Устранение неполадок механизма секретов PKI и ACME

В данной статье представлены решения распространенных проблем, связанных с интеграцией клиента ACME с сервером ACME StarVault механизма секретов PKI.

1. Ошибка: ACME требует установки конфигурации поля 'path' локального кластера

Если ACME работает на одних узлах кластера StarVault, но не работает на других, это, скорее всего, означает, что адрес кластера не установлен.

1.1. Проявления ошибки

Когда клиент StarVault читает конфигурацию ACME (`/config/acme`) на узле Performance Secondary или когда клиент ACME пытается подключиться к каталогу на этом узле, появится сообщение об ошибке:

```
ACME feature requires local cluster 'path' field configuration to be set
```

1.2. Причина

В большинстве случаев ошибки пути к кластеру означают, что в параметре конфигурации кластера не задан требуемый адрес кластера.

1.3. Решение

Для каждого кластера Performance Replication прочитайте значение `/config/cluster` и убедитесь, что поле `path` установлено. Если оно отсутствует, обновите URL-адрес, чтобы он указывал на путь этого монтирования на адресе с поддержкой TLS для этого кластера PR; этот домен может быть адресом балансировки нагрузки или DNS round robin. Например:

BASH

```
$ starvault write pki/config/cluster path=https://cluster-
b.starvault.example.com/v1/pki
```

После этого перечитайте конфигурацию ACME и убедитесь, что больше не отображаются предупреждения:

```bash
$ starvault read pki/config/acme
```

2. Ошибка: Невозможно зарегистрировать учетную запись на сервере ACME

2.1. Проявления ошибки

При регистрации новой учетной записи без внешней привязки учетной записи (EAB) сервер StarVault отклоняет запрос с ответом типа:

```
Unable to register an account with ACME server
```

с дополнительной информацией в журналах отладки (в случае `certbot`):

```
Server requires external account binding.
```

или, если клиент отправил некорректный запрос серверу, ошибка типа:

```
The request must include a value for the 'externalAccountBinding' field
```

В любом случае необходимо создать новую учетную запись с помощью токена EAB, созданного StarVault.

2.2. Причина

Если сервер был обновлен для требования `eab_policy=always-required` в конфигурации ACME, регистрация новых учетных записей (и повторное использование существующих) будет неудачной.

2.3. Решение

Используя токен StarVault, получите новую привязку внешней учетной записи для нужного каталога:

```bash
$ starvault write -f pki/roles/my-role-name/acme/new-eab
...
directory roles/my-role-name/acme/directory
id        bc8088d9-3816-5177-ae8e-d8393265f7dd
key       MHcCAQE... additional data elided ...
...
```

Затем передайте этот новый токен EAB в клиент ACME. Например, с помощью `certbot`:

```bash
$ certbot [... additional parameters ...] \
    --server https://cluster-b.starvault.example.com/v1/pki/roles/my-role-name/acme/directory \
    --eab-kid bc8088d9-3816-5177-ae8e-d8393265f7dd \
    --eab-hmac-key MHcCAQE... additional data elided ...
```

Убедитесь, что каталог ACME, переданный клиенту ACME, совпадает с каталогом, полученным из хранилища.

3. Ошибка: Не удалось проверить eab

3.1. Проявления ошибки

При инициализации новой учетной записи на этом сервере StarVault клиент ACME может выдать ошибку с сообщением типа:

```bash
The client lacks sufficient authorization :: failed to verify eab
```

Ошибка возникает, если EAB-токен получен из каталога, отличающегося от того, с которым работает клиент.

3.2. Причина

Если токен учетной записи EAB используется с неподходящим каталогом, сервер ACME отклонит запрос с ошибкой о недостаточных разрешениях.

3.3. Решение

Убедитесь, что запрашиваемый токен EAB соответствует каталогу. Для заданной директории по адресу `/some/path/acme/directory` возьмите токены EAB из `/some/path/acme/new-eab`. Остальные шаги по решению проблемы такие же, как и при отладке сбоев регистрации учетной записи.

4. Ошибка: Не удалось выполнить проверку ACME для `{challenge_id}`

4.1. Проявления ошибки

При просмотре журналов сервера StarVault или попытке получить сертификат с помощью клиента ACME возникает сообщение об ошибке вида:

```
ACME validation failed for a465a798-4400-6c17-6735-e1b38c23de38-tls-alpn-01: ...
```

Указывает на то, что сервер не смог подтвердить этот вызов, принятый клиентом.

4.2. Причина

StarVault не может проверить идентичность сервера через запрошенный клиентом тип вызова (`dns-01` , `http-01` или `tls-alpn-01`). StarVault не выпустит сертификат, запрошенный клиентом.

4.3. Решение

Убедитесь, что DNS корректно настроен с точки зрения сервера StarVault, включая настройку любого пользовательского DNS-резольвера.

Убедитесь, что все брандмауэры настроены так, чтобы StarVault мог общаться с соответствующими системами (DNS-сервер в случае `dns-01` , порт 80 на целевой машине для `http-01` или порт 443 на целевой машине для вызовов `tls-alpn-01`).

5. Ошибка: Клиент не может авторизоваться: учетная запись имеет статус: отозвана

5.1. Проявления ошибки

При попытке обновить сертификат клиент ACME сообщает об ошибке:

```
The client lacks sufficient authorization: account in status: revoked
```

5.2. Причина

Если была запущена ручная очистка или включена автоматическая очистка с `tidy_acme=true` , StarVault будет периодически удалять устаревшие учетные записи ACME.

Соединения от клиентов, использующих удаленные учетные записи, будут отклонены.

5.3. Решение

Обратитесь к документации клиента ACME для удаления кэшированной локальной конфигурации и настройте новую учетную запись, указав все необходимые EAB.

6. Справочная

Пожалуйста, предоставьте следующую информацию при обращении в службу поддержки OrionSoft, чтобы помочь нам в расследовании и воспроизведении:

- Имя и версия клиента ACME
- Журналы клиента ACME и/или выходные данные
- Журналы сервера StarVault уровня **DEBUG**.

7. API

Механизм секретов PKI имеет полноценный HTTP API. Более подробную информацию можно найти в разделе API движка PKI secrets.

Рекомендации по улучшению безопасности боевой среды

В этом руководстве представлены рекомендации по оптимальным методам развертывания StarVault с усиленной защитой. Рекомендации основаны на модели безопасности StarVault и ориентированы на глубинную защиту.

Эти рекомендации разделены на два раздела. Базовые рекомендации следует выполнять, если это возможно, при любом развертывании StarVault в боевой среде. Расширенные рекомендации обеспечивают дополнительные уровни безопасности, которые могут потребовать дополнительных административных затрат или могут не подходить для каждого развертывания.

1. Базовые рекомендации

- **Не запускайте от учетной записи root.** Для запуска StarVault используйте специальную непривилегированную сервисную учетную запись, а не учетную запись root или администратора. StarVault рассчитан на запуск от непривилегированного пользователя, и это значительно повышает защиту от различных атак с повышением привилегий.
- **Разрешите минимальные права на запись.** Непривилегированная сервисная учетная запись StarVault не должна иметь доступа к перезаписи исполняемого двоичного файла или любых конфигурационных файлов StarVault. Пользователь StarVault может записывать только каталоги и файлы для локального хранилища StarVault (например, для бэкенда Integrated Storage) или логов аудита.
- **Сковзное шифрование TLS.** В боевой среде StarVault всегда должен использоваться с TLS. Если для доступа к StarVault используются промежуточные балансировщики нагрузки или обратные прокси, необходимо использовать TLS для всех сетевых соединений между всеми компонентами системы (включая бэкенды хранилища), чтобы обеспечить шифрование всего трафика при передаче в StarVault и из него. По возможности следует установить заголовок HTTP Strict Transport Security (HSTS) с помощью функции пользовательских заголовков ответа StarVault.
- **Отключить подкачки.** StarVault шифрует данные в процессе передачи и в состоянии покоя, однако для его работы конфиденциальные данные все равно должны находиться в памяти. Риск заражения должен быть сведен к минимуму путем отключения подкачки, чтобы операционная система не перемещала конфиденциальные данные на диск. Это особенно важно при использовании интегрированного бэкэнд-хранилища.

- **Отключите дампы ядра.** Пользователь или администратор, который может принудительно выполнить дамп ядра и имеет доступ к полученному файлу, потенциально может получить доступ к ключам шифрования StarVault. Предотвращение дампов ядра зависит от конкретной платформы; в Linux установка ограничения ресурсов `RLIMIT_CORE` равным 0 отключает дампы ядра. В файле блока службы systemd установка `LimitCORE=0` обеспечит выполнение этого параметра для службы StarVault.
- **Одноразовая аренда.** StarVault должен быть единственным основным процессом, запущенным на машине. Это снижает риск того, что другой процесс, запущенный на той же машине, скомпрометирован и может взаимодействовать с StarVault. Аналогично, выполнение на пустом железе должно быть предпочтительнее, чем на ВМ, а выполнение на ВМ должно быть предпочтительнее, чем выполнение в контейнере.
- **Трафик файерволла.** Используйте локальный брандмауэр или функции сетевой безопасности поставщика облачных услуг, чтобы ограничить входящий и исходящий трафик для StarVault и основных системных служб, таких как NTP. Это включает в себя ограничение входящего трафика разрешенными подсетями и исходящего трафика для служб, к которым StarVault необходимо подключиться, например баз данных.
- **Избегайте корневых токенов.** При первой инициализации StarVault предоставляет корневой токен. Этот токен следует использовать для первоначальной настройки системы, в частности для установки методов аутентификации пользователей. Мы рекомендуем относиться к конфигурации StarVault как к коду и использовать контроль версий для управления политиками. После настройки корневой токен должен быть отозван, чтобы исключить риск воздействия. Корневые токены могут генерироваться по мере необходимости и должны быть отозваны как можно скорее.
- **Настройте блокировку пользователя.** StarVault предоставляет функцию блокировки пользователей для методов аутентификации approle, ldap и userpass. **Блокировка пользователей включена по умолчанию**. Убедитесь, что порог блокировки и продолжительность блокировки соответствуют политике безопасности вашей организации.
- **Включите ведение журнала аудита.** StarVault поддерживает несколько устройств аудита. Включение регистрации аудита позволяет получить историю всех операций, выполняемых StarVault, а также след для экспертизы в случае неправомерного использования или компрометации. Журналы аудита надежно хэшируют конфиденциальные данные, но доступ к ним все равно должен быть ограничен, чтобы предотвратить непреднамеренное раскрытие информации.
- **Отключение истории команд оболочки.** Возможно, вы захотите, чтобы сама команда `starvault` вообще не отображалась в истории.
- **Часто обновляйтесь.** StarVault активно развивается, поэтому важно часто обновлять его, чтобы включить исправления безопасности и любые изменения в настройках по умолчанию, таких как длина ключа или набор шифров.

- **Синхронизируйте часы.** Используйте NTP или любой другой механизм, подходящий для вашей среды, чтобы убедиться, что все узлы StarVault согласны с тем, который сейчас час. StarVault использует часы для таких вещей, как обеспечение TTL и установка дат в сертификатах PKI, и если узлы имеют значительную разницу во времени - это может привести к ошибкам.
- **Ограничение доступа к хранилищу.** StarVault шифрует все данные в состоянии покоя, независимо от того, какой бэкэнд для хранения используется. Несмотря на то что данные зашифрованы, злоумышленник с произвольным контролем может привести к повреждению или потере данных, изменив или удалив ключи. Во избежание несанкционированного доступа или операций - доступ к внутреннему хранилищу должен быть ограничен только StarVault.
- **Никаких учетных данных с открытым текстом.** Блок `seal` в файле конфигурации StarVault настраивает тип печати для дополнительной защиты данных, например с помощью облачных KMS-решений для шифрования и расшифровки корневого ключа (также известного как мастер-ключ). НЕ храните учетные данные облака открытым текстом в блоке `seal`. Если сервер StarVault размещен на той же облачной платформе, что и служба KMS, используйте идентификационные решения для конкретной платформы. Например:
    - Учетная запись службы на Google Cloud Platform.
- **Используйте самые безопасные из доступных алгоритмов.** Слушатель TLS в StarVault поддерживает различные устаревшие алгоритмы для обратной совместимости. Хотя эти алгоритмы доступны, их не рекомендуется использовать, особенно если имеется альтернатива лучше. Если возможно, использование TLS 1.3 обеспечивает применение современных алгоритмов шифрования для шифрования данных при передаче и обеспечения секретности при пересылке.
- **Следуйте лучшим практикам для плагинов.** Хотя плагины обычно имеют безопасную конфигурацию по умолчанию, вам следует помнить о неправильно настроенных или вредоносных плагинах StarVault. Они могут нанести ущерб безопасности вашего развертывания StarVault.
- **Недетерминированное слияние файлов.** Объединение конфигурационных файлов StarVault происходит недетерминированно, и несоответствие настроек в разных файлах может привести к несоответствию настроек StarVault. Убедитесь, что конфигурации наборов согласованы во всех файлах (и в любых объединенных файлах, обозначенных командой `-config`).
- **Используйте правильные права доступа к файловой системе.** Перед запуском StarVault всегда проверяйте, чтобы к файлам, особенно содержащим конфиденциальную информацию, были применены соответствующие разрешения.
- **Используйте стандартный ввод для секретов StarVault.** StarVault login и StarVault un-seal позволяют операторам предоставлять секретные значения как из стандартного ввода, так и из аргументов командной строки. Аргументы командной строки могут быть

прочитаны другими непривилегированными пользователями на том же хосте или сохранены в истории оболочки.

- **Вопросы, связанные с увольнением.** Удаление учетных записей в StarVault или связанных с ними поставщиков идентификационных данных может не сразу отменить доступ на основе токенов. В зависимости от того, как управляется доступ к StarVault, операторы должны рассмотреть следующие варианты:
  - Удаление сущности из групп, предоставляющих доступ к ресурсам.
  - Отмена активных аренд для данной учетной записи пользователя.
  - Удаление канонической сущности пользователя после удаления учетных записей в StarVault или связанных с ними поставщиков идентификационных данных. Одного удаления канонической сущности недостаточно, так как она автоматически создается при успешном входе в систему, если ее не существует.
  - Отключение методов аутентификации вместо их удаления, что приводит к отзыву всех токенов, сгенерированных этим методом аутентификации.
- **Используйте короткие TTL.** По возможности, учетные данные, выдаваемые StarVault (например, токены, сертификаты x.509), должны быть недолговечными, чтобы защитить их от возможной компрометации и уменьшить необходимость использования методов отзыва.

2. Расширенные рекомендации

- **Отключите SSH/удаленный рабочий стол.** При запуске StarVault как приложения с одним арендатором - пользователи никогда не должны получать доступ к машине напрямую. Вместо этого они должны обращаться к StarVault через API по сети. Для отладки используйте централизованное решение для ведения логов и телеметрии. Обязательно ограничьте доступ к логам по мере необходимости.
- **Использование функций безопасности systemd.** Systemd предоставляет ряд функций, которые можно использовать для блокировки доступа к файловой системе и административным возможностям. Файл сервисных блоков, поставляемый с официальными пакетами StarVault Linux, устанавливает некоторые из них по умолчанию, в том числе:

```
ProtectSystem=full
PrivateTmp=yes
CapabilityBoundingSet=CAP_SYSLOG CAP_IPC_LOCK
AmbientCapabilities=CAP_IPC_LOCK
ProtectHome=read-only
PrivateDevices=yes
NoNewPrivileges=yes
```

Дополнительные сведения и подробности см. на странице руководства systemd.exec.

- **Неизменяемые обновления.** StarVault полагается на внешнее хранилище для сохранения данных. Такое разделение позволяет управлять серверами, на которых работает StarVault, без изменений. При обновлении до новых версий в сеть включаются новые сервера с обновленной версией StarVault. Они подключаются к тому же бэкенду общего хранилища и снимают печать. Затем старые серверы удаляются. Это снижает необходимость в удаленном доступе и оркестровке обновлений, которые могут внести бреши в систему безопасности.
- **Настройте SELinux/AppArmor.** Использование дополнительных механизмов, таких как SELinux и AppArmor, поможет обеспечить дополнительные уровни безопасности при использовании StarVault.
- **Измените пределы.** Возможно, в вашем дистрибутиве Linux установлены строгие ограничения (`ulimits`) на количество процессов. Перед запуском в боевой среде просмотрите `ulimits` на максимальное количество открытых файлов, соединений и т.д.; возможно, их нужно увеличить.
- **Контейнеры Docker.** Чтобы задействовать функцию "блокировки памяти" в контейнере StarVault, вам, скорее всего, потребуется использовать `overlayfs2` или другой поддерживаемый драйвер.

Рекомендованные шаблоны

Чтобы обеспечить эффективную работу сред StarVault, внедрите следующие лучшие практики и избегайте распространенных антипаттернов.

- Регулирование время аренды по умолчанию
- Увеличение IOPS
- Улучшение периодичности обновлений
- Тестируйте перед обновлениями
- Ротация логов устройств аудита
- Контролируйте метрики
- Сформируйте базовый уровень потребления
- Сведите к минимуму использование корневого токена
- Переключевание при необходимости

1. Регулирование время аренды по умолчанию

Время аренды по умолчанию в StarVault составляет 32 дня или 768 часов. Это время позволяет выполнять некоторые операции, например: повторная аутентификация или продление. Дополнительные сведения см. в документации по аренде.

Рекомендуемый шаблон:

Настроите значение аренды TTL в соответствии с потребностями. StarVault хранит договоры аренды в памяти до тех пор, пока срок аренды не истечет. Мы рекомендуем сохранять TTL настолько коротким, насколько это возможно в конкретном случае.

- Auth tune
- Secrets tune

> Настройка или корректировка TTL не влияет на уже выпущенные токены. После настройки TTL необходимо выпустить новые токены.

Решение Anti-pattern:

Если создаете аренды, не изменяя установленное по умолчанию время жизни (TTL), то аренды будут существовать в StarVault до истечения времени аренды установленного по умолчанию. В зависимости от инфраструктуры и доступной системной памяти

использование стандартного или длительного TTL может вызвать проблемы с производительностью, поскольку StarVault хранит аренды в памяти.

2. Увеличение IOPS

IOPS (операции ввода/вывода в секунду) измеряет производительность членов кластера StarVault. StarVault ограничен лимитами ввода-вывода бэкенда хранилища, а не вычислительными требованиями.

Рекомендованный шаблон:

Используйте справочные руководства для определения размеров аппаратного обеспечения серверов StarVault и сетевых параметров.

- Хранилище с интегрированной эталонной архитектурой хранения
- Настройка производительности
- Механизм преобразования секретов

В зависимости от количества клиентов механизмы секретов Transit могут занимать много ресурсов.

Решение Anti-pattern:

Ограниченное количество операций ввода-вывода может значительно снизить производительность StarVault.

3. Улучшение периодичности обновлений

Хотя обновлять StarVault при каждом удобном случае несложно, отсутствие частого обновления может повлиять на производительность и безопасность StarVault.

Рекомендованный шаблон:

Мы рекомендуем обновить StarVault до последней версии. Подпишитесь на релизы в репозитории StarVault на GitHub, и уведомления от OrionSoft StarVault discuss будут.

- Руководства по обновлению StarVault
- Уведомление об устаревании функций StarVault и планы

Решение Anti-pattern:

Если вы не следите за регулярностью обновлений, в вашей среде StarVault могут отсутствовать ключевые функции и улучшения.

- Отсутствующие исправления для ошибок или уязвимостей.

- Новые функции для улучшения рабочего процесса.
- Должны использовать документацию по конкретной версии, а не по последней.
- Некоторые образовательные ресурсы требуют определенной минимальной версии StarVault.
- Обновления могут потребовать поэтапного подхода, который использует промежуточную версию перед установкой последнего бинарного файла.

4. Тестируйте перед обновлениями

Рекомендуем тестировать StarVault в тестовой среде перед развертыванием в боевой среде. Хотя обновить сразу в боевой среде может быть быстрее, но тестирование поможет выявить любые проблемы совместимости. Обратите внимание на историю изменений и учитывайте все новые функции, улучшения, известные проблемы и исправления ошибок при тестировании.

Рекомендованный шаблон:

Перед обновлением в боевой среде протестируйте новые версии StarVault в тестовой среде и следуйте документации по обновлению. Рекомендуем добавить этап тестирования к вашей стандартной процедуре обновления.

- Стандартная процедура обновления StarVault
- Обновление StarVault

Решение Anti-pattern:

Без надлежащего тестирования перед обновлением в боевой среде вы рискуете столкнуться с проблемами совместимости и производительности.

Это может привести к простою или ухудшению работы вашей боевой среды StarVault.

5. Ротация логов устройств аудита

Устройства аудита в StarVault ведут подробный журнал каждого клиентского запроса и ответа сервера. Если позволите логам устройств аудита работать бесконечно и без ротации, то можете столкнуться с блокировкой устройств аудита, если хранилище файловой системы будет заполнено.

Рекомендованный шаблон:

Периодически проверяйте и ротируйте журналы аудита.

- Заблокированные устройства аудита
- Руководство по заблокированным устройствам аудита

Решение Anti-pattern:

StarVault не будет отвечать на запросы, если устройства аудита не включены для записи запросов. Устройство аудита может исчерпать объем локального хранилища, если журнал устройства аудита не обслуживается и не ротируется с течением времени.

6. Контролируйте метрики

Полагаясь только на операционные логи StarVault и данные в StarVault UI, вы получите неполное представление о производительности кластера.

Рекомендованный шаблон:

Непрерывный мониторинг позволит организациям обнаруживать незначительные проблемы и оперативно устранять их. Переход от реактивного к проактивному мониторингу поможет предотвратить сбои в работе системы. StarVault имеет несколько выходов, которые помогают отслеживать активность кластера: логи аудита, операционные логи и данные телеметрии. Эти данные могут работать с инструментом SIEM (управление информацией о безопасности и событиями) для агрегации, проверки и оповещения.

- Телеметрия
- Ссылка на метрики телеметрии

Добавление решения для мониторинга:

- Мониторинг телеметрии и аудит логов устройств
- Мониторинг телеметрии с помощью Prometheus и Grafana

По умолчанию StarVault логирует стандартные выводы и стандартные ошибки, которые автоматически перехватываются журналом systemd. Вы также можете указать StarVault перенаправлять записи оперативных логов в файл.

Решение Anti-pattern:

Частичное понимание активности кластера может привести к тому, что бизнес окажется в реактивном состоянии.

7. Сформируйте базовый уровень потребления

Базовый уровень дает представление о текущем использовании и пороговых значениях. Показатели телеметрии очень ценны, особенно если они отслеживаются с течением времени. Вы можете использовать показатели телеметрии для сбора базовой информации о деятельности кластера, а предупреждения информируют вас об аномальной активности.

Рекомендованный шаблон:

Информация о телеметрии также может передаваться непосредственно из StarVault в ряд решений для агрегирования показателей и сохраняться для агрегирования и проверки.

- Показатели использования хранилища
- Диагностика проблем с сервером

Решение Anti-pattern:

Этот вопрос тесно связан с рекомендуемым шаблоном для отслеживания метрик. Данные телеметрии хранятся в памяти только в течение короткого периода времени.

8. Сведите к минимуму использование корневого токена

При инициализации сервера StarVault выдается начальный корневой токен, который предоставляет доступ на корневом уровне ко всем функциям StarVault.

Рекомендованный шаблон:

Мы рекомендуем отозвать корневой токен после инициализации StarVault в вашей среде. Если пользователям требуется повышенный доступ, создайте политики списка управления доступом, которые предоставляют соответствующие возможности на нужных путях в StarVault. Если для выполнения операций требуется токен root, сохраняйте его как можно дольше, прежде чем отозвать.

- Руководство по генерации корневых токенов
- Корневые токены
- Политики StarVault

Решение Anti-pattern:

Корневой токен может выполнять все действия в StarVault, и срок его действия никогда не истекает. Неограниченный доступ может дать пользователям более высокие привилегии, чем необходимо, для всех операций и путей StarVault. Совместное использование и предоставление доступа к корневому токену представляет собой риск для безопасности.

9. Смена ключей при необходимости

StarVault распространяет нераспечатанные ключи среди заинтересованных сторон. Для разблокировки StarVault необходим кворум ключей в соответствии с настройками инициализации.

Рекомендованный шаблон:

StarVault поддерживает смену ключей, и вам следует установить рабочий процесс для смены ключей, когда это необходимо.

- Смена ключей и оборот ключей.
- Оператор смены ключей.

Решение Anti-pattern:

Если несколько заинтересованных лиц покинут организацию, вы рискуете не набрать необходимое количество ключей для обеспечения кворума по снятию печати, что может привести к потере возможности снятия печати с хранилища.