Руководство пользователя

Данный раздел содержит информацию по управлению Nova Container Platform.

1. Содержание раздела

Примеры использования Logging Operator

Раздел содержит примеры использования Logging Operator.

1. Отправка логов из Syslog-NG в Opensearch

В данном пункте рассказывается как настроить отправку логов из Syslog-NG в Opensearch, используя компонент Logging Operator.

Syslog-NG имеет модуль для отправки логов в ElasticSearch. Поскольку OpenSearch является ответвлением ElasticSearch, этот модуль также можно использовать для отправки логов в OpenSearch. OpenSearch поддерживает авторизацию по TLS, поэтому вы можете использовать сертификаты для настройки Output, но также доступна авторизация по имени пользователя и паролю.

1.1. Предварительные условия

- ✓ Вы ознакомились с архитектурой и концепциями `Logging operator` в `Nova Container Platform`.
- ✓ У вас есть доступ к кластеру с учетной записью, имеющей роль `cluster-admin` в Kubernetes.
- ✓ Вы установили утилиту `kubectl` для работы с Kubernetes.
- ✓ Вы создали отдельное Namespace для компонентов Logging operator. Например, `logging`.

1.2. Добавление секрета

1. В Nova Console перейдите на вкладку **Workloads** > **Secrets** и выберите Namespace `nova-logs`.
2. Найдите секрет `nova-opensearch` и скопируйте его в Namespace, где установлен Syslog-NG (например, `logging`). Этот секрет содержит сертификаты, необходимые для авторизации в Opensearch.

1.3. Установка Output для Syslog-ng

Установите Output через `kubectl` или через Nova Console, используя следующий манифест:

```yaml
apiVersion: logging.banzaicloud.io/v1beta1
kind: SyslogNGClusterOutput ①
metadata:
  name: syslogngoutput
  namespace: logging
spec:
  elasticsearch:
    logstash_prefix: nova-syslog ②
    url: https://nova-logs-cluster.nova-logs.svc.cluster.local:9200/_bulk
    tls:
      ca_file:
        mountFrom:
          secretKeyRef:
            key: ca.crt
            name: nova-opensearch
      cert_file:
        mountFrom:
          secretKeyRef:
            key: tls.crt
            name: nova-opensearch
      key_file:
        mountFrom:
          secretKeyRef:
            key: tls.key
            name: nova-opensearch
      peer_verify: false ③
```

① Происходит установка Output для всего кластера (Global Output).

② Имя индекса в Opensearch, куда будут отправляться логи. Индекс создастся автоматически.

③ Позволяет Logging Operator работать с недоверенными сертификатами.

1.4. Установка Flow для Syslog-ng

Установите Flow через `kubectl` или через Nova Console, используя следующий манифест:

```yaml
apiVersion: logging.banzaicloud.io/v1beta1
kind: SyslogNGClusterFlow ①
metadata:
  name: syslogngflow
  namespace: logging
spec:
  globalOutputRefs:
    - syslogngoutput
  match:
    regexp: ②
      pattern: '*'
```

```
      type: glob
      value: json.kubernetes.labels.app.kubernetes.io/instance
```

① Происходит установка Flow для всего кластера.

② Логи будут собираться со всех экземпляров и со всех Namespace.

1.5. Проверка в OpenSearch

1. Откройте консоль OpenSearch и перейдите на вкладку **Management > Index Management > Indices**.
2. Найдите индекс с именем `nova-syslog-дата`. Если индекс не отображается, подождите несколько минут, так как создание индекса может занять некоторое время.

2. Настройка отправки логов из NeuVector на внешний сервер Syslog

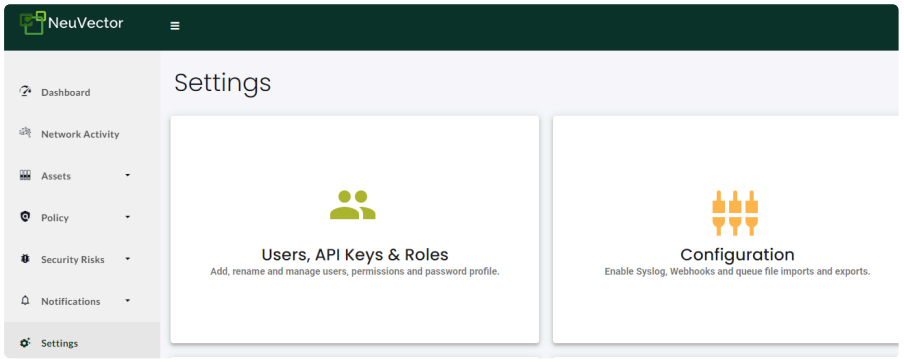
В данной статье будет рассматриваться отправка логов из NeuVector на внешний сервер Syslog средствами самого NeuVector.

2.1. Предварительные условия

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

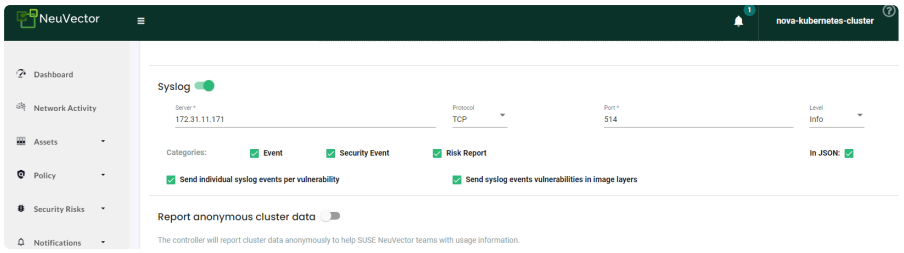
2.2. Настройка NeuVector

1. Откройте консоль NeuVector и перейдите на вкладку **Settings > Configuration**.

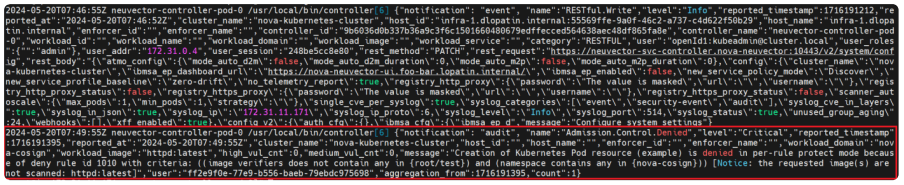


2. Найдите блок Syslog в нижней части страницы. Настройте параметры в соответствии с настройками внешнего Syslog сервера. В данном случае оставлен стандартный порт,

выбран протокол TCP.
Выберите нужные параметры. В данном случае настроено получение всех логов с сервера, а также активирована опция `In JSON`, которая позволяет получать данные в JSON формате.



3. После настройки сгенерируйте событие в логе или просмотрите логи на внешнем сервере Syslog. В приведённом примере было настроено правило, запрещающее установку pod'а, если образ не подписан через cosign, и была сделана попытка создания pod'а.



3. Настройка отправки логов из Neuvector в Opensearch

В данной разделе описывается процесс отправки логов из NeuVector в OpenSearch с использованием Syslog-ng и Fluentd через компонент Logging Operator.

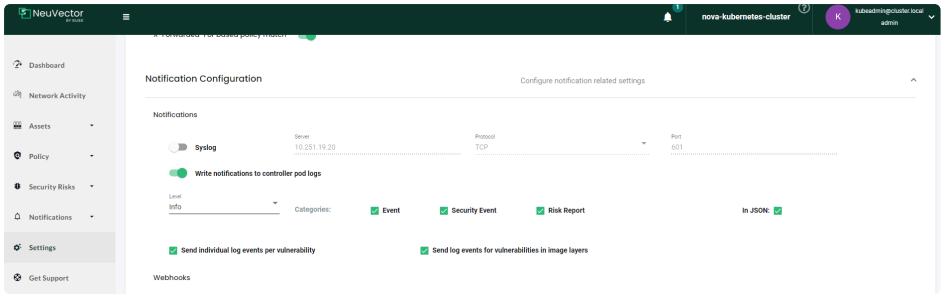
3.1. Предварительные условия

- ✓ Вы ознакомились с архитектурой и концепциями `Logging operator` в `Nova Container Platform`.
- ✓ Вы ознакомились с архитектурой и концепциями `NeuVector` в `Nova Container Platform`.
- ✓ У вас есть доступ к кластеру с учетной записью, имеющей роль `cluster-admin` в Kubernetes.
- ✓ Вы установили утилиту `kubectl` для работы с Kubernetes.
- ✓ Создано новое Namespace. Например, `logging`.

3.2. Отправка логов через Fluentd

3.2.1. Включаем запись событий из Neuvector в логи pod'а контроллера

1. Откройте консоль Neuvector.
2. Перейдите на вкладку **Settings > Configuration** и раскройте блок **Notification Configuration**.
3. Включите опцию *Write notifications to controller pod logs* и укажите необходимые опции.



3.2.2. Настройка Fluentd

Создайте новый Fluentd или настройте уже существующий согласно инструкции. В данном случае был настроен уже существующий Fluentd.

> Рекомендуется создать новый Fluentd, чтобы не нарушить работу встроенного компонента.

3.2.3. Установка Output

Установите Output согласно инструкции через `kubectl` или через Nova Console, используя следующий манифест:

```yaml
apiVersion: logging.banzaicloud.io/v1beta1
kind: ClusterOutput ①
metadata:
  name: os-output
  namespace: nova-logs
spec:
  opensearch:
    buffer:
      flush_interval: 30s
      path: /buffers/neuvector
      retry_timeout: 96h
      retry_wait: 2s
      chunk_limit_records: 1000000
      timekey: 1h
      flush_thread_count: 2
      delayed_commit_timeout: 150s
      retry_max_interval: 180s
      chunk_limit_size: 300K
      flush_mode: interval
    logstash_prefix: nova-neuvector ②
    port: 9200
    logstash_format: true
    scheme: https
```

```
    host: nova-logs-cluster.nova-logs.svc.cluster.local
    user: nova-logging
    ssl_verify: false
    reload_on_failure: true
    reconnect_on_error: true
    password:
      valueFrom:
        secretKeyRef:
          key: password
          name: nova-logging-credentials
    include_timestamp: true
```

① Происходит установка Output для всего кластера.

② Указывается имя индекса в Opensearch, куда будут направляться логи. Индекс создастся автоматически.

3.2.4. Установка Flow

Установите Flow через `kubectl` или через Nova Console используя следующий манифест:

YAML

```
apiVersion: logging.banzaicloud.io/v1beta1
kind: ClusterFlow ①
metadata:
  name: os-flow
  namespace: nova-logs
spec:
  globalOutputRefs:
    - os-output
  match:
    - select:
        labels:
          app: neuvector-controller-pod ②
```

① Происходит установка Flow для всего кластера.

② В Opensearch будут отправляться только логи с контейнера `neuvector-controller-pod`.

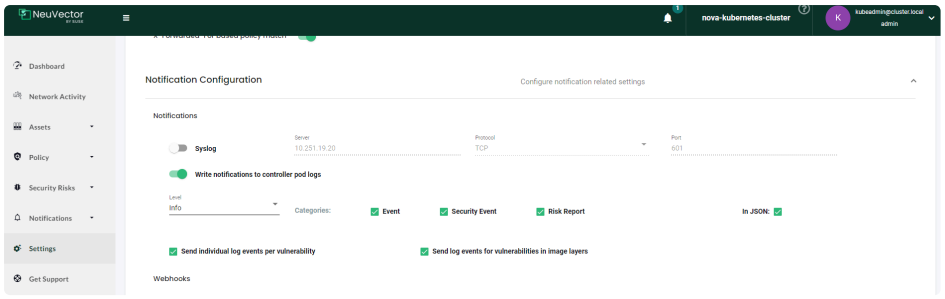
3.2.5. Проверка в OpenSearch

1. Откройте консоль OpenSearch и перейдите на вкладку **Management > Index Management > Indices**.
2. Найдите индекс с именем `nova-neuvector-дата`. Если такого индекса ещё нет, то подождите несколько минут.

3.3. Отправка логов через Syslog-ng

3.3.1. Включение записи событий из Neuvector в логи pod'а контроллера

1. Откройте консоль Neuvector.
2. Перейдите на вкладку **Settings > Configuration** и раскройте блок **Notification Configuration**.
3. Включите опцию *Write notifications to controller pod logs* и укажите необходимые опции.



3.3.2. Настройка Syslog-ng

Создайте Syslog-ng согласно инструкции.

3.3.3. Добавление секрета

1. В Nova Console перейдите на вкладку **Workloads > Secrets** и Namespace `nova-logs`.
2. Найдите секрет `nova-opensearch` и скопируйте его в Namespace, где установлен Syslog-ng. В данном случае - `logging`. Этот секрет содержит сертификаты и ключи, которые нужны для авторизации в Opensearch.

3.3.4. Установка Output

Установите Output через `kubectl` или через Nova Console, используя следующий манифест:

YAML

```yaml
apiVersion: logging.banzaicloud.io/v1beta1
kind: SyslogNGClusterOutput
metadata:
  name: random-log-output
  namespace: logging
spec:
  elasticsearch:
    logstash_prefix: nova-neuvector
    url: https://nova-logs-cluster.nova-logs.svc.cluster.local:9200/_bulk
    tls:
      ca_file:
        mountFrom:
          secretKeyRef:
            key: ca.crt
            name: nova-opensearch
      cert_file:
        mountFrom:
          secretKeyRef:
            key: tls.crt
            name: nova-opensearch
```

```
      key_file:
        mountFrom:
          secretKeyRef:
            key: tls.key
            name: nova-opensearch
      peer_verify: false
```

3.3.5. Установка Flow

Установите Flow через `kubectl` или через Nova Console, используя **любой** из следующих манифестов:

YAML

```yaml
apiVersion: logging.banzaicloud.io/v1beta1
kind: SyslogNGClusterFlow
metadata:
  name: random-log-flow
  namespace: logging
spec:
  filters:
    - match:
        and:
          - regexp:
              pattern: notification
          - regexp:
              pattern: neuvector-controller-pod-0
  globalOutputRefs:
    - random-log-output
```

В этом манифесте происходит установка Flow для всего кластера. В Opensearch будут отправляться только логи, которые содержат слова `notification` и `neuvector-controller-pod-0`.

YAML

```yaml
apiVersion: logging.banzaicloud.io/v1beta1
kind: SyslogNGClusterFlow
metadata:
  name: random-log-flow
  namespace: logging
spec:
  globalOutputRefs:
    - random-log-output
  match:
    regexp:
      pattern: neuvector-controller-pod
      type: glob
      value: json.kubernetes.labels.app
```

В этом манифесте происходит установка Flow для всего кластера. В Opensearch будут отправляться только логи с контейнера `neuvector-controller-pod`, у которого есть соответствующая метка.

3.3.6. Проверка в OpenSearch

1. Откройте консоль OpenSearch и перейдите на вкладку **Management > Index Management > Indices**.
2. Найдите индекс с именем `nova-neuvector-дата`. Если такого индекса ещё нет, то подождите несколько минут.

4. Настройка отправки логов kubelet в Opensearch

4.1. Предварительные условия

- ✓ Вы ознакомились с архитектурой и концепциями `Logging operator` в `Nova Container Platform`.
- ✓ У вас есть доступ к кластеру с учетной записью, имеющей роль `cluster-admin` в Kubernetes.
- ✓ Вы установили утилиту `kubectl` для работы с Kubernetes.

4.2. Настройка

1. Создайте агенты Fluent Bit, которые будут собирать логи сервиса kubelet.

```yaml
apiVersion: logging-extensions.banzaicloud.io/v1alpha1
kind: HostTailer
metadata:
  name: nova-node-kubelet-host-tailer
  namespace: nova-logs
spec:
  systemdTailers:
    - containerOverrides:
        image: 'hub.nova-platform.io/registry/fluent/fluent-bit:2.1.8'
      name: nova-node-kubelet
      systemdFilter: kubelet.service ①
  workloadMetaOverrides:
    labels:
      nova-log-type: nova-node-kubelet ②
  workloadOverrides:
    tolerations:
      - operator: Exists
```

① Фильтр по имени сервиса.

② Метка, которая будет присутствовать на созданных ресурсом pod'ах.

2. Создайте точку выхода для логов.

```yaml
apiVersion: logging.banzaicloud.io/v1beta1
kind: Output
metadata:
  name: nova-node-kubelet-output
  namespace: nova-logs
spec:
  opensearch:
    buffer:
      flush_interval: 30s
      path: /buffers/kubelet ①
      retry_timeout: 96h
      retry_wait: 2s
      chunk_limit_records: 1000000
      timekey: 1h
      flush_thread_count: 2
      delayed_commit_timeout: 150s
      retry_max_interval: 180s
      chunk_limit_size: 300K
      flush_mode: interval
    logstash_prefix: nova-node-kubelet ②
    port: 9200
    logstash_format: true
    scheme: https
    host: nova-logs-cluster.nova-logs.svc.cluster.local ③
    user: nova-logging ④
    ssl_verify: false
    reload_on_failure: true
    reconnect_on_error: true
    password: ⑤
      valueFrom:
        secretKeyRef:
          key: password
          name: nova-logging-credentials
    include_timestamp: true
```

① Путь до буфера.

② Имя нового индекса в Opensearch.

③ Адрес Opensearch.

④ Имя пользователя в Opensearch.

⑤ Пароль пользователя в Opensearch.

3. Создайте правило фильтрации логов для отправки их в Opensearch.

```yaml
apiVersion: logging.banzaicloud.io/v1beta1
kind: Flow
metadata:
  name: nova-node-kubelet-flow
  namespace: nova-logs
spec:
  localOutputRefs:
    - nova-node-kubelet-output ①
  match:
    - select:
        labels:
          nova-log-type: nova-node-kubelet ②
```

① Точка выхода для отфильтрованных логов.

② Метка для pod’ов, с которых будут собираться логи.