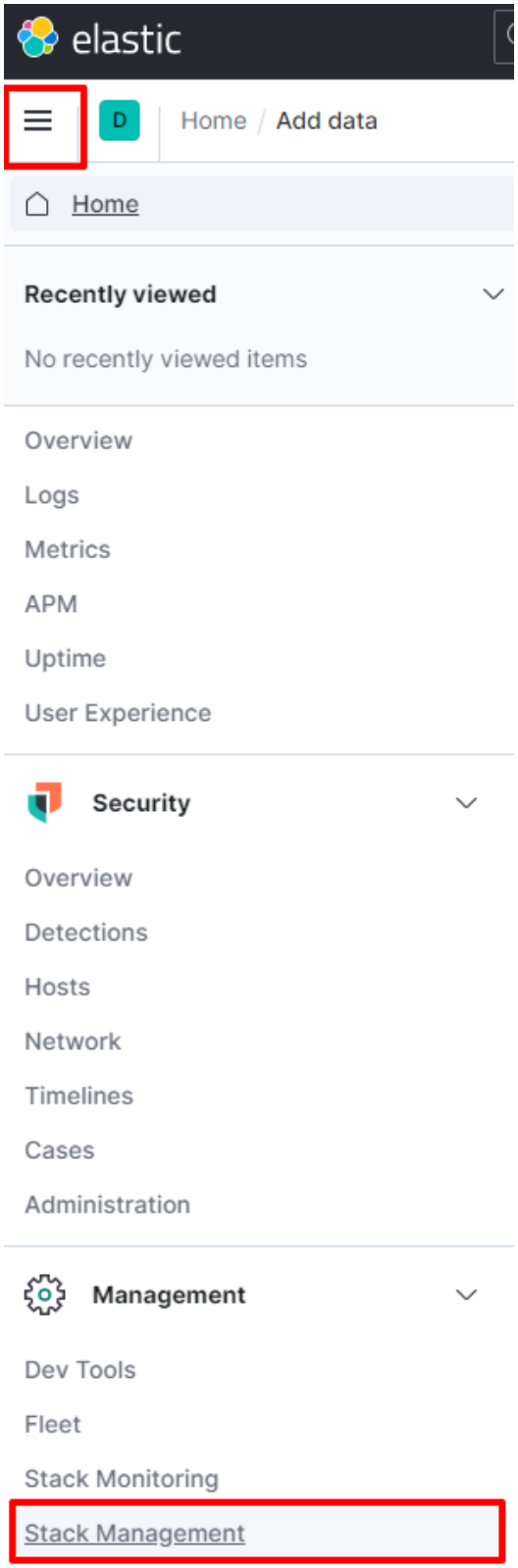
Настройка Kibana

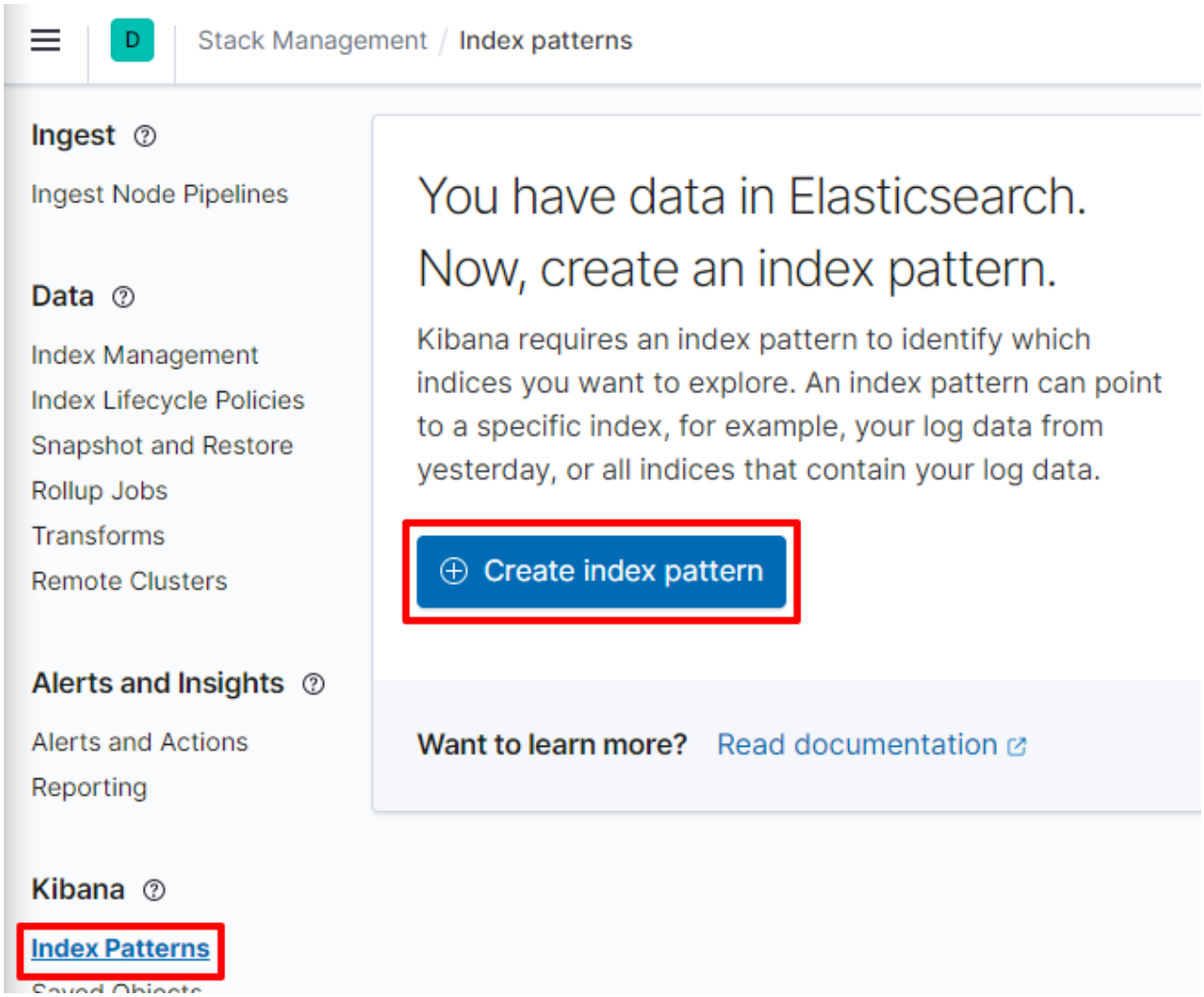
!!! ВНИМАНИЕ: Работы продолжаем на стенде из предыдущего шага

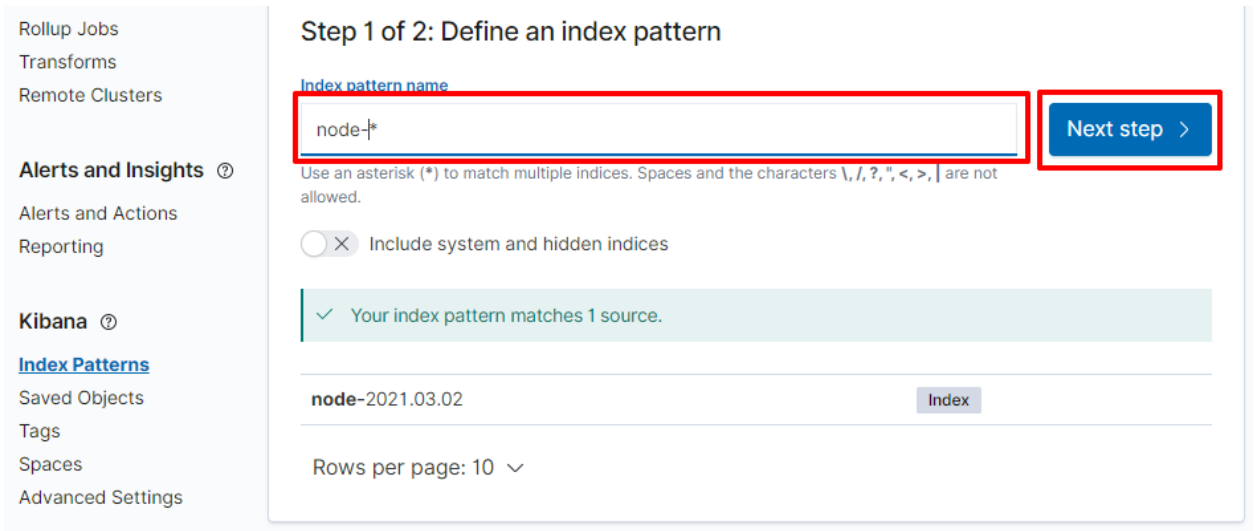
1. Откройте в браузере интерфейс Kibana по адресу (в режиме "инкогнито")

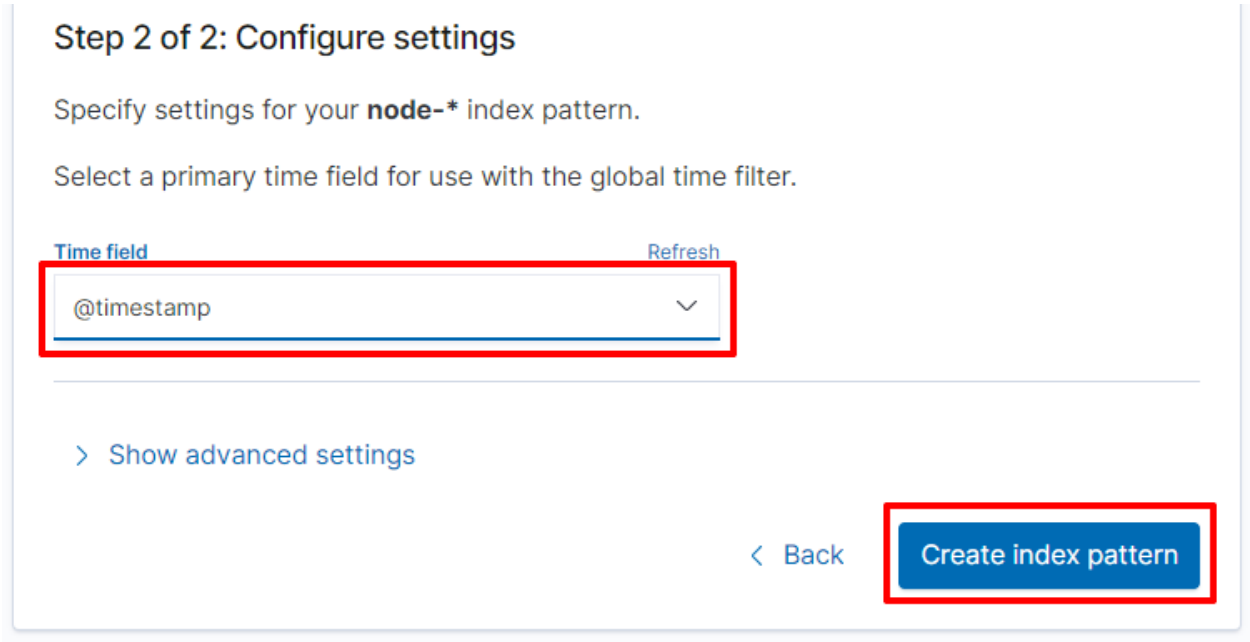
`kibana.s<ваш номер логина>.edu.slurm.io`

2. Выполните настройки Kibana для индекса node-*.

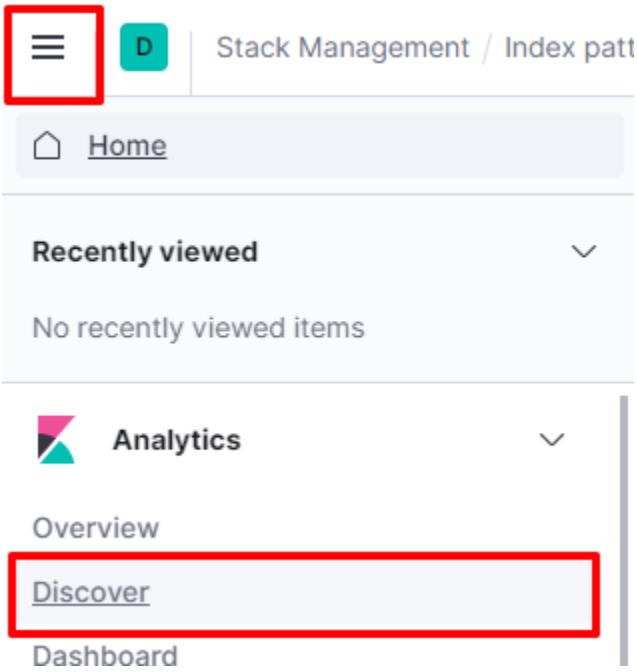

elastic
D
Home / Add data
Home
Recently viewed
No recently viewed items
Overview
Logs
Metrics
APM
Uptime
User Experience
Security
Overview
Detections
Hosts
Network
Timelines
Cases
Administration
Management
Dev Tools
Fleet
Stack Monitoring
Stack Management

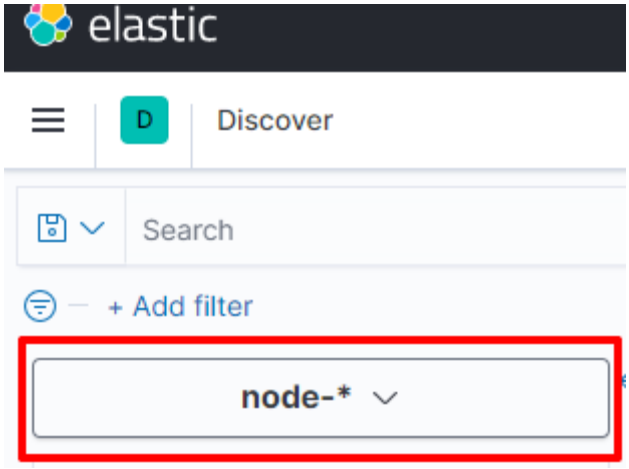

D
Stack Management / Index patterns
Ingest
Ingest Node Pipelines
Data
Index Management
Index Lifecycle Policies
Snapshot and Restore
Rollup Jobs
Transforms
Remote Clusters
Alerts and Insights
Alerts and Actions
Reporting
Kibana
Index Patterns
You have data in Elasticsearch.
Now, create an index pattern.
Kibana requires an index pattern to identify which indices you want to explore. An index pattern can point to a specific index, for example, your log data from yesterday, or all indices that contain your log data.
Create index pattern
Want to learn more? Read documentation


Rollup Jobs
Transforms
Remote Clusters
Alerts and Insights
Alerts and Actions
Reporting
Kibana
Index Patterns
Saved Objects
Tags
Spaces
Advanced Settings
Step 1 of 2: Define an index pattern
Index pattern name
node-*
Next step
Use an asterisk (*) to match multiple indices. Spaces and the characters \, /, ?, ", <, >, | are not allowed.
Include system and hidden indices
Your index pattern matches 1 source.
node-2021.03.02
Index
Rows per page: 10

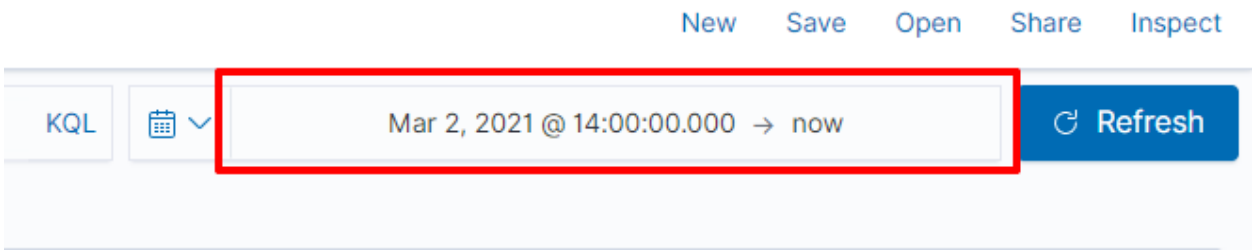


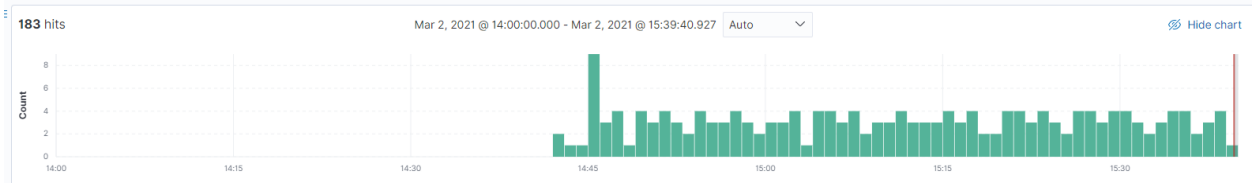
Проверьте, что вы можете видеть логи из кластера.





Тут меняем начальный период, если на графике не выдало вдруг информацию.





Теперь настройте индекс для logstash-*.

3. Внесите настройки в values fluent-bit и примените их в кластер.

В systemd добавим ещё фильтр для сервиса docker

```
    [INPUT]
        Name systemd
        Tag host.*
        Systemd_Filter _SYSTEMD_UNIT=kubelet.service
        Systemd_Filter _SYSTEMD_UNIT=docker.service <== эту строчку
        Read_From_Tail On
```

Добавим префикс для логов с тэгом kube.*. Индекс logstash-* станет не актуальным. И `Replace_Dots On` для замены точек в лейблах на нижнее подчеркивание.

```
    [OUTPUT]
        Name es
        Match kube.*
        Host elasticsearch-master
        Logstash_Prefix kube    <== эту строчку
        Logstash_Format On
        Retry_Limit False
        Replace_Dots On    <== эту строчку
```

Запустим обновление

```
helm upgrade -i fluent-bit fluent/fluent-bit -f fluent-values.yaml -n logging
```

4. После перенастройки fluent-bit добавьте переименованный индекс в интерфейсе Kibana и проверьте возможность просмотра логов.