Проверка уязвимостей в кластере

1. Общие сведения

Компонент Scanner в системе безопасности NeuVector (далее - сканер) отвечает за сканирование уязвимостей и проверку соответствия стандартам безопасности образов контейнеров и узлов кластера.

Сканер развернут в Kubernetes в составе системы Neuvector в виде отдельного ресурса Deployment и выполняет следующие функции:

- **Сканирование образов в реестрах**: подключается к указанным реестрам образов контейнеров, извлекает список доступных образов и проводит их анализ на наличие уязвимостей. Для повышения производительности и масштабируемости для сканнера поддерживается автоматическое масштабирование количества его реплик, которые могут параллельно сканировать образы в реестрах.
- **Сканирование на этапе сборки**: интегрируется с процессами CI/CD, позволяя сканировать образы на наличие уязвимостей еще на этапе сборки, до их размещения в реестре или развертывания в среде выполнения.
- **Сканирование узлов и контейнеров в реальном времени**: автоматически сканирует запущенные контейнеры и узлы на наличие уязвимостей и соответствие стандартам безопасности.

2. Источники уязвимостей

Сканер в Neuvector содержит в себе базу данных уязвимостей (CVE), которая использует следующие источники:

- Общие источники информации об уязвимостях:
  - Банк данных угроз безопасности информации ФСТЭК
  - РЕД ОС
  - NVD (National Vulnerability Database)
  - Mitre
- Операционные системы:
  - РЕД ОС

    - Alpine, Amazon, Debian, Microsoft Mariner, Oracle, Rancher OS, Red Hat, SUSE Linux, Ubuntu
- Приложения и языки программирования:
    - .NET, Apache, BusyBox, GoLang, Java, Maven, Kubernetes, Nginx, npm/Node.js, Python, OpenSSL, Ruby.

Актуализация баз уязвимостей выполняется один раз в сутки. По умолчнию в Nova Container Platform для сканнера установлен автоматический перезапуск каждый день в 00:00. При перезапуске загружается новая версия сканера с актуальной базой уязвимостей.

3. Обновление базы уязвимостей

3.1. Обновление при онлайн-установке

Если ваш кластер Nova Container Platform установлен в онлайн-режиме, то для обновления баз уязвимостей (сканера) дополнительные настройки не требуются. Актульная версия сканера будет загружаться ежедневно из публичных репозиториев Nova.

3.2. Обновление при офлайн-установке

Для регулярного обновления сканера в кластерах, установленных без доступа к сети Интернет с использованием Nova Universe вы можете использовать варианты ниже.

3.3. Кеширование образа сканера в корпоративном реестре

Вы можете настроить кеширование публичного репозитория Nova или образа сканера в частности в собственном корпоративном реестре образов и использовать его для обновления. Для настройки следуйте процедуре ниже:

1. Настройте кеширование публичного репозитория Nova или образа сканера. Актуальная версия сканера доступна по ссылке: `hub.nova-platform.io/registry/neuvector/scanner-nova:latest`.

    

    Для получения токена доступа к публичному репозиторию Nova при офлайн-установке обратитесь в техническую поддержку.

2. Если доступ в корпоративный реестр осуществляется с обязательным использованием учетной записи, подготовьте секрет Kubernetes:

```bash
kubectl create secret docker-registry custom-registry-credentials -n nova-neuvector \
--docker-server=<Адрес реестра> \
--docker-username=<Имя пользователя> \
--docker-password=<Пароль или токен> \
--docker-email=<Почтовый адрес пользователя>
```

3. В веб-консоли Nova Container Platform перейдите на вкладку **Administration** > **CustomResourceDefinitions**, найдите ресурс Kustomization, перейдите на вкладку **Экземпляры**, найдите `nova-release-neuvector-main`.
4. На вкладке **YAML** добавьте блок `patches`:

```yaml
spec:
  patches:
    - patch: |-
        apiVersion: apps/v1
        kind: Deployment
        metadata:
          name: neuvector-scanner-pod
          namespace: nova-neuvector
        spec:
          template:
            spec:
              imagePullSecrets: ①
              - name: custom-registry-credentials
              containers:
              - name: neuvector-scanner-pod
                image: "" ②
      target:
        kind: Deployment
        name: neuvector-scanner-pod
        namespace: nova-neuvector
```

① Блок конфигурации учетной записи для доступа к корпоративному реестру (при необходимости).

② Адрес образа в корпоративном реестре с тегом latest.

3.4. Загрузка образа сканера в корпоративный реестр

Если ваш корпоратинвый реестр не поддерживает кеширование и проксирование запросов, вы можете получить актуальный образ сканера в архиве, обратившись в техническую поддержку. Вы также можете самостоятельно выгрузить актуальный образ сканера вручную, используя утилиты docker, podman и аналогичные, из публичного репозитория Nova. Далее вам необходимо будет самостоятельно загрузить данный образ в ваш реестр образов.

Обратите внимание, что для корректного использования собственного реестра образов в кластере Nova, необходимо добавить соответствующие TLS- сертификаты в доверенные. Это можно сделать на этапе установке кластера, используя параметр спецификации `caTrustBundle` . Подробную информацию можно получить в разделе документации по ссылке.

Установка Neuvector в конфигурации по умолчанию

Для установки модуля Neuvector в Nova Container Platform SE используйте один из представленных далее манифестов:

▸ Для кластера в конфигурации по умолчанию

▸ Для высокодоступного кластера в рекомендуемой конфигурации

1. Установка модуля Neuvector

1.1. Предварительные условия

- ✓ Вы ознакомились с архитектурой и концепциями Neuvector в Nova Container Platform.
- ✓ Вы ознакомились с документацией по планированию установки и системным требованиям Neuvector.
- ✓ У вас есть доступ к кластеру с учетной записью, имеющей роль `cluster-admin` в Kubernetes.
- ✓ Вы установили утилиту `kubectl` для работы с Kubernetes.

1.2. Установка с помощью kubectl

1. Сохраните представленный выше манифест в файл, например, `neuvector.yaml`.
2. Установите манифест в кластер Kubernetes, выполнив команду:

```bash
kubectl apply -f neuvector.yaml
```

3. Проверьте состояние запущенных компонентов Neuvector, выполнив команду:

```bash
kubectl get pods -n nova-neuvector
```

4. Проверьте состояние Cluster Kustomizations, выполнив команду:

```bash
kubectl get ks -l nova-application-group=cluster-security -n nova-gitops
```

1.3. Установка с помощью Nova Console

1. Скопируйте представленный выше манифест в буфер обмена.
2. Выполните вход в Nova Console.
3. Используйте опцию импорта нового объекта и вставьте в форму ранее скопированный манифест.

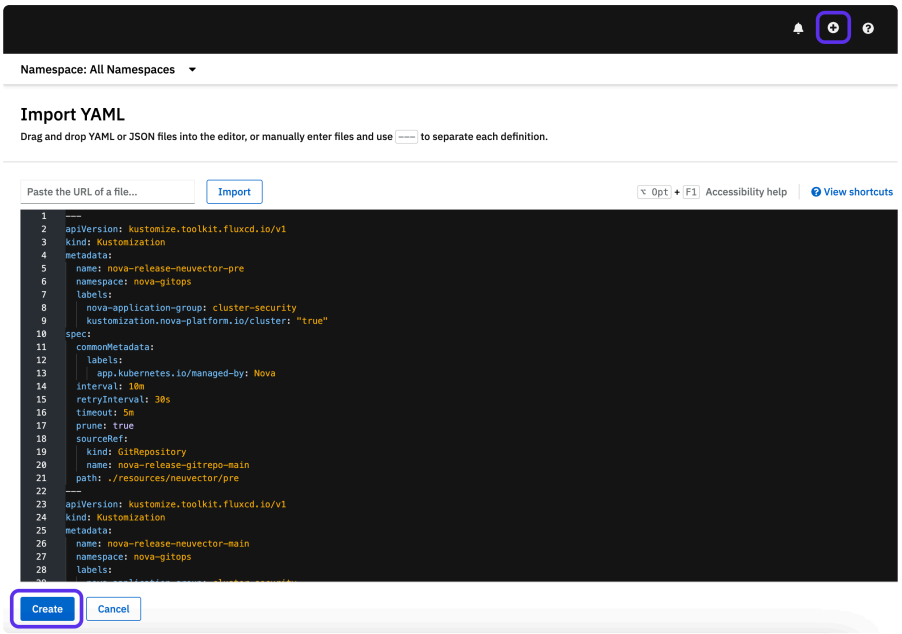

Рисунок 1. Установка модуля Neuvector

4. Перейдите в раздел *Workloads*, далее *Pods* и выберете пространство имен `nova-neuvector`. Проверьте состояние запущенных компонентов Neuvector.
5. Перейдите в раздел *Administration*, далее *Cluster Settings*, во вкладке *Configuration* выберете *Cluster Kustomizations*. Проверьте состояние *Cluster Kustomizations* с именем `nova-neuvector`.