Безопасность установки

При установке и настройке ПО Nova Container Platform Special Edition для обеспечения безопасности необходимо выполнение следующих условий:

- при установке платформы в средах виртуализации с использованием провайдера инфраструктуры инсталляция должна осуществляться на виртуальных серверах в защищенной среде виртуализации сотрудником соответствующей квалификации, имеющим права администратора с присвоенными ему идентификационными данными для работы в среде виртуализации;
- при установке платформы на физических серверах инсталляция должна осуществляться в защищенной серверной инфраструктуре сотрудником соответствующей квалификации, имеющим права администратора с присвоенными ему идентификационными данными для работы в серверной инфраструктуре;
- при установке платформы на предварительно подготовленные серверы с ОС инсталляция должна осуществляться в защищенной инфраструктуре сотрудником соответствующей квалификации, имеющим права администратора с присвоенными ему идентификационными данными для работы в ОС узлов, на которые устанавливается ПО;
- установка и настройка платформы должны осуществляться в соответствии с эксплуатационной документацией;
- должно обеспечиваться предотвращение несанкционированного доступа к идентификаторам и паролям пользователей платформы и привилегированных пользователей (администратора информационной безопасности) платформы;
- должно обеспечиваться предотвращение несанкционированного доступа к идентификаторам и паролям администраторов среды виртуализации, которые необходимы для установки и настройки платформы.

1. Действия по безопасной установке

Действия по безопасной установке Nova Container Platform Special Edition, обновлению и удалению приведены в документе Руководство по установке

2. Действия по безопасной настройке

Ознакомьтесь со следующими статьями:

- Настройка выявления уязвимостей
- Настройка контроля целостности
- Настройка регистрации событий безопасности и управления доступом
- Настройка идентификации и аутентификации Настройка централизованного управления образами контейнеров и контейнерами

Настройка выявления уязвимостей

Выявление известных уязвимостей при установке образа контейнера в ИС и хранении образов контейнеров осуществляется на основе сведений, содержащихся в банке данных угроз безопасности информации путем взаимодействия с компонентом Платформы – системой безопасности **Neuvector**.

Уязвимости в образах контейнеров могут быть выявлены в результате сканирования уже запущенных образов в платформе, загружаемых в платформу образов, а также образов, которые хранятся в подключенном к Neuvector реестре образов.

Для настройки сканирования образов в Платформе необходимо выполнить следующие действия:

1. Установить и настроить модуль системы безопасности Neuvector согласно процедурам, описанным в документе Обеспечение безопасности с помощью модуля Neuvector
    - Ознакомиться с системными требованиями к модулю Neuvector и спланировать установки согласно документу Планирование и системные требования
    - Выполнить установку модуля Neuvector согласно руководству Установка в конфигурации по умолчанию
2. Для запуска сканирования уже запущенных в платформе образов дополнительные действия не требуются. Сканирование выполняется сразу после установки модуля Neuvector.
3. Для запуска сканирования образов, хранимых во внешнем реестре, необходимо:
    - Подготовить отдельный внешний реестр контейнеров для хранения образов контейнеров;
    - Подготовить анализируемые образы контейнеров и загрузить их в реестр контейнеров;
    - Открыть в браузере веб-интерфейс модуля Neuvector, перейти в раздел **Assets**, далее – **Registries**;
    - Добавить конфигурацию реестра образов и выполнить сканирование и указать требуемую периодичность сканирования.

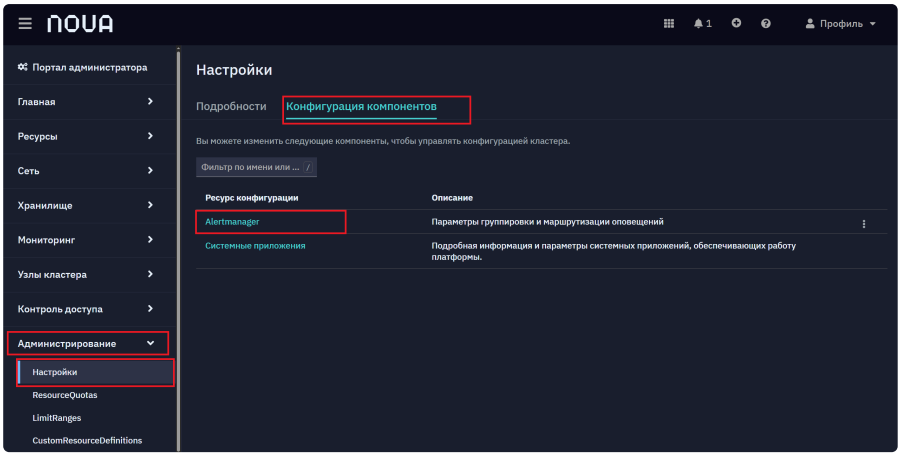
      Периодичность сканирования образов контейнеров зависит от среды, где выполняется их сканирование:

        - Для запущенных и первоначально запускаемых контейнеров сканирование выполняется автоматически в порядке очереди. Данная настройка установлена по умолчанию и не требует дополнительной конфигурации.

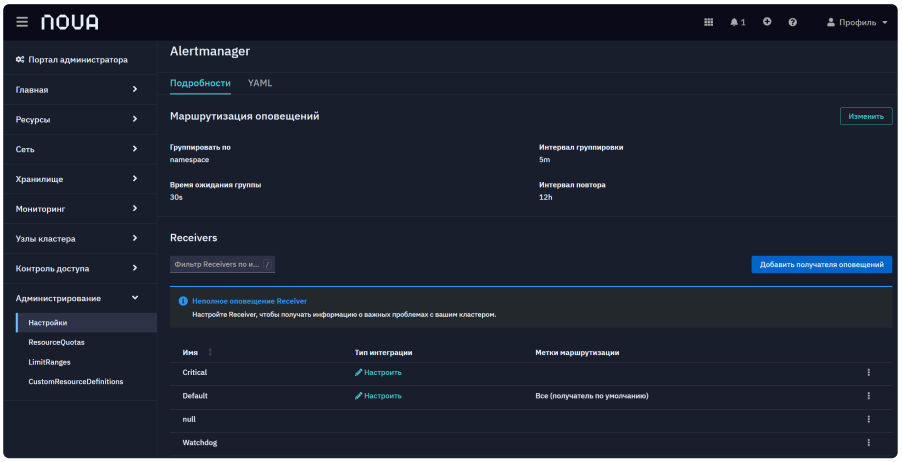
- Периодичность сканирования образов контейнеров в подключаемом в Neuvector реестре настраивается в диапазоне от 5 минут до 1 недели.

Для настройки оповещений о выявленных уязвимостях в образах контейнеров разработчика образов контейнеров администратор безопасности ИС или администратор платформы должны выполнить следующие действия:

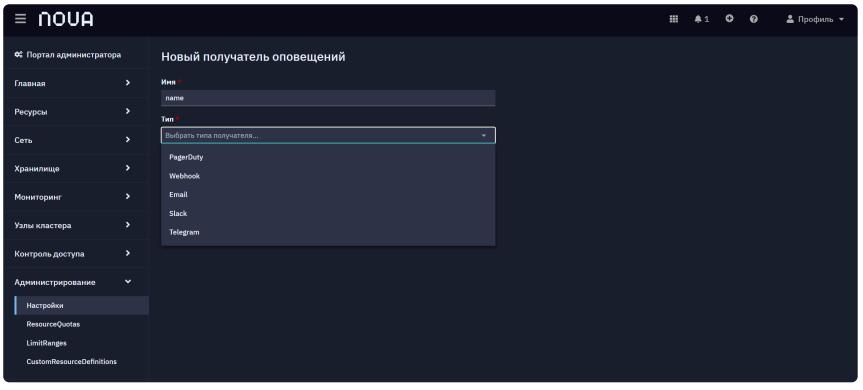
1. Открыть в браузере веб-интерфейс консоли управления Nova, перейти в раздел **Администрирование**, далее – **Настройки**, выбрать вкладку **Конфигурация компонентов**.



2. Выбрать ресурс конфигурации **Alertmanager** и указать данные для настройки оповещений используя кнопку **Добавить получателя оповещений**.



- Указать имя и тип получателя;
- Указать параметры получателя в зависимости от его типа.



1. Рекомендуется к ознакомлению

- Настройка контроля целостности