

Настройка уведомлений в Opensearch

В данной статье описывается процесс настройки уведомлений в OpenSearch, включая создание оповещений и проверку.

1. Предварительные условия

- ✓ Вы ознакомились с архитектурой и концепциями Opensearch 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 установили модуль [Opensearch](#).

2. Настройка почтовых уведомлений

1. Перейдите на вкладку **Management > Notifications > Email senders** и нажмите на кнопку [**Create SMTP sender**].
2. Укажите имя, адрес электронной почты, адрес SMTP-сервера, порт и метод шифрования для почтового ящика, с которого будут отправляться уведомления.
3. Перейдите на вкладку **Management > Notifications > Email recipient groups** и нажмите на кнопку [**Create recipient group**].
4. Укажите имя группы и адреса электронной почты получателей уведомлений.
5. Перейдите на вкладку **Management > Notifications > Channels** и нажмите на кнопку [**Create channel**].
6. Укажите имя канала уведомлений, тип канала `Email`, тип отправителя `SMTP sender` и выберите, от кого будут отправляться уведомления, а также кто будет их получать.
7. Если SMTP-сервер требует авторизации, откройте веб-консоль Nova Container Platform, зайдите в pod `nova-logs-0`, перейдите на вкладку **Терминал** и выберите контейнер `opensearch`.

Также вы можете зайти в консоль контейнера через `kubectl` (если он настроен), используя следующую команду:

```
kubectl exec --stdin --tty nova-logs-0 -c opensearch -n nova-logs --  
/bin/bash
```

BASH | 

8. Для авторизации почтового адреса отправителя выполните две команды, заменив **<имя созданного ранее Email sender>**, почтовый адрес отправителя и пароль от почтового адреса отправителя.

```
/usr/share/opensearch/bin/opensearch-keystore add  
opensearch.notifications.core.email.<имя созданного ранее Email  
sender>.username <<< 'почтовый адрес отправителя'  
/usr/share/opensearch/bin/opensearch-keystore add  
opensearch.notifications.core.email.<имя созданного ранее Email  
sender>.password <<< 'пароль от почтового адреса отправителя'
```

BASH | 

9. Для обновления учётных данных в Opensearch перейдите на вкладку **Management > Dev Tools** и выполните команду:

```
POST _nodes/reload_secure_settings  
{  
  "secure_settings_password": ""  
}
```

BASH | 

10. Откройте созданный канал и нажмите на кнопку **[Actions]**, а далее **[Send test message]** для отправки тестового письма.

3. Настройка оповещения

1. Создайте новый индекс. Для этого перейдите на вкладку **Management > Index Management > Indexes** и нажмите на кнопку **[Create Index]** и укажите имя индекса.
2. Откройте веб-консоль Nova Container Platform, зайдите в под `nova-logs-0`, перейдите на вкладку **Терминал** и выберите контейнер `opensearch`.

Также вы можете зайти в консоль контейнера через `kubectl` (если он настроен), используя следующую команду:

```
kubectl exec --stdin --tty nova-logs-0 -c opensearch -n nova-logs --  
/bin/bash
```

BASH | 

3. Добавьте лог в новый индекс. Выполните следующую команду, заменив **<имя индекса>**.

```
curl -X POST "https://nova-logs-cluster.nova-logs.svc.cluster.local:9200/<имя индекса>/_doc/" -H 'Content-Type: application/json' -d '{"timestamp": "2024-06-30T12:34:56Z", "loglevel": "CRITICAL", "message": "Something went wrong"}' --cert /usr/share/opensearch/config/certs/transport/tls.crt --key /usr/share/opensearch/config/certs/transport/tls.key --cacert /usr/share/opensearch/config/certs/transport/ca.crt --insecure
```

BASH | 

4. Перейдите на вкладку **OpenSearch Plugins > Alerting > Monitors** и нажмите на кнопку **[Create monitor]**.
5. Заполните следующие поля:
 - **Monitor name** - укажите имя.
 - Выберите **Per document monitor**.
 - В блоке **Schedule** выберите интервал: каждую минуту.
 - Выберите созданный индекс в поле **Index**.
 - **Query name** - укажите имя.
 - **Field** - выберите *loglevel is CRITICAL*.
 - Нажмите на кнопку **[Add trigger]**.
 - **Trigger name** - укажите имя.
 - **Specify queries or tags** - выберите **Query name** из предыдущего пункта.
 - **Action name** - укажите имя.
 - **Channels** - выберите канал, который был настроен ранее.
6. Выполните пункты 2 и 3, чтобы сгенерировать новое сообщение.
7. Проверьте почту получателя уведомлений. Обратите внимание, что оповещение проверяется каждую минуту, поэтому письмо может не прийти сразу.
8. Перейдите на вкладку **OpenSearch Plugins > Alerting > Alerts** и убедитесь, что появилось оповещение.

Запрет на удаление индексов

Чтобы запретить ручное удаление индексов (*immutability*) в OpenSearch, выполните следующие шаги:

1. В веб-консоли Nova Container Platform перейдите на вкладку **Administration > CustomResourceDefinitions**.
2. Найдите ресурс *Kustomization* и зайдите в него.
3. Перейдите на вкладку **Экземпляры**, найдите `nova-release-logs-main` и зайдите в него.
4. Перейдите на вкладку **YAML** и добавьте patch, который будет содержать текущие настройки из *ConfigMap* `nova-logs-config` в Namespace `nova-logs`, а также ваши изменения.

Пример:

► **Details**