Deckhouse
ФЛАНТ

2025

Не просто форк

Сравнение Deckhouse Stronghold
с HashiCorp Vault Community Edition

Содержание

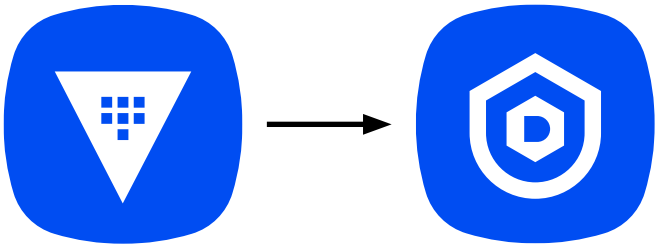
Введение

В мире управления секретами HashiCorp Vault стал своего рода «золотым стандартом», заслужив признание как надёжное решение для защиты конфиденциальных данных. Однако в России Vault доступен исключительно в редакции Community Edition (CE) и лицензирован по проприетарной лицензии BSL (Business Source License), что значительно ограничивает условия его использования.

В то же время российский рынок предлагает новые альтернативы, а некоторые российские решения не просто копируют функционал Vault CE, но и превосходят его, предлагая уникальные функции. Один из таких продуктов — хранилище секретов Deckhouse Stronghold. В этом документе рассмотрены его функциональные и продуктовые преимущества в сравнении с HashiCorp Vault Community Edition.

«Под капотом» Deckhouse Stronghold

Deckhouse Stronghold — это решение для централизованного управления жизненным циклом секретов. В его основе — форк HashiCorp Vault CE версии 1.14.8, последнего коммита под лицензией MPL (Mozilla Public License). Такая лицензия позволяет использовать копию репозитория при создании собственного коммерческого продукта.



HashiCorp Vault 1.14.8 **Deckhouse Stronghold**

За время разработки команда Deckhouse Stronghold значительно расширила функциональность исходного продукта, добавив много полезных возможностей.

> **Мы не просто скопировали Vault, мы переосмысливаем то, каким должно быть идеальное хранилище секретов для российского бизнеса.**

Deckhouse Stronghold Enterprise Edition vs HashiCorp Vault Community Edition

Ниже представлены основные функциональные различия и сходства Deckhouse Stronghold Enterprise Edition и HashiCorp Vault в версиях Enterprise Edition и Community Edition, а также отечественных аналогов Vault.

Сравнение с конкурентами	Stronghold EE	Vault EE	Vault CE	Аналог Vault 1	Аналог Vault 2
Пространства имён (namespaces)	✓	✓	✗	✗	✓
Межкластерная репликация данных	✓	✓	✗	✗	✗
Автоматическое резервное копирование данных по заданному расписанию	✓	✓	✗	✗	✗
Поддержка внешних HSM для двойного шифрования данных	✓	✓	✗	✗	✗
Безопасный auto unseal без использования внешних KMS	✓	✗	✗	✗	✗
Управление AppRole, OIDC/JWT Role в UI	✓	✗	✗	✗	✗
Встроенная безопасная доставка секретов в приложения	✓	✗	✗	✗	✗
Сертификация ФСТЭК России	✓	✗	✗	✗	✓

✓ Появится в 2025 году.

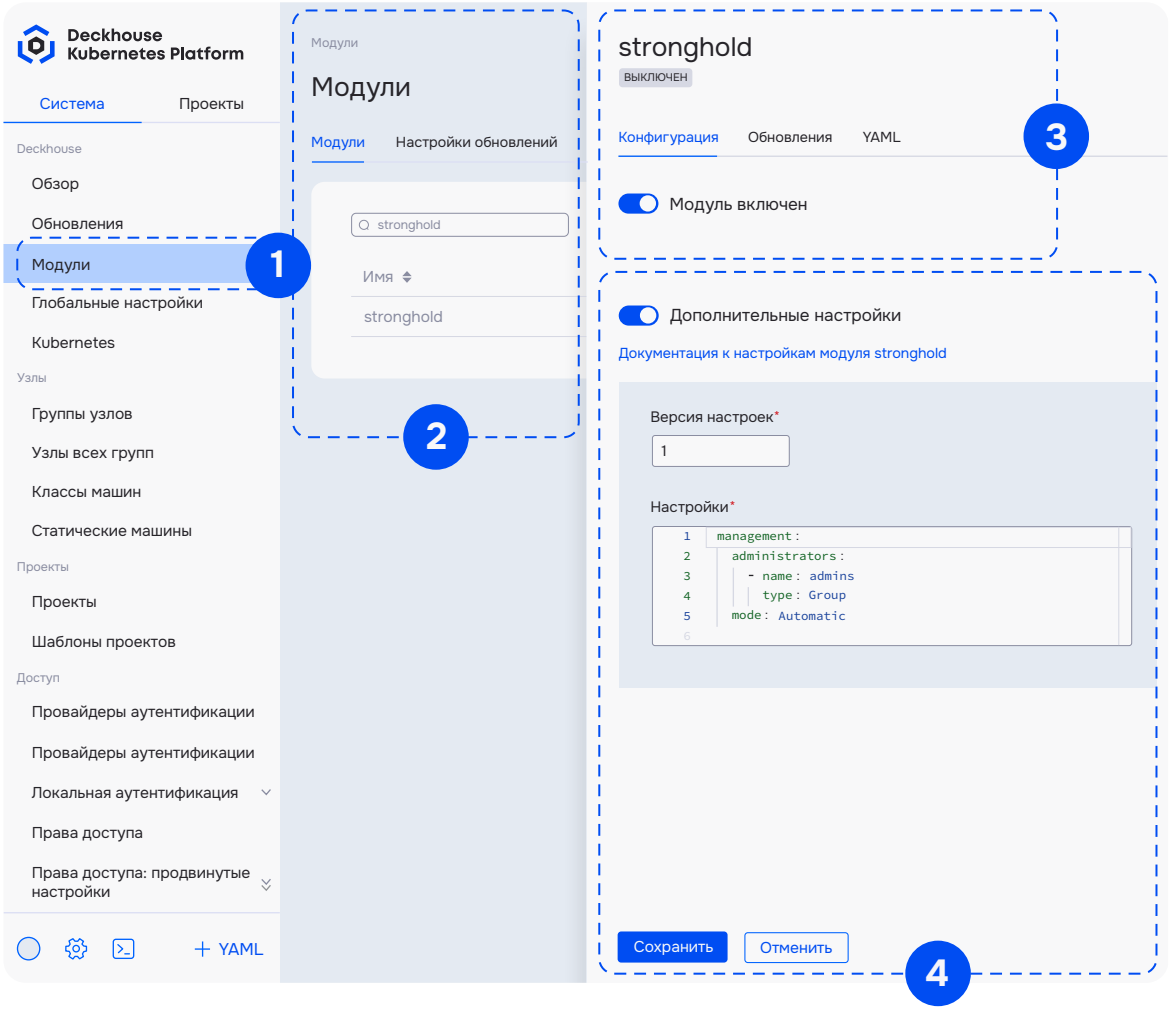
В российских компаниях для управления жизненным циклом секретов наиболее широко применялась и применяется по сей день Community-версия Vault, поэтому ниже мы рассмотрим уникальные функции Deckhouse Stronghold, которых нет в Vault CE или которые работают иначе.

Подробнее о том, как эти возможности реализованы в Deckhouse Stronghold и как их можно частично реализовать в Vault CE, мы рассказали в нашей технической статье на «Хабре».

Открыть статью

Автоматическое развёртывание

Благодаря интеграции Deckhouse Stronghold с Deckhouse Kubernetes Platform (DKP) установка и настройка хранилища выполняются одной кнопкой в веб-интерфейсе или одной строчкой при работе через CLI.



Выполнив несколько простых действий, пользователь получает уже настроенное хранилище секретов со всеми необходимыми функциями, включая балансировку входящего трафика, отказоустойчивую работу, мониторинг, генерацию конфигурации, сертификатов, сетевых настроек, а также auto-discovery сервисов.

Простая установка продукта уменьшает нагрузку на ИТ-специалистов. Это позволяет ИТ-отделам сосредоточиться на развитии и улучшении других компонентов системы.

Автоматическое пересоздание узлов

Одна из ключевых функций, обеспечивающих высокую доступность приложений в Deckhouse Stronghold, — автоматическое пересоздание узлов, или так называемый селф-хилинг (self-healing).

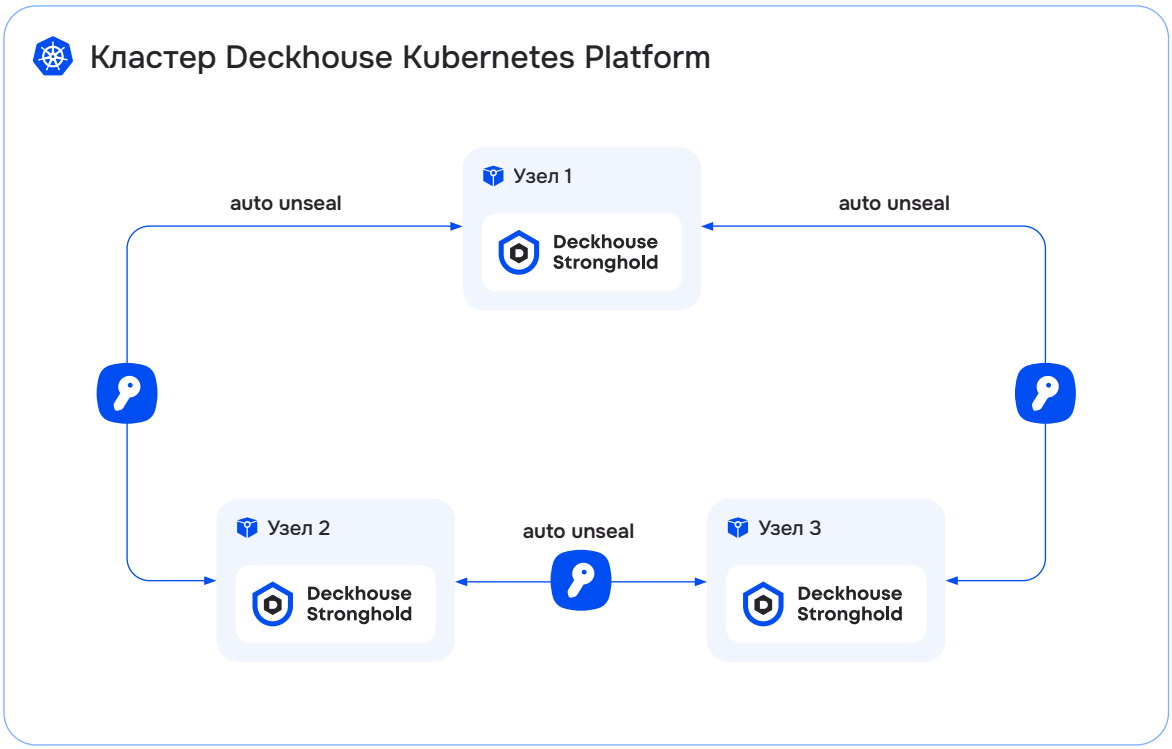
В Deckhouse Stronghold есть автоматизированные системы мониторинга, которые постоянно отслеживают состояние приложений и узлов, на которых они работают. Если наблюдаются отклонения от нормальной работы (например, контейнер не отвечает или потребляет сверх нормы), система запускает процессы восстановления.

Селф-хилинг помогает минимизировать время простоя — это особенно важно для поддержания приложений в рабочем состоянии с максимальной доступностью.

Автоматическое распечатывание (auto unseal)

Ещё одним компонентом high availability в Deckhouse Stronghold является функция автоматического распечатывания хранилища. Изучив наиболее популярные подходы, в том числе применяемые в Vault CE, мы реализовали свой собственный способ распечатывания хранилища.

Его принцип действия заключается в том, что любой активный узел в кластере обнаруживает и автоматически распечатывает остальные узлы при условии, что у них валидный сертификат. Такой способ позволяет обновлять компоненты без ручного вмешательства пользователя, а также автоматически восстанавливать кластеры при перезапуске узлов. При этом ключ для распечатывания хранилища находится только в памяти Deckhouse Stronghold, что обеспечивает его максимальную безопасность.



Подробнее о том, как реализован auto unseal в Deckhouse Stronghold, вы можете прочитать в нашем блоге.

Открыть статью

Автоматическое обновление версий

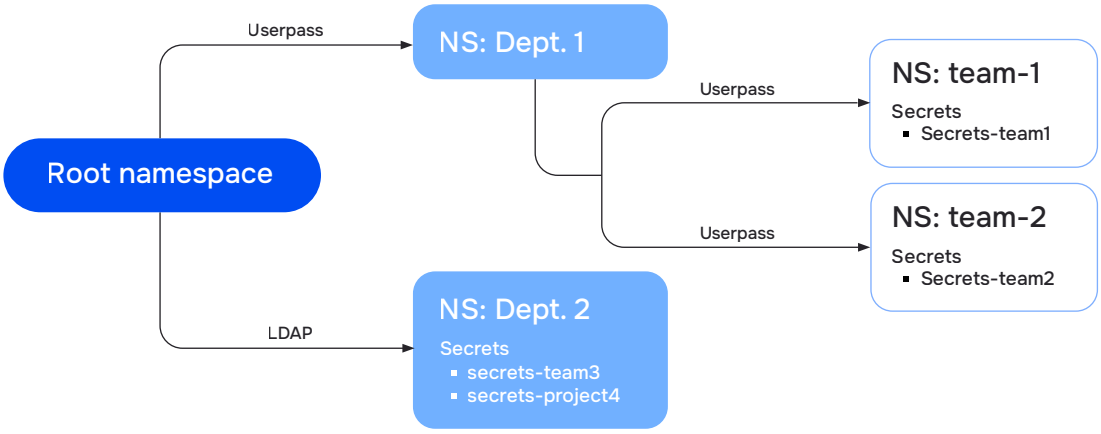
Обычно, чтобы иметь возможность обновлять Vault CE, пользователю прежде всего необходимо развернуть Vault в отказоустойчивой конфигурации из нескольких узлов. Перед кластером, в котором развёрнут Vault, требуется настроить балансировщик. В момент обновления нужно последовательно вывести узлы из балансировки, выключить сервис и обновить бинарный файл Vault, а затем — после обновления — запустить сервис и провести распечатывание каждого узла Vault.

В нашем случае всё гораздо проще. DKP поддерживает автоматическое обновление версий, в том числе и обновление Deckhouse Stronghold, поэтому пользователю не нужно выполнять множество ручных операций по обновлению версии продукта.

Однако если в компании есть, например, внутренние требования ИБ, которые не разрешают автоматические обновления, то их можно перевести в ручной режим.

Пространства имён (namespaces)

В Deckhouse Stronghold реализована функция namespaces, обеспечивающая максимальную совместимость с HashiCorp Vault Enterprise по возможностям и методам API. Это позволяет создавать дочерние рабочие пространства, выдавать права на управление ими, а также поддерживать вложенность и создавать иерархии.



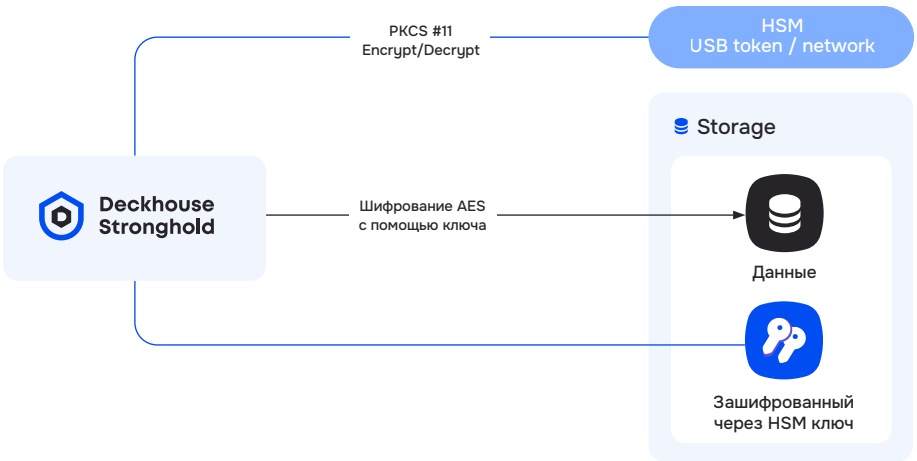
Благодаря этой функции можно использовать одну инсталляцию Deckhouse Stronghold для работы нескольких изолированных и независимых сред. Кроме того, пользователи могут изолировать секреты в пространстве имён одного тенанта, а также гибко настраивать политики контроля доступа, при которых администратор каждого тенанта имеет определённые права, независимые от администраторов других тенантов.

Поддержка аппаратных модулей безопасности (HSM)

В Deckhouse Stronghold реализована интеграция с HSM, поддерживающими PKCS #11. HSM обеспечивает дополнительную защиту секретов и может применяться в Deckhouse Stronghold в двух сценариях: шифрование root-ключа и двойное шифрование данных (seal wrap).

Шифрование root-ключа

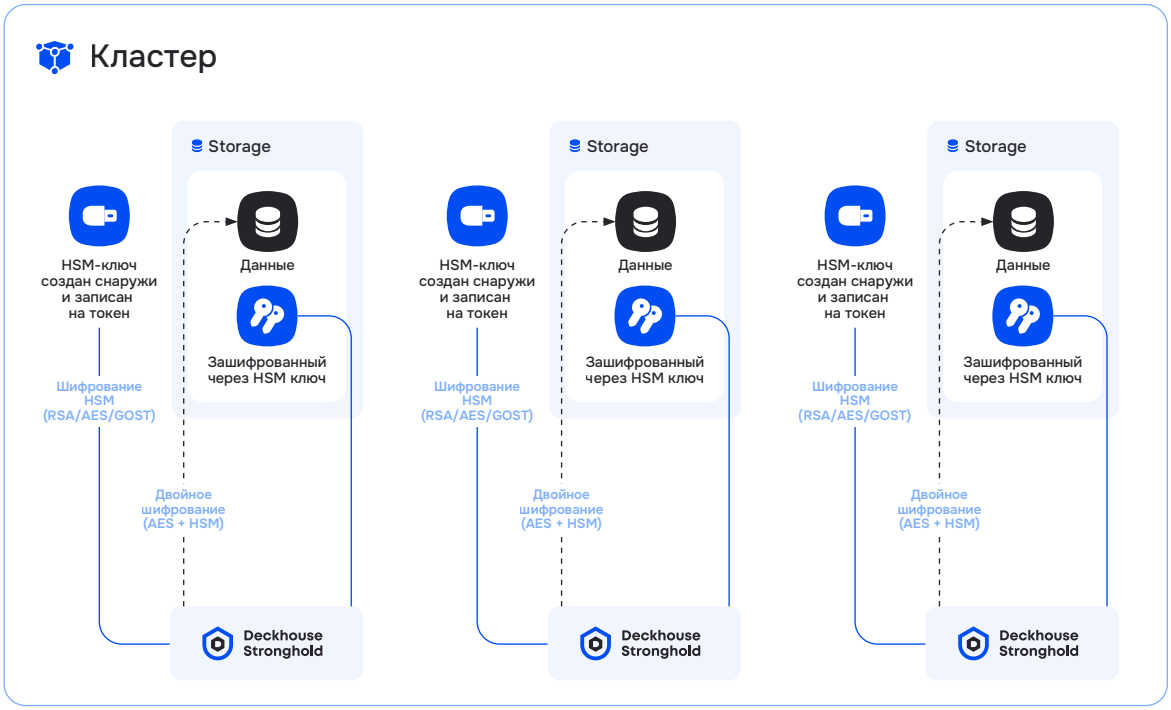
HSM позволяет обеспечить усиленную защиту root-ключа, который используется Deckhouse Stronghold при работе с данными. Он размещается в Storage в зашифрованном виде и расшифровывается при запуске системы через HSM, что обеспечивает дополнительный уровень безопасности.



Двойное шифрование данных

Помимо встроенного в Deckhouse Stronghold шифрования секретов с использованием AES, для особо чувствительных данных может применяться дополнительная криптозащита с помощью HSM.

Deckhouse Stronghold и HSM обеспечивают двойное шифрование методом seal wrap, основанным на различных комбинациях криптографических алгоритмов: AES + RSA, AES + AES и AES + ГОСТ. Такой подход существенно усиливает безопасность секретов: даже в случае компрометации одного из алгоритмов — AES в Deckhouse Stronghold или AES/RSA/ГОСТ в HSM — второй продолжает обеспечивать надёжную защиту данных.

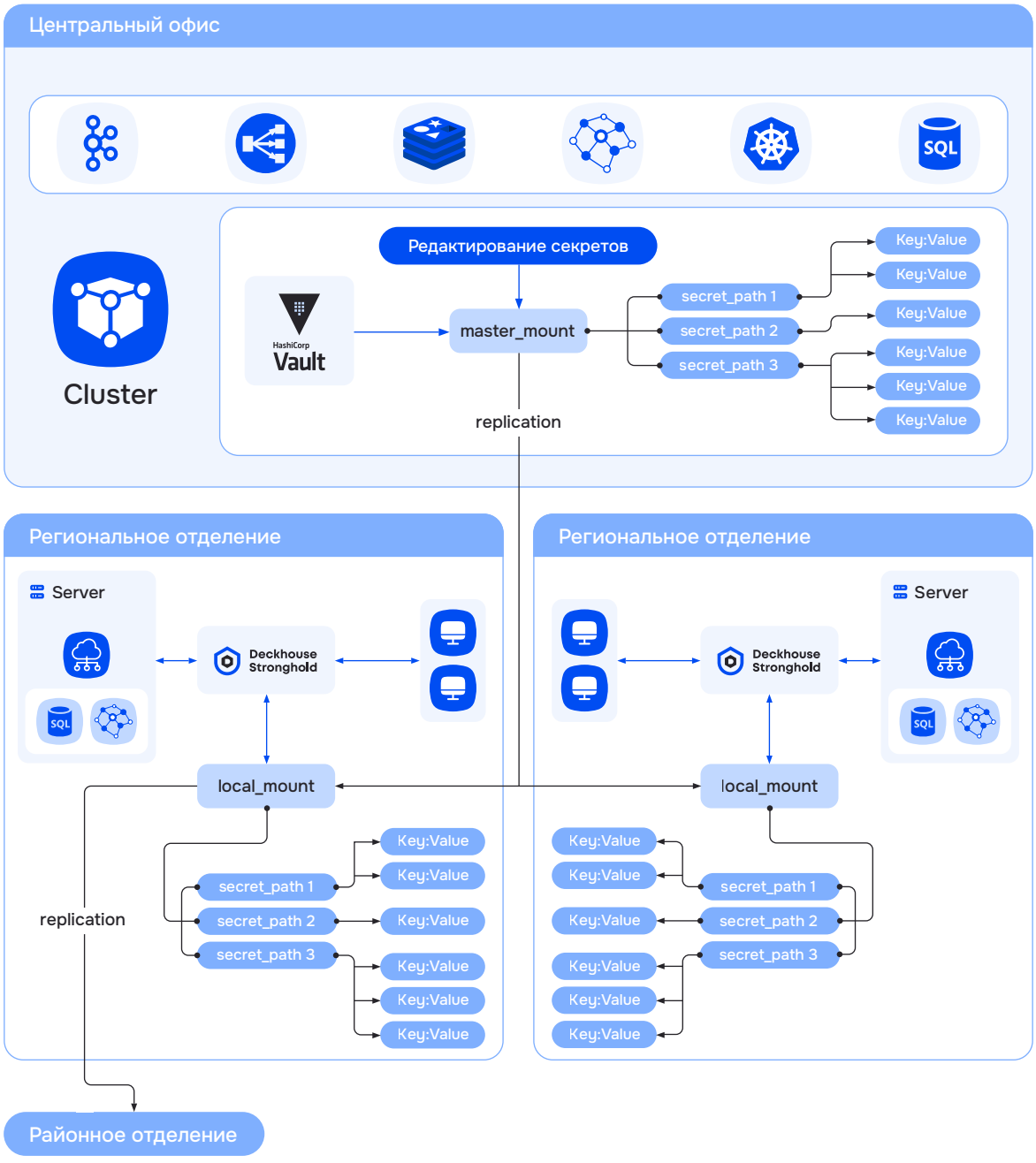


Двойное шифрование, включая использование российских криптографических алгоритмов «Кузнечик» и «Магма» (ГОСТ Р 34.12-2018), особенно важно для защиты данных в критической информационной инфраструктуре (КИИ), государственных информационных системах (ГИС) и информационных системах персональных данных (ИСПДн).

Репликация данных

> **Ещё одна важная фича — это возможность реплицировать хранилища секретов типа KV1/KV2.**

Репликация построена на архитектуре master-slave с применением pull-модели получения данных: подчинённые slave-узлы сами опрашивают master-узел.



Параметры репликации задаются дополнительными настройками при монтировании нового KV-хранилища. После завершения настройки локальное хранилище автоматически переводится в режим «только чтение». Это гарантирует, что все изменения проводятся только в исходном хранилище, а на подчинённые узлы они поступят при очередной синхронизации. Режим «только чтение» отключается вместе с отключением репликации в настройках хранилища секретов.

> **Подробнее о том, как устроен механизм репликации в Deckhouse Stronghold, а также о тонкостях и сложностях его разработки вы можете прочитать в нашей статье на «Хабре».**
>
> **Открыть статью**

Репликация хранилищ секретов позволяет удобно и более безопасно управлять секретами в больших компаниях с георасределённой структурой. Этот механизм повышает уровень устойчивости и доступности данных, минимизируя риски и повышая эффективность управления корпоративными секретами.

Интеграция с системами аутентификации DKP

Как и Vault CE, Deckhouse Stronghold поддерживает большое количество интеграций с системами аутентификации, такими как OIDC, JWT, Cert, LDAP, Kubernetes, AppRole, Userpass. Однако в дополнение к поддерживаемым Vault CE методам аутентификации в нашем продукте возможно использовать кластерный Dex и выдавать доступ внутренним пользователям кластера или, например, пользователям из корпоративного ActiveDirectory.

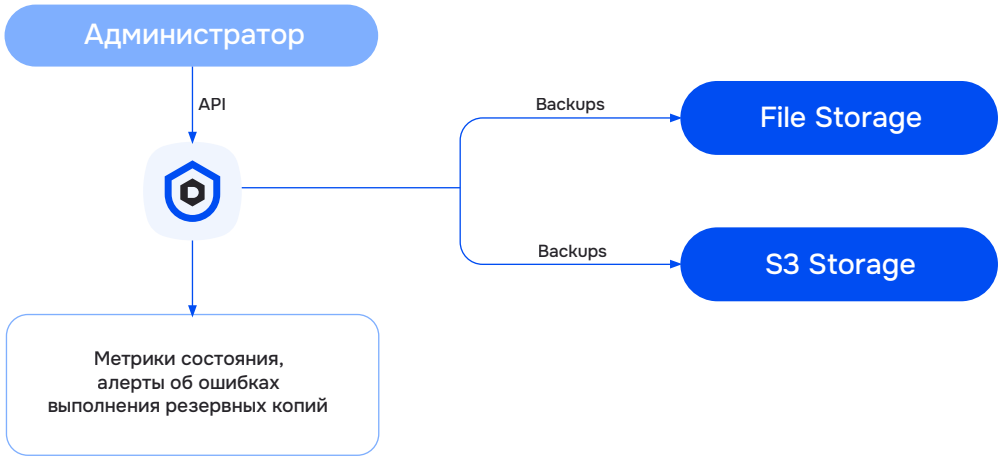
Интеграция с Dex и другими службами аутентификации на корпоративном уровне обеспечивает более централизованное управление доступом, повышает общую безопасность за счёт использования уже установленных и надёжных механизмов аутентификации и контроля доступа.

Резервное копирование данных

Резервные копии выполняются автоматически по настроенному расписанию и могут сохраняться как в файлы, так и в S3-совместимое объектное хранилище.

Чтобы сделать бэкапы в Deckhouse Stronghold, пользователю не нужно генерировать отдельные скрипты для создания снапшотов — все взаимодействия происходят через API, а хранилище секретов самостоятельно создаёт снапшоты согласно заданному расписанию.

При переносе настроек файлы конфигурации сохраняются внутри резервных копий. Поэтому, когда нужно восстановить данные из резервной копии, достаточно просто загрузить снапшот, а в случае полного выхода инфраструктуры из строя — развернуть новую инфраструктуру и восстановить снапшот.



Безопасная доставка секретов в приложения

В Deckhouse Stronghold реализована сквозная интеграция с модулем secrets-store-integration, разработанным для безопасной доставки секретов в приложения, запущенные в кластере Kubernetes. Модуль реализует доставку секретов для приложения в Kubernetes-кластерах путём подключения секретов, ключей и сертификатов, хранящихся во внешних хранилищах секретов. В зависимости от сценариев пользователям доступны два способа доставки секретов в приложение.

Способ 1. Мутирующий вебхук

В этом способе реализована доставка переменных окружения через инъекцию entrypoint в контейнер. Модуль добавляет в под приложения дополнительный контейнер, содержащий бинарный файл инжектора (init-container), который затем копирует сам себя из контейнер-образа во временное хранилище в поде. Вместо запуска основного приложения запускается инжектор, который, используя ServiceAccount приложения, получает необходимые секреты из Deckhouse Stronghold и запускает основное приложение, используя execve.

Доставка секретов через env-injector эффективна, когда, с одной стороны, в приложениях не требуется работать с API Stronghold или Vault, а с другой — нужно доставить секрет в приложение максимально безопасно и с минимальным расходом ресурсов CPU/памяти. Инжектор запускается только в момент запуска вашего приложения и завершается после извлечения секрета, добавления его в ENV и запуска приложения.

Способ 2. CSI-провайдер

При доставке секретов через файлы необходимые для подключения секреты описываются в ресурсе SecretsStoreImport, а в манифесте пода описывается подключение Volume с использованием драйвера secrets-store.csi.deckhouse.io.

При запуске пода драйвер читает ресурс SecretsStoreImport и получает список необходимых секретов и, используя ServiceAccount приложения, секреты из Deckhouse Stronghold. Для приложения такие секреты выглядят как файлы на диске, список которых перечислен в ресурсе SecretsStoreImport.

Рекомендуем использовать этот способ доставки секретов, если вам требуется доставка секрета в виде файла либо вы хотите, чтобы секрет в файле автоматически обновлялся при его обновлении в хранилище, причём без перезапуска пода с приложениями.

Улучшенная безопасность

Последнее по порядку, но не по значимости — безопасность. При разработке мы также уделяем большое внимание различным аспектам защищённости нашего продукта.

С точки зрения базовой безопасности запуск приложения в Deckhouse Stronghold производится только в distroless-контейнере под управлением пользователей с непривилегированным доступом, которым корневая файловая система rootfs доступна только в режиме чтения. В самом контейнере находится только бинарный файл Deckhouse Stronghold, что сводит к минимуму количество возможных векторов атаки.

Все сетевые взаимодействия происходят только по TLS (Transport Layer Security) — специальному криптографическому протоколу, который поддерживает конфиденциальность и целостность данных. При межсервисном взаимодействии производится обязательная проверка удостоверяющего центра (Certificate Authority).

Кроме того, в рамках прохождения процедуры сертификации на соответствие требованиям ТУ и приказа ФСТЭК России № 76 мы регулярно проводим комплексную проверку защищённости различными методами тестирования. Среди них — статический анализ исходного кода (SAST), динамический анализ исходного (DAST), тестирования на проникновение и фаззинг-тесты. Мы также постоянно мониторим CVE и оперативно устраняем найденные уязвимости.

Заключение

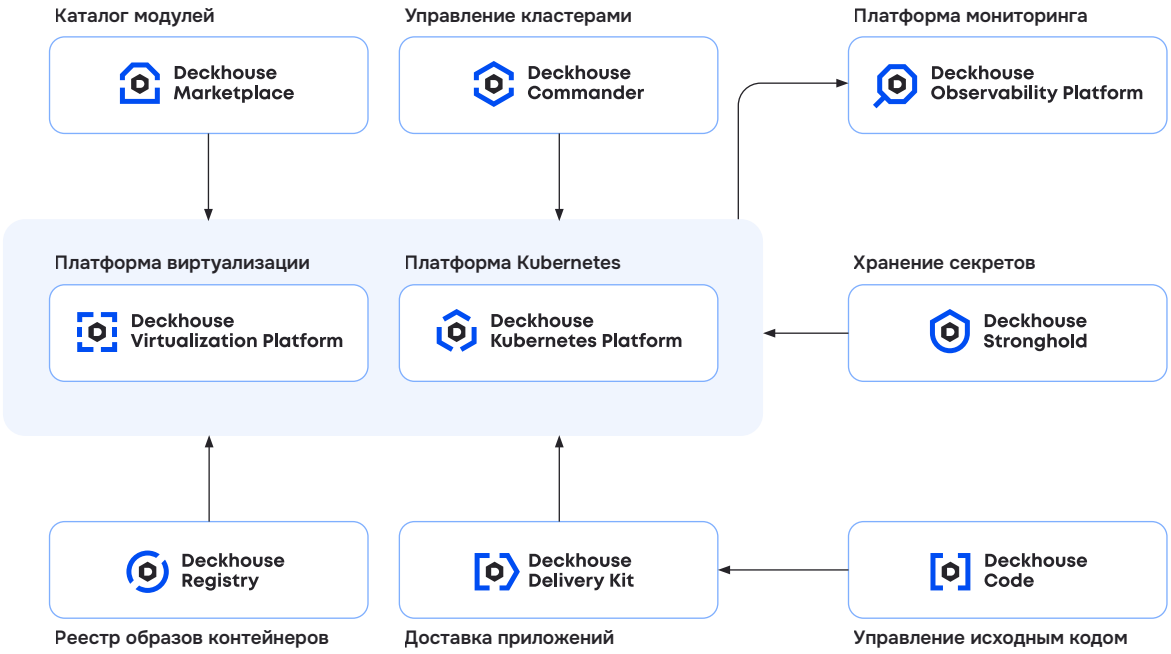
Сегодня мы с уверенностью можем сказать, что Deckhouse Stronghold — это не просто аналог Vault CE, а российское корпоративное хранилище секретов, не уступающее, а местами даже превосходящее функциональность Vault Enterprise.

Мы планируем и дальше активно развивать продукт и добавлять новые функции. В течение 2025 года мы планируем пройти сертификацию ФСТЭК России, а также внедрить disaster- и performance-реплики.

О Deckhouse

Deckhouse — российский разработчик решений для построения надёжной enterprise-инфраструктуры. Лидер рынка DevOps и № 1 контрибьютор Kubernetes в России. Решения Deckhouse более 8 лет в эксплуатации. За это время проведено более 260 внедрений, есть референсные клиенты из разных отраслей.

Продукты Deckhouse позволяют безопасно разрабатывать и доставлять Cloud Native-приложения, эксплуатировать legacy-приложения, облегчить и ускорить переход с монолита на микросервисы. В экосистему бренда входят решения для контейнеризации и виртуализации ИТ-ресурсов, мониторинга инфраструктуры и приложений, а также хранения секретов и управления ими.



Deckhouse

ФЛАНТ

2025