Kubernetes Infrastructure Stack

Production-Ready Infrastructure as Code

Полнофункциональный Kubernetes кластерс автоматизацией DNS, TLS, CI/CD и мониторингом

Содержание

Введение

Цели проекта

- **Infrastructure as Code** - полная автоматизация через Terraform/OpenTofu
- **Zero-touch DNS** - автоматическое создание DNS записей
- **Auto TLS** - автоматическая выдача и обновление сертификатов
- **GitOps** - декларативное управление приложениями
- **Observability** - полный мониторинг и логирование
- **Security** - централизованная аутентификация и управление секретами

An error occurred on this slide. Check the terminal for more information.

Базовая инфраструктура

DNS Infrastructure

BIND9

- Внутренний DNS сервер
- RFC2136 динамические обновления
- TSIG ключи для безопасности

External DNS

- Автоматическая синхронизация DNS записей
- Интеграция с Kubernetes Services и Ingress
- Поддержка FQDN template

Базовая инфраструктура

TLS Management

Cert-Manager

- Автоматическое управление TLS сертификатами
- DNS-01 challenge (BIND9, CloudFlare)
- HTTP-01 challenge
- Let’s Encrypt интеграция

Internal CA

- Внутренний Certificate Authority
- Self-signed сертификаты для внутренних сервисов
- ClusterIssuer для автоматической выдачи

Базовая инфраструктура

Load Balancing

MetalLB

- LoadBalancer для bare-metal кластеров
- L2 режим балансировки
- Настраиваемый IP pool (172.15.172.210-225)

Ingress Nginx

- HTTP/HTTPS маршрутизация
- SSL/TLS termination
- Интеграция с Cert-Manager для автоматических сертификатов

An error occurred on this slide. Check the terminal for more information.

An error occurred on this slide. Check the terminal for more information.

Хранение данных

PostgreSQL

- PostgreSQL Operator для управления базами данных
- Поддержка PgBouncer для connection pooling
- Отдельные базы для Grafana и Harbor
- Persistent volumes для данных

Nexus3

- Artifact Repository Manager
- Docker registry
- Maven, npm, PyPI repositories
- S3 backend для blob storage
- LDAP интеграция

Хранение данных

Harbor

- Enterprise-grade Docker и Helm registry
- Trivy для сканирования образов
- OIDC интеграция через Vault
- S3 backend для хранения образов
- Helm ChartMuseum

Внешний MinIO S3

- **Внешний сервис** (не часть кластера)
- Используется для:
  - Terraform state backend
  - Velero backups
  - Loki log storage

Идентификация и безопасность

OpenLDAP

- Централизованная аутентификация
- Управление пользователями и группами
- Интеграция с Vault, Forgejo, Nexus, Harbor
- Группы: `devops` (admin), `support` (read-only)

Vault

- HashiCorp Vault для управления секретами
- KV secrets engine
- LDAP authentication
- OIDC provider для SSO
- Интеграция с OpenLDAP

Идентификация и безопасность

External Secrets Operator

- Автоматическая синхронизация секретов из Vault
- ClusterSecretStore для Vault
- Kubernetes auth method
- Periodic refresh секретов
- Webhook для validation

Kyverno

- Kubernetes-native policy engine
- Policy validation и enforcement
- Resource mutation
- Background scanning
- PolicyReports для анализа

An error occurred on this slide. Check the terminal for more information.

An error occurred on this slide. Check the terminal for more information.

CI/CD платформа

Forgejo

- Self-hosted Git сервис (Gitea fork)
- Git repositories
- Pull Requests, Issues
- OIDC/LDAP интеграция
- SSH доступ через LoadBalancer

Forgejo Runner

- CI/CD runners для Forgejo
- Docker-in-Docker
- Act runner для GitHub Actions-совместимых workflows
- Поддержка различных runner labels

CI/CD платформа

ArgoCD

- GitOps continuous delivery
- Declarative GitOps workflow
- OIDC SSO через Vault
- Forgejo/Gitea интеграция
- AppProjects для организации
- Web UI + CLI
- High Availability mode

Renovate

- Автоматизация обновления зависимостей
- Автообновление Docker images, Helm charts, Terraform, Java, Node
- Интеграция с Forgejo

Мониторинг и логирование

VictoriaMetrics Stack

Компоненты:

- **VMSingle** - хранение метрик (50Gi по умолчанию)
- **VMAgent** - сбор метрик из кластера
- **VMAlert** - alerting rules
- **Grafana** - визуализация с OIDC интеграцией

Возможности:

- Предустановленные Kubernetes dashboards
- Node Exporter и kube-state-metrics
- ServiceMonitor для автоматического discovery
- Интеграция с Loki для log correlation

Мониторинг и логирование

Loki Stack

Компоненты:

- **Loki** - индексирование и хранение логов
- **Promtail** - DaemonSet для автоматического сбора логов
- **Gateway** - load balancing

Возможности:

- S3 backend (внешний MinIO) для хранения
- Retention: 30 дней (настраивается)
- Интеграция с Grafana (автоматический datasource)
- LogQL для мощных запросов
- Log correlation с метриками

An error occurred on this slide. Check the terminal for more information.

Backup и восстановление

Velero

- Автоматизация backup и restore для Kubernetes
- Scheduled backups (daily/weekly)
- S3-совместимое хранилище (внешний MinIO)
- Restic для volume backups
- Настраиваемая retention policy
- Выборочный backup по namespaces

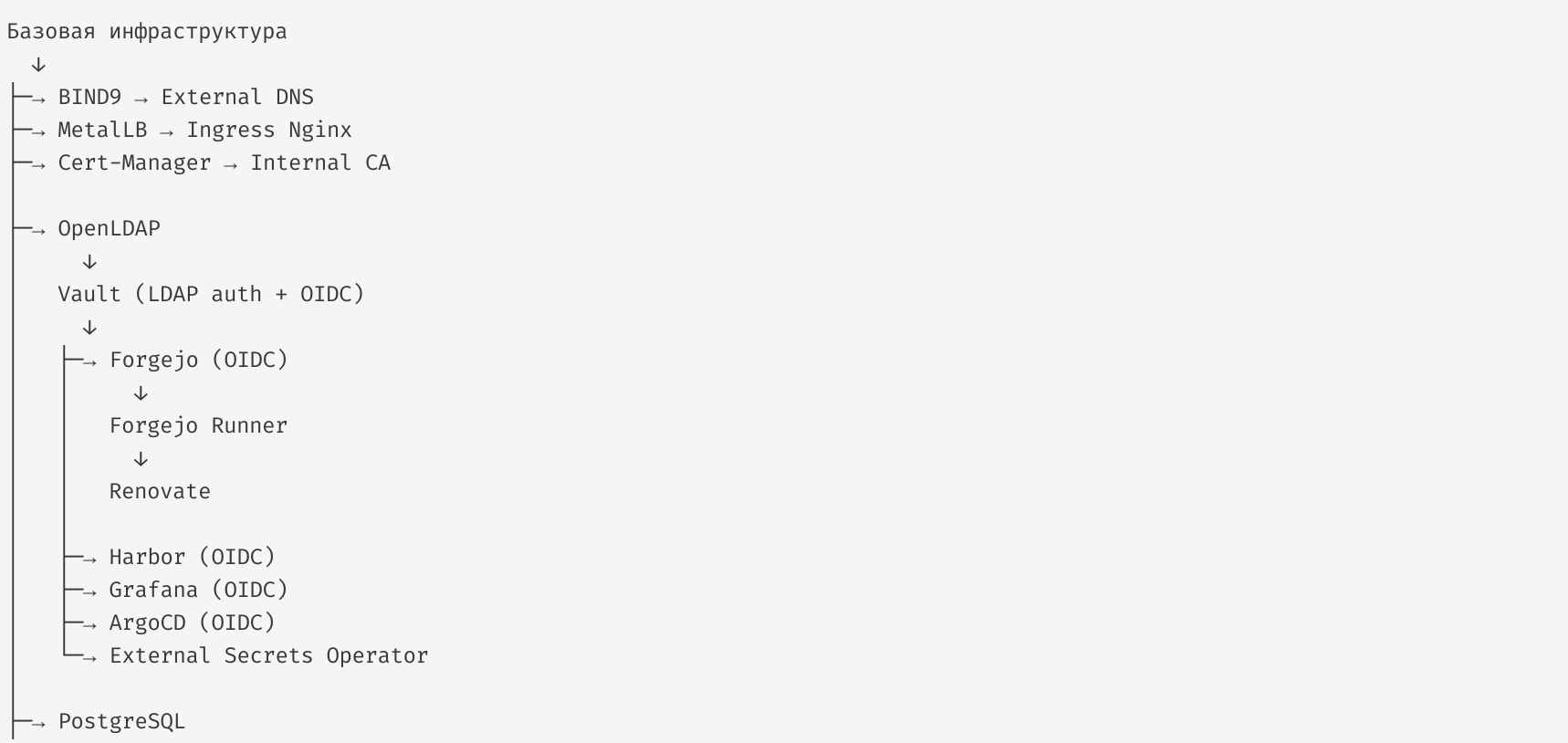
Backup стратегия:

- Daily backup в 2:00 AM
- Weekly backup в 3:00 AM (воскресенье)
- Retention: 30 дней (daily), 60 дней (weekly)
- Namespaces: vault, harbor, forgejo, nexus3, openldap

An error occurred on this slide. Check the terminal for more information.

Зависимости и интеграции

Граф зависимостей



Зависимости и интеграции

Внешние сервисы

External MinIO S3

- **Не часть кластера**
- Используется для:
  - Terraform/OpenTofu state backend
  - Velero backups storage
  - Loki chunks и ruler storage

CloudFlare (опционально)

- DNS-01 challenge для Let’s Encrypt
- Публичные сертификаты

An error occurred on this slide. Check the terminal for more information.

An error occurred on this slide. Check the terminal for more information.

Заключение

Ключевые достижения

✅ **Полная автоматизация** - DNS, TLS, развертывание
✅ **Infrastructure as Code** - Terraform/OpenTofu
✅ **GitOps** - ArgoCD для декларативного управления
✅ **Observability** - Метрики (VictoriaMetrics) + Логи (Loki)
✅ **Security** - Policy engine (Kyverno) + Secret management (ESO + Vault)
✅ **Backup** - Velero для disaster recovery
✅ **Automation** - Renovate для обновлений

Заключение

Преимущества

🚀 Автоматизация

- Zero-touch DNS
- Auto TLS
- Infrastructure as Code

🔒 Безопасность

- Централизованная аутентификация (LDAP + Vault)
- Policy enforcement (Kyverno)
- Secret management (ESO + Vault)

📈 Масштабируемость

- Load Balancing
- Централизованное управление
- GitOps для быстрого развертывания

🛠️ Удобство разработки

Production-Ready Infrastructure Stack

Готово к продакшену! 🚀

Спасибо за внимание!

Вопросы?