Управление доступом

1. Общие сведения

StarVault предлагает гибкую и безопасную систему управления доступом, включающую в себя аутентификацию, назначение политик, аренду секретов, управление пользователями и интеграцию с внешними поставщиками удостоверений.

2. Содержание раздела

Аудит

1. Общие сведения

Устройства аудита - это компоненты StarVault, которые ведут подробный журнал всех запросов к StarVault и их ответов. Поскольку каждая операция с StarVault - это запрос/ответ API, то журнал аудита при использовании одного устройства аудита содержит все взаимодействия с API StarVault, включая ошибки, за исключением нескольких путей, которые не проходят через систему аудита.

Пример 1. К путям не включенным в аудит относятся:

```
sys/init
sys/seal-status
sys/seal
sys/step-down
sys/unseal
sys/leader
sys/health
sys/rekey/init
sys/rekey/update
sys/rekey/verify
sys/rekey-recovery-key/init
sys/rekey-recovery-key/update
sys/rekey-recovery-key/verify
sys/storage/raft/bootstrap
sys/storage/raft/join
sys/internal/ui/feature-flags
```

Также к путям не включенным в аудит относятся параметры конфигурации слушателя, которые разрешают неаутентифицированный доступ:

```
sys/metrics
sys/pprof/*
sys/in-flight-req
```

2. Включение нескольких устройств

Если включено несколько устройств аудита, StarVault попытается отправить журналы аудита на каждое устройство. Это позволяет дублировать файлы аудита, проверять подделку данных в самих журналах.

StarVault считает запрос успешным, если он может отправить журнал хотя бы на одно настроенное устройство аудита (см. раздел «Заблокированные устройства аудита» ниже). Поэтому, чтобы составить полную картину всех проверяемых действий, используйте совокупность/объединение журналов с каждого устройства аудита.

Настоятельно рекомендуется настроить StarVault на использование нескольких устройств аудита. Сбои в работе аудита могут помешать StarVault обслуживать запросы, поэтому важно обеспечить дополнительное устройство аудита.

3. Формат

Каждая строка в журнале аудита представляет собой объект JSON. Поле `type` указывает, к какому типу относится объект. Существует только два типа: запрос и ответ. Строка содержит всю информацию для любого запроса и ответа. По умолчанию вся конфиденциальная информация сначала хешируется перед записью в журнал аудита.

4. Чувствительная информация

Журналы аудита содержат полные объекты запроса и ответа для каждого взаимодействия с StarVault. Запрос и ответ можно сопоставить по уникальному идентификатору, присвоенному каждому запросу.

Большинство строк, содержащихся в запросах и ответах, хешируются с помощью *соли* с использованием *HMAC-SHA256*. Цель хеширования заключается в том, чтобы секреты не попадали в открытый текст в журналах аудита. Однако все равно можете проверить значение секретов, самостоятельно сгенерировав HMAC — это можно сделать с помощью хэш-функции и соли устройства аудита, используя конечную точку API `/sys/audit-hash/`

Строки обрабатываются HMAC если были получены из JSON или возвращены в JSON. Другие типы данных, такие как целые числа, булевы и так далее, передаются в открытом виде. Рекомендуем предоставлять все конфиденциальные данные в виде строковых значений во всех JSON, отправляемых в StarVault (т. е. целочисленные значения должны быть заключены в кавычки).

Хотя большинство строк хэшируются, StarVault можно настроить так, чтобы сделать некоторые исключения. Например, в методах аутентификации и механизмах секретов пользователи могут включить дополнительные исключения с помощью команды secrets enable и затем настроить ее.

5. Включение/отключение устройств аудита

При первой инициализации сервера StarVault аудит не включен. Устройства аудита должны быть включены пользователем `root` с помощью команды `starvault audit enable`.

Во время включения устройства аудита могут быть переданы параметры для настройки. Например, приведенная ниже команда включает устройство аудита файлов:

```bash
starvault audit enable file file_path=/var/log/starvault_audit.log
```

В приведенной выше команде передан параметр `file_path`, чтобы указать путь, куда будет записываться журнал аудита. Каждое устройство аудита имеет собственный набор параметров.

Конфигурация устройства аудита по умолчанию реплицируется на все узлы кластера. Перед включением устройства аудита убедитесь, что все узлы в кластере (кластерах) смогут успешно регистрироваться на устройстве аудита, чтобы избежать блокировки StarVault от обслуживания запросов. Устройство аудита может быть ограничено только в пределах узла кластера с помощью параметра `local`.

Когда устройство аудита отключается, оно немедленно прекращает получать журналы. Существующие журналы, которые оно хранило, остаются нетронутыми.

После отключения устройства аудита больше не сможете использовать значения HMAC для сравнения с записями в журналах аудита. Это верно, даже если снова включите устройство аудита по тому же пути, поскольку для хэширования будет создана новая соль.

6. Заблокированные устройства аудита

Журналы устройств аудита очень важны, и игнорирование сбоев аудита открывает возможности для атак. StarVault не будет отвечать на запросы, если ни одно из включенных устройств аудита не может их записать.

StarVault различает два типа сбоев в работе устройств аудита:

- Блокирующий сбой — это сбой, при котором попытка записи на устройство аудита не завершается. Это маловероятно при использовании локального дискового устройства, но может произойти при использовании сетевого устройства аудита.
- Неблокирующий сбой — запросы StarVault могут успешно завершиться, если хотя бы одно из нескольких устройство аудита успешно запишет запись аудита. Однако если какое-либо из устройств аудита окажется в блокирующем режиме, запросы StarVault будут зависать до тех пор, пока блокировка не будет устранена.

Другими словами, StarVault не будет завершать запросы до тех пор, пока заблокированное устройство аудита не сможет выполнить запись.

7. Общие параметры конфигурации

- `elide_list_responses` (`bool: false`) — см. раздел «Сокращение объема данных в ответах на запросы списка» ниже.
- `format` (`string: «json»`) — позволяет выбрать формат вывода. Допустимыми значениями являются `«json»` и `«jsonx»`, которые форматируют обычные записи журнала как XML.
- `hmac_accessor` (`bool: true`) — если true, то включает хэширование указателей токенов.
- `log_raw` (`bool: false`) — если включено, то запись в журнал конфиденциальной информации без хеширования, в необработанном формате.
- `prefix` (`string: «»`) -е настраиваемый строковый префикс для записи перед фактической строкой журнала.

8. Сокращение объема данных в ответах на запросы списка

Некоторые ответы StarVault могут быть очень большими. В первую очередь это относится к операциям со списками — поскольку в API StarVault отсутствует пагинация, листинг очень большой коллекции может привести к ответу длиной в десятки мегабайт. Некоторые бэкенды аудита не могут обрабатывать отдельные записи аудита больших размеров.

Содержимое ответа для операции со списком часто не очень интересно; большинство из них содержит только поле «ключи», содержащее список идентификаторов. Некоторые конечные точки API дополнительно возвращают поле `«key_info»`, представляющее собой данные от ID до некоторой дополнительной информации о записи списка — примером может служить `identity/entity/id/`. Даже в этом случае ответ на операцию со списком обычно представляет собой менее конфиденциальную или публичную информацию, для которой наличие полного ответа в журналах аудита имеет меньшее значение.

Параметр аудита `elide_list_responses` предоставляет возможность не записывать полные данные ответа списка в журнал аудита, чтобы избежать создания очень длинных отдельных записей аудита.

Если опция включена, то влияет только на записи аудита с `type=response` и `request.operation=list`. Значения `response.data.keys` и `response.data.key_info` будут заменены простым целым числом, записывающим, сколько записей содержалось в

списке (`keys`) или карте (`key_info`) — поэтому даже при включенной этой функции можно узнать, сколько элементов было возвращено операцией со списком.

Эта дополнительная обработка затрагивает только поля данных ответа `keys` и `key_info`, и только тогда, когда они имеют ожидаемые типы данных — если ответ списка содержит данные, выходящие за рамки обычных соглашений, применяемых к ответам списка StarVault, то будет оставлен без изменений этой функцией.

Вот пример записи аудита, обработанной этой функцией (отформатированной с дополнительными пробелами и с опущенными полями, не относящимися к данному примеру):

JSON

```
{
  "type": "response",
  "request": {
    "operation": "list"
  },
  "response": {
    "data": {
      "key_info": 4,
      "keys": 4
    }
  }
}
```

9. Содержание раздела

- Устройство для файлового аудита
- Устройство аудита Syslog
- Устройство аудита Socket

Инструкции

1. Общие сведения

В данном разделе представлены инструкции и основные операции StarVault, которые являются общими для пользователей.

2. Содержание раздела