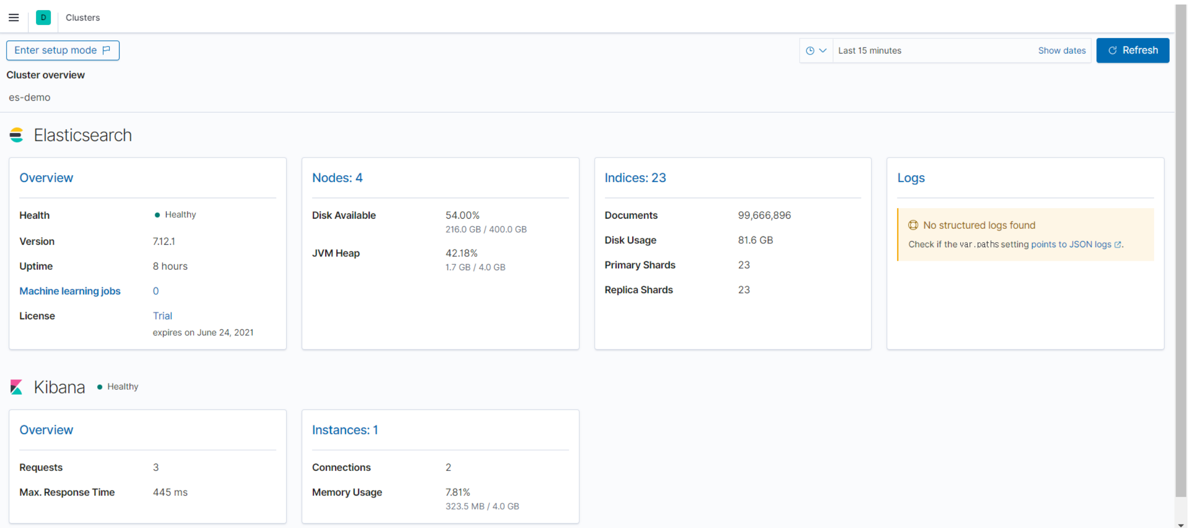
모니터링 방안

1. Self hosted ES

1. ELK Stack Monitoring

전체 Service들에 대한 Monitoring 가능



Clusters

Enter setup mode

Last 15 minutes | Show dates | Refresh

Cluster overview

es-demo

Elasticsearch

Overview

Health: ● Healthy
Version: 7.12.1
Uptime: 8 hours
Machine learning jobs: 0
License: Trial
expires on June 24, 2021

Nodes: 4

Disk Available: 54.00%
216.0 GB / 400.0 GB
JVM Heap: 42.18%
1.7 GB / 4.0 GB

Indices: 23

Documents: 99,666,896
Disk Usage: 81.6 GB
Primary Shards: 23
Replica Shards: 23

Logs

No structured logs found
Check if the var.paths setting points to JSON logs.

Kibana ● Healthy

Overview

Requests: 3
Max. Response Time: 445 ms

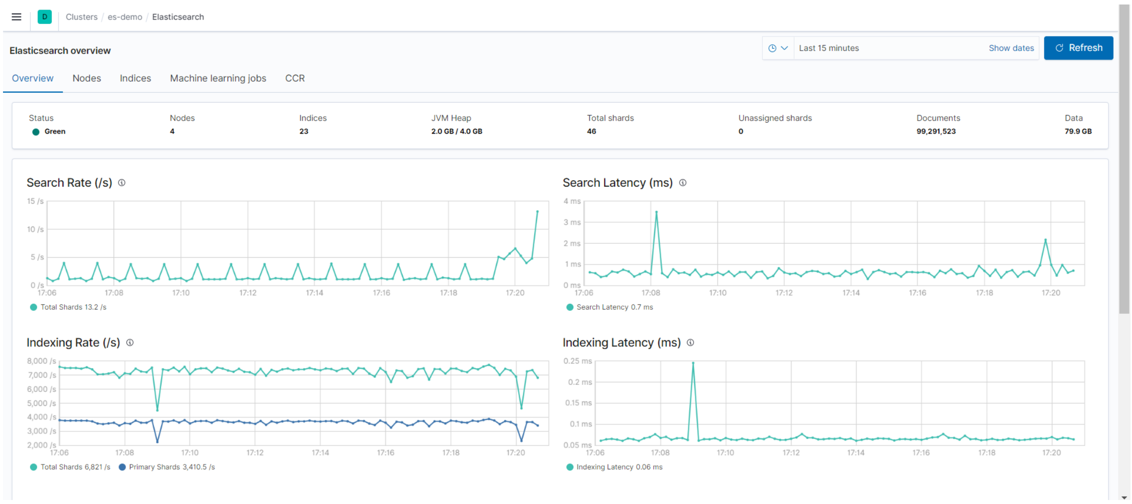
Instances: 1

Connections: 2
Memory Usage: 7.81%
323.5 MB / 4.0 GB

2. Elasticsearch Monitoring

Tab에 따라 Elasticsearch Cluster에 대한 Monitoring이 가능합니다.

1. Summary



Clusters / es-demo / Elasticsearch

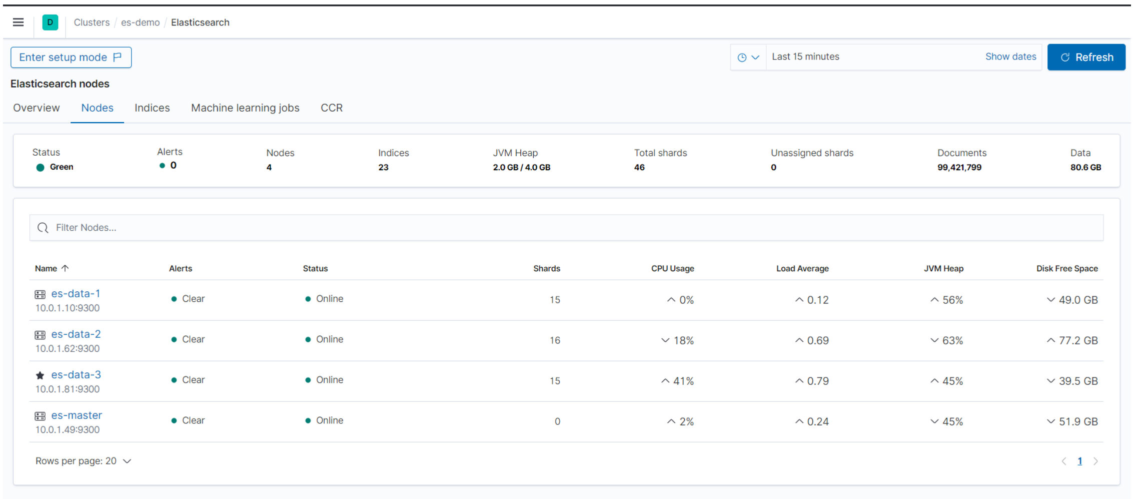
Elasticsearch overview

Last 15 minutes | Show dates | Refresh

Overview | Nodes | Indices | Machine learning jobs | CCR

Status	Nodes	Indices	JVM Heap	Total shards	Unassigned shards	Documents	Data
● Green	4	23	2.0 GB / 4.0 GB	46	0	99,291,523	79.9 GB

2. Nodes Status

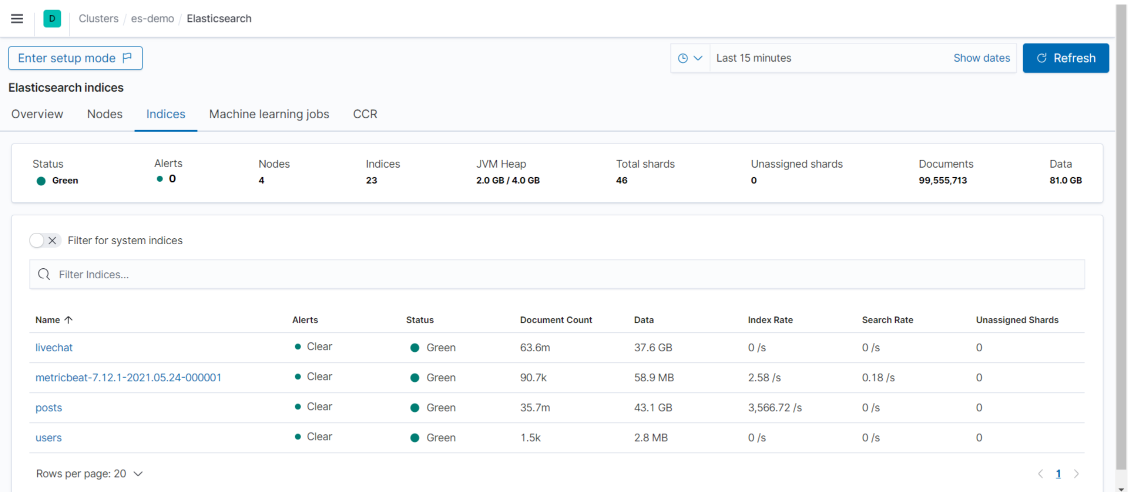


Elasticsearch nodes

Status	Alerts	Nodes	Indices	JVM Heap	Total shards	Unassigned shards	Documents	Data
● Green	● 0	4	23	2.0 GB / 4.0 GB	46	0	99,421,799	80.6 GB

Name ↑	Alerts	Status	Shards	CPU Usage	Load Average	JVM Heap	Disk Free Space
es-data-1 10.0.1.10:9300	● Clear	● Online	15	^ 0%	^ 0.12	^ 56%	˅ 49.0 GB
es-data-2 10.0.1.62:9300	● Clear	● Online	16	˅ 18%	^ 0.69	˅ 63%	^ 77.2 GB
★ es-data-3 10.0.1.81:9300	● Clear	● Online	15	^ 41%	^ 0.79	^ 45%	˅ 39.5 GB
es-master 10.0.1.49:9300	● Clear	● Online	0	^ 2%	^ 0.24	˅ 45%	˅ 51.9 GB

3. Index Monitoring



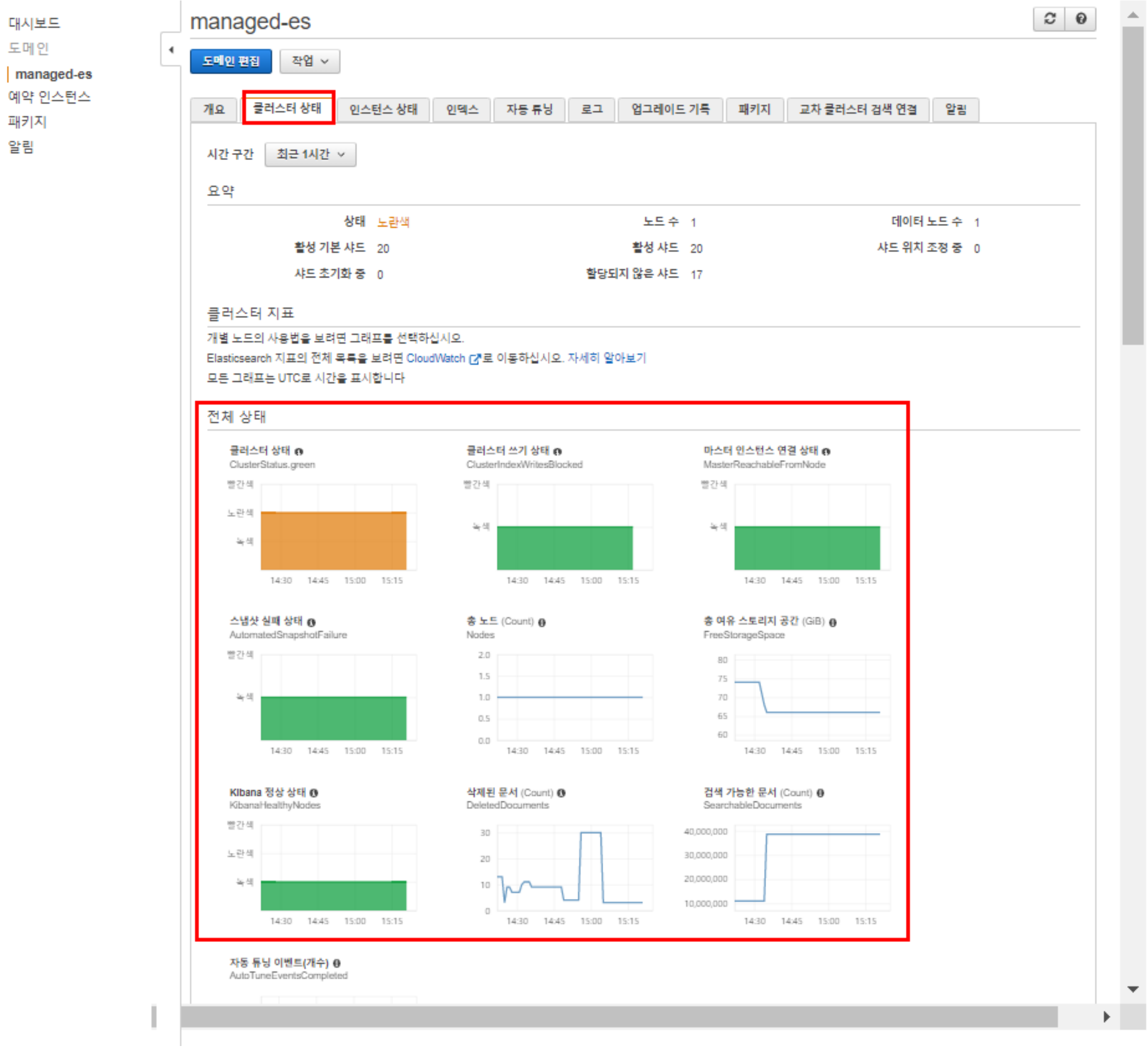
Elasticsearch indices

Status	Alerts	Nodes	Indices	JVM Heap	Total shards	Unassigned shards	Documents	Data
● Green	● 0	4	23	2.0 GB / 4.0 GB	46	0	99,555,713	81.0 GB

Name ↑	Alerts	Status	Document Count	Data	Index Rate	Search Rate	Unassigned Shards
livechat	● Clear	● Green	63.6m	37.6 GB	0 /s	0 /s	0
metricbeat-7.12.1-2021.05.24-000001	● Clear	● Green	90.7k	58.9 MB	2.58 /s	0.18 /s	0
posts	● Clear	● Green	35.7m	43.1 GB	3,566.72 /s	0 /s	0
users	● Clear	● Green	1.5k	2.8 MB	0 /s	0 /s	0

2. Managed ES

1. Managed ES Graph



요약

상태 노란색 | 노드 수 1 | 데이터 노드 수 1
활성 기본 샤드 20 | 활성 샤드 20 | 샤드 위치 조정 중 0
샤드 초기화 중 0 | 할당되지 않은 샤드 17

클러스터 지표

개별 노드의 사용법을 보려면 그래프를 선택하십시오.
Elasticsearch 지표의 전체 목록을 보려면 CloudWatch 로 이동하십시오. 자세히 알아보기
모든 그래프는 UTC로 시간을 표시합니다

2. Graph 들로 CloudWatch DashBoard 구성

aws_sdk로 구성
소스 코드

1. app.py : cdk 실행 파일

```
#!/usr/bin/env python3

from aws_cdk import core
from cw_dashboard.cw_dashboard_stack import CwDashboardStack
import boto3

session = boto3.Session(profile_name='default')
account_id = session.resource('iam').CurrentUser().arn.split(':')[4]
env_US = core.Environment(account=account_id,region="us-west-2")
app = core.App()
CwDashboardStack(app, "es-dashboard-stack", env=env_US)

app.synth()
```

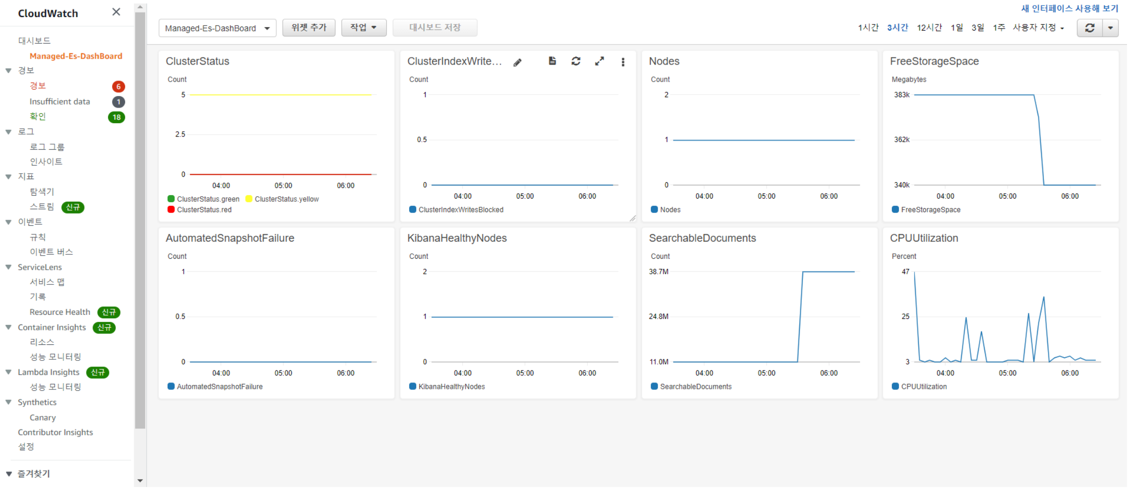
2. cw_dashboard_es.py : Dashboard 구성 파일

```
from aws_cdk import core
from aws_cdk import aws_cloudwatch as cw
from aws_cdk.aws_cloudwatch import GraphWidget
import boto3

session = boto3.Session(profile_name='default')
account_id = session.resource('iam').CurrentUser().arn.split(':')[4]

# Returns CloudWatch Metrics on each functions
def get_metrics(_metricName, _statistic):
    metrics = []
    metrics.append(
        cw.Metric(
            metric_name = _metricName,
            namespace = 'AWS/ES',
            dimensions={
                "DomainName" :'{Elasticsearch Domain Name}',
                "ClientId" : account_id
            },
            statistic = _statistic,
        )
    )

    return metrics

# Returns GraphicWidget
def get_GrapthWidget(_title, _metricName, _statistic, _width, _height):
    return GraphWidget(
                title=_title,
                left=get_metrics(_metricName, _statistic),
                width=_width,
                height=_height
            )



class Elasticsearch(core.Construct):

    def __init__(self, scope: core.Construct, id: str, **kwargs):
        super().__init__(scope, id, **kwargs)

        dashboard = cw.Dashboard(self, id, dashboard_name=id) # 3rd Arg is
the name of dashboard.
        dashboard.add_widgets(
            GraphWidget(title='ClusterStatus',
            left=[
                cw.Metric(metric_name='ClusterStatus.green',
namespace='AWS/ES', color='#2ca02c', dimensions={"DomainName":'managed-es',
"ClientId":account_id}, statistic='Sum'),
                cw.Metric(metric_name='ClusterStatus.yellow',
namespace='AWS/ES', color='#FFFF33', dimensions={"DomainName":'managed-es',
"ClientId":account_id}, statistic='Sum'),
                cw.Metric(metric_name='ClusterStatus.red',
namespace='AWS/ES', color='#FF0000', dimensions={"DomainName": 'managed-es',
"ClientId": account_id}, statistic='Sum')
            ],
            width=6,
            height=6),

            get_GrapthWidget('ClusterIndexWritesBlocked','ClusterIndexWritesBlocked','Maximum',6,6),
 get_GrapthWidget('Nodes','Nodes','Maximum',6,6),

 get_GrapthWidget('FreeStorageSpace','FreeStorageSpace','Sum',6,6),

 get_GrapthWidget('AutomatedSnapshotFailure','AutomatedSnapshotFailure','Maximum',6,6),

 get_GrapthWidget('KibanaHealthyNodes','KibanaHealthyNodes','Average',6,6),

 get_GrapthWidget('SearchableDocuments','SearchableDocuments','Average',6,6),

 get_GrapthWidget('CPUUtilization','CPUUtilization','Maximum',6,6),
        )
```

3. cw_dashboard_stack.py : CloudFormaion Stack 구성

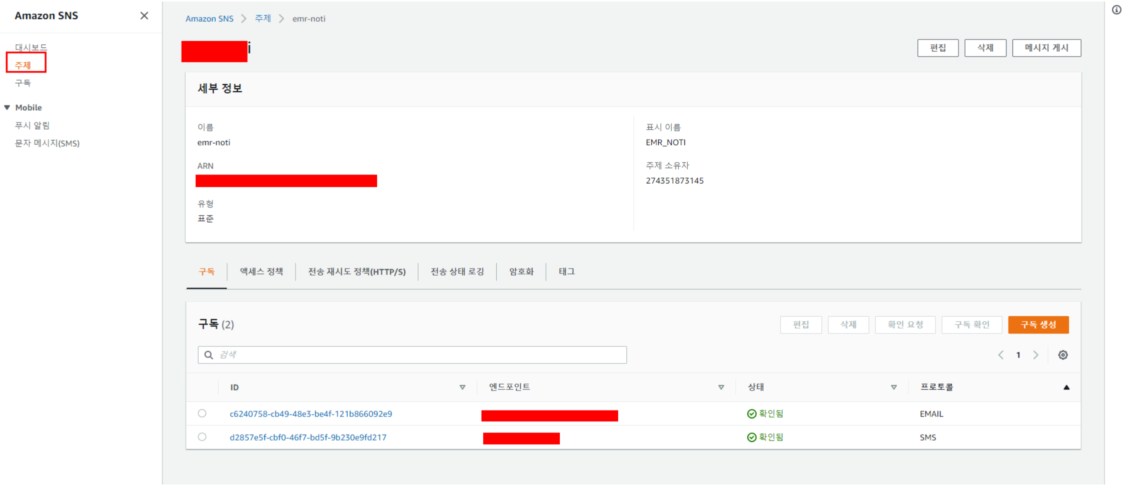
```python
from aws_cdk import core
from cw_dashboard.cw_dashboard_es import Elasticsearch

class CwDashboardStack(core.Stack):

    def __init__(self, scope: core.Construct, id: str, **kwargs) -> None:
        super().__init__(scope, id, **kwargs)

        dashboard_es_creation = Elasticsearch(self, '{DashBoard Name}')  # 2nd Arg is the id of dashboard.
```

4. 결과



3. Alert 구성

1. Target이 될 SNS 생성



[redacted]

세부 정보

이름
emr-noti

ARN
[redacted]

유형
표준

표시 이름
EMR_NOTI

주제 소유자
274351873145

구독 (2)

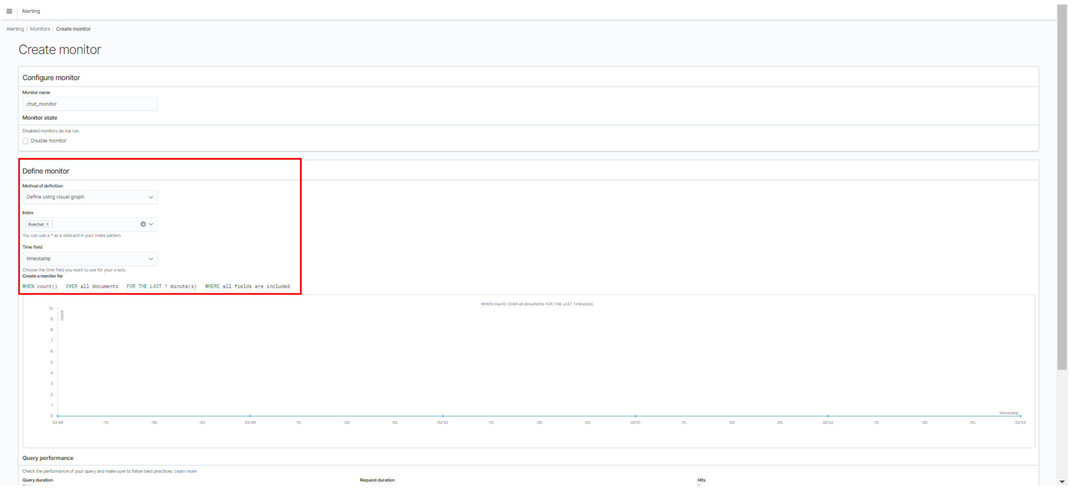
ID	엔드포인트	상태	프로토콜
○ c6240758-cb49-48e3-be4f-121b866092e9	[redacted]	✓ 확인됨	EMAIL
○ d2857e5f-cbf0-46f7-bd5f-9b230e9fd217	[redacted]	✓ 확인됨	SMS

2. IAM Role 권한 부여
   기존 Role에 정책 추가

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": "sns:*",
    "Resource": "sns-topic-arn"
  }]
}
```

3. Kibana Alerting 구성

    1. monitor 구성



Create monitor

Configure monitor

Monitor name
chat_monitor

Monitor state
Disabled monitors do not run.
□ Disable monitor

Define monitor

Method of definition
Define using visual graph

Index
livechat ×
You can use a * as a wildcard in your index pattern

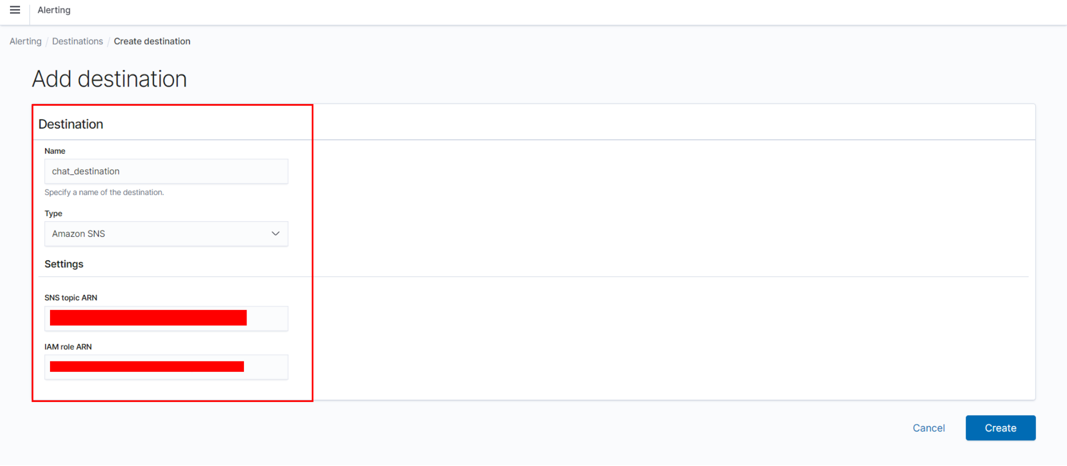
Time field
timestamp
Choose the time field you want to use for your x-axis

Create a monitor for
WHEN count() OVER all documents FOR THE LAST 1 minute(s) WHERE all fields are included

WHEN count() OVER all documents FOR THE LAST 1 minute(s)

Query performance
Check the performance of your query and make sure to follow best practices. Learn more
Query duration
Request duration
Hits

2. Target 설정



Add destination

Destination

Name: chat_destination

Specify a name of the destination.

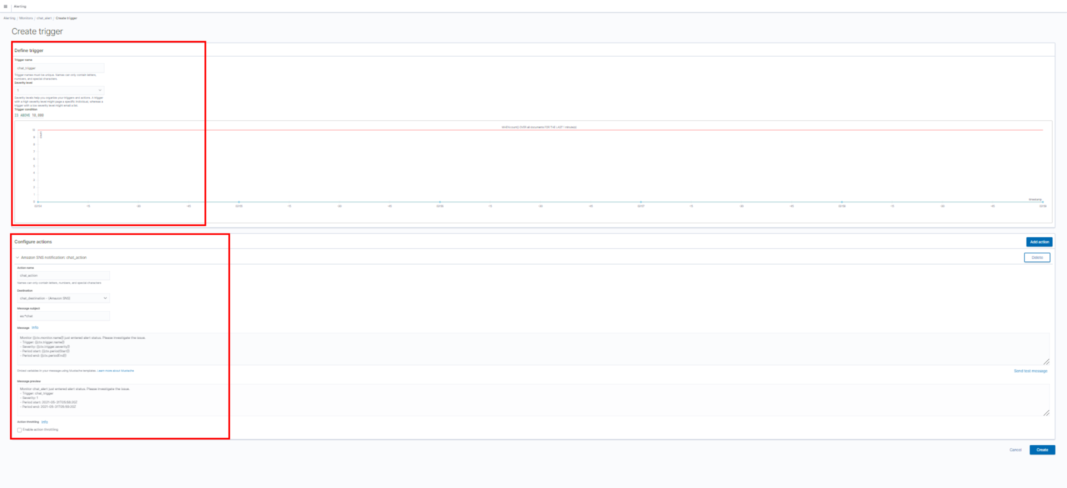
Type: Amazon SNS

Settings

SNS topic ARN: [redacted]

IAM role ARN: [redacted]

3. Trigger 및 Action 설정



Create trigger

Define trigger

Trigger name: chat_trigger

Trigger names must be unique. Names can only contain letters, numbers, and special characters.

Severity level: 1

Severity levels help you organize your triggers and actions. A trigger with a high severity level might page a specific individual, whereas a trigger with a low severity level might email a list.

Trigger condition: IS ABOVE 10,000

Configure actions

Amazon SNS notification: chat_action

Action name: chat_action

Names can only contain letters, numbers, and special characters

Destination: chat_destination - (Amazon SNS)

Message subject: es:*chat

Message Info

```
Monitor {{ctx.monitor.name}} just entered alert status. Please investigate the issue.
- Trigger: {{ctx.trigger.name}}
- Severity: {{ctx.trigger.severity}}
- Period start: {{ctx.periodStart}}
- Period end: {{ctx.periodEnd}}
```

Embed variables in your message using Mustache templates. Learn more about Mustache

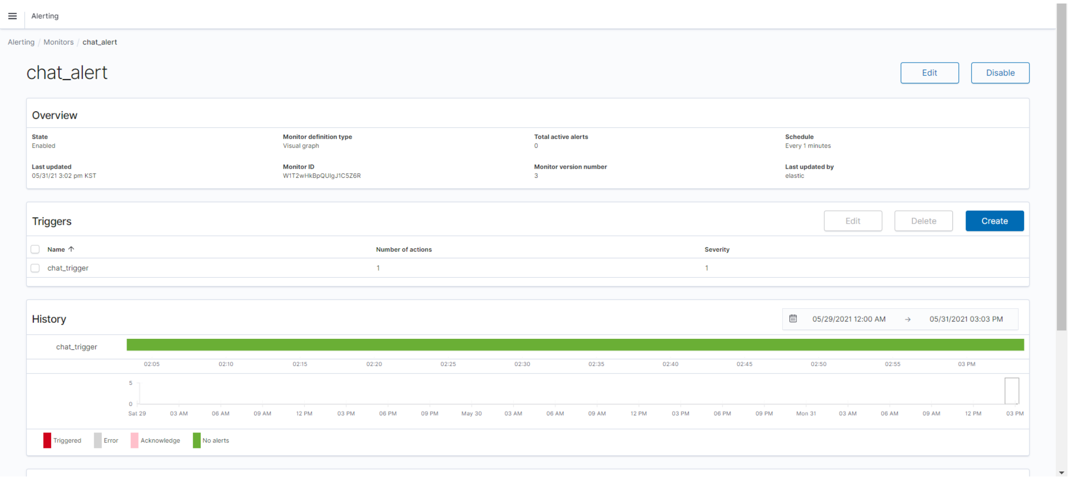
Message preview

```
Monitor chat_alert just entered alert status. Please investigate the issue.
- Trigger: chat_trigger
- Severity: 1
- Period start: 2021-05-31T05:58:20Z
- Period end: 2021-05-31T05:59:20Z
```

Action throttling Info

□ Enable action throttling

4. Alerting 구성



chat_alert

Overview

State Enabled	Monitor definition type Visual graph	Total active alerts 0	Schedule Every 1 minutes
Last updated 05/31/21 3:02 pm KST	Monitor ID W1T2wHkBpQUIgJ1C5Z6R	Monitor version number 3	Last updated by elastic

Triggers

Name	Number of actions	Severity
chat_trigger	1	1

History

05/29/2021 12:00 AM → 05/31/2021 03:03 PM

🟥 Triggered ▨ Error 🟥 Acknowledge 🟩 No alerts