УТВЕРЖДЕНО

RU.86432418.00002-01 91 01-1 - ЛУ

Программное обеспечение «Deckhouse Stronghold»

Руководство пользователя

RU.86432418.00002-01 91 01-1

Листов 44

2025

Содержание

Список используемых обозначений и сокращений

API	Application Programming Interface (прикладной программный интерфейс)
CLI	Command line interface (интерфейс командной строки)
ОС	Операционная система
ПО, ПО «Deckhouse Stronghold»	Программное обеспечение «Deckhouse Stronghold»
ФСТЭК России	Федеральная служба по техническому и экспортному контролю

1. Назначение средства

1.1. Область применения

Данное руководство предназначено для пользователей программного обеспечения «Deckhouse Stronghold» (далее по тексту – ПО «Deckhouse Stronghold», ПО).

1.2. Краткое описание возможностей

Объектом оценки является ПО «Deckhouse Stronghold», назначением которого является обеспечение безопасного хранения и управления жизненным циклом конфиденциальных данных. Не все возможности, описанные в этом руководстве, могут быть доступны для пользователя. Возможности пользователя определяются администратором ПО «Deckhouse Stronghold», исходя из разрешающих политик, назначенных для пользователя.

1.3. Уровень подготовки пользователя

Пользователи ПО «Deckhouse Stronghold» должны обладать базовыми навыками:

- наличие практических навыков работы с компьютерной техникой, операционным системами и Интернет-браузерами;
- знание технологических процессов обработки информации, выполняемых автоматизированным способом и знакомство с эксплуатационной документацией.

1.4. Перечень эксплуатационной документации, с которой необходимо ознакомиться пользователю

Пользователи обязаны до начала эксплуатации ПО «Deckhouse Stronghold» ознакомиться с эксплуатационной документацией, поставляемой с ПО «Deckhouse Stronghold», включая руководство пользователя.

2. Подготовка к работе

Для работы с ПО «Deckhouse Stronghold» пользователям требуется рабочее место, дистрибутив ПО «Deckhouse Stronghold» и, в случае поставки ПО «Deckhouse Stronghold» в контейнерном исполнении, актуальная версия ПО «Deckhouse Platform Certified Security Edition» (не ниже 1.67).

В рамках подготовки к работе с ПО «Deckhouse Stronghold» пользователям необходимо ознакомиться с данным руководством. Дополнительной подготовки для работы с ПО «Deckhouse Stronghold» не требуется.

3. Режимы работы средства

ПО «Deckhouse Stronghold» функционирует в режиме клиента, выполняющего запросы к API сервера.

В ПО предусмотрен режим высокой доступности (HA - high availability). В HA-режиме ПО запускается в нескольких экземплярах на разных серверах. В определенный момент времени основным является только один экземпляр ПО «Deckhouse Stronghold», остальные экземпляры выполняют функцию прокси, пересылая запросы. Также они получают все изменения данных, происходящих на лидер-узле. В случае выхода из строя серверного обеспечения или в любом другом случае, когда основной экземпляр не может работать (физический сервер выключен, отсутствует сетевая связность между узлами, не работают дисковые операции), оставшиеся экземпляры проводят голосование и выбирают нового лидера.

Регламентные работы производятся с учетом требований о доступности ПО «Deckhouse Stronghold».

Функционирование ПО «Deckhouse Stronghold» при отказах и сбоях серверного общесистемного и специального программного обеспечения, оборудования, в том числе структурных узлов ПО «Deckhouse Stronghold», не предусматривается.

4. Функции и интерфейсы, доступные пользователю

ПО «Deckhouse Stronghold» предназначено для управления секретами.

Интерфейсы, доступные пользователю ПО «Deckhouse Stronghold», определяются в соответствии с назначенными политиками доступа. В разделе 5 описана процедура взаимодействия с интерфейсами ПО.

5. Описание операций

5.1. Аутентификация

Перед взаимодействием с ПО «Deckhouse Stronghold» пользователь должен пройти аутентификацию, используя один из настроенных и назначенных для аутентификации пользователя методов аутентификации. После аутентификации генерируется токен. Этот токен концептуально похож на идентификатор сессии на веб-сайте. К токену может быть прикреплена политика доступа пользователя, настроенная администратором, которая отображается во время аутентификации. Пользователь осуществляет вход в ПО через интерфейс аутентификации (Рисунок 1).

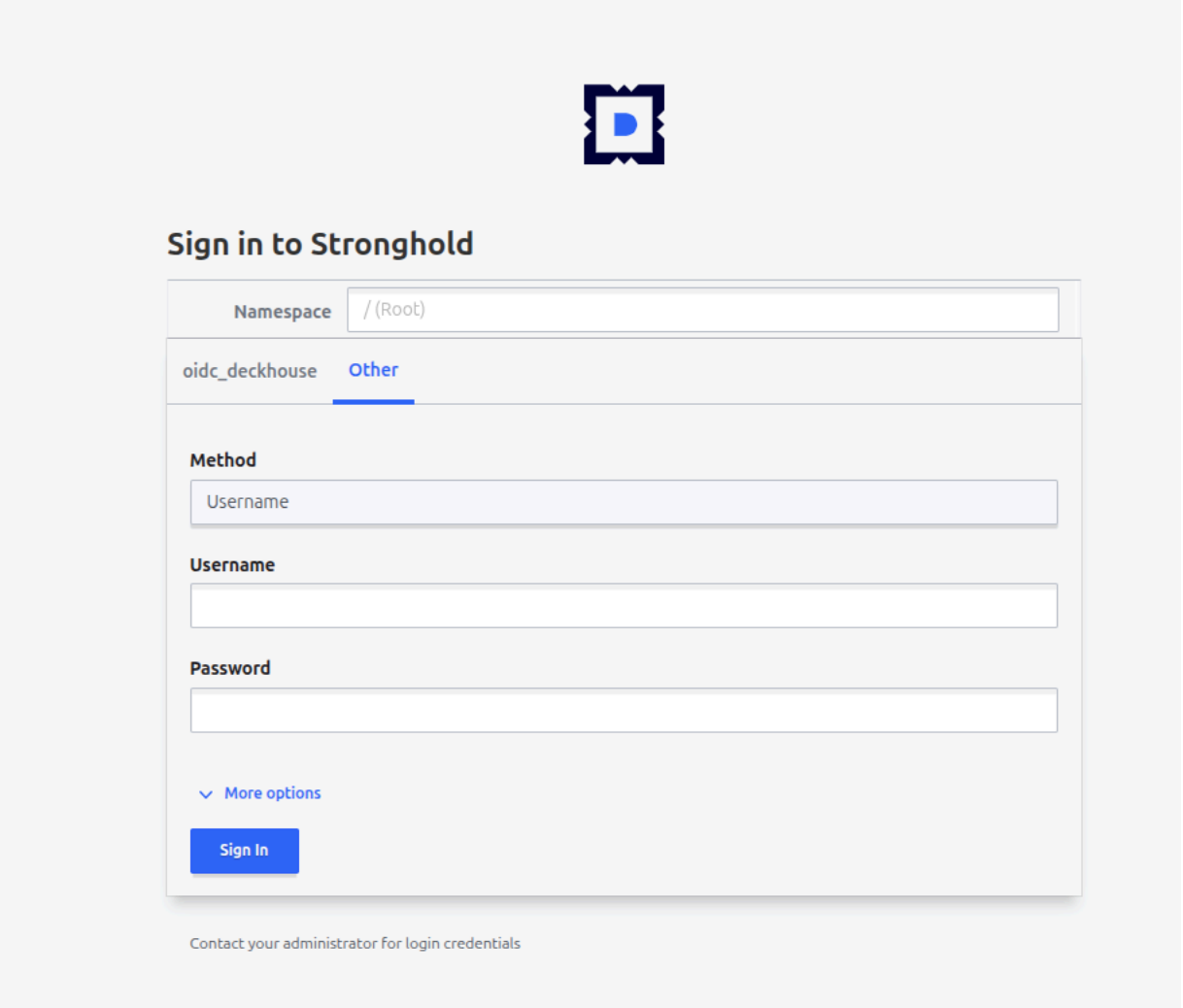

Рисунок 1. Окно аутентификации веб-интерфейса

При успешной аутентификации пользователя откроется главный экран ПО «Deckhouse Stronghold».

5.1.1. Главный экран и работа с механизмами секретов

Главный экран ПО «Deckhouse Stronghold» представлен на Рисунке 2.

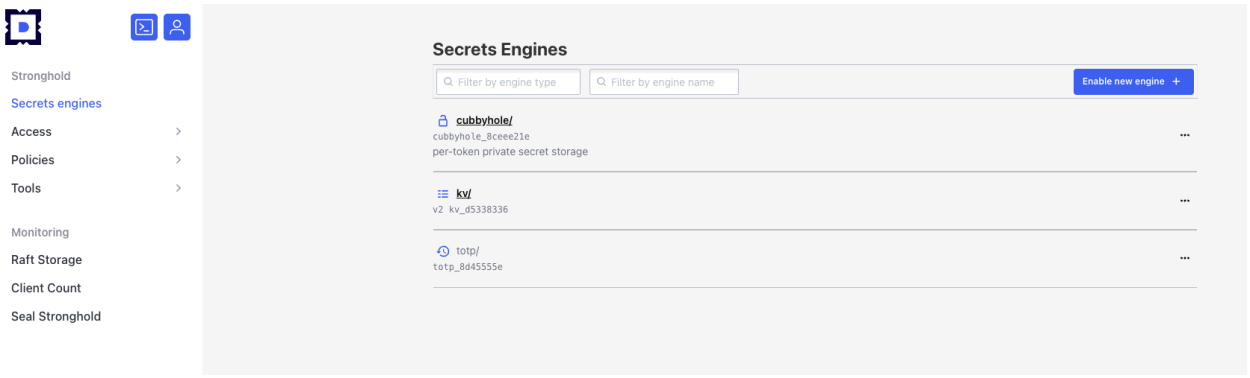

Рисунок 2. Веб-интерфейс ПО «Deckhouse Stronghold»

В левой части главного экрана находится окно навигации по основным разделам пользовательского интерфейса. В центре — список механизмов секретов, используемых в кластере, и кнопка для добавления нового механизма секретов.

5.1.1.1. Просмотр информации о механизме секретов

Названия механизмов секретов интерактивные. При нажатии на название, можно посмотреть информацию о механизме и добавленных секретах. В окне с информацией отображаются вкладки:

- «Secrets» — список секретов (заведенных ролей, ключей и т.д., в зависимости от механизма секретов);
- «Configuration» — конфигурация механизма и кнопка для добавления секрета (роли, ключа и т.д., в зависимости от механизма секретов).

Например, для механизма «KV» («Ключ-значение») доступна следующая информация и элементы управления:

- список секретов;
- конфигурация механизма;
- кнопка добавления секрета.

Интерфейс просмотра информации о механизме «KV» представлена на Рисунке 3.

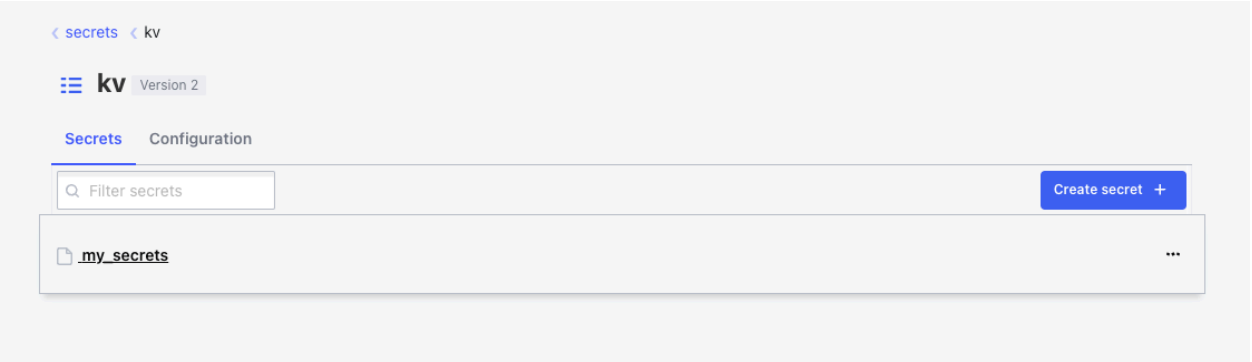

Рисунок 3. Просмотр информации о механизме секретов

Для просмотра конфигурации механизма секретов необходимо нажать на вкладку «Configuration» (пример на Рисунке 4).

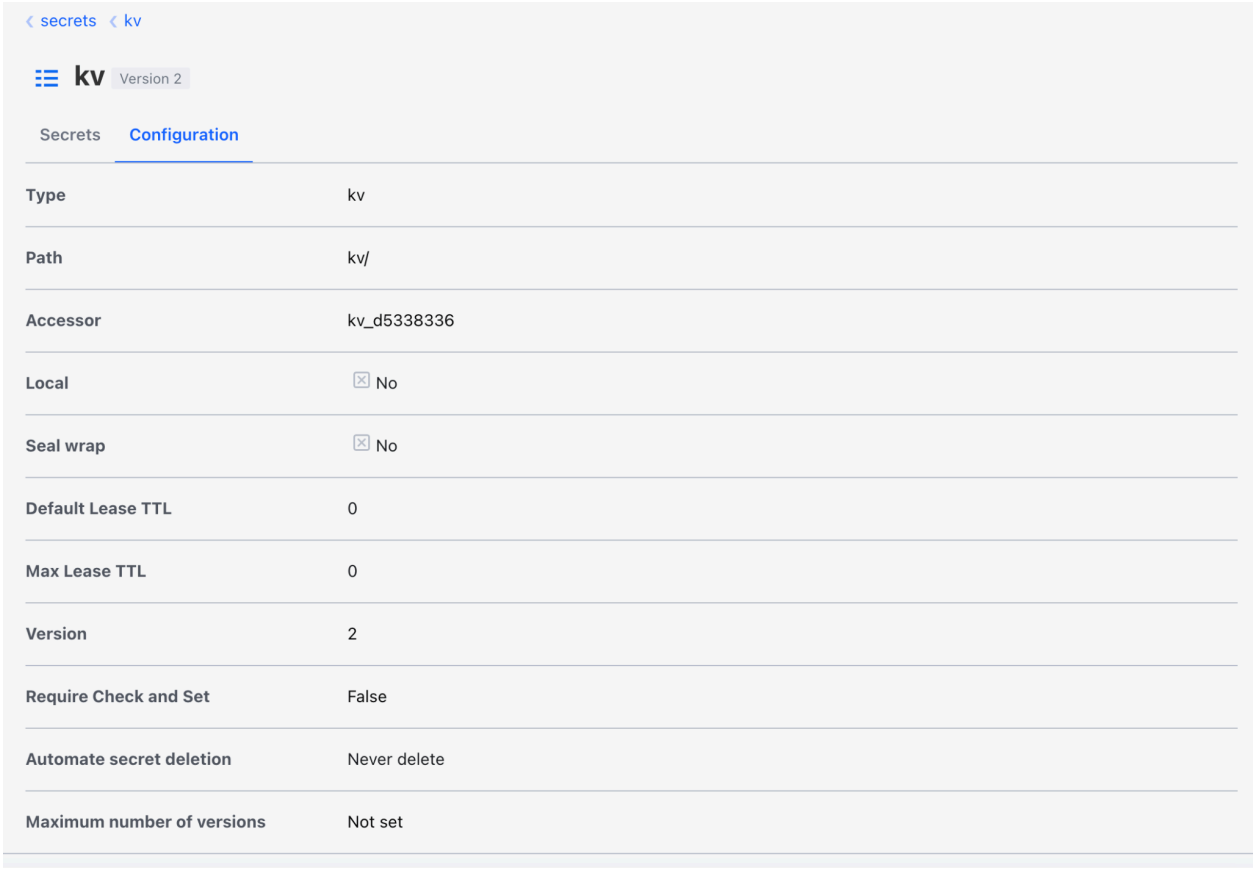

Рисунок 4. Просмотр конфигурации механизма секретов

5.1.1.1.1. Просмотр информации о секрете и его версиях (на примере механизма «Ключ-значение»)

Пользователь может посмотреть информацию о секрете, нажав на его название в окне информации о механизме секретов. В окне с информацией о секрете отображается две вкладки: вкладка с общей информацией о секрете и его версиях, вкладка с метаданными секрета.

На вкладке «Secret» с общей информацией о секрете отображается переключатель для просмотра сведений о секрете в формате JSON (Рисунок 5).

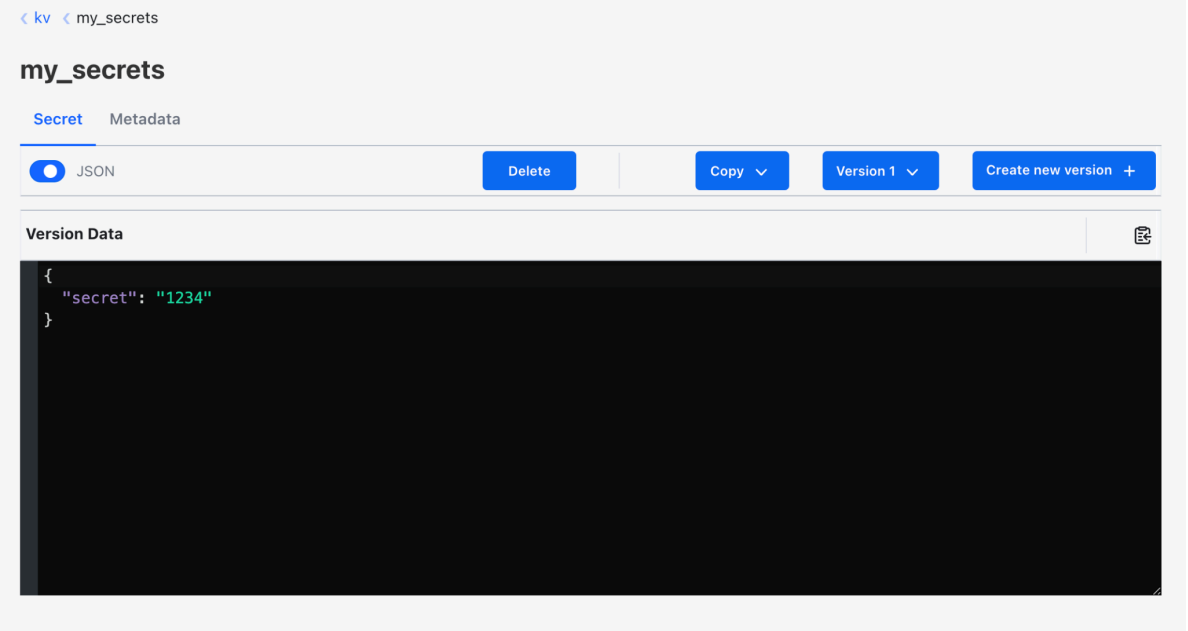

Рисунок 5. Просмотр информации о секрете и его версиях

Также на вкладке «Secret» с общей информацией о секрете отображаются кнопки для работы с секретом и его версиями:

- удаление;
- копирование;
- выбор версии (не для всех механизмов секретов);
- добавление новой версии.

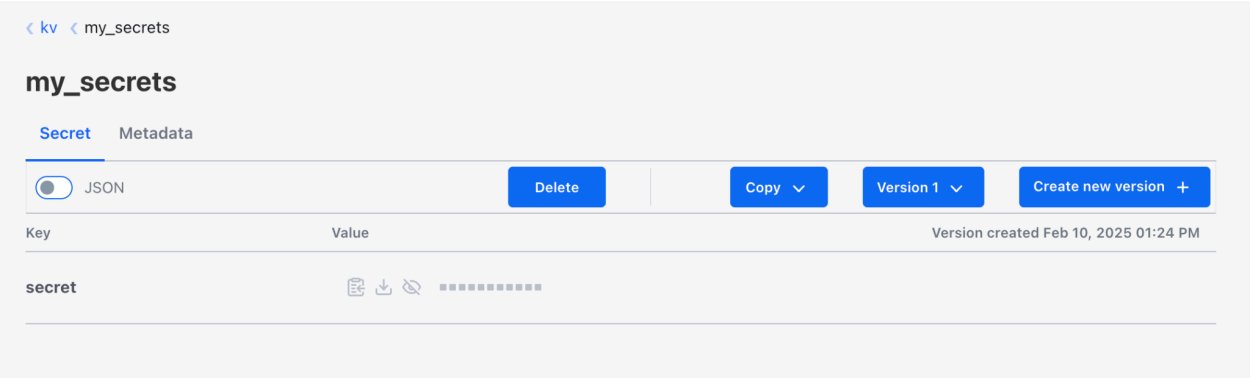

Рисунок 6. Вкладка «Secret»

Просмотреть метаданные секрета можно, нажав на вкладку «Metadata». При нажатии на вкладку отобразится окно для просмотра и редактирования метаданных секрета. На вкладке отображаются метаданные секрета, кнопка для их редактирования и ссылка для добавления пользовательских метаданных (Рисунок 7).

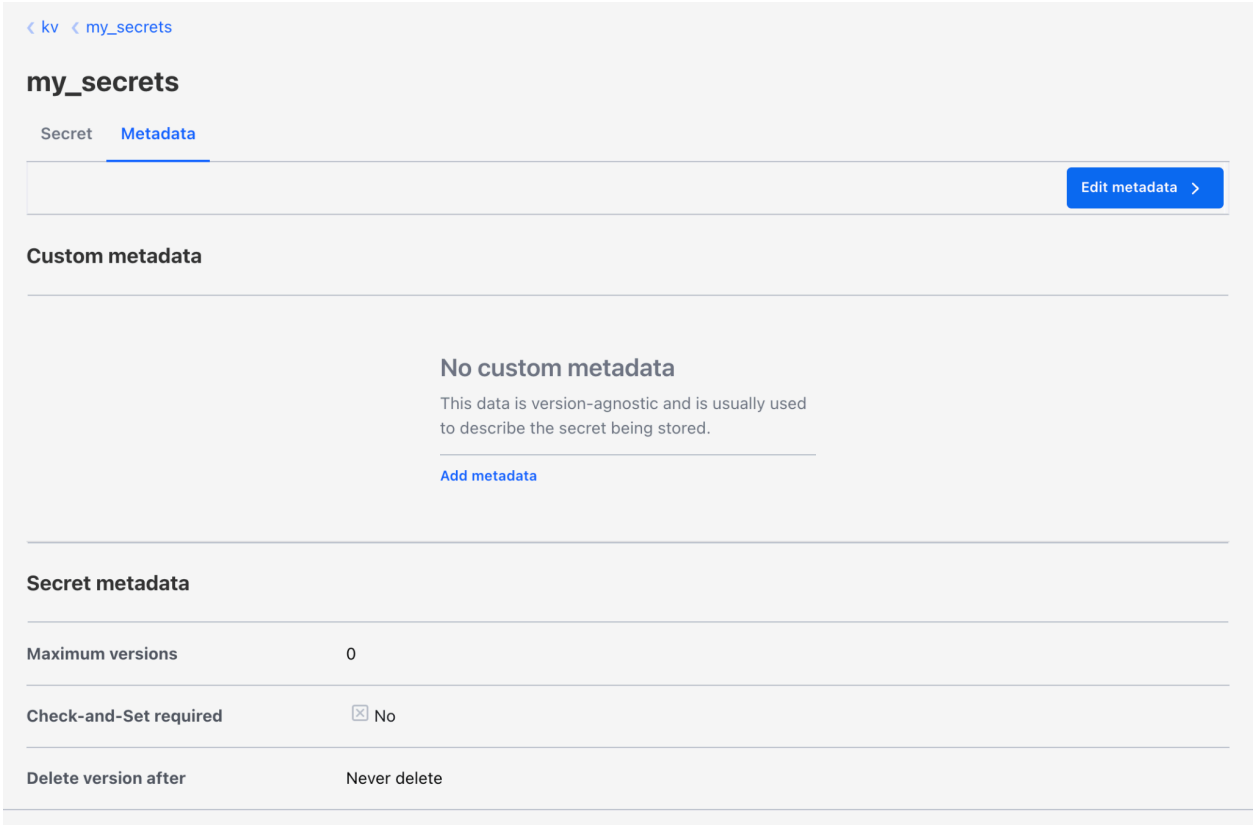

Рисунок 7. Просмотр метаданных секрета

5.1.1.1.2. Добавление секрета

Добавить секрет можно, нажав на кнопку «Create secret» (роли, ключа и т.д. — название кнопки зависит от механизма секретов).

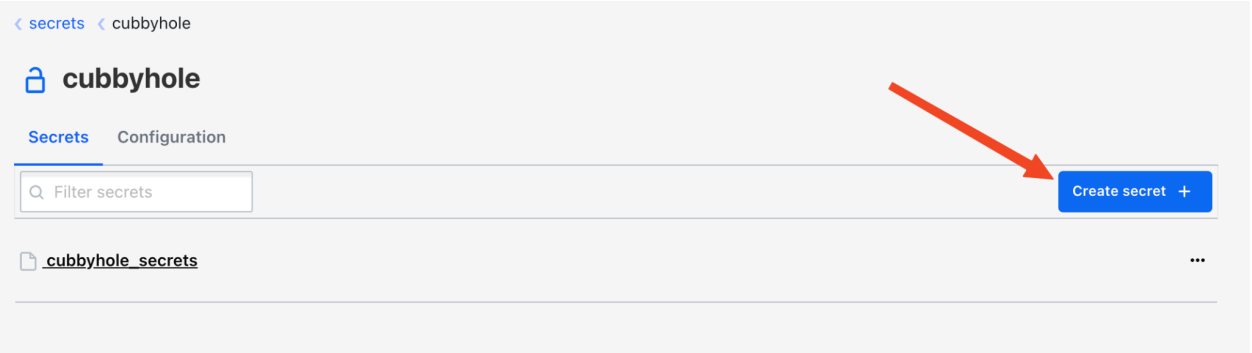

Рисунок 8. Добавление секрета

После нажатия кнопки «Create secret» откроется форма добавления секрета (роли, ключи и т.д. — название кнопки зависит от механизма секретов (Рисунок 9). Состав формы зависит от механизма секретов. Например, форма добавления секрета «Cubbyhole» содержит:

- переключатель для просмотра и редактирования секрета в формате JSON;
- поле для указания пути к секрету («Path»);
- поле для указания ключа;
- поле для указания значения;
- кнопку для добавления новой пары ключ-значение (если необходимо добавить несколько ключей с одинаковым путем к секрету («Path»)).

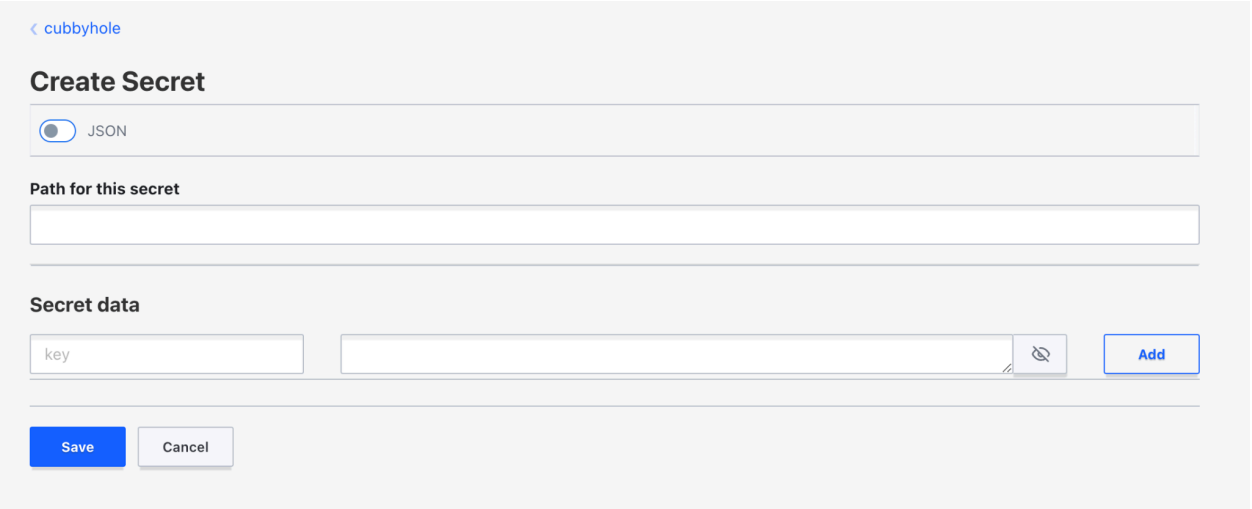

Рисунок 9. Форма добавления секрета

5.1.1.1.3. Добавление механизма секретов

Добавить новый механизм секретов можно, нажав на кнопку «Enable new engine» на главном экране (Рисунок 2). После этого откроется экран выбора типа добавляемого механизма секретов. Для создания нового механизма секретов необходимо выбрать нужный механизм (Рисунок 10) и нажать кнопку «Next».

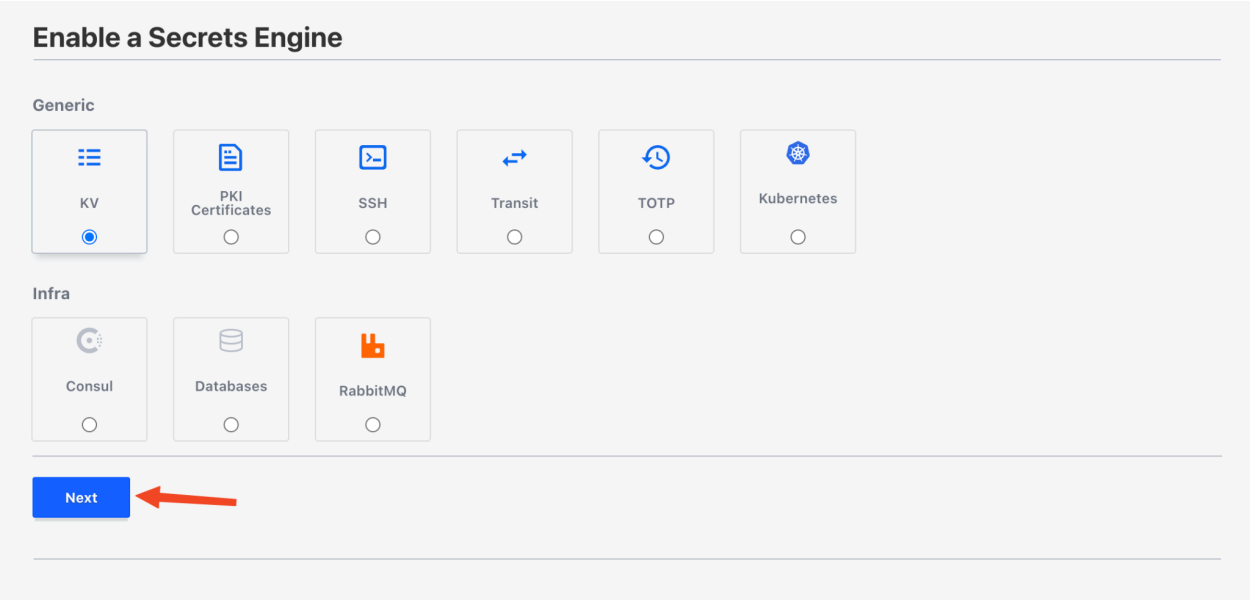

Рисунок 10. Добавление механизма секретов

После этого откроется окно с настройками добавляемого механизма секретов. Оно состоит из двух блоков:

- основные настройки (различаются в зависимости от добавляемого механизма секретов);
- опции («Method options» — по умолчанию блок свернут, чтобы открыть его, нужно кликнуть на его название).

Внизу окна находятся две кнопки (Рисунок 11):

- «Enable Engine» — для сохранения механизма секретов после его настройки;
- «Back» — для возврата без сохранения на экран выбора механизма секретов.

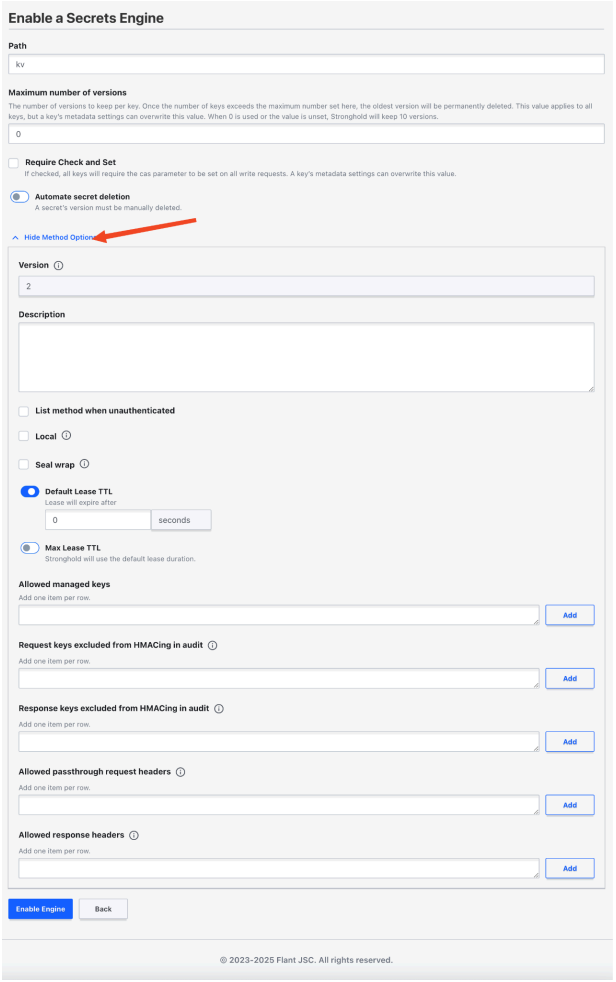

Рисунок 11. Окно с настройками добавляемого механизма секретов

5.2. Управление доступом к данным и функциям ПО «Deckhouse Stronghold»

Управление доступом к данным и функциям ПО «Deckhouse Stronghold» осуществляется в разделе «Access». Перейти в него можно, нажав на вкладку «Access» на главном экране (Рисунок 2). В центральной части окна отображается информация, в зависимости от выбранного в данный момент подраздела (по умолчанию — «Методы аутентификации» («Authentication Methods»). В левой части экрана раздела находится окно навигации по подразделам, вверху которого расположена ссылка для быстрого перехода на главный экран ПО «Deckhouse Stronghold» (Рисунок 12).

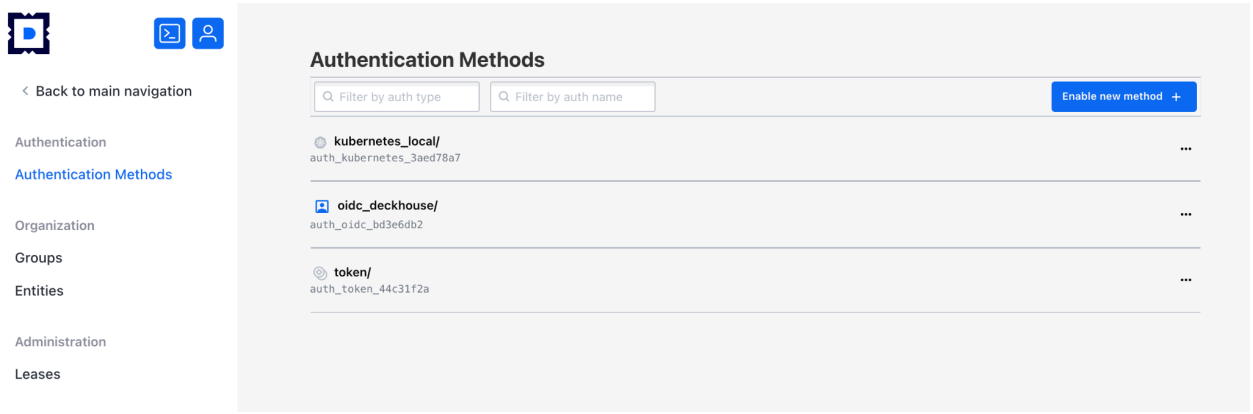

Рисунок 12. Управление доступом к данным и функциям ПО «Deckhouse Stronghold»

5.2.1. Работа с методами аутентификации

Подраздел для работы с методами аутентификации открывается по умолчанию при переходе в раздел «Access» с главного экрана. Для перехода в него из других подразделов необходимо нажать на вкладку «Authentication Methods» в меню слева (Рисунок 13).

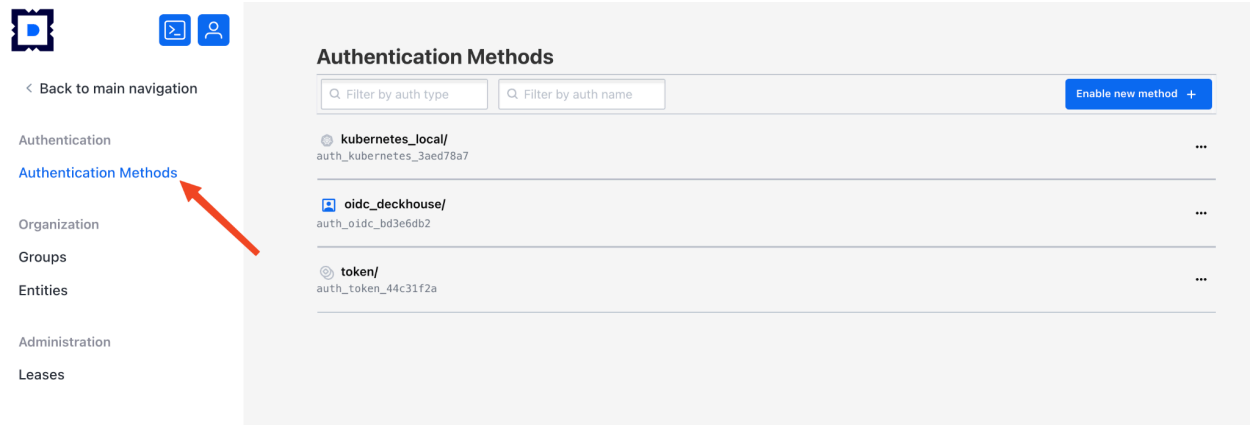

Рисунок 13. Работа с методами аутентификации

В центре экрана находится список методов аутентификации, используемых в кластере, поля для фильтрации элементов списка и кнопка для добавления нового метода.

Для методов из списка доступны следующие действия:

- просмотр конфигурации;
- изменение конфигурации;
- удаление метода.

Для выбора нужного действия необходимо нажать на кнопку с тремя точками, размещенную в конце строки с названием метода (Рисунок 14).

Рисунок 14. Список методов аутентификации

5.2.1.1. Просмотр информации о методе аутентификации

Для просмотра информации о методе аутентификации, необходимо нажать на его название или выбрать действие «View configuration» (доступно в выпадающем меню при нажатии на кнопку с тремя точками (Рисунок 14)). В окне с информацией о методе аутентификации отображается одна или две вкладки (количество и содержимое вкладок зависит от метода аутентификации) с информацией о методе и кнопка для его конфигурирования.

Например, для метода аутентификации «oidc_deckhouse» в окне просмотра информации о методе отображается одна вкладка «Configuration» и кнопка «Configure» (Рисунок 15).

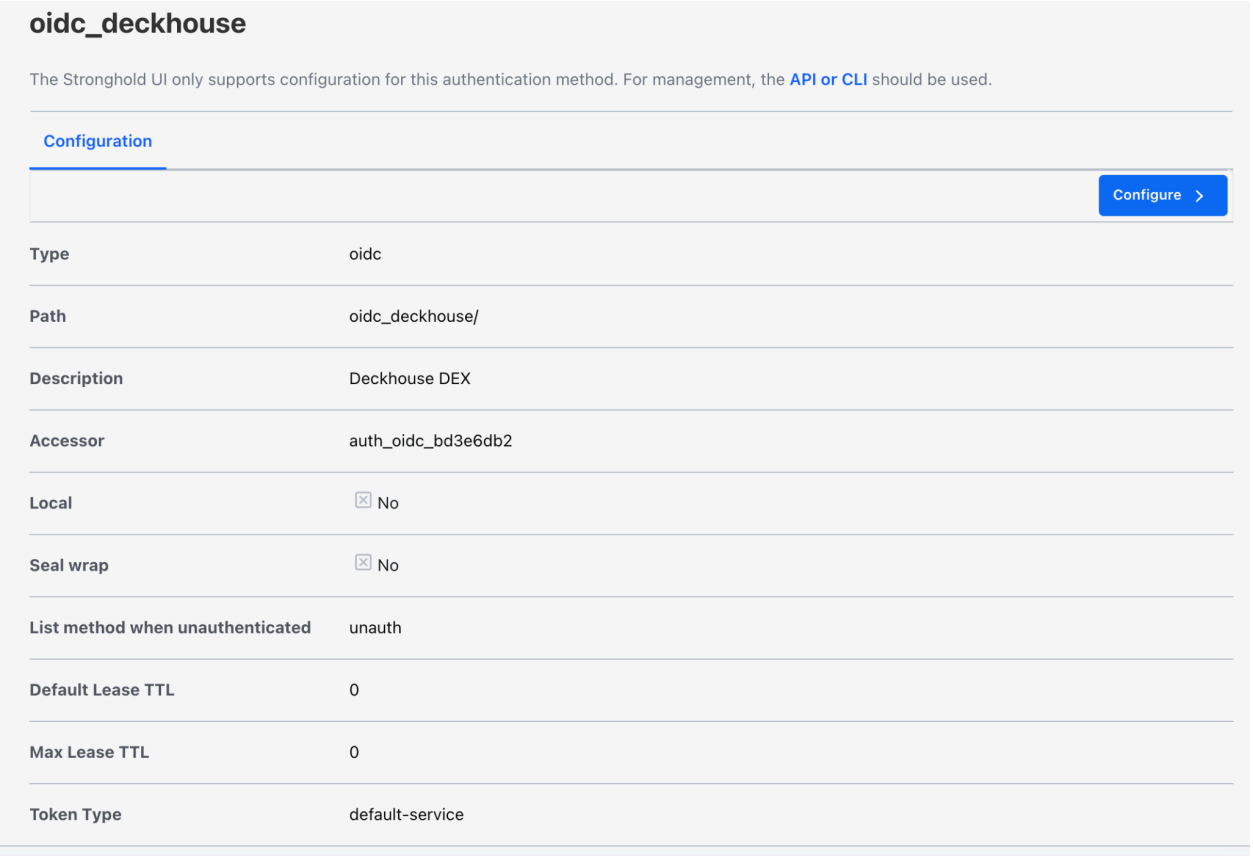

Рисунок 15. Просмотр информации о методе аутентификации

5.2.1.2. Добавление метода аутентификации

Добавить метод аутентификации можно, нажав кнопку для добавления метода в окне для работы с методами аутентификации (п. 5.2.1). Пример представлен на (Рисунок 16).

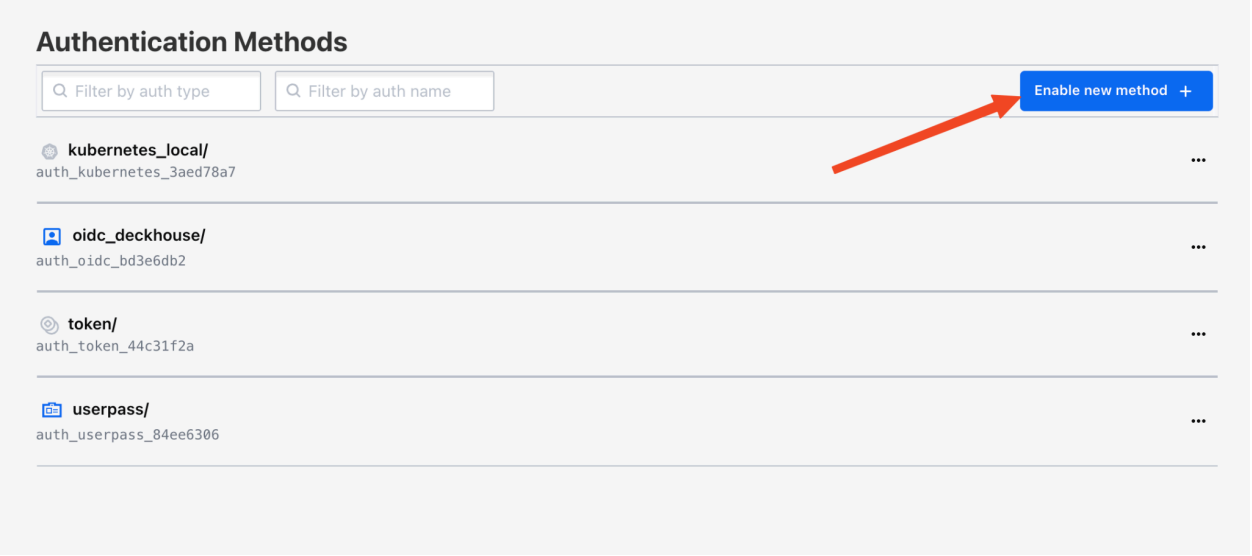

Рисунок 16. Добавление метода аутентификации

После этого откроется экран выбора добавляемого метода аутентификации. На нем необходимо выбрать нужный метод и нажать на кнопку «Next» (Рисунок 17).

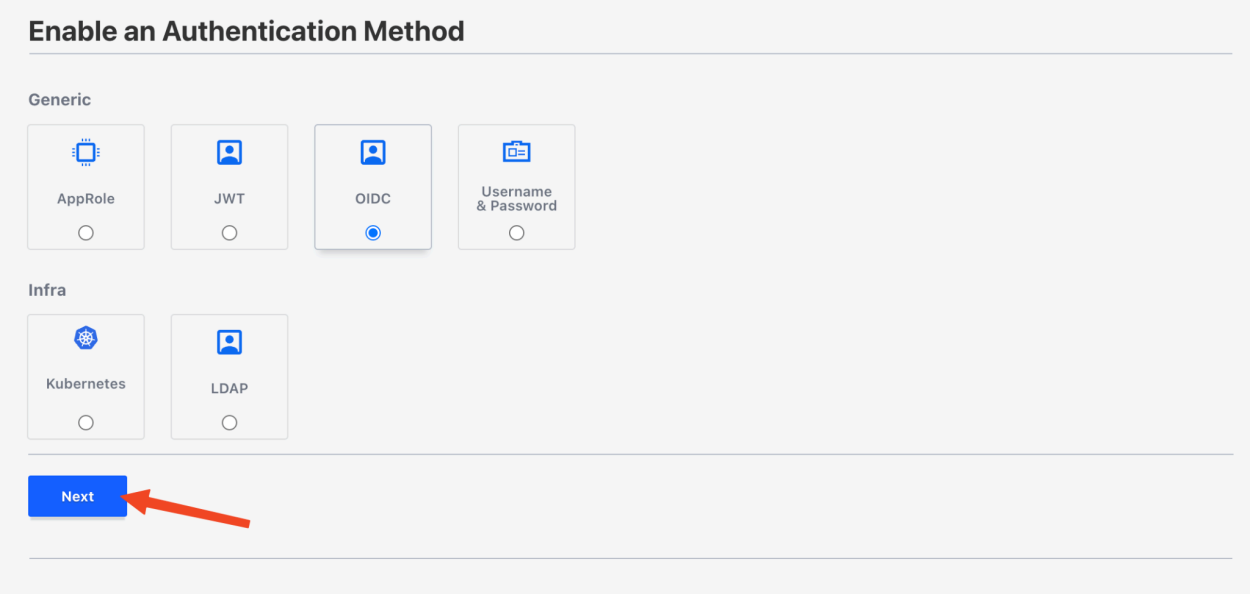

Рисунок 17. Выбор добавляемого метода аутентификации

После этого откроется окно с настройками добавляемого метода аутентификации. Оно состоит из двух блоков: поле «Path» и опции («Method options» — по умолчанию блок свернут, чтобы открыть его, нужно кликнуть по его названию). Внизу окна находятся кнопки «Enable Method» (для сохранения метода после его настройки) и «Back» (для возврата без сохранения на экран выбора метода аутентификации).

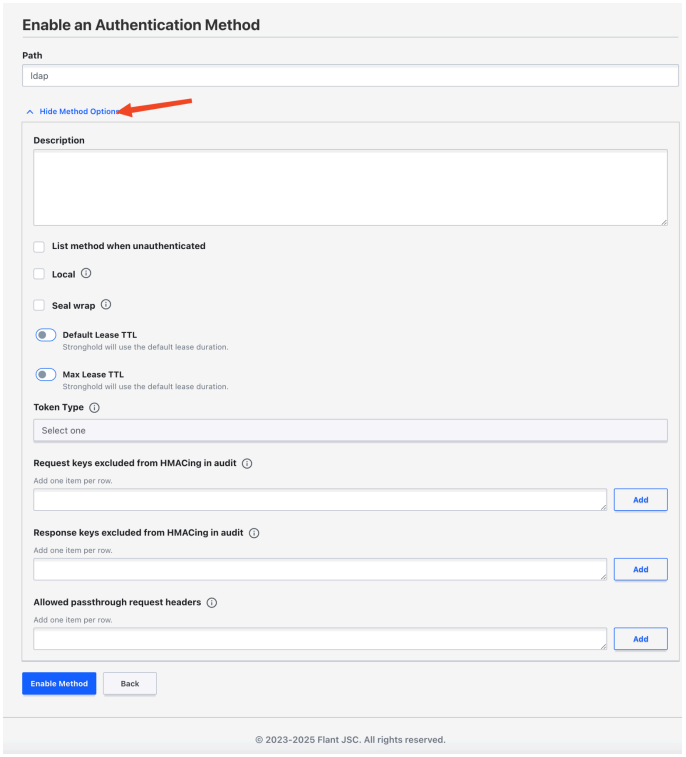

Рисунок 18. Настройки добавляемого метода аутентификации

5.2.2. Работа с группами пользователей

Для перехода в подраздел необходимо нажать на вкладку «Groups» в меню слева.

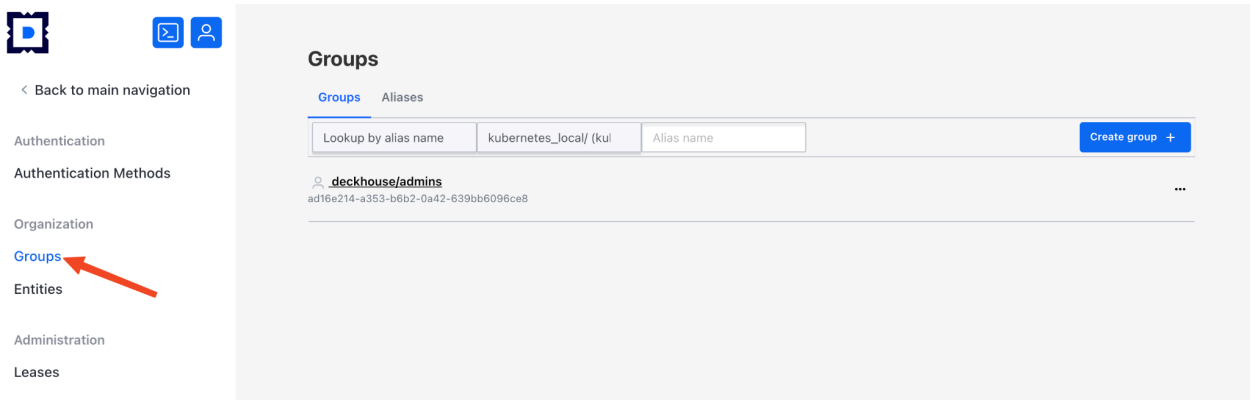

Рисунок 19. Работа с группами пользователей

В центре экрана находится список групп пользователей, имеющихся в кластере, поля для фильтрации элементов списка и кнопка для добавления новой группы.

Для групп из списка доступны следующие действия:

- просмотр детальной информации о группе;
- изменение настроек группы;

– удаление группы.

Выбрать нужное действие можно, нажав кнопку с тремя точками, которая находится в конце строки с названием группы.

Рисунок 20. Список групп пользователей

5.2.2.1. Просмотр информации о группе пользователей

Информацию о группе пользователей можно посмотреть, нажав на ее название или выбрав пункт «Details» (доступен в выпадающем меню при нажатии кнопки с тремя точками, которая находится в конце строки с названием группы). В окне с информацией о группе отображаются вкладки с разными видами информации и кнопка для редактирования группы.

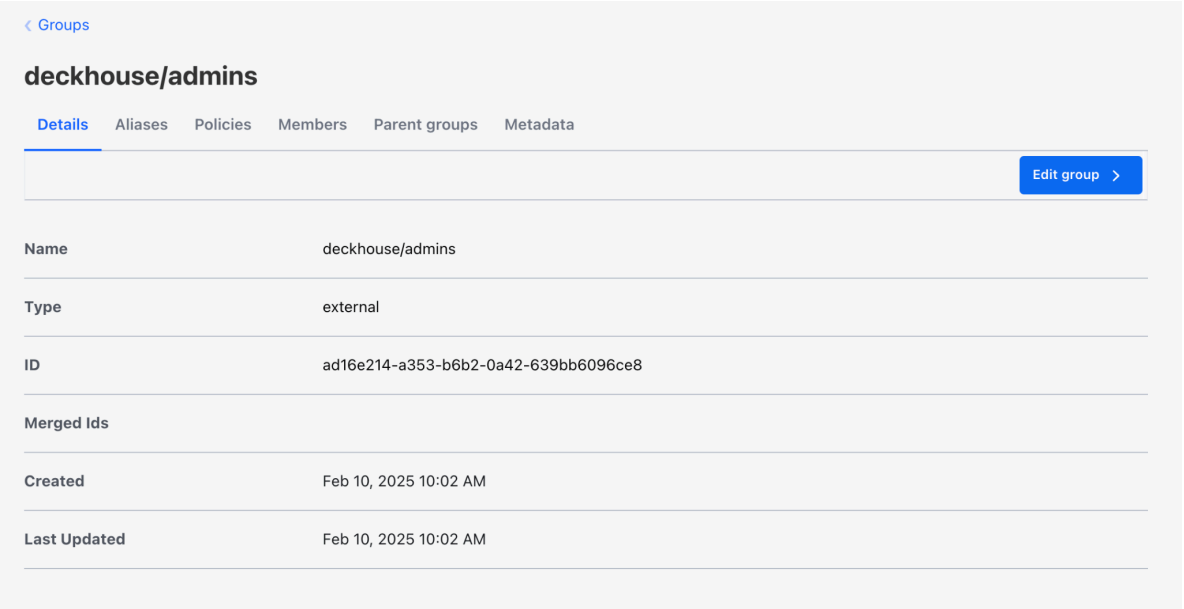

Рисунок 21. Просмотр информации о группе пользователей

5.2.2.2. Добавление группы пользователей

Добавить группу пользователя можно, нажав кнопку добавления группы («Create group») в окне для работы с группами.

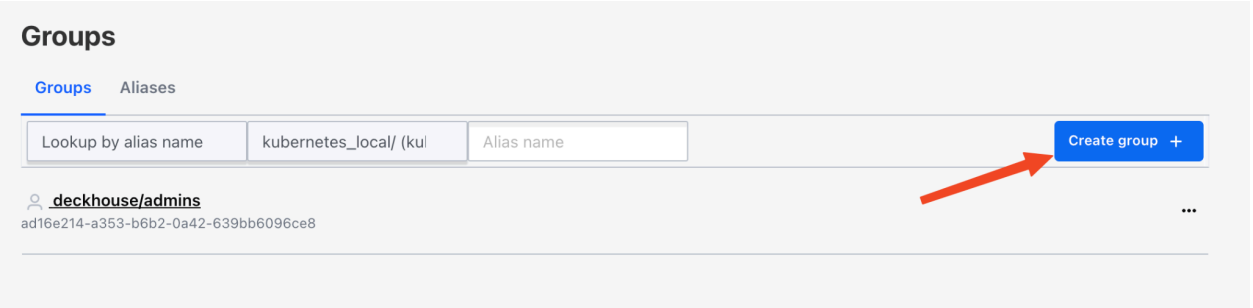

Рисунок 22. Добавление группы пользователей

После этого откроется форма создания группы. Под формой находятся кнопки «Create» (для сохранения группы) и «Cancel» (для возврата без сохранения на экран со списком групп).

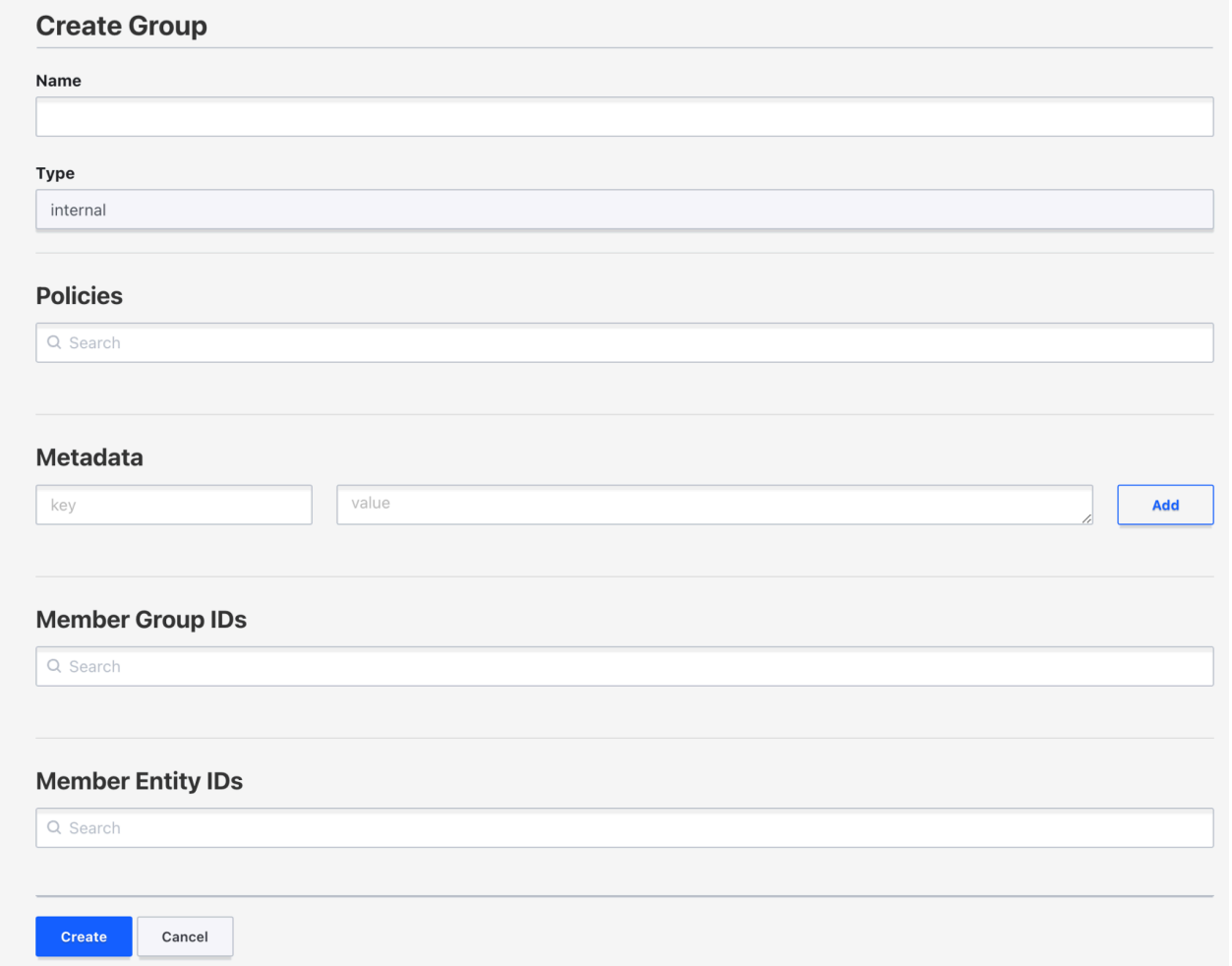

Рисунок 23. Форма создания группы пользователей

5.2.3. Работа с сущностями и алиасами

Сущности (Entities) в ПО «Deckhouse Stronghold» представляют собой абстракцию пользователя или приложения, объединяющие несколько методов аутентификации под одним логическим идентификатором.

Для перехода в подраздел для работы с сущностями и алиасами необходимо нажать на пункт «Entities» в меню слева раздела для работы с доступами (п. 5.1.2).

В центре экрана находится две вкладки: «Entities» (список сущностей) и «Aliases» (список алиасов), поля для фильтрации элементов списка, кнопка объединения сущностей и кнопка добавления новой сущности.

Для сущностей из списка на вкладке «Entities» доступны следующие действия:

- просмотр детальной информации о сущности;
- создание алиаса.

Выбрать нужное действие можно, нажав на кнопку с тремя точками, которая находится в конце строки с названием сущности.

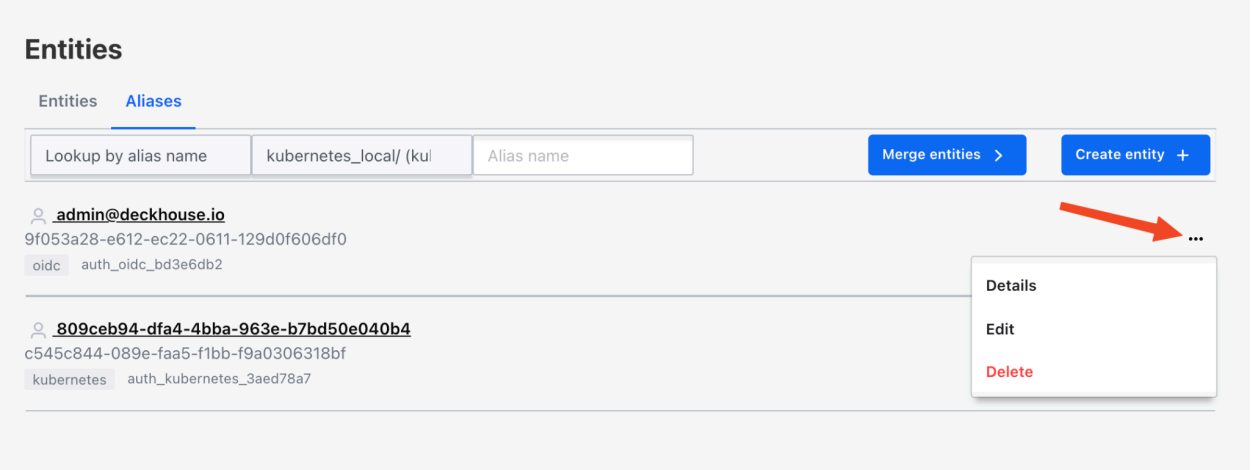

Рисунок 24. Работа с сущностями и алиасами

Для алиасов из списка на вкладке «Aliases» доступны следующие действия:

- просмотр детальной информации об алиасе;
- редактирование алиаса;
- удаление алиаса.

Выбрать нужное действие можно, нажав на кнопку с тремя точками, которая находится в конце строки с названием алиаса.

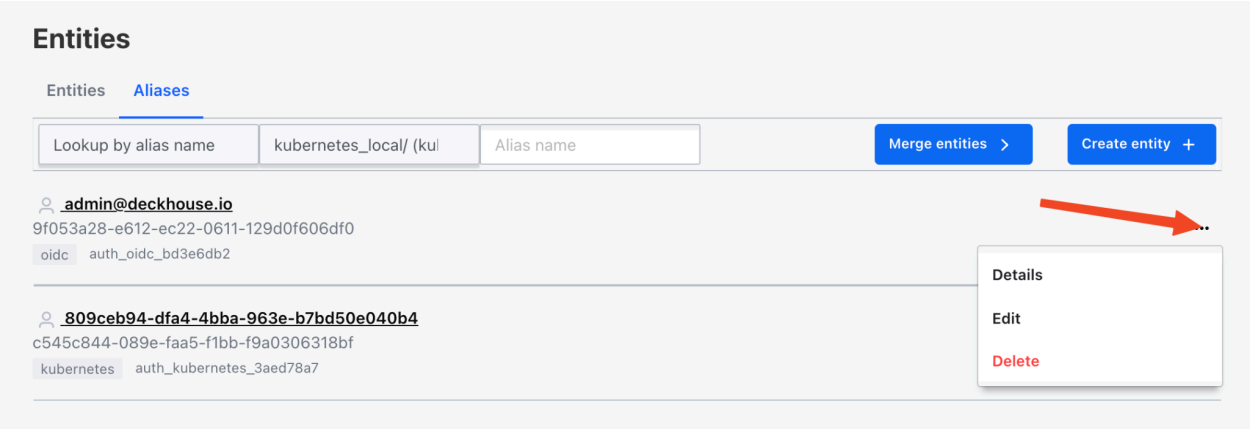

Рисунок 25. Вкладка «Aliases»

5.2.3.1. Просмотр информации о сущности

Информацию о сущности можно посмотреть, нажав на ее название в списке на вкладке «Entities» окна работы с сущностями (п. 5.2.3) или выбрав пункт «Details» (доступен в выпадающем меню при нажатии кнопки с тремя точками, которая находится в конце строки с названием сущности). В окне с информацией о сущности отображаются вкладки с разными видами информации, кнопка добавления сущности и кнопка редактирования сущности.

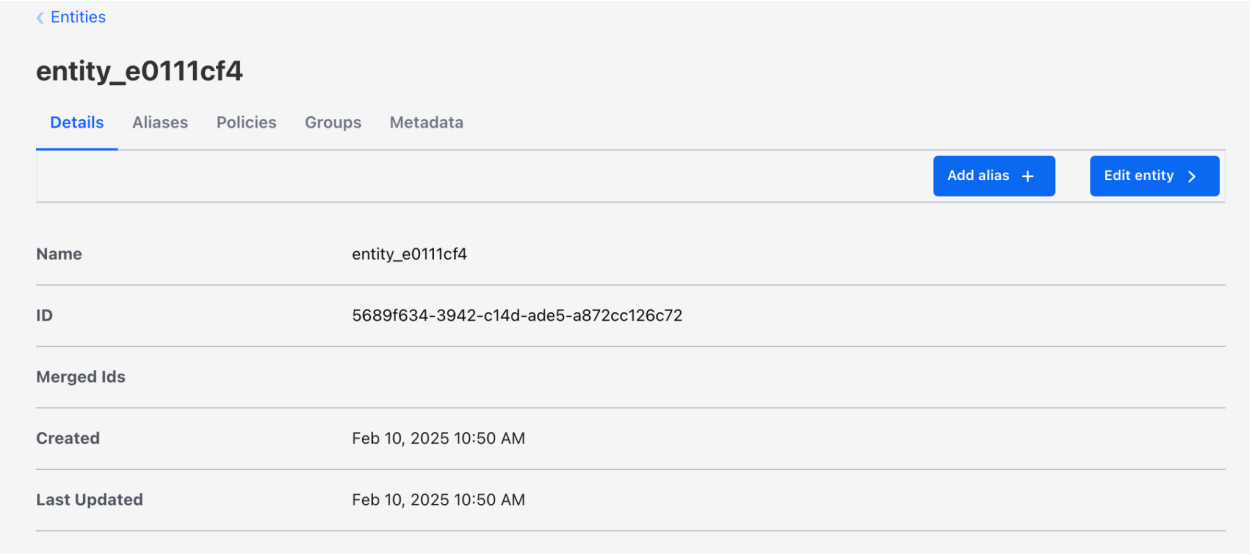

Рисунок 26. Просмотр информации о сущности

5.2.3.2. Просмотр информации об алиасе

Информацию об алиасе можно посмотреть, нажав на его название в списке на вкладке «Aliases» окна работы с сущностями (п. 5.2.3) или выбрав пункт «Details» (доступен в выпадающем меню при нажатии кнопки с тремя точками, которая находится в конце строки с

названием алиаса). В окне с информацией об алиасе отображаются вкладки с общей информацией, метаданными и кнопка редактирования алиаса.

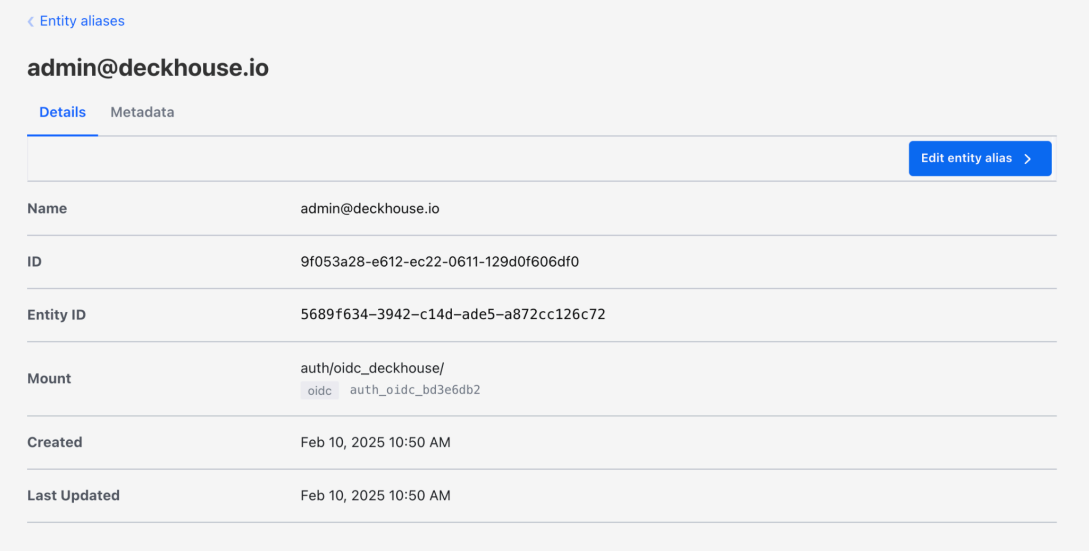

Рисунок 27. Просмотр информации об алиасе

5.2.3.3. Создание сущности

Создать сущность можно, нажав кнопку добавления сущности («Create entity») в окне для работы с сущностями и алиасами (п. 5.2.3). Пример представлен на Рисунке 28.

Рисунок 28. Создание сущности

После этого откроется форма создания сущности. Под формой находятся кнопки «Create» — для сохранения сущности и «Cancel» — для возврата без сохранения на экран со списком сущностей.

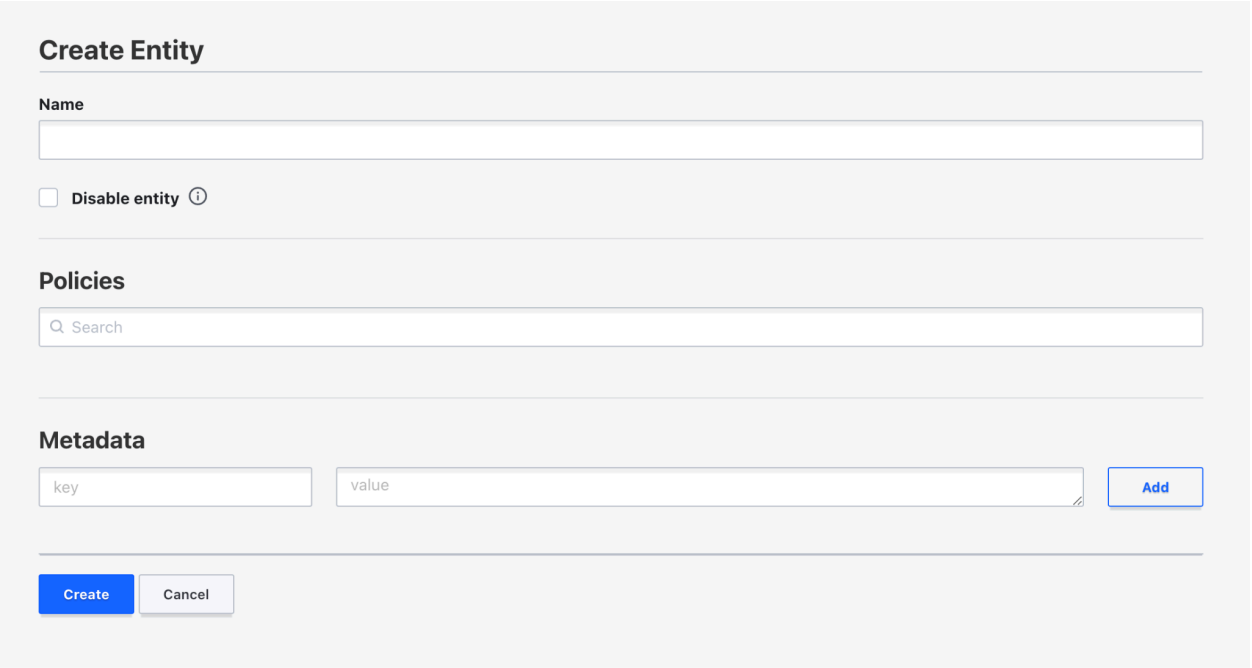

Рисунок 29. Форма создания сущности

5.2.3.4. Создание алиаса

Добавить алиас для сущности можно, нажав кнопку с тремя точками, которая находится в конце строки с названием сущности (в окне работы с сущностями и алиасами (п 5.2.3.2)) и выбрав пункт «Create alias».

После этого откроется форма создания алиаса. Под формой находятся кнопки «Create» — для сохранения алиаса и «Cancel» — для отмены.

Рисунок 30. Создание алиаса

5.2.3.5. Объединение сущностей

Объединить сущности можно, нажав кнопку «Merge entities» в окне для работы с сущностями и алиасами (п. 5.2.5). После этого откроется форма для объединения сущностей.

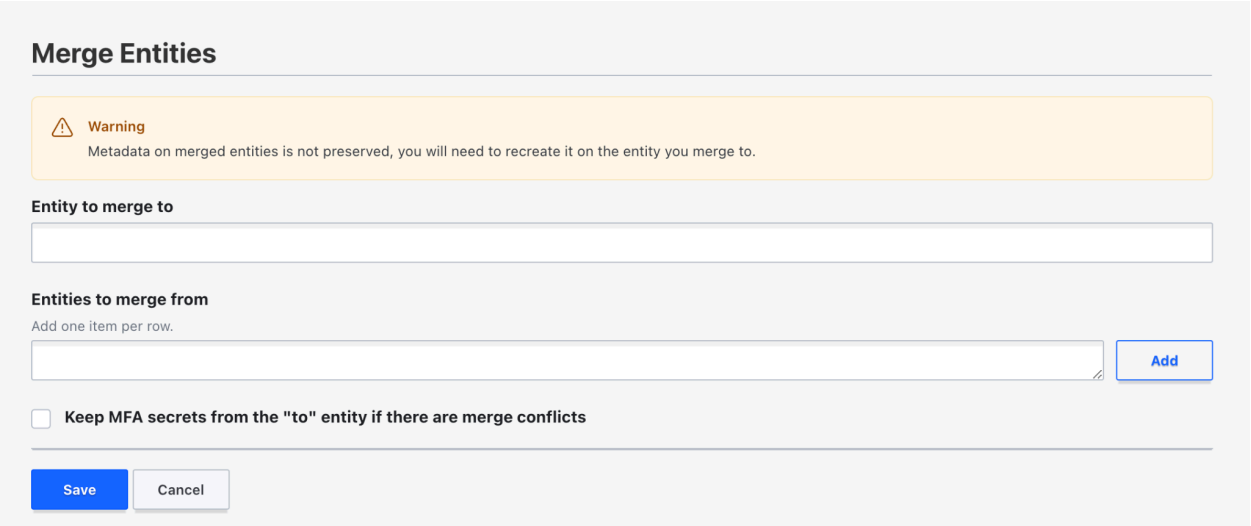

Рисунок 31. Объединение сущностей

5.2.3.6. Управление временными правами доступа к секретам и ресурсам (Leases)

Для перехода в подраздел для управления временными правами доступа к секретам и ресурсам (Leases) необходимо нажать на пункт «Leases» в меню слева в разделе для работы с доступами (п. 5.1.2). Откроется окно поиска информации об аренде по ее идентификатору.

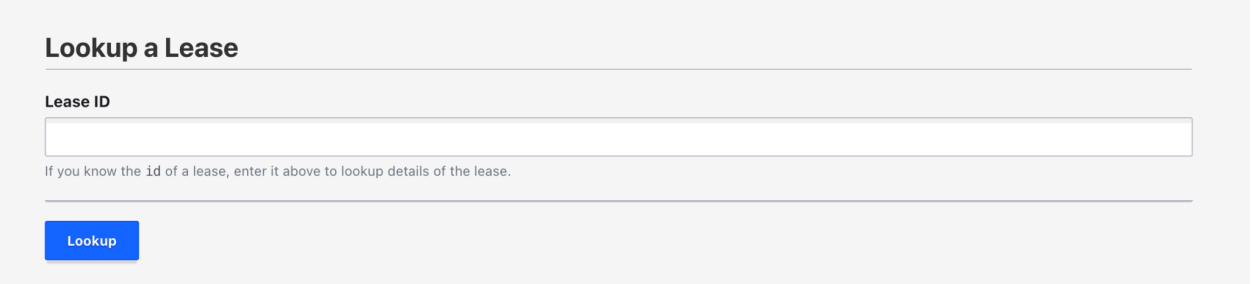

Рисунок 32. Управление временными правами доступа к секретам и ресурсам (Leases)

5.2.4. Работа с политиками контроля доступа

Работа с политиками контроля доступа в ПО «Deckhouse Stronghold» осуществляется в разделе «Policies». Перейти в него можно, нажав на пункт меню «Access» на главном экране веб-интерфейса ПО «Deckhouse Stronghold» (п. 5.1.1). В левой части экрана раздела для работы с политиками находится окно навигации, наверху которого расположена ссылка для быстрого

перехода на главный экран веб-интерфейса ПО «Deckhouse Stronghold». В центре размещены список политик, фильтр для поиска нужной политики и кнопка добавления новой политики.

Для политик из списка доступны следующие действия:

- просмотр детальной информации о политике;
- редактирование политики;
- удаление политики.

Выбрать нужное действие можно, нажав кнопку с тремя точками, которая находится в конце строки с названием политики.

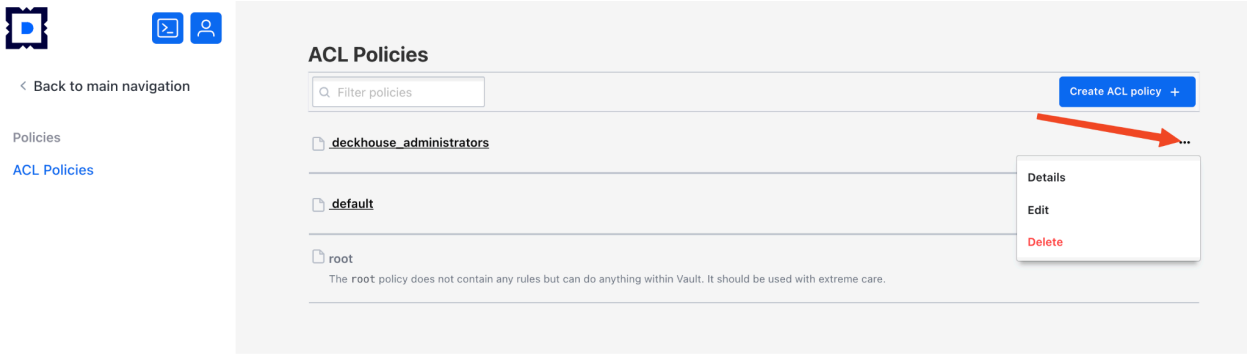

Рисунок 33. Работа с политиками контроля доступа

5.2.4.1. Просмотр информации о политике

Информацию о политике можно посмотреть, нажав на ее название или выбрав пункт «Details» (доступен в выпадающем меню при нажатии кнопки с тремя точками, которая находится в конце строки с названием политики). В окне с информацией о политике отображаются сведения в формате HCL, а также кнопка для загрузки данных на компьютер и кнопка редактирования политики.

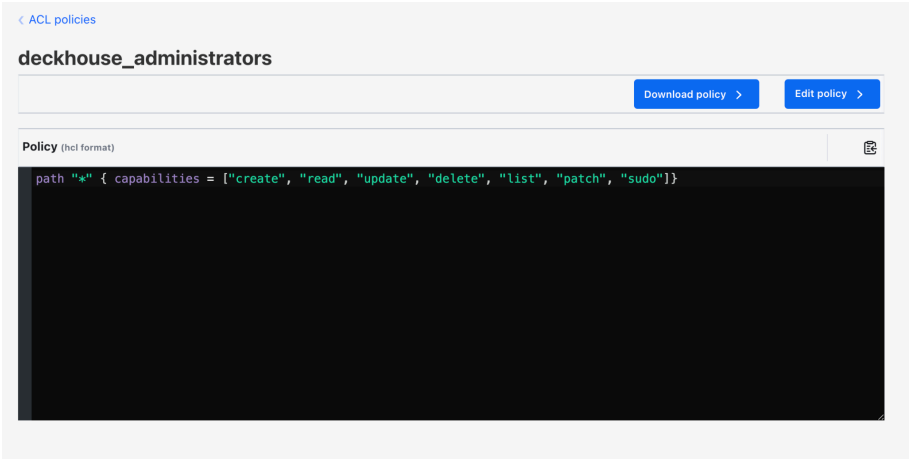

Рисунок 34. Просмотр информации о политике

5.2.4.2. Добавление политики

Чтобы добавить политику, необходимо нажать кнопку «Create ACL policy» на экране для работы с политиками (п. 5.3.3). После этого откроется форма с полями для ввода имени политики и ее описания в формате HCL.

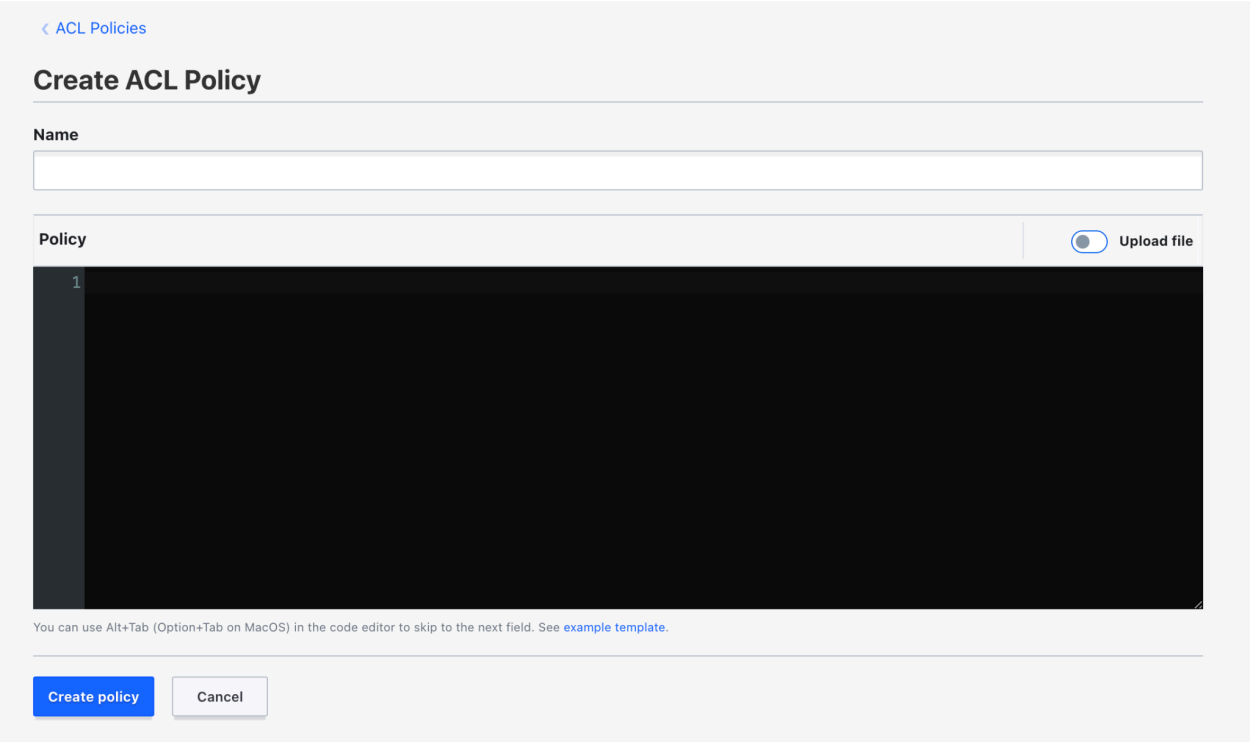

Рисунок 35. Добавление политики

5.3. Работа с дополнительными инструментами

Работа с дополнительными инструментами в ПО «Deckhouse Stronghold» осуществляется в разделе «Tools». Перейти в него можно, нажав на пункт меню «Tools», размещенном на главном экране веб-интерфейса ПО «Deckhouse Stronghold» (п. 5.1.1). В левой части раздела находится окно навигации по инструментам, наверху которого расположена ссылка для быстрого перехода на главный экран веб-интерфейса ПО «Deckhouse Stronghold». В центре отображаются поля выбранного инструмента.

5.3.1. Инструмент «Wrap»

Инструмент «Wrap» предназначен для создания wrapping token (токена обертки) для безопасной передачи секретов, который временно «упаковывает» конфиденциальные данные/секреты. Этот токен может быть передан другому пользователю или приложению, которое затем сможет «развернуть» (unwrap) его и получить доступ к «упакованным» данным.

Для доступа к инструменту нажмите на пункт меню «Wrap» раздела «Tools».

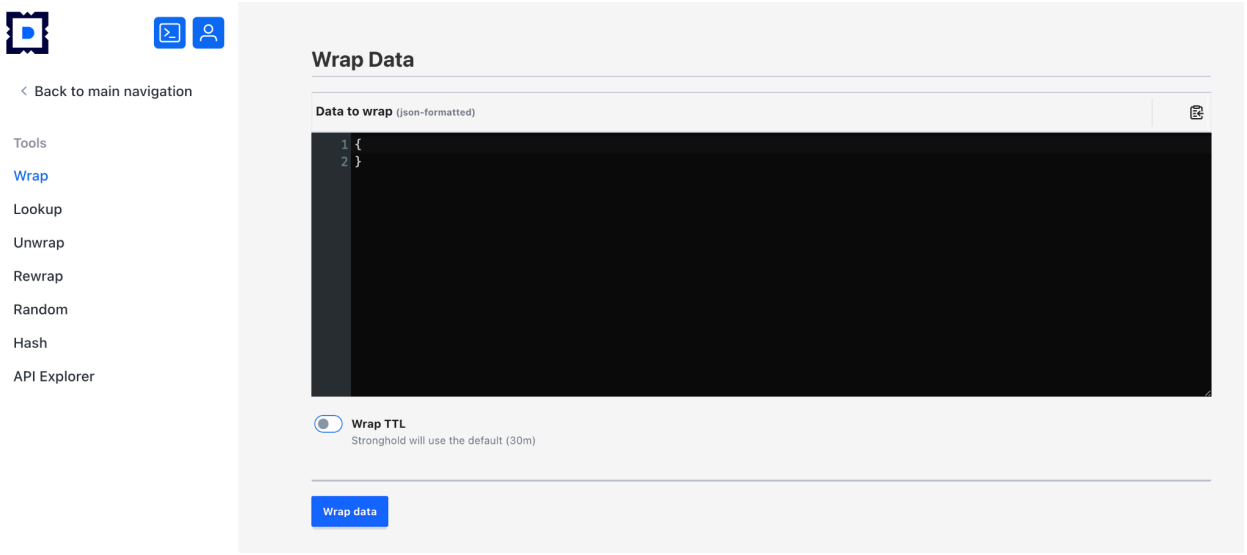

Рисунок 36. Инструмент «Wrap»

5.3.2. Инструмент «Lookup»

Инструмент «Lookup» используется для просмотра информации о токенах, секретах, арендах (Lease) и иных объектах в ПО «Deckhouse Stronghold». С его помощью можно просматривать метаданные, сроки действия, политики доступа и другую информацию, связанную с объектами.

Для доступа к инструменту нажмите на пункт меню «Lookup» раздела «Tools».

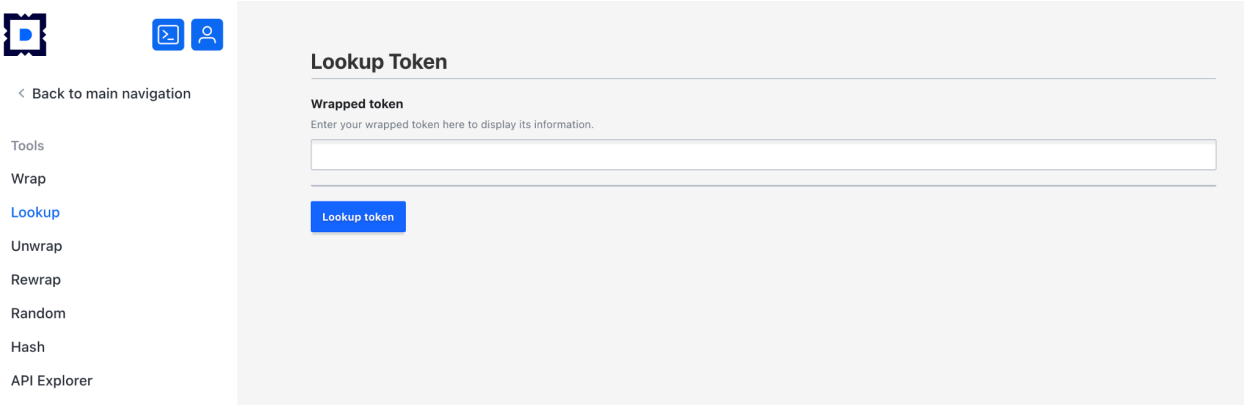

Рисунок 37. Инструмент «Lookup»

5.3.3. Инструмент «Unwrap»

Инструмент «Unwrap» предназначен для распаковки wrapping token (токена обертки) и получения доступа к «упакованным» данным.

Для доступа к инструменту, необходимо нажать на пункт меню «Unwrap» раздела «Tools».

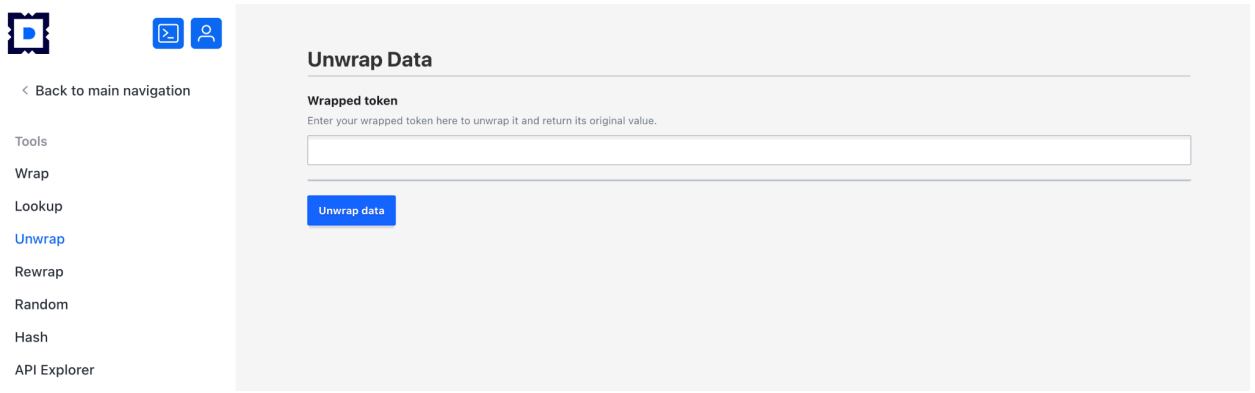

Рисунок 38. Инструмент «Unwrap»

5.3.4. Инструмент «Rewrap»

Инструмент «Rewrap» предназначен для переупаковки — создания нового wrapping token (токена обертки) на основе существующего. Это позволяет продлить срок действия токена или изменить его параметры без необходимости раскрывать защищаемые данные.

Для доступа к инструменту, необходимо нажать на пункт меню «Rewrap» раздела «Tools».

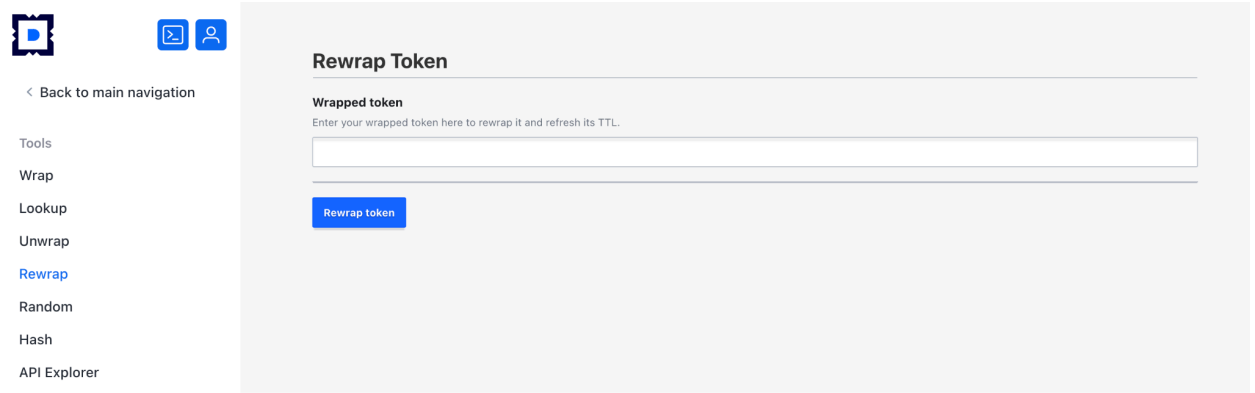

Рисунок 39. Инструмент «Rewrap»

5.3.5. Инструмент «Random»

Инструмент «Random» предназначен для генерации криптографически безопасных случайных данных для создания уникальных идентификаторов, токенов, паролей или иных данных, для которых важна высокая степень случайности и безопасности.

Для доступа к инструменту нажмите на пункт меню «Random» раздела «Tools».

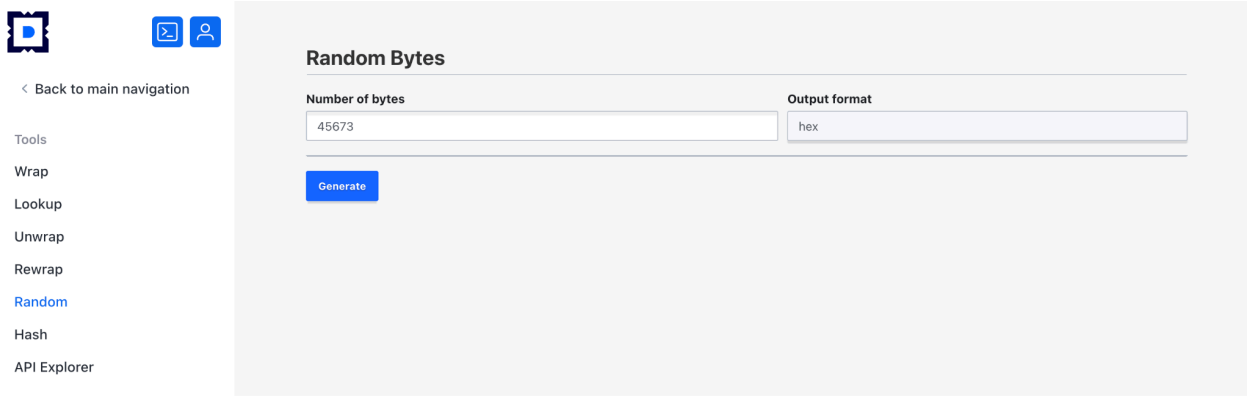

Рисунок 40. Инструмент «Random»

5.3.6. Инструмент «Hash»

Инструмент «Hash» выполняет генерацию хешей для различных данных. Поддерживается несколько алгоритмов кэширования.

Для доступа к инструменту необходимо нажать на пункт меню «Hash» раздела «Tools».

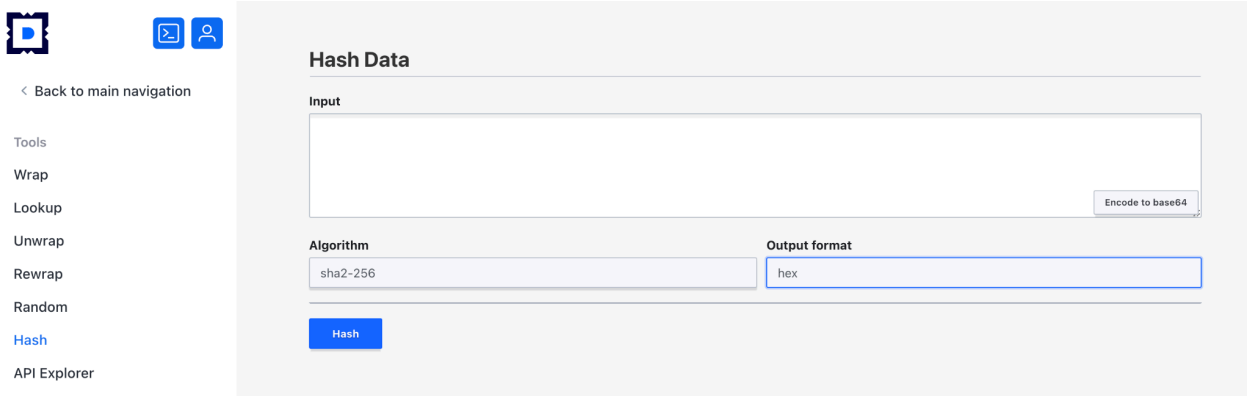

Рисунок 41. Инструмент «Hash»

5.3.7. Инструмент «API Explorer»

Инструмент «API Explorer» предоставляет пользователям удобный способ взаимодействия с API ПО «Deckhouse Stronghold» через графический интерфейс.

Для доступа к инструменту необходимо нажать на пункт меню «API Explorer» раздела «Tools».

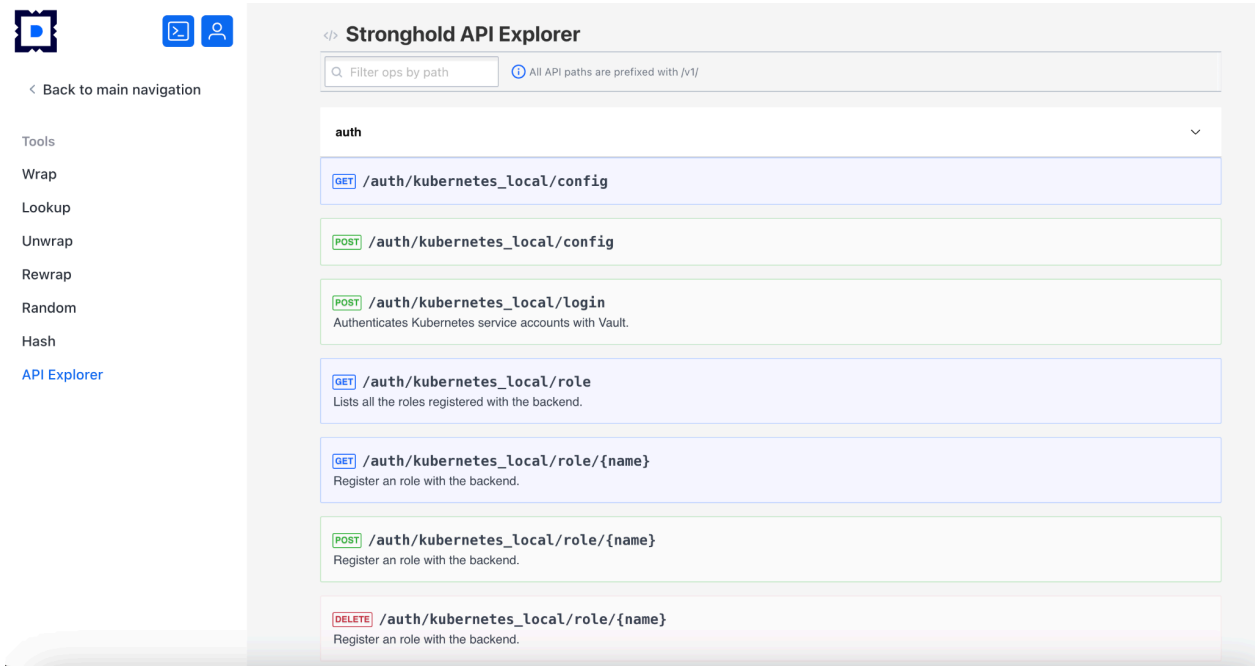

Рисунок 42. Инструмент «API Explorer»

5.4. Мониторинг состояния Raft кластера ПО «Deckhouse Stronghold»

Мониторинг состояния Raft кластера ПО «Deckhouse Stronghold» осуществляется в разделе «Raft Storage». Перейти в него можно, нажав на пункт меню «Raft Storage» на главном экране веб-интерфейса ПО «Deckhouse Stronghold» (п. 5.1.1). В левой части интерфейса находится окно навигации по разделам. В центре отображается информация о лидере и узлах кластера, а также кнопка «Snapshots» для создания резервной копии данных Raft кластера ПО «Deckhouse Stronghold» и восстановления данных из резервной копии.

Рисунок 43. Мониторинг состояния Raft кластера ПО «Deckhouse Stronghold»

5.5. Мониторинг активности и оценка нагрузки ПО «Deckhouse Stronghold»

Мониторинг активности и оценка нагрузки на ПО «Deckhouse Stronghold» осуществляется в разделе «Client Count». Перейти в него можно, нажав на пункт меню «Client Count» на главном экране веб-интерфейса ПО «Deckhouse Stronghold» (п. 5.1.1). В левой части интерфейса находится окно навигации по разделам. В центре размещены две вкладки. Первая — «Dashboard» с информацией о количестве уникальных клиентов за текущий месяц и кнопками выбора периода.

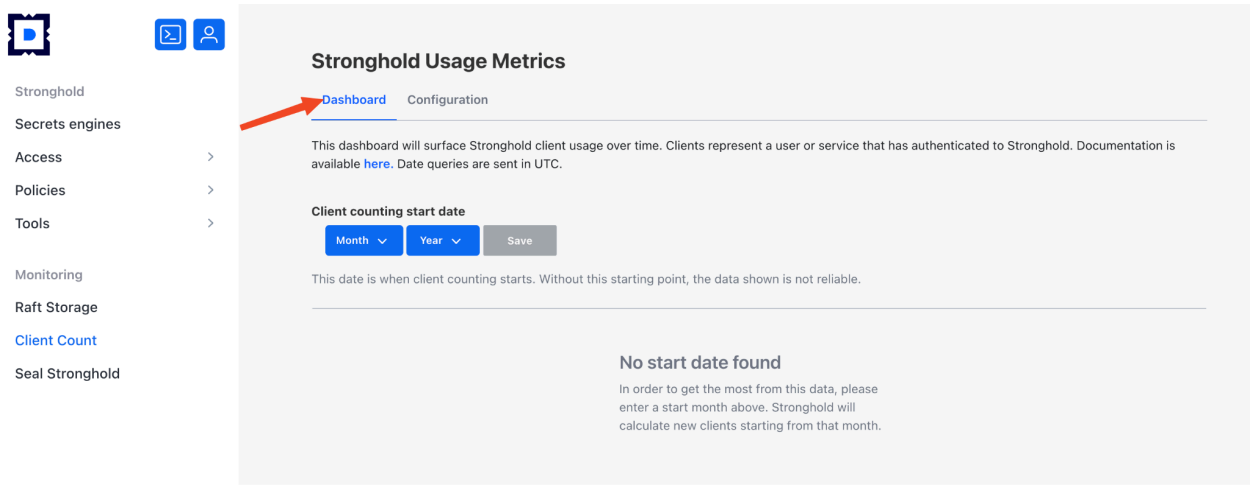

Рисунок 44. Мониторинг активности и оценка нагрузки на ПО «Deckhouse Stronghold»

Вторая вкладка — «Configuration». Здесь можно посмотреть и отредактировать настройки сбора метрик (для этого необходимо нажать кнопку «Edit configuration»).

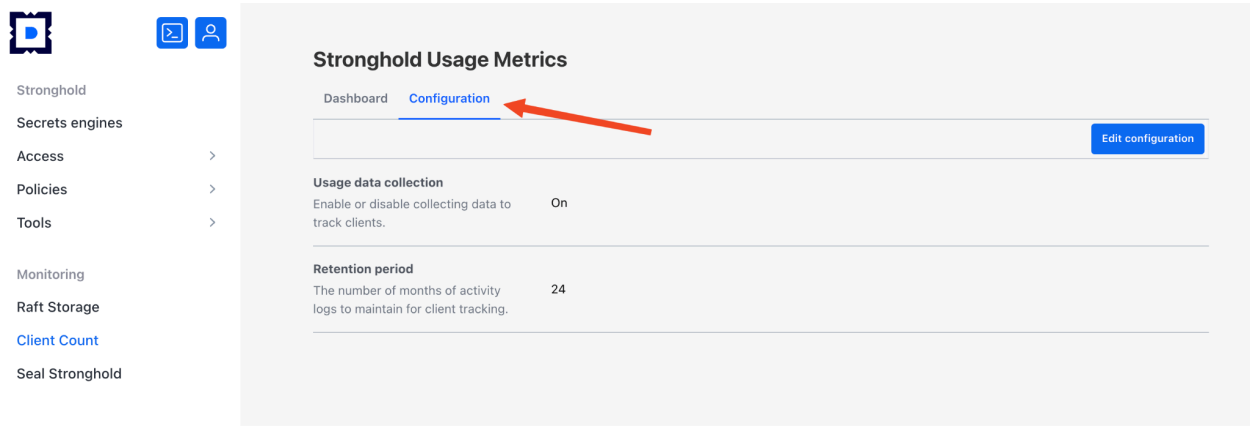

Рисунок 45. Вкладка «Configuration»

5.6. Запечатывание и распечатывание хранилища секретов

Запечатывание и распечатывание хранилища секретов осуществляется в разделе «Seal Stronghold». Перейти в него можно, нажав на пункт меню «Seal Stronghold» на главном экране веб-интерфейса ПО «Deckhouse Stronghold» (п. 5.1.1). В левой части интерфейса находится окно

навигации по разделам. В центре отображается кнопка для запечатывания и распечатывания хранилища секретов (в зависимости от его текущего состояния).

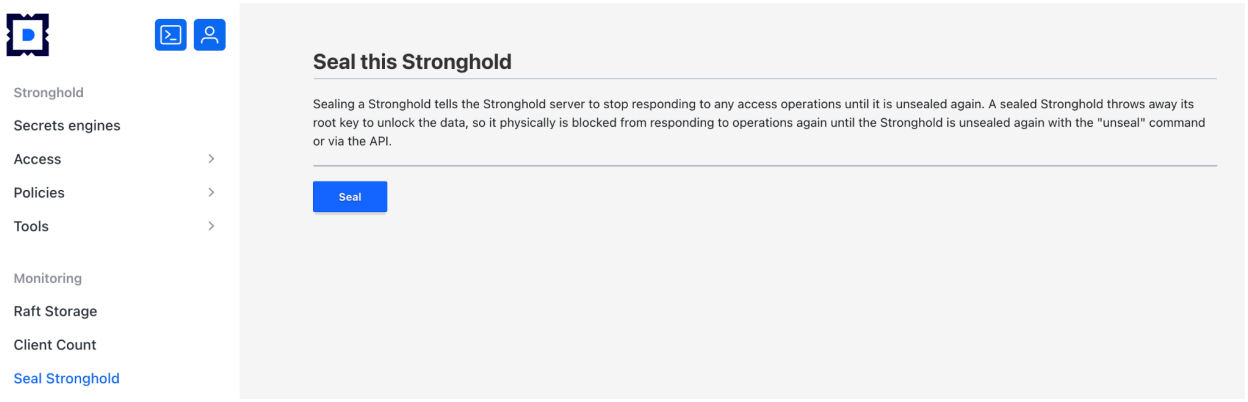

Рисунок 46. Запечатывание и распечатывание хранилища секретов

Когда хранилище находится в состоянии «запечатано» (sealed), оно не может обрабатывать запросы на чтение или запись секретов.

5.7. Работа со Stronghold CLI

Stronghold CLI — инструмент для взаимодействия с ПО «Deckhouse Stronghold», который позволяет выполнять операции по управлению секретами, настройке политик, управлению пользователями и т.д. Вызвать Stronghold CLI можно из любого раздела интерфейса. Для его запуска необходимо нажать кнопку в левом верхнем углу окна.

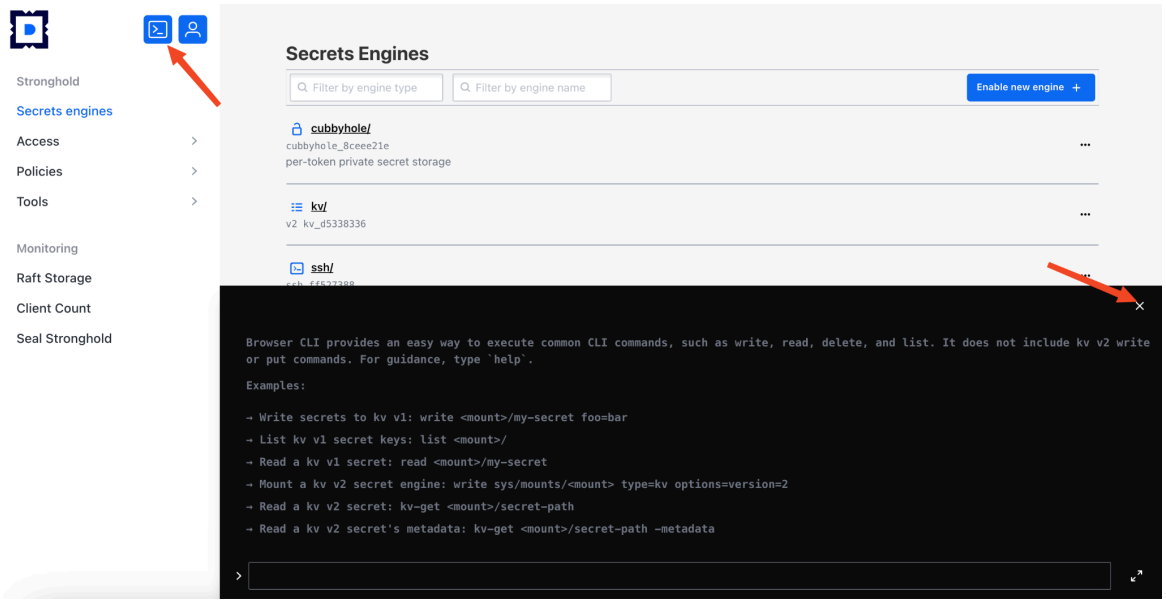

Рисунок 47. Работа со Stronghold CLI

Закрыть Stronghold CLI можно, нажав на крестик в правом верхнем углу окна инструмента.

5.8. Резервное копирование

ПО «Deckhouse Stronghold» позволяет настроить расписание для автоматического создания резервных копий хранилища секретов. Поскольку ПО хранит данные на диске в зашифрованном виде, резервная копия также содержит только зашифрованные данные. Для получения доступа к данным необходимо развернуть резервную копию в кластере ПО и выполнить процедуру распечатывания хранилища.

Резервные копии можно сохранять на локальный диск в выбранную директорию или в S3-совместимое хранилище.

Управлять настройками резервных копий и просматривать их статус можно через API, CLI и веб-интерфейс.

5.8.1. Создание или обновление конфигурации автоматического резервного копирования

Метод	Путь
POST	/sys/storage/raft/snapshot-auto/config/:name

Для работы с данным методом API потребуются права sudo.

5.8.2. Описание параметров

- name (строка) – имя конфигурации, которую необходимо создать или изменить;
- interval (целое число или строка) – интервал между резервными копиями. Может задаваться в секундах или в формате Go duration (например, 24h);
- retain (целое число) – количество резервных копий, которые должны храниться. При превышении этого числа самые старые резервные копии удаляются;
- path_prefix (неизменяемая строка) – если в параметре storage_type выбрано локальное хранилище, здесь указывается директория хранения резервных копий. Если выбрано облачное хранилище, здесь указывается bucket-префикс (начальный / игнорируется, последующие / необязательны);
- file_prefix(неизменяемая строка) – префикс имени файла или объекта резервной копии в пределах директории или bucket, заданного в path_prefix;
- storage_type(неизменяемая строка) – тип хранилища резервных копий: local (локальное) или aws-s3 (облачное). Остальные параметры ниже зависят от выбранного типа хранилища.

5.8.3. Дополнительные параметры для локального хранилища

- local_max_space (Целое число) – максимальный объём (в байтах), доступный для хранения резервных копий с заданным file_prefix в директории path_prefix. При недостатке места создание резервной копии завершится с ошибкой. Значение 0 отключает проверку занимаемого места на диске.

5.8.4. Дополнительные параметры для облачного хранилища

- aws_s3_bucket (строка) – имя S3 bucket для хранения резервных копий;
- aws_s3_region (строка) – регион S3 bucket;
- aws_access_key_id (строка) – идентификатор ключа для доступа к S3 bucket;
- aws_secret_access_key(строка) – секретный ключ для доступа к S3 bucket;
- aws_s3_endpoin(строка) – эндпойнт S3-сервиса;
- aws_s3_disable_tls(булевый) – отключает TLS для S3-эндпойнта. Используется только для тестирования, обычно в сочетании с aws_s3_endpoint;
- aws_s3_ca_certificate (строка) – сертификат CA для S3-эндпойнта в формате PEM.

5.8.5. Примеры запросов

5.8.5.1. Создание конфигурации

Указываются все обязательные поля.

```
d8 stronghold write sys/storage/raft/snapshot-auto/config/s3every5min - <<EOF
{
   "interval":        "5m",
   "path_prefix":      "backups",
   "file_prefix":      "main_stronghold",
   "retain":          "4",
   "storage_type":     "aws-s3",
   "aws_s3_bucket":       "my_bucket",
   "aws_s3_endpoint":      "minio.domain.ru",
   "aws_access_key_id":    "oWdPcQ50zTuMjJI",
   "aws_secret_access_key": "4NzZjboafWyfNTe7aUVgLUdrMurHjty43iUXHFBw"
}
EOF
```

Пример ответа:

```
Key    Value
---    -----
msg    successfully created config
```

5.8.5.2. Обновление конфигурации

Допускается указывать не все поля. Уже существующие поля не будут изменены.

```
d8 stronghold write sys/storage/raft/snapshot-auto/config/s3every5min - <<EOF
{
  "interval":       "3m",
  "retain":         "10",
  "aws_access_key_id":    "vnR9Rfp0toPPgK3",
  "aws_secret_access_key": "FuloGN1RZCtwINCLJtwHXTQ50zCL7s"
}
EOF
```

Пример ответа:

```
Key    Value
---    -----
msg    successfully updated config
```

5.8.6. Просмотр списка существующих конфигураций

Метод	Путь
LIST	`/sys/storage/raft/snapshot-auto/config`

Возвращает список всех существующих конфигураций автоматического резервного копирования.

5.8.7. Пример запроса

```
d8 stronghold list sys/storage/raft/snapshot-auto/config
```

Пример ответа:

```
Keys
----
s3every5min
localEvery3min
```

5.8.8. Получение параметров конфигурации

Метод	Путь
GET	/sys/storage/raft/snapshot-auto/config/:name

Возвращает значения всех параметров указанной конфигурации.

5.8.9. Пример запроса

```
d8 stronghold read sys/storage/raft/snapshot-auto/config/s3every5min
```

Пример ответа:

```
Key                 Value
---                 -----
interval            300
path_prefix         backups
file_prefix         main_stronghold
retain              4
storage_type        aws-s3
aws_s3_bucket       my_bucket
aws_s3_disable_tls  false
aws_s3_endpoint     minio.domain.ru
aws_s3_region       n/a
aws_s3_ca_certificate  n/a
```

5.8.10. Удаление конфигурации

Метод	Путь
DELETE	`/sys/storage/raft/snapshot-auto/config/:name`

Удаляет указанную конфигурацию и возвращает информацию о последней созданной резервной копии.

5.8.10.1. Пример запроса

```
d8 stronghold delete
sys/storage/raft/snapshot-auto/config/s3every5min
```

Пример ответа:

```
Key                 Value
---                 -----
consecutive_errors  0
last_snapshot_end   2025-01-31T15:24:14Z
last_snapshot_error  n/a
last_snapshot_start  2025-01-31T15:24:12Z
last_snapshot_url   https://minio.domain.ru/my_bucket/backups/main_stronghold_2025-01-31T15:24:12Z
next_snapshot_start  2025-01-31T15:29:12Z
snapshot_start      2025-01-31T15:24:12Z
snapshot_url        https://minio.domain.ru/my_bucket/backups/main_stronghold_2025-01-31T15:24:12Z
```

5.8.11. Получение статуса резервной копии

Метод	Путь
GET	/sys/storage/raft/snapshot-auto/status/:name

Возвращает информацию о текущем статусе указанной резервной копии.

5.8.11.1. Пример запроса

```
d8 stronghold read sys/storage/raft/snapshot-auto/status/s3every5min
```

Пример ответа:

```
Key    Value
---    -----
msg    successfully deleted config
```

6. Принципы безопасной работы средства

При эксплуатации ПО «Deckhouse Stronghold» должно быть обеспечено выполнение следующих условий:

- наличие администраторов безопасности, обеспечивающих правильную эксплуатацию ПО «Deckhouse Stronghold», в том числе:
  - предотвращение несанкционированного доступа к идентификаторам и паролям привилегированных пользователей (администраторов и пользователей с административными правами);
  - предотвращение реализации некорректных методов управления доступом, типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа;
  - обеспечение физической сохранности оборудования, на которое установлено изделие, и исключение возможности доступа к ним посторонних лиц;
- периодический контроль целостности изделия;
- ежедневная проверка рабочих мест администратором безопасности на наличие вредоносного ПО;
- ежемесячный поиск актуальных уязвимостей и сведений об уязвимостях изделия и среды функционирования, анализ идентифицированных уязвимостей на предмет возможности их использования для нарушения безопасности.

В ПО «Deckhouse Stronghold» реализованы следующие функции безопасности:

- идентификация и аутентификация пользователей (ИАФ);
- управление доступом субъектов доступа к объектам доступа (УПД);
- регистрация событий безопасности (РСБ);
- обеспечение доступности информации (ОДТ).

7. Типы событий безопасности, связанные с доступными пользователю функциями средства

В ПО «Deckhouse Stronghold» регистрируются следующие события безопасности, связанные с доступными пользователю функциями ПО «Deckhouse Stronghold»:

- использование идентификационного и аутентификационного механизма;
- запрос на доступ к защищаемому ресурсу;
- создание, изменение и уничтожение объекта и субъекта;
- действия по изменению правил разграничения доступа.

8. Аварийные ситуации

8.1. Действия после сбоев и ошибок эксплуатации ПО «Deckhouse Stronghold»

В случае несоблюдения условий выполнения технологического процесса, в том числе при возникновении сбоев и ошибок эксплуатации ПО «Deckhouse Stronghold», необходимо обратиться к техническому персоналу и представителям эксплуатирующих подразделений.

8.2. Несанкционированное вмешательство в данные

В случаях обнаружения несанкционированного вмешательства в данные необходимо обратиться к техническому персоналу и представителям эксплуатирующих подразделений.

Лист регистрации изменений

Номер изменения	Номера страниц				Всего страниц в документе	Наименование и номер документа, вводящего изменения	Подпись, Ф.И.О. внесшего изменения в данный экземпляр	Дата внесения изменения в данный экземпляр	Дата введения изменения
	измененных	замененных	новых	аннулированных					