

**ORION
SOFT**

HyperDrive

Описание функциональных характеристик ПО

Содержание

Обозначения и сокращения.....	3
Термины и определения	5
1 Назначение платформы HyperDrive.....	7
2 Основные функции платформы HyperDrive.....	8
3 Компоненты HyperDrive.....	9
3.1 Перечень компонентов	9
3.2 OpenTofu	9
3.3 ingress-nginx	10
3.4 Gitea.....	10
3.5 Keycloak	10
3.6 Longhorn.....	10
3.7 PgBouncer	10
3.8 PostgreSQL.....	11
3.9 postgresql-operator	11
3.10 NATS.....	11
3.11 vault-operator	11
3.12 VictoriaMetrics	11
3.13 StarVault.....	12
3.14 Nova Container Platform	12
3.15 zVirt.....	12
4 Состав комплекта поставки платформы HyperDrive	13

Обозначения и сокращения

В настоящем документе применяют следующие сокращения и обозначения:

- | | | |
|---------|---|---|
| IaC | - | Infrastructure as Code, методология управления и автоматизации инфраструктуры с помощью программного кода вместо ручных настроек и операций. |
| on-prem | - | On-premise, локальная инфраструктура в собственных дата-центрах. |
| VM | - | Виртуальная машина |
| IaaS | - | Infrastructure as a Service, модель облачных вычислений, предоставляющая пользователю виртуализованные вычислительные ресурсы через интернет. |
| DNS | - | Domain Name System, система доменных имен |
| IPAM | - | IP Address Management, управление IP-адресным пространством. |
| HTTP(S) | - | HyperText Transfer Protocol (Secure), протокол передачи гипертекста (с шифрованием). |
| SSO | - | Single Sign-On, концепция, при которой для доступа к различным сервисам используется единая система аутентификации (единый вход) |
| OIDC | - | OpenID Connect, надстройка над протоколом OAuth2 для аутентификации. |
| SAML | - | Security Assertion Markup Language, формат обмена данными аутентификации/авторизации. |

- CI/CD - Continuous Integration / Continuous Delivery (Deployment), непрерывная интеграция и поставка.
- СУБД - система управления базами данных
- БД - база данных
- API - Application Programming Interface, программный интерфейс приложения
- ПО - программное обеспечение
- KVM - Kernel-based Virtual Machine, гипервизор уровня ядра Linux

Термины и определения

В настоящем документе применяют следующие термины с соответствующими определениями:

- | | |
|--|--|
| GitOps | - подход управления инфраструктурой и приложениями через Git-репозитории как единственный источник правды. |
| Configuration Drift/Расхождение (дрифт) конфигурации | - расхождение между сохранённым (эталонным) состоянием инфраструктуры и её фактическим состоянием |
| Контейнер | - реализация технологии виртуализации на уровне операционной системы, которая позволяет изолировать приложения и их зависимости в отдельных «контейнерах». Контейнеры обеспечивают инкапсуляцию и управление ресурсами, что позволяет приложениям работать стабильно и независимо от окружающей инфраструктуры |
| Контейнеризированные приложения | - приложения, функционирующие в контейнерах |
| Контейнерная платформа | - платформа (например, Kubernetes/Nova Container Platform) для развёртывания, оркестрации и эксплуатации контейнеризированных приложений |
| Балансировщик нагрузки | - компонент, распределяющий входящий трафик между несколькими экземплярами сервисов/кластеров. |
| Kubernetes | - система с открытым исходным кодом для автоматизации развёртывания, масштабирования и управления контейнеризированными приложениями |

- Ingress-контроллер - компонент Kubernetes, который на основе ресурсов Ingress маршрутизирует HTTP(S)-трафик снаружи кластера к внутренним сервисам
- Reverse-proxy - прокси-сервер, принимающий запросы от клиентов и перенаправляющий их к внутренним сервисам.
- Пулер - сервис, который управляет пулами соединений к базе данных и снижает накладные расходы на установку подключений

1 Назначение платформы HyperDrive

HyperDrive — основная платформа и единый источник правды для управления гибридной инфраструктурой. Предназначен для автоматизации процессов, таких как развертывание кластеров, управление ресурсами и устранение расхождений конфигураций, с помощью подходов Infrastructure as Code и GitOps. Основная задача платформы – предоставить единый интерфейс для управления ресурсами в различных инфраструктурных средах (On-premise, облака).

Платформа постоянно сравнивает своё сохранённое состояние с реальным состоянием инфраструктуры, реализуя таким образом концепцию Configuration Drift. При обнаружении расхождений (дрифтов), созданных вручную, HyperDrive не будет автоматически применять изменения. Вместо этого он будет создана запись о дрифте и от пользователя потребуются принять решение: обновить состояние в HyperDrive или вернуть инфраструктуру к исходному виду. Это защитный механизм, предотвращающий случайное разрушение среды.

2 Основные функции платформы HyperDrive

Платформа HyperDrive обеспечивает выполнение следующих функций:

1) Автоматизированное развертывание и управление жизненным циклом кластеров контейнерной платформы и балансировщиков нагрузки (создание, масштабирование, удаление, обслуживание).

2) Централизованный учет и обнаружение инфраструктурных ресурсов (платформы, подключения, зоны, центры данных, инфраструктурные кластеры, хосты).

3) Управление IaaS-слоем: каталог типов виртуальных машин, шаблонов операционных систем и cloud-init шаблонов для стандартизации конфигураций и ускорения развертывания VM.

4) Управление сетевой адресацией и DNS-инфраструктурой: настройка сетевых сегментов и подсетей (IPAM), а также динамических DNS-провайдеров, DNS-зон и DNS-записей для сервисов и кластеров.

5) Централизованное управление секретами и стартовыми конфигурациями.

6) Выявление и сопровождение расхождений конфигураций управляемых виртуальных машин.

7) Мониторинг и аудит операций платформы.

8) Поддержка GitOps-подхода для кластеров: интеграция с системами контроля версий и GitOps-инструментами, автоматическая инициализация шаблонов и модулей (логирование, безопасность, резервное копирование и др.) для последующего применения к кластерам.

3 Компоненты HyperDrive

3.1 Перечень компонентов

HyperDrive включает следующие компоненты:

- opentofu 1.10.6;
- ingress-nginx 1.12.6;
- Gitea 1.24.6;
- keycloak 20.0.5;
- longhorn 1.7.3;
- pgbouncer 1.21;
- postgresql 16.2;
- postgresql-operator 5.5.1;
- NATS 2.12.0;
- vault-operator 1.23.0;
- victoria-metrics 1.108.1;
- starvault 1.2.0;
- Nova Container Platform 6.x - 7.x;
- ZVirt 4.4.

3.2 OpenTofu

Инструмент инфраструктуры как кода (IaC) для описания и автоматического развёртывания инфраструктуры в виде декларативных конфигураций. Совместим с экосистемой Terraform и используется для управления ресурсами в облаках и on-prem.

3.3 ingress-nginx

Ingress-контроллер для Kubernetes, использующий NGINX как reverse-проxy и балансировщик нагрузки. Обеспечивает маршрутизацию HTTP(S)-трафика снаружи кластера к внутренним сервисам по правилам Ingress.

3.4 Gitea

Самостоятельно размещаемый Git-сервис для управления репозиториями кода, код-ревью и командной разработки. Поддерживает CI/CD, пакетные реестры и веб-интерфейс, являясь альтернативой GitHub/GitLab.

3.5 Keycloak

Сервер управления идентификацией и доступом с поддержкой SSO, OAuth2/OIDC, SAML и федерации пользователей. Обеспечивает централизованную аутентификацию, авторизацию и управление пользователями для приложений и API.

3.6 Longhorn

Сервер управления идентификацией и доступом с поддержкой SSO, OAuth2/OIDC, SAML и федерации пользователей. Обеспечивает централизованную аутентификацию, авторизацию и управление пользователями для приложений и API.

3.7 PgBouncer

Лёгковесный пулер подключений для PostgreSQL. Уменьшает накладные расходы на установку соединений с БД и повышает производительность приложений при большом количестве запросов.

3.8 PostgreSQL

Реляционная СУБД общего назначения для транзакционных и аналитических нагрузок. Обеспечивает надёжное хранение данных, развитый SQL, расширения и репликацию.

3.9 postgresql-operator

Оператор PostgreSQL для Kubernetes, автоматизирующий жизненный цикл кластеров БД (развёртывание, обновления, репликация, отказоустойчивость). Облегчает настройку резервного копирования, масштабирования и управления конфигурацией Postgres в кластере.

3.10 NATS

Высокопроизводительная система обмена сообщениями для микросервисных и распределённых систем. Поддерживает паттерны публикация/подписка, запрос-ответ и стриминг, обеспечивая масштабируемый и надёжный транспорт данных.

3.11 vault-operator

Оператор для развёртывания и управления кластерами HashiCorp Vault в Kubernetes. Автоматизирует создание, обновление и поддержание отказоустойчивых инсталляций Vault.

3.12 VictoriaMetrics

Система мониторинга и база данных временных рядов для хранения метрик. Подходит для высоконагруженных сценариев, обеспечивает быстрый приём, хранение и выборку временных рядов.

3.13 StarVault

Корпоративная система управления секретами и доступом, российский аналог HashiCorp Vault. Обеспечивает централизованное хранение и ротацию паролей, токенов, ключей и сертификатов, а также управление доступом на основе политик.

3.14 Nova Container Platform

Российская платформа контейнеризации и оркестрации приложений на базе Kubernetes. Предоставляет инструменты для развёртывания, обновления и эксплуатации контейнерных нагрузок с учётом требований информационной безопасности.

3.15 zVirt

Российская платформа виртуализации корпоративного уровня на базе KVM и oVirt. Обеспечивает управление виртуальными машинами, хранилищами, кластерами и сетевой инфраструктурой из единой консоли, с упором на соответствие требованиям российского законодательства и импортозамещение.

4 Состав комплекта поставки платформы HyperDrive

Комплект поставки программного обеспечения «автоматизированная платформа управления инфраструктурой и процессами разработки HyperDrive» включает:

- Экземпляр ПО «автоматизированная платформа управления инфраструктурой и процессами разработки HyperDrive»;
- Инструкцию по установке, включающая описание действий по настройке ПО с помощью установщика;
- Руководство пользователя и администратора, включающее описание действий в интерфейсе HyperDrive.