

Аутентификация и авторизация

1. Содержание раздела

- [Провайдеры идентификации](#)
- [Настройка провайдеров идентификации](#)
- [Использование RBAC для разграничения доступа в Kubernetes](#)
- [Реализация модели доступа на основе ролей в Nova на основе групп LDAP](#)

Платформа управления безопасностью контейнеров Neuvector

В данном разделе документации вы можете получить подробную информацию по платформе Neuvector, предназначенной для управления безопасностью контейнеров в кластерах Nova Container Platform SE.

Платформа NeuVector является одним из дополнительных модулей Nova Container Platform SE и устанавливается в кластер Kubernetes с целью обеспечить дополнительную безопасность и защиту контейнеров во время их выполнения.

Neuvector выпускается компанией [SUSE](#), исходный код платформы открыт, доступен по лицензии Apache 2.0 в репозитории [Github](#).

1. Основные возможности Neuvector в Nova Container Platform SE

Neuvector расширяет стандартные функции безопасности в Nova Container Platform SE и Kubernetes, а именно:

- Обеспечивает Nova Container Platform SE комплексным автоматизированным решением для защиты контейнеров во время их работы
- Обеспечивает среду Kubernetes необходимыми вебхуками для контроля запросов к серверу Kubernetes API
- Предоставляет в интерактивном графическом интерфейсе полную картину движения сетевого трафика (как для E-W, так и N-S)
- Использует поведенческий анализ сервисов, запущенных в контейнерах и автоматическую изоляцию нелегитимных сервисов
- Использует L7 межсетевой экран для блокировки несанкционированных соединений между контейнерами
- Использует механизмы автоматического обнаружения и предотвращения атак на контейнеры
- Предоставляет механизмы обеспечения безопасности всей цепочки процессов CI/CD, а именно:
 - Сканирование образов контейнеров на уязвимости
 - Сканирование хранилищ образов контейнеров на уязвимости

- Проверка цифровой подписи образов контейнеров
- Интерфейс для запуска сканирования образа после его сборки из CI-пайплайнов
- Выполняет непрерывный аудит безопасности узлов Nova Container Platform SE и запущенных контейнеров
- Предоставляет инструментарий для работы с отчетными данными для оценки рисков
- Предоставляет инструментарий для экспорта событий безопасности в различные системы

2. Интеграция с Nova Container Platform SE

Модуль Neuvector в Nova Container Platform SE поставляется преднастроенным и содержит следующие интеграции, доступные сразу после его установки:

- Интеграция со службой непрерывного развертывания FluxCD, с помощью которой выполняется установка, настройка и поддержание консистентности модуля в кластере Kubernetes
- Интеграция с Nova OAuth: после установки модуля администратор кластера может выполнить вход в Neuvector с помощью OIDC и существующих учетных записей
- Интеграция с StarVault: конфигурационные файлы Neuvector, содержащие чувствительные данные, не хранятся в Kubernetes, а генерируются “на лету” из секретов в StarVault.
- Преднастроенные правила Admission Control, определяющие базовые политики контроля операций в Kubernetes
- Преднастроенные политики автоматического сканирования узлов и кластера Kubernetes
- Дополнительный сервис Neuvector API Docs с офлайн-документацией по работе с Neuvector API

3. Содержание раздела

- [Архитектура и концепции](#)
- [Планирование и системные требования](#)
- [Установка в конфигурации по умолчанию](#)
- [Проверка уязвимостей в кластере](#)