

Постоянный кэш. Kubernetes

Если в `kubernetes` настроен тип постоянного кэша, StarVault Agent оптимизирует постоянный кэш специально для Kubernetes. Для этого типа постоянного кэша требуется токен учетной записи службы Kubernetes. Токен учетной записи службы используется при шифровании и расшифровке постоянного кэша в качестве дополнительной проверки целостности.

Файл постоянного кэша StarVault Agent в Kubernetes следует использовать только для передачи токенов StarVault и аренды между контейнерами StarVault Agent для инициализации и sidecar. Этот файл кэша должен использоваться совместно с использованием объема памяти между контейнерами StarVault Agent.

Если используется Injector StarVault Agent для Kubernetes, постоянный кэш автоматически настраивается и используется в хранилище аннотаций hashicorp.com/agent-cache-enable: true.

1. Конфигурация

- `service_account_token_file` (string: optional) - Если для параметра `type` задано значение `kubernetes`, это настраивает путь на диске, по которому можно найти токен учетной записи службы Kubernetes. По умолчанию используется `/var/run/secrets/kubernetes.io/serviceaccount/token`.

Кэширование. Постоянный кэш

StarVault Agent может восстанавливать токены и договоры аренды из файла постоянного кэша, созданного предыдущим процессом StarVault Agent. Постоянный кэш - это файл BoltDB, который содержит кортежи, зашифрованные сгенерированным ключом шифрования. Зашифрованные кортежи включают токен хранилища, используемый для извлечения секретов, права аренды токенов/секретов и секретные значения.

i Постоянное кэширование StarVault Agent восстановит только секреты с арендой. Секреты, которые не подлежат восстановлению, такие как KV v2, сохранены не будут.

Чтобы использовать постоянный кэш StarVault Agent, необходимо использовать функцию автоматической аутентификации. Если срок действия токена автоматической аутентификации истек к моменту восстановления кэша, кэш будет признан недействительным, и потребуется повторно извлечь секретные данные из хранилища.

Если в StarVault Agent наряду с постоянным кэшем включена функция создания шаблонов, StarVault Agent автоматически направит запросы на создание шаблонов через кэш. Это гарантирует, что запросы на создание шаблонов будут кэшироваться и восстанавливаться должным образом.

i Постоянный кэш StarVault Agent в настоящее время поддерживается только в среде Kubernetes.

1. Типы постоянного кэша агента хранилища

Пожалуйста, ознакомьтесь с информацией о доступных типах и их использовании/конфигурации на боковой панели.

2. Пример конфигурации постоянного кэша

Вот пример конфигурации постоянного кэша:

```
# Другие блоки конфигурации агента хранилища
# ...

cache {
  persist "kubernetes" {
    path = "/vault/agent-cache"
```

```
}  
}
```

Агент. Сервис Windows

StarVault Agent можно запустить как службу Windows. Для этого вам необходимо зарегистрировать StarVault Agent в диспетчере управления службами Windows. После регистрации StarVault Agent его можно запустить как любую другую службу Windows.



Эти команды следует запускать в сеансе PowerShell с правами администратора.

1. Регистрация агента StarVault как службы Windows

Существует несколько способов зарегистрировать StarVault Agent в качестве службы Windows. Один из способов — использовать `sc.exe`. `sc.exe` работает лучше всего, если путь к двоичному файлу StarVault и связанному с ним файлу конфигурации агента не содержат пробелов. `sc.exe` может быть довольно сложно заставить работать правильно, если ваш путь содержит пробелы, так как пути, содержащие пробелы, должны быть заключены в кавычки, а правильное экранирование кавычек таким образом, чтобы `sc.exe` был удовлетворен, — нетривиальная задача. Если ваш путь содержит пробелы или вы предпочитаете не использовать `sc.exe`, другой альтернативой является использование командлета `New-Service`. `New-Service` менее требователен к методу, используемому для экранирования кавычек, и иногда может быть проще. Ниже будут показаны примеры обоих.

2. Использование `sc.exe`



ВАЖНО: Убедитесь, что путь к исполняемому файлу службы заключен в кавычки, особенно если он содержит пробелы, чтобы избежать потенциальных рисков повышения привилегий.

Если вы используете `sc.exe`, убедитесь, что вы явно указали `sc.exe`, а не просто `sc`. Приведенная ниже команда показывает создание StarVault Agent как службы, используя "StarVault Agent" в качестве отображаемого имени и запускаясь автоматически при запуске Windows. Аргумент `binPath` должен включать полный путь к исполняемому файлу StarVault, а также любые требуемые аргументы.

BASH |

```
PS C:\Windows\system32> sc.exe create StarVaultAgent
binPath="C:\starvault\starvault.exe agent -config=C:\starvault\agent-config.hcl"
displayName="StarVault Agent" start=auto
[SC] CreateService SUCCESS
```

Обратите внимание, что пробел после `=` во всех аргументах является намеренным и обязательным.

Если вы получили сообщение об успешном выполнении, ваша служба зарегистрирована в диспетчере служб.

Если вы получили ошибку, проверьте путь к двоичному файлу и аргументы, запустив содержимое `binPath=` непосредственно в сеансе PowerShell и наблюдая за результатами.

3. Использование New-Service

Синтаксис немного отличается для `New-Service`, но суть та же. Вызов ниже эквивалентен вызову `sc.exe`.

```
PS C:\Windows\system32> New-Service -Name "StarVaultAgent" -BinaryPathName "C:\starvault\starvault.exe agent -config=C:\starvault\agent-config.hcl" -DisplayName "StarVault Agent" -StartupType "Automatic"
```

Status	Name	DisplayName
Stopped	StarVaultAgent	StarVault Agent

Как упоминалось ранее, `New-Service` проще использовать, если путь к исполняемому файлу StarVault и/или конфигурации агента содержит пробелы. Ниже приведен пример того, как настроить StarVault Agent как службу с использованием пути с пробелами.

```
PS C:\Windows\system32> New-Service -Name "StarVaultAgent" -BinaryPathName "C:\my dir\starvault.exe" agent -config="C:\my dir\agent-config.hcl" -DisplayName "StarVault Agent" -StartupType "Automatic"
```

Status	Name	DisplayName
Stopped	StarVaultAgent	StarVault Agent

Обратите внимание, что только сами пути заключены в двойные кавычки, а весь `BinaryPathName` заключен в одинарные кавычки, чтобы экранировать двойные кавычки, используемые для путей.


Если что-то пойдет не так во время этого процесса и вам позже понадобится вручную отредактировать путь, используйте редактор реестра, чтобы найти следующий ключ: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\StarVaultAgent`. Вы можете изменить значение `ImagePath` в этом ключе на правильный путь.

4. Запуск службы StarVault Agent

Существует несколько способов запустить службу. * С помощью команды `sc.exe`. * С помощью командлета `Start-Service`. * Перейдя в диспетчер служб Windows и найдите **StarVaultAgent** в столбце имени службы. Нажмите кнопку «Запустить», чтобы запустить службу.

5. Пример запуска агента StarVault с помощью `sc.exe`


```
PS C:\Windows\system32> sc.exe start StarVaultAgent
```

BASH | 

```
SERVICE_NAME: StarVaultAgent
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE                : 4   RUNNING
                               (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE       : 0   (0x0)
        SERVICE_EXIT_CODE    : 0   (0x0)
        CHECKPOINT            : 0x0
        WAIT_HINT             : 0x0
        PID                   : 6548
        FLAGS                  :
```

6. Пример запуска агента StarVault с помощью `Start-Service`

```
PS C:\Windows\system32> Start-Service -Name "StarVaultAgent"
```

BASH | 



В случае успешного запуска службы `New-Service` не возвращает никаких выходных данных.