлы здоровыми. • Значение 0 на датчике означает, что Autopilot считает, что как минимум 1 узел нездоров

Название метрики	Тип метрики	Единицы измерения	Описание	Примечание
vault.autopilot.node.healthy	датчик	логическое значение	Указывает, здоров ли активный узел	• Значение 1 на датчике означает, что Autopilot считает указанный узел (по node_id) здоровым. • Значение 0 на датчике означает, что Autopilot не может связаться с указанным узлом (по node_id) или считает узел нездоровым.
vault.barrier.delete	сводная	мс	Время, необходимое для завершения операции DELETE на барьере StarVault	---
vault.barrier.get	сводная	мс	Время, необходимое для завершения операции GET на барьере StarVault	---
vault.barrier.list	сводная	мс	Время, необходимое для завершения операции LIST на барьере StarVault	---
vault.barrier.put	сводная	мс	Время, необходимое для завершения операции PUT на барьере StarVault	---
vault.cache.hit	счетчик	число	Количество обращений к LRU-кэшу, которые позволили избежать чтения из настроенного хранилища	---
vault.cache.miss	счетчик	число	Количество промахов в LRU-кэше, которые потребовали чтения из настроенного хранилища	---
vault.cache.write	счетчик	число	Количество записей в LRU-кэш	---
vault.core.active	датчик	логическое значение	Указывает, активен ли узел StarVault	• Значение 1 указывает на активность узла. • Значение 0 указывает, что узел находится в режиме ожидания.

Название метрики	Тип метрики	Единицы измерения	Описание	Примечание
vault.core.activity.segment_write	сводная	мс	Время, необходимое для записи сегментов журнала активности в хранилище	---
vault.core.check_token	сводная	мс	Время, необходимое для проверки токена	---
vault.core.fetch_acl_and_token	сводная	мс	Время, необходимое для получения записей ACL и токена	---
vault.core.handle_login_request	сводная	мс	Время, необходимое для выполнения запроса на вход (логин)	---
vault.core.handle_request	сводная	мс	Время, необходимое для выполнения запроса, не связанного с входом (логином)	---
vault.core.in_flight_requests	датчик	запросы	Количество запросов, выполняемых в данный момент	---
vault.core.leadership_lost	сводная	мс	Общее время, в течение которого узел высокодоступного кластера последний раз сохранял лидерство	Обновления времени лидерства происходят при каждом изменении лидера. Частые обновления метрики `vault.core.leadership_lost` с малыми значениями времени лидерства указывают на нестабильность, когда статус лидера переключается между узлами.
vault.core.locked_users	датчик	пользователи	Количество пользователей, заблокированных в StarVault в данный момент	Количество заблокированных пользователей обновляется каждые 15 минут.
vault.core.mount_table.num_entries	датчик	объекты	Количество точек монтирования в данной таблице монтирования	Метрики количества точек монтирования включают метки, указывающие, относится ли таблица к аутентификации или логическим операциям, а также является ли таблица реплицируемой или локальной.
vault.core.mount_table.size	датчик	байты	Текущий размер соответствующей таблицы монтирования.	Метрики размера таблицы включают метки, указывающие, является ли таблица аутентификационной или логической, а также реплицируется она или локальна.

Название метрики	Тип метрики	Единицы измерения	Описание	Примечание
vault.core.performance_standby	датчик	логическое значение	Указывает, является ли узел производительным резервным (performance standby)	• Значение 1 указывает, что узел является производительным; • Значение 0 указывает, что узел не является производительным резервным.
vault.core.post_unseal	сводная	мс	Время, необходимое для завершения операций после распечатывания	---
vault.core.pre_seal	сводная	мс	Время, необходимое для завершения операций перед запечатыванием	---
vault.core.replication.dr.primary	датчик	логическое значение	Указывает, является ли узел StarVault основным для аварийного восстановления (disaster recovery primary)	• Значение 1 указывает, что узел является основным для аварийного восстановления; • Значение 0 указывает, что узел не является основным для аварийного восстановления.
vault.core.replication.dr.secondary	датчик	логическое значение	Указывает, является ли узел StarVault резервным для аварийного восстановления (disaster recovery secondary)	• Значение 1 указывает, что узел **является** резервным для аварийного восстановления; • Значение 0 указывает, что узел **не является** резервным для аварийного восстановления.
vault.core.replication.performance.primary	датчик	логическое значение	Указывает, является ли узел StarVault основным для производительности (performance primary)	• Значение 1 указывает, что узел **является** основным для производительности; • Значение 0 указывает, что узел **не является** основным для производительности.
vault.core.replication.performance.secondary	датчик	логическое значение	Указывает, является ли узел StarVault резервным для производительности (performance secondary)	• Значение 1 указывает, что узел **является** резервным для производительности; • Значение 0 указывает, что узел **не является** резервным для производительности.
vault.core.replication.write_undo_logs	датчик	логическое значение	Указывает, включены ли журналы отмены (undo logs)	• Значение 1 указывает, что StarVault **генерирует** журналы отмены. • Значение 0 указывает, что StarVault **не генерирует** журналы отмены.

Название метрики	Тип метрики	Единицы измерения	Описание	Примечание
vault.core.seal-internal	сводная	мс	Время, необходимое для завершения внутренних операций запечатывания StarVault	---
vault.core.seal-with-request	сводная	мс	Время, необходимое для завершения операций запечатывания, вызванных явным запросом	---
vault.core.step_-down	сводная	мс	Время, необходимое для снятия лидерства в кластере	---
vault.core.unseal	сводная	мс	Время, необходимое для завершения операций распечатывания	---
vault.core.unsealed	датчик	логическое значение	Указывает, распечатан ли StarVault в данный момент	• Значение 1 указывает, что StarVault **распечатан**, и клиенты могут читать секреты; • Значение 0 указывает, что StarVault **запечатан**, и клиенты не могут читать секреты
vault.etcd.delete	сводная	мс	Время, необходимое для выполнения операции DELETE в бэкенде хранения etcd	---
vault.etcd.get	сводная	мс	Время, необходимое для выполнения операции GET в бэкенде хранения etcd	---
vault.etcd.list	сводная	мс	Время, необходимое для выполнения операции LIST в бэкенде хранения etcd	---
vault.etcd.put	сводная	мс	Время, необходимое для выполнения операции PUT в бэкенде хранения etcd	---

Название метрики	Тип метрики	Единицы измерения	Описание	Примечание
vault.expire.fetch-lease-times-by-token	сводная	мс	Время, необходимое для получения времени аренды по токену	---
vault.expire.fetch-lease-times	сводная	мс	Время, необходимое для получения времени аренды	---
vault.expire.job_-manag-er.queue_length	сводная	аренды	Общее количество ожидающих заданий на отзыв по `queue_id`	Идентификатор очереди в метке `queue_id` указывает на точку монтирования, связанную с истекающей арендой. Например, это может быть механизм секретов или метод аутентификации.
vault.expire.job_-manager.total_jobs	сводная	аренды	Общее количество ожидающих заданий на отзыв	---
vault.expire.lease_-expiration	счетчик	число	Количество истечений аренды на текущий момент	---
vault.expire.lease_-expiration.-time_in_queue	сводная	мс	Время, необходимое для того, чтобы аренда дошла до начала очереди отзыва	---
vault.expire.num_ir-revocable_leases	датчик	аренды	Количество аренд, которые не могут быть автоматически отозваны	---
vault.ex-pire.num_leases	датчик	аренды	Общее количество аренд, которые могут истечь	---
vault.expire.regis-ter-auth	сводная	мс	Время, необходимое для регистрации аренд, связанных с новыми токенами службы	---
vault.expire.register	сводная	мс	Время, необходимое для операций регистрации	---
vault.expire.renew-token	сводная	мс	Время, необходимое для обновления токена	---
vault.expire.renew	сводная	мс	Время, необходимое для обновления аренды	---

Название метрики	Тип метрики	Единицы измерения	Описание	Примечание
vault.expire.revoke-by-token	сводная	мс	Время, необходимое для отзыва всех секретов, выданных с данным токеном	---
vault.expire.revoke-force	сводная	мс	Время, необходимое для принудительного отзыва токена	---
vault.expire.revoke-prefix	сводная	мс	Время, необходимое для отзыва всех токенов по префиксу	---
vault.expire.revoke	сводная	мс	Время, необходимое для отзыва токена	---
vault.ha.rpc.client.e-cho	сводная	мс	Время, необходимое для отправки запроса эхо от резервного узла на активный узел	---
vault.ha.rpc.client.e-cho.errors	счетчик	число	Количество сбоев запросов эхо от резервных	---
vault.ha.rpc.client.-forward	сводная	мс	Время, необходимое для пересылки запроса от резервного узла на активный узел	---
vault.ha.rpc.client.-forward.errors	счетчик	число	Количество сбоев пересылки запросов от резервных узлов	---
vault.identity.entity.-count	датчик	сущности	Количество псевдонимов сущностей (по пространству имен), хранящихся в StarVault	---
vault.identi-ty.num_entities	датчик	сущности	Общее количество сущностей, хранящихся в StarVault	---

Название метрики	Тип метрики	Единицы измерения	Описание	Примечание
vault.identity.upsert_entity_txn	сводная	мс	Время, необходимое для обновления или вставки сущности в базу данных в памяти и, на активном узле, сохранения данных в хранилище	---
vault.identity.upsert_group_txn	сводная	мс	Время, необходимое для обновления или вставки членства в группу в базу данных в памяти и, на активном узле, сохранения данных в хранилище	---
vault.metrics.collection	сводная	мс	Среднее время, необходимое (для каждой метрики датчика) для сбора данных об использовании	---
vault.metrics.collection.interval	сводная	время продолжительности	Текущее значение usage_gauge_period	---
vault.mssql.delete	сводная	мс	Время, необходимое для выполнения операции DELETE в бэкенде хранения Microsoft SQL Server	---
vault.mssql.get	сводная	мс	Время, необходимое для выполнения операции GET в бэкенде хранения Microsoft SQL Server	---
vault.mssql.list	сводная	мс	Время, необходимое для выполнения операции LIST в бэкенде хранения Microsoft SQL Server	---
vault.mssql.put	сводная	мс	Время, необходимое для выполнения операции PUT в бэкенде хранения Microsoft SQL Server	---

Название метрики	Тип метрики	Единицы измерения	Описание	Примечание
vault.mysql.delete	сводная	мс	Время, необходимое для выполнения операции DELETE в бэкенде хранения MySQL	---
vault.mysql.get	сводная	мс	Время, необходимое для выполнения операции GET в бэкенде хранения MySQL	---
vault.mysql.list	сводная	мс	Время, необходимое для выполнения операции LIST в бэкенде хранения MySQL	---
vault.mysql.put	сводная	мс	Время, необходимое для выполнения операции PUT в бэкенде хранения MySQL	---
vault.policy.delete_policy	сводная	мс	Время, необходимое для удаления политики	---
vault.policy.get_policy	сводная	мс	Время, необходимое для чтения политики	---
vault.policy.list_policies	сводная	мс	Время, необходимое для перечисления всех политик	---
vault.policy.set_policy	сводная	мс	Время, необходимое для установки политики	---
vault.postgres.delete	сводная	мс	Время, необходимое для выполнения операции DELETE в бэкенде хранения PostgreSQL	---
vault.postgres.get	сводная	мс	Время, необходимое для выполнения операции GET в бэкенде хранения PostgreSQL	---

Название метрики	Тип метрики	Единицы измерения	Описание	Примечание
vault.postgres.list	сводная	мс	Время, необходимое для выполнения операции LIST в бэкенде хранения PostgreSQL	---
vault.postgres.put	сводная	мс	Время, необходимое для выполнения операции PUT в бэкенде хранения PostgreSQL	---
vault.raft_storage.bolt.cursor.count	датчик	число	Количество курсоров, созданных в базе данных Bolt	---
vault.raft_storage.bolt.freelist.allocated_bytes	датчик	байты	Общее пространство, выделенное для списка свободных страниц в базе данных Bolt	---
vault.raft_storage.bolt.freelist.free_pages	датчик	число	Количество свободных страниц в списке свободных страниц базы данных Bolt	---
vault.raft_storage.bolt.freelist.pending_pages	датчик	число	Количество ожидающих страниц в списке свободных страниц базы данных Bolt	---
vault.raft_storage.bolt.freelist.used_bytes	датчик	байты	Общее пространство, используемое списком свободных страниц в базе данных Bolt	---
vault.raft_storage.bolt.node.count	датчик	число	Количество выделений узлов для базы данных Bolt	---
vault.raft_storage.bolt.node.dereferences	датчик	число	Общее количество разыменований узлов базой данных Bolt	---

Название метрики	Тип метрики	Единицы измерения	Описание	Примечание
vault.raft_storage.bolt.page.bytes_allocated	датчик	байты	Общее пространство, выделенное для базы данных Bolt	---
vault.raft_storage.bolt.page.count	датчик	число	Количество выделений страниц в базе данных Bolt	---
vault.raft_storage.bolt.rebalance.count	датчик	число	Количество перебалансировок узлов, выполненных базой данных Bolt	---
vault.raft_storage.bolt.rebalance.time	сводная	мс	Время, необходимое базе данных Bolt для перебалансировки узлов	---
vault.raft_storage.bolt.spill.count	датчик	число	Количество узлов, сброшенных базой данных Bolt	---
vault.raft_storage.bolt.spill.time	сводная	мс	Общее время, затраченное на сброс базой данных Bolt	---
vault.raft_storage.bolt.split.count	датчик	число	Количество узлов, разделенных базой данных Bolt	---
vault.raft_storage.bolt.transaction.currently_open_read_transactions	датчик	число	Количество текущих транзакций чтения для базы данных Bolt	---
vault.raft_storage.bolt.transaction.started_read_transactions	датчик	число	Количество начатых транзакций чтения базой данных Bolt	---
vault.raft_storage.bolt.write.count	датчик	число	Количество операций записи, выполненных базой данных Bolt	---
vault.raft_storage.bolt.write.time	счетчик	мс	Общее кумулятивное время, затраченное базой данных Bolt на запись на диск	---

Название метрики	Тип метрики	Единицы измерения	Описание	Примечание
vault.raft_storage.-follower.applied_in-dex_delta	датчик	число	Разница между индексом, примененным лидером, и индексом, примененным резервным узлом, как сообщается эхо-запросами	---
vault.raft_storage.-follower.last_heart-beat_ms	счетчик	мс	Время с момента последнего получения запроса на проверку активности резервным узлом	---
vault.raft_storage.s-tats.applied_index	датчик	число	Наивысший индекс журнала Raft, примененный к конечному автомату или добавленный в очередь `fsm_pending`	---
vault.raft_storage.s-tats.commit_index	датчик	число	Индекс последнего журнала Raft, зафиксированного на диске на узле	---
vault.raft_storage.s-tats.fsm_pending	датчик	число	Количество журналов Raft, поставленных в очередь узлом для применения конечным автоматом	---
vault.raft-storage.delete	таймер	мс	Время, необходимое для вставки записи журнала для удаления пути	---
vault.raft-storage.entry_size	сводная	байты	Общий размер записи Raft во время применения журнала	---
vault.raft-storage.get	таймер	мс	Время, необходимое для получения значения по указанному пути из конечного автомата	---

Название метрики	Тип метрики	Единицы измерения	Описание	Примечание
vault.raft-storage.list	таймер	мс	Время, необходимое для перечисления всех записей по префиксу из конечного автомата	---
vault.raft-storage.put	таймер	мс	Время, необходимое для вставки записи журнала для сохранения пути	---
vault.raft.apply	счетчик	число	Количество транзакций в настроенном интервале	Метрика `vault.raft.apply` обычно является хорошим индикатором нагрузки на запись в вашем внутреннем хранилище Raft.
vault.raft.candidate.electSelf	сводная	мс	Время, необходимое узлу для отправки запроса на голосование на другой узел	---
vault.raft.commitNumLogs	датчик	число	Количество журналов, обработанных для применения к конечному автомату в одной партии	---
vault.raft.commitTime	сводная	мс	Время, необходимое для фиксации новой записи в журнале Raft на узле-лидере.	---
vault.raft.fsm.applyBatch	сводная	мс	Время, необходимое конечному автомату для применения последней партии журналов	---
vault.raft.fsm.applyBatchNum	счетчик	число	Количество журналов, примененных в последней партии	---
vault.raft.fsm.enqueue	сводная	мс	Время, необходимое для постановки партии журналов в очередь для применения конечным автоматом	---

Название метрики	Тип метрики	Единицы измерения	Описание	Примечание
vault.raft.fsm.snapshot	сводная	мс	Время, необходимое конечному автомату для записи информации о состоянии для текущего снимка	---
vault.raft.get	сводная	мс	Время, необходимое для получения записи из базового хранилища	---
vault.raft.leader.dispatchLog	таймер	мс	Время, необходимое узлу-лидеру для записи записи журнала на диск	---
vault.raft.leader.dispatchNumLogs	датчик	число	Количество журналов, зафиксированных на диске в последней партии	---
vault.raft.leader.lastContact	сводная	мс	Время с момента последнего контакта лидера с резервными узлами при проверке аренды лидерства	---
vault.raft.list	сводная	мс	Время, необходимое для получения списка ключей из базового хранилища	---
vault.raft.peers	датчик	число	Количество узлов в конфигурации кластера Raft	---
vault.raft.replication.appendEntries.log	сводная	число	Количество журналов, реплицированных на узел для установления паритета с журналами лидера	---
vault.raft.replication.appendEntries.rpc	таймер	мс	Время, необходимое для репликации записей журнала узла-лидера на все резервные узлы с помощью `appendEntries`	---

Название метрики	Тип метрики	Единицы измерения	Описание	Примечание
vault.raft.replication.heartbeat	таймер	мс	Время, необходимое для вызова `appendEntries` на узле, чтобы узел не вышел из времени ожидания	---
vault.raft.replication.installSnapshot	таймер	мс	Время, необходимое для обработки вызова RPC `installSnapshot`	Только узлы, находящиеся в состоянии `follower`, сообщают метрики `vault.raft.replication.installSnapshot`.
vault.raft.restore	счетчик	число	Количество раз, когда узел выполнил операцию восстановления	В контексте хранилища Raft операция восстановления относится к процессу, при котором Raft потребляет внешний снимок для восстановления своего состояния
vault.raft.restoreUserSnapshot	таймер	мс	Время, необходимое для восстановления конечного автомата из пользовательского снимка	---
vault.raft.rpc.appendEntries	таймер	мс	Время, необходимое для обработки удаленного вызова `appendEntries` от узла	---
vault.raft.rpc.appendEntries.processLogs	таймер	мс	Время, необходимое для полной обработки ожидающих журналов для данного узла	---
vault.raft.rpc.appendEntries.storeLogs	таймер	мс	Время, необходимое для записи любых ожидающих журналов с момента последнего запроса на добавление записей для данного узла	---
vault.raft.rpc.requestVote	сводная	мс	Время, необходимое для завершения вызова requestVote	---
vault.raft.snapshot.create	таймер	мс	Время, необходимое для создания нового снимка	---

Название метрики	Тип метрики	Единицы измерения	Описание	Примечание
vault.raft.snapshot.persist	таймер	мс	Время, необходимое для записи метаинформации снимка на диск при создании снимков	---
vault.raft.snapshot.takeSnapshot	таймер	мс	Общее время, необходимое для создания и сохранения текущего снимка	В большинстве случаев `vault.raft.snapshot.takeSnapshot` примерно равно `vault.raft.snapshot.create` + `vault.raft.snapshot.persist`
vault.raft.state.candidate	счетчик	число	Количество раз, когда сервер Raft инициировал выборы	---
vault.raft.state.follower	сводная	число	Количество раз в настроенном интервале, когда сервер Raft стал резервным узлом	Узлы переходят в состояние follower в следующих случаях: • когда узел присоединяется к кластеру; • когда выбирается лидер, но узел не был выбран лидером.
vault.raft.state.leader	счетчик	число	Количество раз, когда сервер Raft стал лидером	---
vault.raft.transition.heartbeat_timeout	сводная	число	Количество раз, когда узел перешел в состояние candidate после того, как не получил сообщение о проверке активности от последнего известного лидерar	---
vault.rollback.attempt.{MOUNTPOINT}	сводная	мс	Время, необходимое для выполнения операции отката на указанной точке монтирования	---
vault.rollback.inflight	датчик	число	Количество выполняющихся операций отката	---
vault.rollback.queued	датчик	число	Количество операций отката, ожидающих начала	---

Название метрики	Тип метрики	Единицы измерения	Описание	Примечание
vault.rollback.wait-ing	сводная	мс	Время между постановкой операции отката в очередь и началом выполнения	---
vault.route.create.{MOUNTPOINT}	сводная	мс	Время, необходимое для отправки запроса на создание в бэкенд и завершения операции для указанной точки монтирования	---
vault.route.delete.{MOUNTPOINT}	сводная	мс	Время, необходимое для отправки запроса на удаление в бэкенд и завершения операции для указанной точки монтирования	---
vault.route.list.{MOUNTPOINT}	сводная	мс	Время, необходимое для отправки запроса на перечисление в бэкенд и завершения операции для указанной точки монтирования	---
vault.route.read.{MOUNTPOINT}	сводная	мс	Время, необходимое для отправки запроса на чтение в бэкенд и завершения операции для указанной точки монтирования	---
vault.route.rollback.{MOUNTPOINT}	сводная	мс	Время, необходимое для отправки запроса на откат в бэкенд и завершения операции для указанной точки монтирования	StarVault автоматически планирует и выполняет операции отката точек монтирования для очистки частичных ошибок.

Название метрики	Тип метрики	Единицы измерения	Описание	Примечание
vault.runtime.al-loc_bytes	датчик	байты	Пространство, выделенное для процессов StarVault	Количество выделенных байт может иногда достигать пиковых значений, но всегда должно возвращаться к стабильному значению в здоровой установке StarVault.
vault.runtime.free_-count	датчик	число	Количество освобожденных объектов	---
vault.runtime.gc_-pause_ns	сводная	нс	Время, необходимое для завершения последнего запуска сборки мусора	---
vault.run-time.heap_objects	датчик	число	Общее количество объектов в куче в памяти	Метрика `vault.runtime.heap_objects` является хорошим индикатором нагрузки на память. Рекомендуется отслеживать `vault.runtime.heap_objects`, чтобы установить точный базовый уровень и пороги для оповещений о состоянии вашей установки StarVault.
vault.runtime.mal-loc_count	датчик	число	Общее количество выделенных объектов в куче в памяти	---
vault.runtime.num_-goroutines	датчик	число	Общее количество выполняющихся в памяти подпрограмм Go	Метрика `vault.runtime.num_goroutines` является хорошим индикатором нагрузки на систему. Рекомендуется отслеживать `vault.runtime.num_goroutines`, чтобы установить точный базовый уровень и пороги для оповещений о состоянии вашей установки StarVault.
vault.run-time.sys_bytes	датчик	число	Общее количество байт, выделенных для StarVault	Общее количество выделенных системных байт включает пространство, используемое кучей, а также пространство, которое было освобождено, но не возвращено операционной системе.
vault.runtime.to-tal_gc_pause_ns	датчик	нс	Общее время паузы сборщика мусора с момента последнего запуска Vault	---
vault.runtime.to-tal_gc_runs	датчик	число	Общее количество запусков сборщика мусора с момента последнего запуска StarVault	---
vault.secret.kv.-count	датчик	число	Количество записей в каждом механизме секретов ключ-значение	StarVault организует количество пар ключ-значение по кластеру и точке монтирования.

Название метрики	Тип метрики	Единицы измерения	Описание	Примечание
vault.secret.lease.creation	счетчик	число	Количество аренд, созданных механизмами секретов	StarVault организует количество аренд по кластеру, механизму секретов, точке монтирования и времени жизни (TTL).
vault.token.count	датчик	число	Количество неистекших и неотозванных токенов, доступных для использования в хранилище токенов	StarVault обновляет количество токенов каждые 10 минут и организует результат по кластеру.
vault.token.count.by_auth	датчик	число	Общее количество токенов, созданных определённым методом аутентификации	StarVault организует количество токенов по кластерам и методам аутентификации.
vault.token.count.by_policy	датчик	число	Общее количество токенов с определённой политикой	StarVault организует количество токенов по кластерам и политикам. Токены с более чем одной политикой учитываются для каждой связанной политики.
vault.token.count.by_ttl	датчик	число	Общее количество токенов с определённым временем жизни (TTL)	StarVault организует количество токенов по кластерам и диапазону TTL, назначенному при создании.
vault.token.create_root	счетчик	число	Количество созданных корневых токенов	Метрика `vault.token.create_root` учитывает общее количество созданных корневых токенов с течением времени, а не количество корневых токенов, используемых в данный момент. В результате значение `vault.token.create_root` не уменьшается при отзыве корневого токена.
vault.token.create	сводная	мс	Время, необходимое для создания токена в StarVault	---
vault.token.createAccessor	сводная	мс	Время, необходимое для создания указателя токена в StarVault	---
vault.token.creation	счетчик	число	Количество созданных сервисных или пакетных токенов	StarVault организует количество созданных токенов по кластерам, методам аутентификации, точкам монтирования, времени жизни (TTL) и типу токена.
vault.token.lookup	сводная	мс	Время, необходимое для поиска токена в StarVault	---

Название метрики	Тип метрики	Единицы измерения	Описание	Примечание
vault.token.revoke-tree	сводная	мс	Время, необходимое для полного отзыва дерева токенов в StarVault	---
vault.token.store	сводная	мс	Время, необходимое для сохранения обновлённой записи токена без записи во вторичный индекс	---
vault.zookeeper.delete	сводная	мс	Время, необходимое для выполнения операции DELETE в бэкенде ZooKeeper	---
vault.zookeeper.get	сводная	мс	Время, необходимое для выполнения операции GET в бэкенде ZooKeeper	---
vault.zookeeper.list	сводная	мс	Время, необходимое для выполнения операции LIST в бэкенде ZooKeeper	---
vault.zookeeper.put	сводная	мс	Время, необходимое для выполнения операции PUT в бэкенде ZooKeeper	---

Метрики логирования. Телеметрия журнала аудита

Телеметрия журнала аудита предоставляет информацию о состоянии настроенных устройств аудита.

1. Стандартные метрики

Стандартные метрики для оценки состояния настроенных устройств аудита перечислены в таблице:

Название метрики	Тип метрики	Единицы измерения	Описание	Примечание
vault.audit.log_request_failure	счетчик	число	Количество неудачных запросов логов аудита по всем устройствам	Количество неудачных запросов является **критически важной метрикой**. Ненулевое значение для `vault.audit.log_request_failure` указывает на то, что все ваши настроенные аудиторские устройства не смогли зарегистрировать запрос (или ответ). Если Starault не может правильно провести аудит запроса или ответа на него, исходный запрос завершится неудачей. Обратитесь к логам StarVault и любым специфичным для устройства метрикам для устранения неполадок в неработающем аудиторском лог-устройстве.
vault.audit.log_request	сводная	мс	Время, необходимое для завершения всех запросов логов аудита по всем устройствам для аудита логов	---

Название метрики	Тип метрики	Единицы измерения	Описание	Примечание
vault.audit.log_response_failure	счетчик	число	Количество неудачных запросов на логи аудита по всем устройствам	Количество неудачных запросов является **критически важной метрикой**. Ненулевое значение для `vault.audit.log_response_failure` указывает на то, что одно из настроенных устройств аудита не смогло ответить StarVault. Если StarVault не может правильно провести аудит запроса или ответа на него, исходный запрос завершится неудачей. Обратитесь к специфичным для устройства метрикам и логам для устранения неполадок в неработающем лог-устройстве аудита.
vault.audit.log_response	сводная	мс	Время, необходимое для завершения ответов на логи аудита по всем устройствам для аудита логов	---
vault.autopilot.failure_tolerance	датчик	узлы	Количество здоровых узлов, превышающих кворум	Допустимый уровень отказов указывает, сколько текущих здоровых узлов может выйти из строя без потери кворума.
vault.autopilot.healthy	датчик	логическое значение	Указывает, все ли узлы здоровы	• Значение 1 на датчике означает, что Autopilot считает все узлы здоровыми. • Значение 0 на датчике означает, что Autopilot считает, что как минимум 1 узел нездоров.
vault.autopilot.node.healthy	датчик	логическое значение	Указывает, здоров ли активный узел	• Значение 1 на датчике означает, что Autopilot считает указанный узел (по node_id) здоровым. • Значение 0 на датчике означает, что Autopilot не может связаться с указанным узлом (по node_id) или считает узел нездоровым.

2. Метрики устройств аудита

Метрики, относящиеся к конкретному устройству, для каждого включенного устройства аудита. Например, если вы включили файловое устройство аудита `file`, то соответствующие метрики будут следующими: `vault.audit.file.log_request` и `vault.audit.file.log_response`.

Далее в таблице представлены метрики устройств аудита и их описания:

Название метрики	Тип метрики	Единицы измерения	Описание	Примечание
vault.audit.{DEVICE}.log_request	сводная	мс	Время, необходимое для завершения всех запросов логов аудита на устройстве	---
vault.audit.{DEVICE}.log_response	сводная	мс	Время, необходимое для завершения всех ответов логов аудита на устройстве	---