ISE의 로그 분석-ELK 스택 이해

목차

소개

이 문서에서는 Cisco ISE(Identity Services Engine) 3.3~System 360 로그 분석에 내장된 ELK 스택 구성 요소에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco ISE
- ELK 스택

사용되는 구성 요소

이 문서의 정보는 Cisco ISE 3.3을 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

시스템(360)은 모니터링 및 로그 분석을 포함한다.

모니터링 기능을 사용하면 다양한 애플리케이션 및 시스템 통계와 배포에 있는 모든 노드의 KPI(핵심 성능 지표)를 중앙 집중식 콘솔에서 모니터링할 수 있습니다. KPI는 노드 환경의 전반적인 상태에 대한 통찰력을 얻는 데 유용합니다. 통계는 시스템 구성 및 사용률별 데이터를 간단하게 보여줍니다.

Log Analytics는 엔드포인트 AAA(Authentication, Authorization, and Accounting)의 심층 분석 및 syslog 데이터 프로파일링을 위한 유연한 분석 시스템을 제공합니다. Cisco ISE 상태 요약 및 프로세스 상태를 분석할 수도 있습니다. Cisco ISE 카운터 및 상태 요약 보고서와 유사한 보고서를 생성할 수 있습니다.

ELK 스택

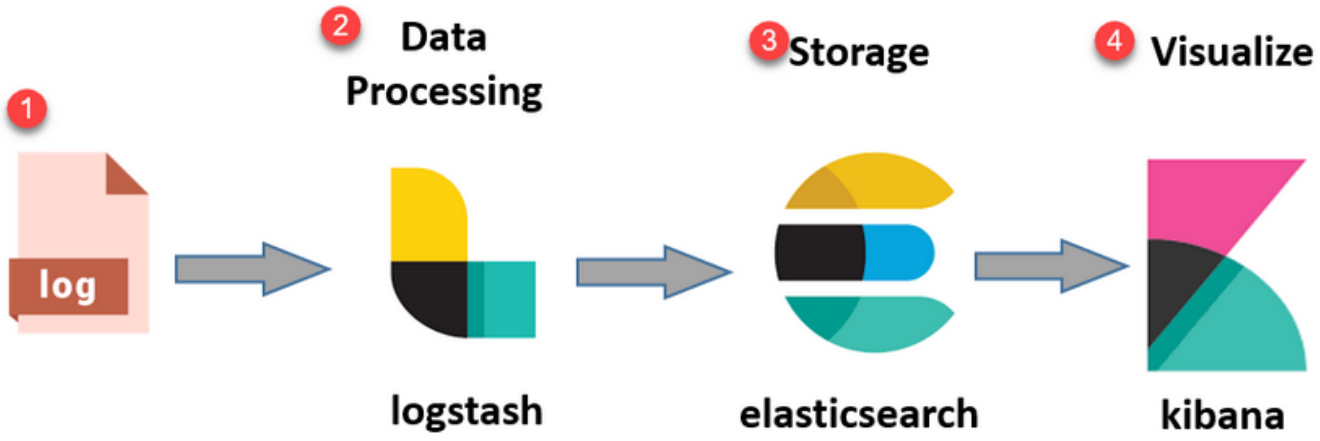
ELK Stack은 대량의 데이터를 수집, 처리 및 시각화하는 데 사용되는 널리 사용되는 오픈 소스 소프트웨어 스택입니다. Elasticsearch, Logstash, Kibana의 약자입니다.

- Elasticsearch: Elasticsearch는 분산형 검색 및 분석 엔진입니다. 대량의 데이터를 거의 실시간으로 신속하게 저장, 검색 및 분석하도록 설계되었습니다. JSON 기반 쿼리 언어를 사용하며 확장성이 뛰어납니다.

- Logstash: Logstash는 여러 소스에서 데이터를 수집, 처리 및 변환하는 데이터 처리 파이프라인입니다. 데이터를 구문 분석하고 강화하여 더 구조화되고 분석에 적합하도록 만들 수 있습니다. Logstash는 다양한 입력 소스 및 출력 대상을 지원합니다.

- 키바나: 키바나는 Elasticsearch와 연동되는 데이터 시각화 플랫폼입니다. 사용자는 인터랙티브 대시보드, 차트, 그래프 및 시각화를 생성하여 Elasticsearch에 저장된 데이터를 탐색하고 이해할 수 있습니다. 키바나의 인터페이스를 통해 데이터를 쉽게 쿼리하고 시각화할 수 있습니다.

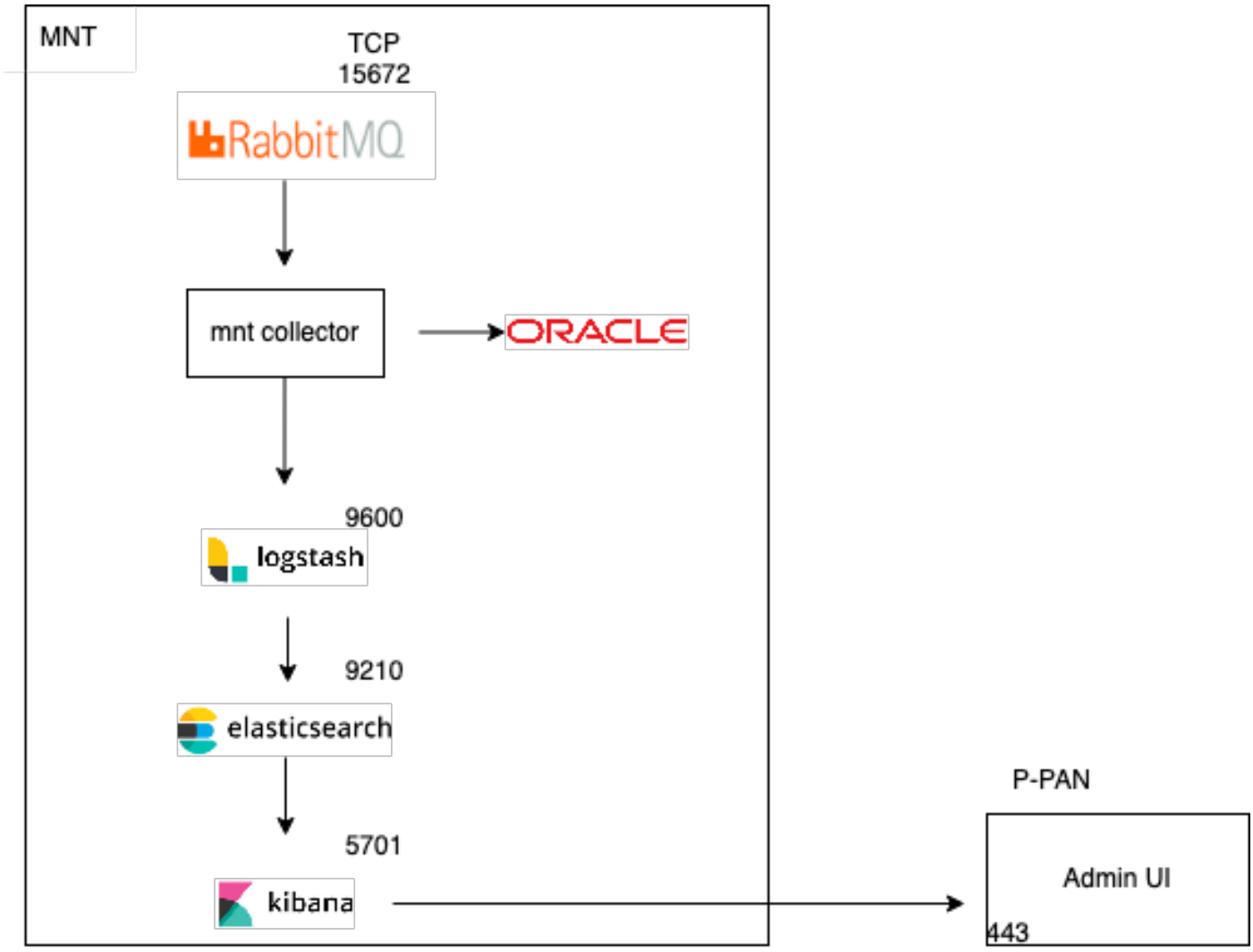
이러한 구성 요소를 결합하면 로그 파일에서 메트릭에 이르기까지 다양한 유형의 데이터를 관리하고 분석하는 동시에 정보를 파악할 수 있는 시각화 기능을 제공할 수 있는 강력한 스택을 형성합니다.



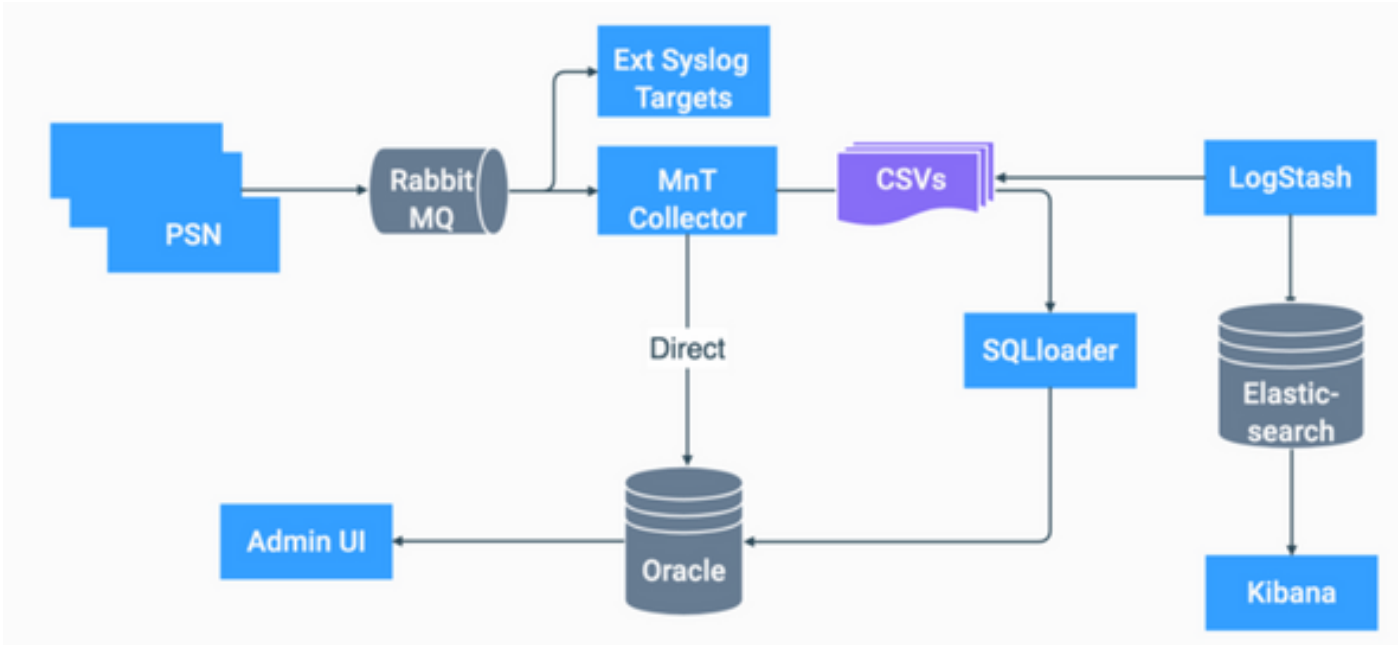
ELK 스택 흐름

로그 분석으로서의 ELK 스택

- 별도의 ElasticSearch+LogStash+Kibana 스택 인스턴스가 MnT 노드에서만 실행되고 있습니다.
  - 이는 Context-Visibility의 Elasticsearch와 상관관계가 없습니다.
  - ELK 7.17 실행
- 기본 및 보조 MNT에는 ELK의 개별 인스턴스가 있습니다.
  - Kibana가 사용 가능한 경우 보조 MNT에서만 활성화되며 이 노드의 데이터만 표시합니다.
- 로그 분석은 기본적으로 비활성화되어 있습니다.
- Oracle 자원을 소비합니다.
- 최대 7일의 데이터를 저장합니다.
- Log Analytics에서 사용하는 총 데이터 크기는 10GB로 제한됩니다.
  - 한계에 도달하면 ElasticSearch에서 데이터를 삭제합니다.



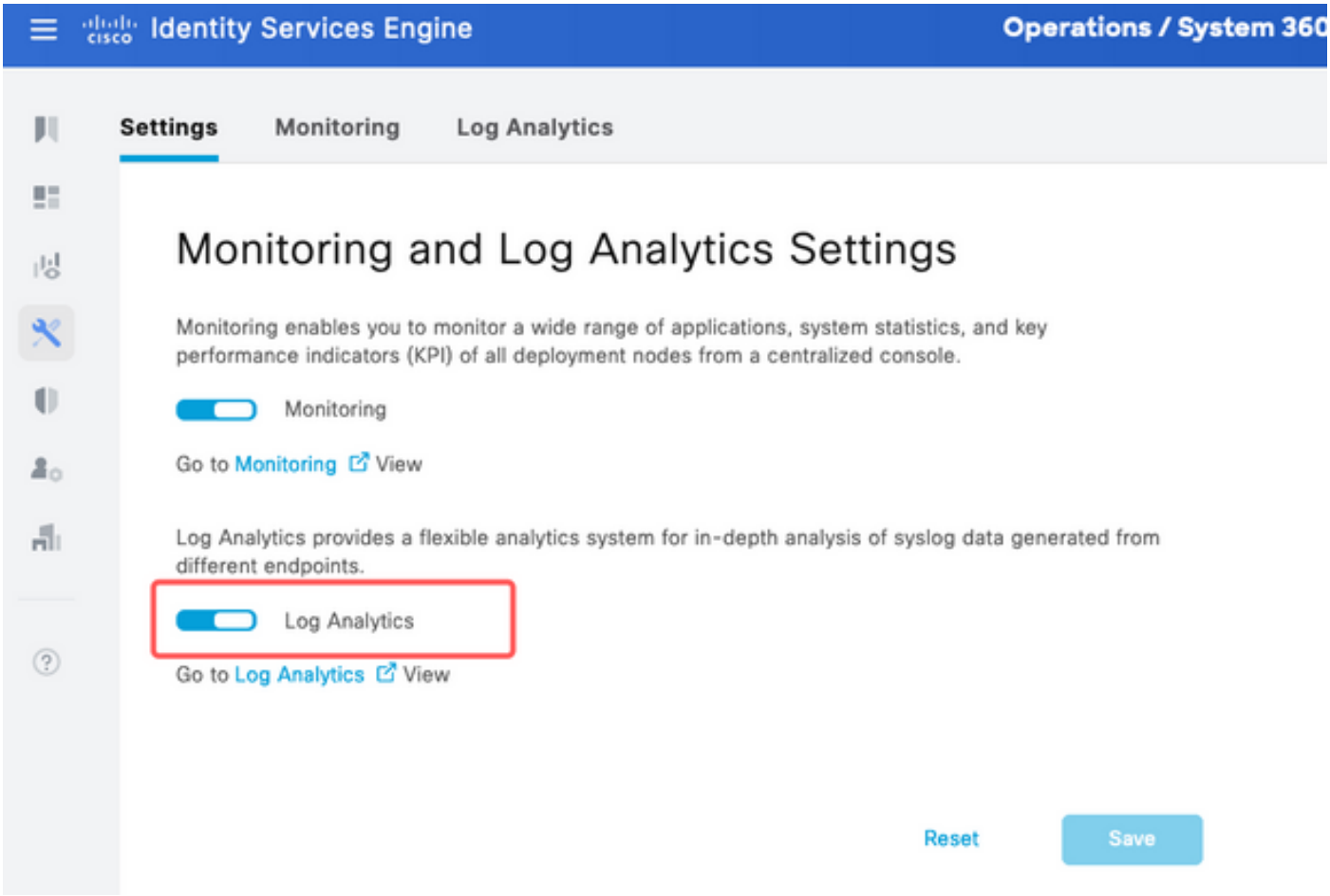
로그 분석으로서의 ELK 흐름



ISE의 ELK 순서도

로그 분석 사용

로그 분석은 ISE에서 기본적으로 비활성화되어 있습니다. 활성화하려면 Operations > System 360 > Settings 그림에 표시된 것과 같습니다.



로그 분석 사용

ISE는 ELK 스택을 초기화하는 데 약 1분이 소요되며, show app stat ise.

또한 루트에서 컨테이너 상태를 확인할 수 있습니다.

<#root>

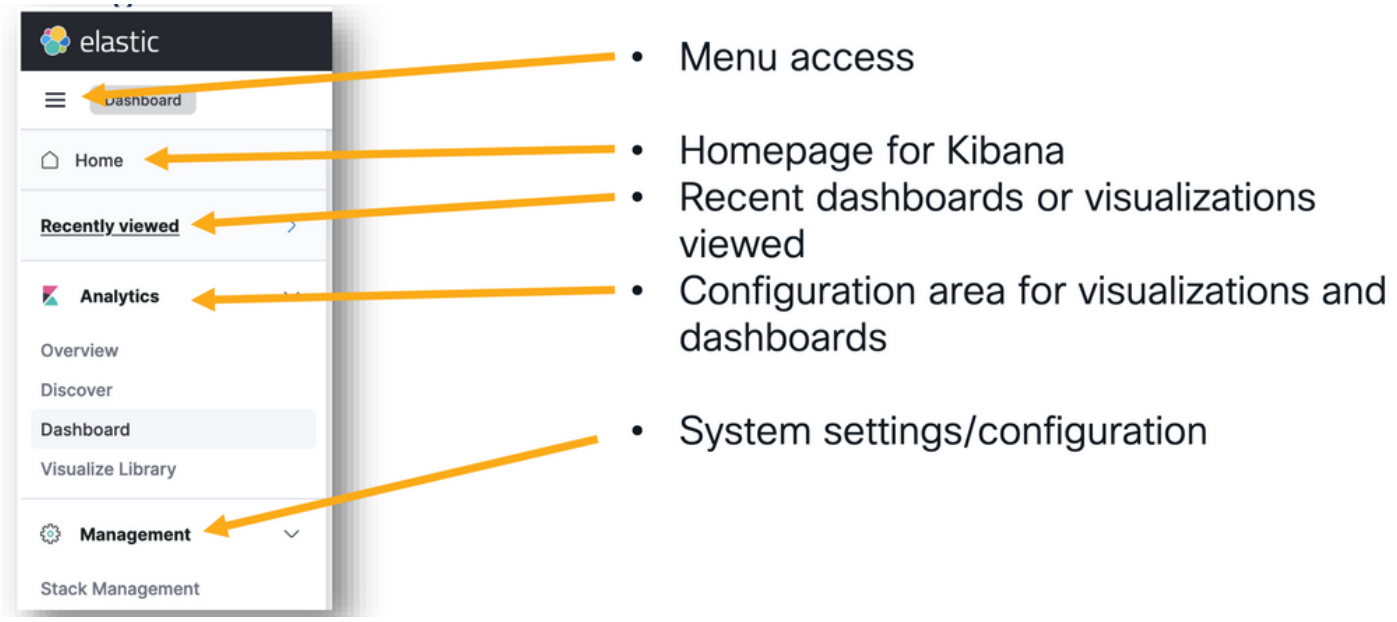
admin#show application status ise

```
ISE PROCESS NAME STATE PROCESS ID
--------------------------------------------------------------------
Database Listener running 7708
Database Server running 132 PROCESSES
Application Server running 551493
Profiler Database running 14281
ISE Indexing Engine running 553168
AD Connector running 41413
M&T Session Database running 26017
M&T Log Processor running 33547
Certificate Authority Service running 41230
```

```
EST Service running 659568
SXP Engine Service disabled
TC-NAC Service disabled
PassiveID WMI Service disabled
PassiveID Syslog Service disabled
PassiveID API Service disabled
PassiveID Agent Service disabled
PassiveID Endpoint Service disabled
PassiveID SPAN Service disabled
DHCP Server (dhcpd) disabled
DNS Server (named) disabled
ISE Messaging Service running 10937
ISE API Gateway Database Service running 13294
ISE API Gateway Service running 586762
ISE pxGrid Direct Service running 637606
Segmentation Policy Service disabled
REST Auth Service disabled
SSE Connector disabled
Hermes (pxGrid Cloud Agent) disabled
McTrust (Meraki Sync Service) disabled
ISE Node Exporter running 44422
ISE Prometheus Service running 47890
ISE Grafana Service running 51094

ISE MNT LogAnalytics Elasticsearch running 611684


ISE Logstash Service running 614339


ISE Kibana Service running 616064


ISE Native IPSec Service running 75883
MFC Profiler running 651910
```

탐색 메뉴

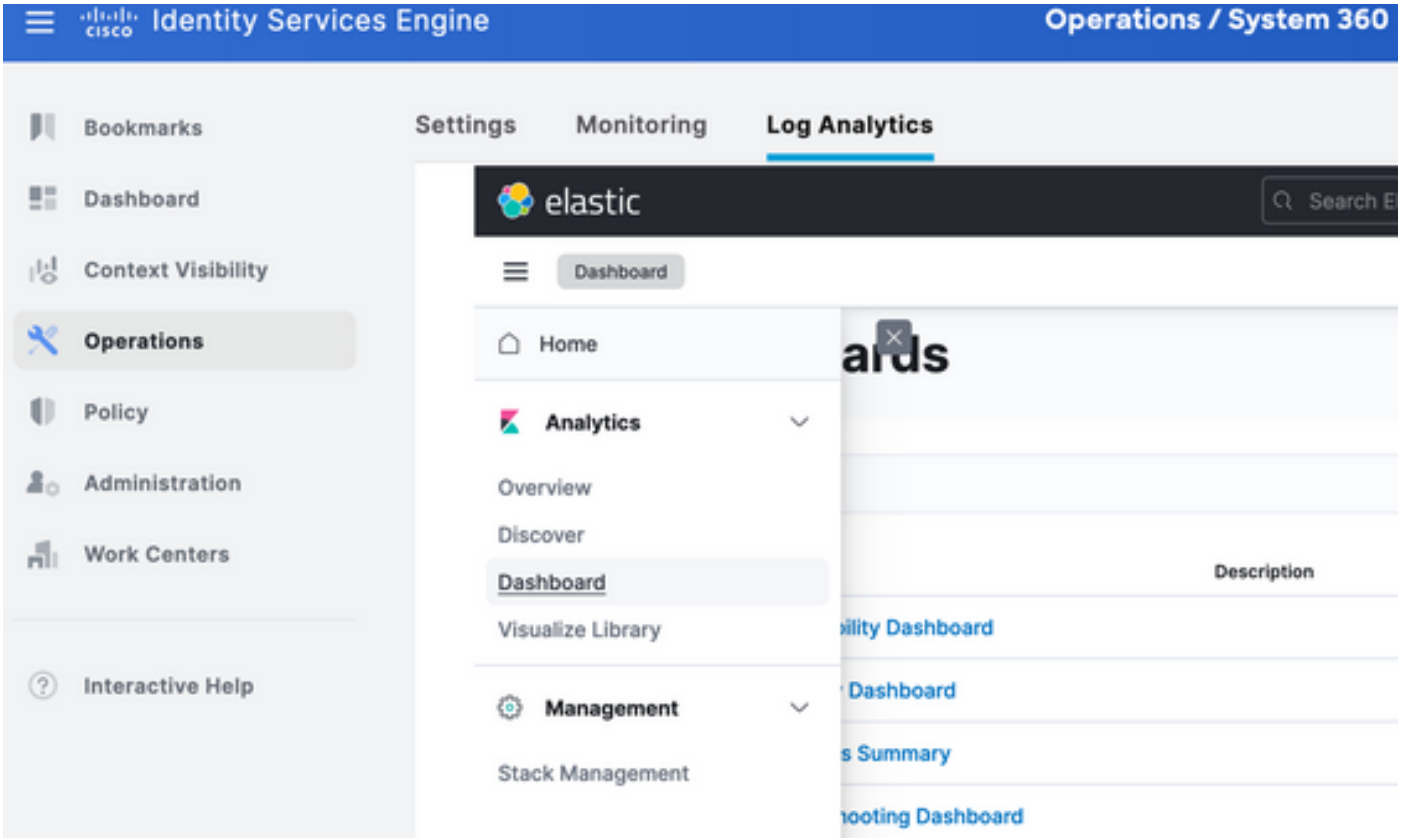
ELK 서비스가 시작되면 Elastic Navigation 메뉴에 액세스할 수 있습니다.



탐색 메뉴

내장 대시보드

- ISE에는 기본적으로 Radius, TACACS, 시스템 성능 및 ISE 관찰 기능의 데이터가 포함된 내장 대시보드가 있습니다.
- 이러한 대시보드는 Operations > Log Analytics .
  - Elastic UI가 열리면 Sandwich Menu > Analytics > Dashboards .



내장 대시보드

- ISE 3.3에서 사용 가능한 대시보드

Title	Description	Tags	Actions
ISE Observability Dashboard			
ISE Overview Dashboard			
ISE Processes Summary			
ISE Troubleshooting Dashboard			
Profiler Performance			
Profiler Summary			
RADIUS Accounting Summary			
RADIUS Authentication Summary			
RADIUS Performance			
RADIUS Step Latency			
TACACS Accounting Summary			
TACACS Authentication Summary			

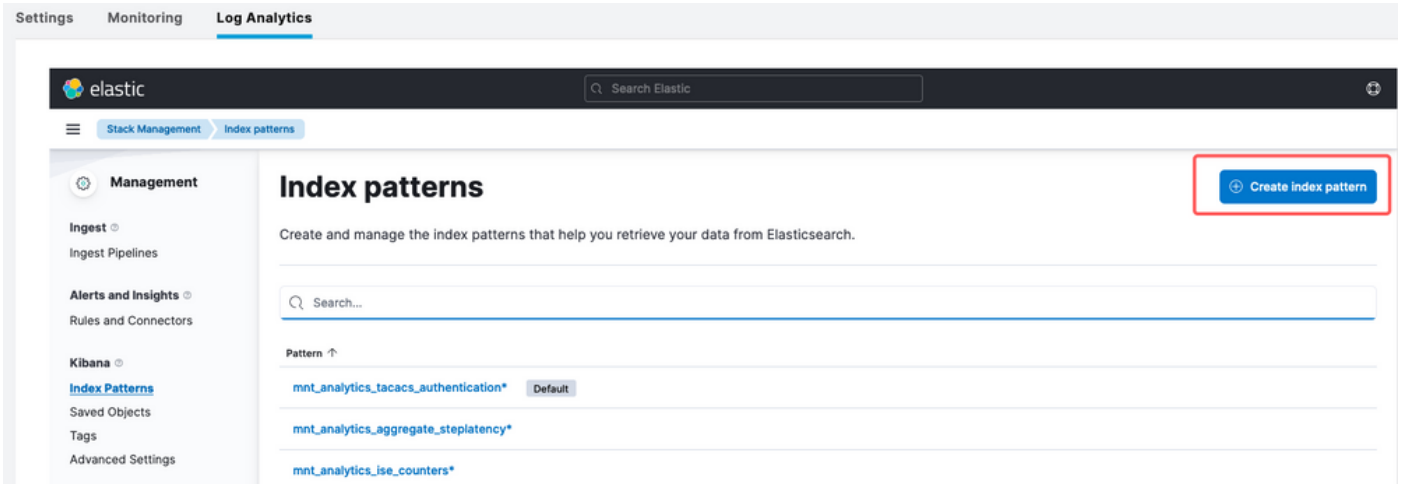
ISE 3.3 로그 분석 대시보드

새 대시보드 생성

1단계. 인덱스 패턴 생성(데이터 소스)

키바나에서 "인덱스 패턴"은 키바나가 하나 이상의 Elasticsearch 인덱스와 상호 작용하는 방법을 정의할 수 있는 구성입니다.

탐색 Management > Stack Management > Kibana > Index Patterns을 클릭하고 Create Index Pattern 그림에 표시된 것과 같습니다.



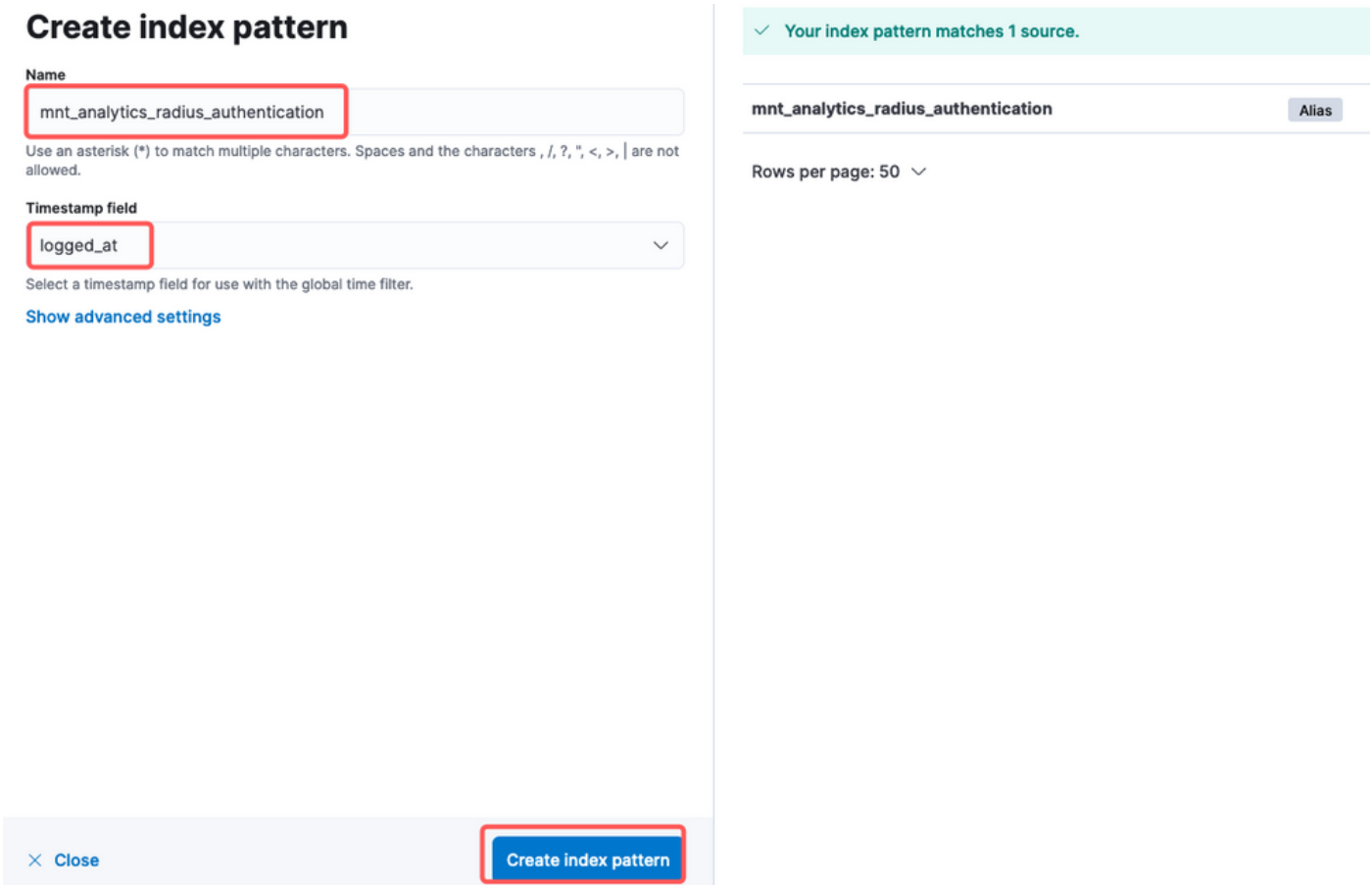
인덱스 패턴 만들기

다음 창에는 ISE에서 사용 가능한 모든 인덱스가 나열되어 있습니다.

- 원하는 인덱스의 이름을 입력합니다. 정확한 일치 또는 와일드카드(*)가 될 수 있습니다.
- Timestamp 필드, logged_at, logged_at_timezone 또는 "I don't want to use time filter"를 선택

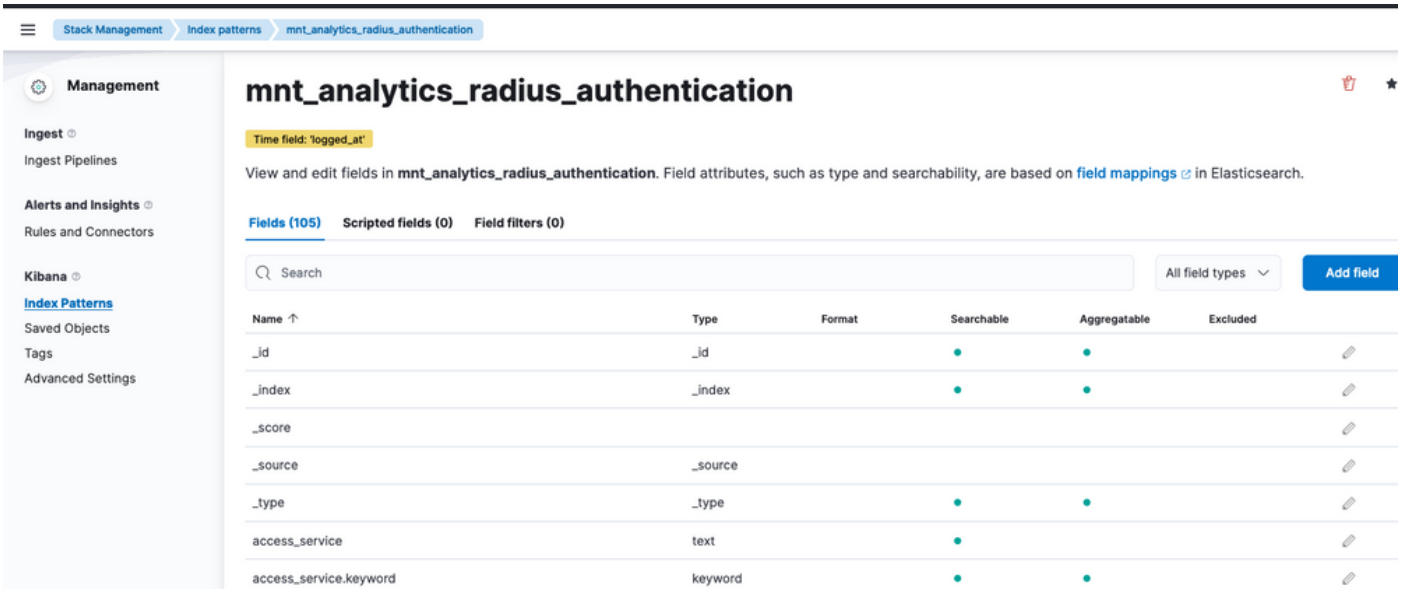
합니다.

- 그런 다음 Create index pattern.



인덱스 선택

작성된 인덱스는 나중에 시각화를 작성하는 데 사용할 수 있는 모든 관련 변수를 나열합니다.



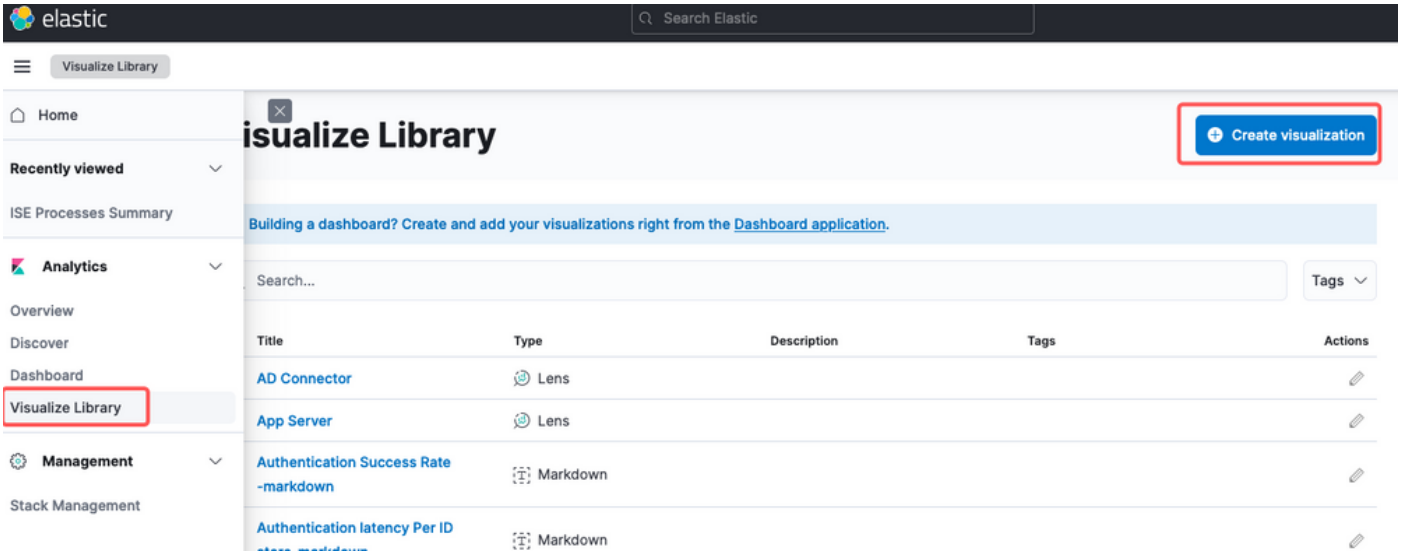
인덱스 변수

2단계. 시각화 만들기

키바나에서 "시각화"는 데이터를 그래픽으로 나타냅니다. Elasticsearch에 저장된 데이터를 가져와서 의미 있는 차트, 그래프, 다이어그램으로 바꾸어 더 쉽게 이해하고 분석할 수 있습니다. 다음과 같은 몇 가지 일반적인 시각화 유형을 만들 수 있습니다.

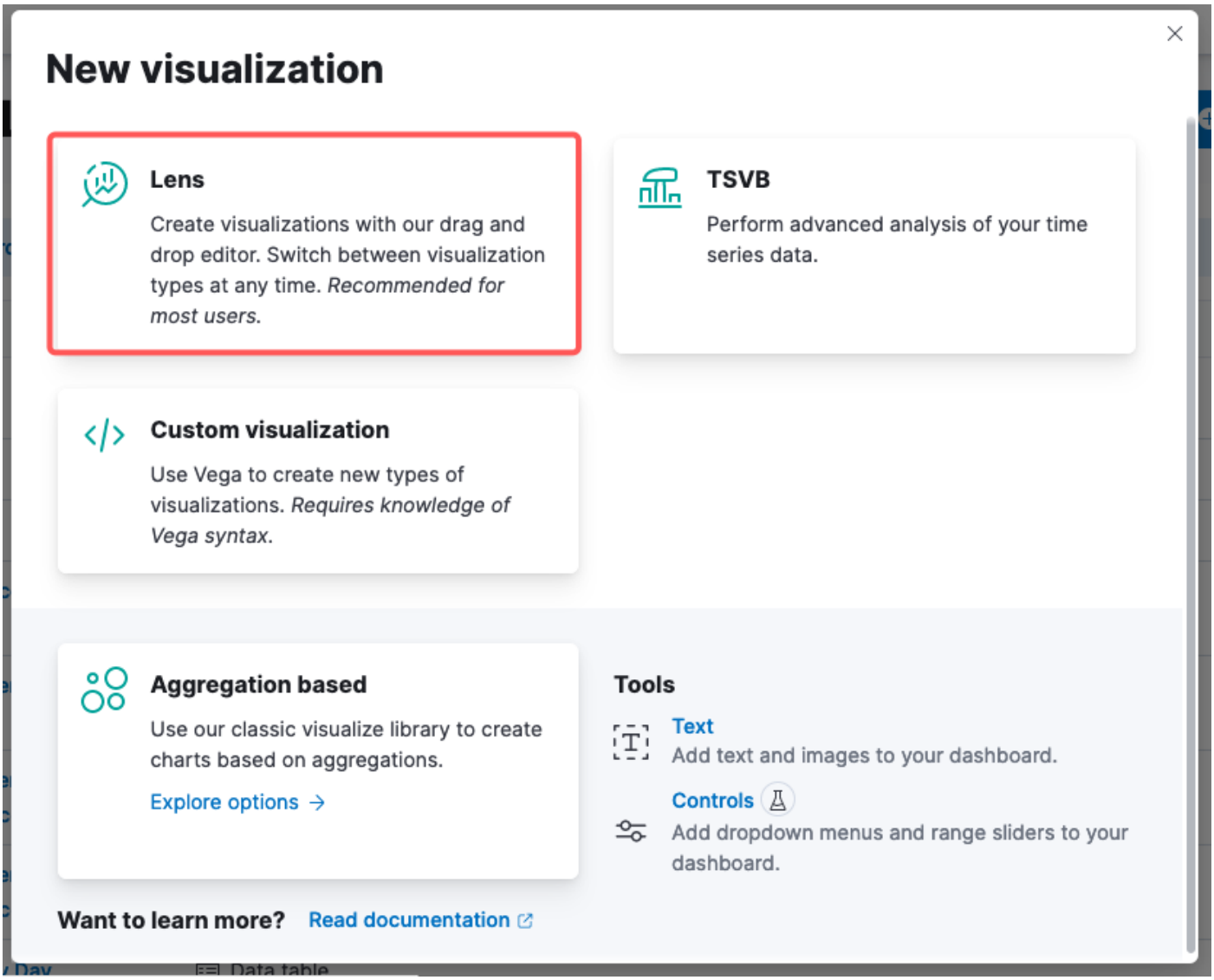
- 렌즈: 드래그 앤 드롭 편집기로 시각화를 만듭니다. 권장.
- 막대형 차트: 세로 막대로 데이터를 표시하여 범주 또는 시간 간격 간에 값을 쉽게 비교할 수 있습니다.
- 라인 차트: 라인 차트는 데이터를 라인으로 연결된 일련의 데이터 포인트로 표시합니다. 이러한 기능은 시간에 따른 트렌드를 시각화하는 데 유용합니다.
- 원형 차트: 원형 차트는 원형 그래프로 데이터를 나타내며, 원형의 각 세그먼트는 범주를 나타내고 세그먼트의 크기는 해당 비율을 나타냅니다.
- 영역 차트: 라인 차트와 비슷하게 영역 차트에도 시간에 따른 추세가 표시되지만 라인 아래 영역을 채우므로 변경 사항을 더 쉽게 확인할 수 있습니다.
- 히트 맵: 히트 맵은 색상을 사용하여 데이터 값을 행렬이나 격자로 나타냅니다. 이러한 필터는 데이터의 농도나 변화를 표시하는 데 유용합니다.
- 메트릭스 시각화: 카운트 또는 평균과 같은 단일 숫자 값을 표시합니다. KPI(핵심 성과 지표)를 표시하는 데 자주 사용됩니다.
- 데이터 테이블: 데이터 테이블은 테이블 형식으로 원시 데이터를 표시하므로 자세한 정보를 보고 데이터를 정렬 또는 필터링할 수 있습니다.
- 히스토그램: 히스토그램은 데이터를 빈 또는 간격으로 나누고 각 빈의 데이터 포인트 빈도 또는 개수를 표시합니다. 데이터 배포를 이해하는 데 유용합니다.
- 좌표 맵: 이러한 기능은 지리공간 데이터를 시각화하여 데이터를 맵에 표시하고 다양한 마커, 색상 또는 크기를 사용하여 데이터 속성을 나타낼 수 있도록 합니다.
- 태그 클라우드: 태그 클라우드는 단어 빈도를 표시하며 각 단어의 크기는 데이터 집합의 중요도나 빈도를 나타냅니다.

탐색 Analytics > Visualize Library 을 클릭한 다음 Create Visualization 그림에 표시된 것과 같습니다.



시각화 만들기

기본 설정의 시각화를 선택합니다. 이 예제에서는 실용성을 위해 렌즈가 선호됩니다.



시각화 유형 선택

키바나 렌즈, 탐색 항목은 다음으로 구성됩니다.

- 데이터 소스 선택: 왼쪽 패널에서 시각화에 사용할 데이터 소스 또는 Elasticsearch 인덱스 패턴을 선택할 수 있습니다.
- Visualization Canvas: 중앙 영역은 필드를 끌어서 놓고, 차트 유형을 선택하고, 차트 설정을 구성하여 시각화를 작성하는 위치입니다.
- 시각화 도구 모음: 캔버스의 맨 위에서 차트 유형 변경, 필터 추가, 차트 설정 구성 옵션 등 시각화를 사용자 정의할 수 있는 도구 모음을 찾을 수 있습니다.

- 데이터 패널: 오른쪽에서 데이터 변환, 집계 및 필드 설정을 관리할 수 있는 "데이터" 패널에 액세스할 수 있습니다.

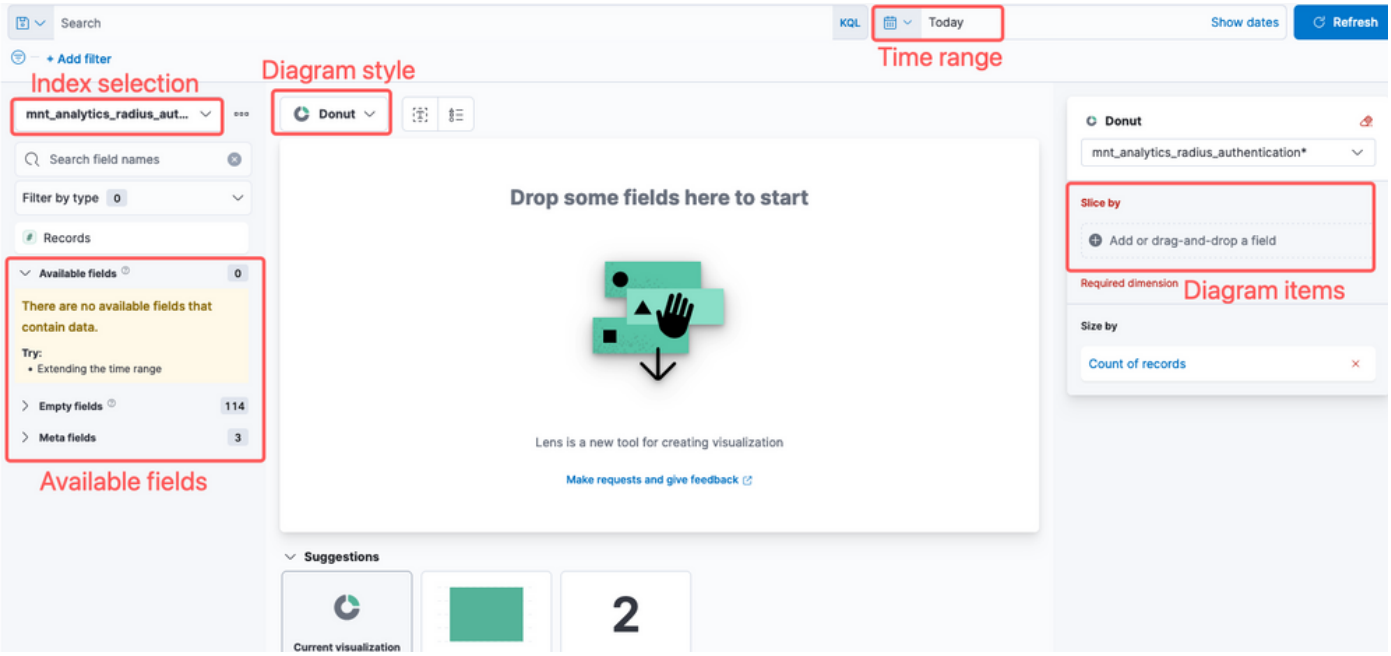
- 레이어 관리: 생성 중인 시각화의 유형(예: 계층화된 차트)에 따라 시각화에서 여러 레이어를 구성하기 위한 레이어 관리 영역을 가질 수 있습니다.

- 미리 보기: 시각화를 변경할 때 일반적으로 실시간 미리 보기가 제공되므로 현재 설정을 사용하여 차트가 어떻게 표시되는지 볼 수 있습니다.

- 시각 형상 설정: 선택한 차트 유형에 따라 축 구성, 색 구성표, 레이블 등 시각 형상 유형의 특

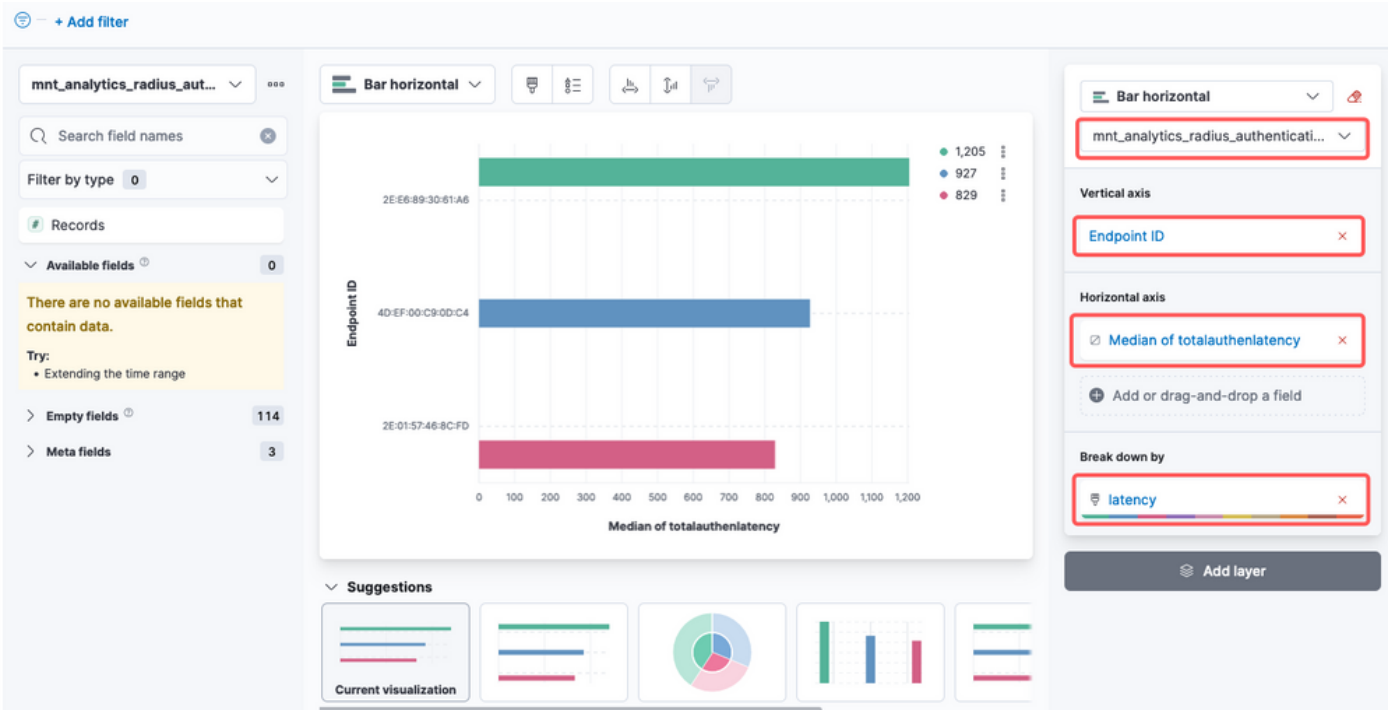
정 설정에 액세스할 수 있습니다.

- Interactivity Settings: 사용자가 데이터를 필터링하거나 Kibana 대시보드의 다른 부분으로 이동할 수 있도록 상호 작용과 작업을 시각화에 추가할 수 있습니다.
- 저장 및 공유: Lens 인터페이스의 상단에는 일반적으로 시각화를 저장하거나 대시보드에 추가하거나 다른 사람과 공유하는 옵션이 있습니다.

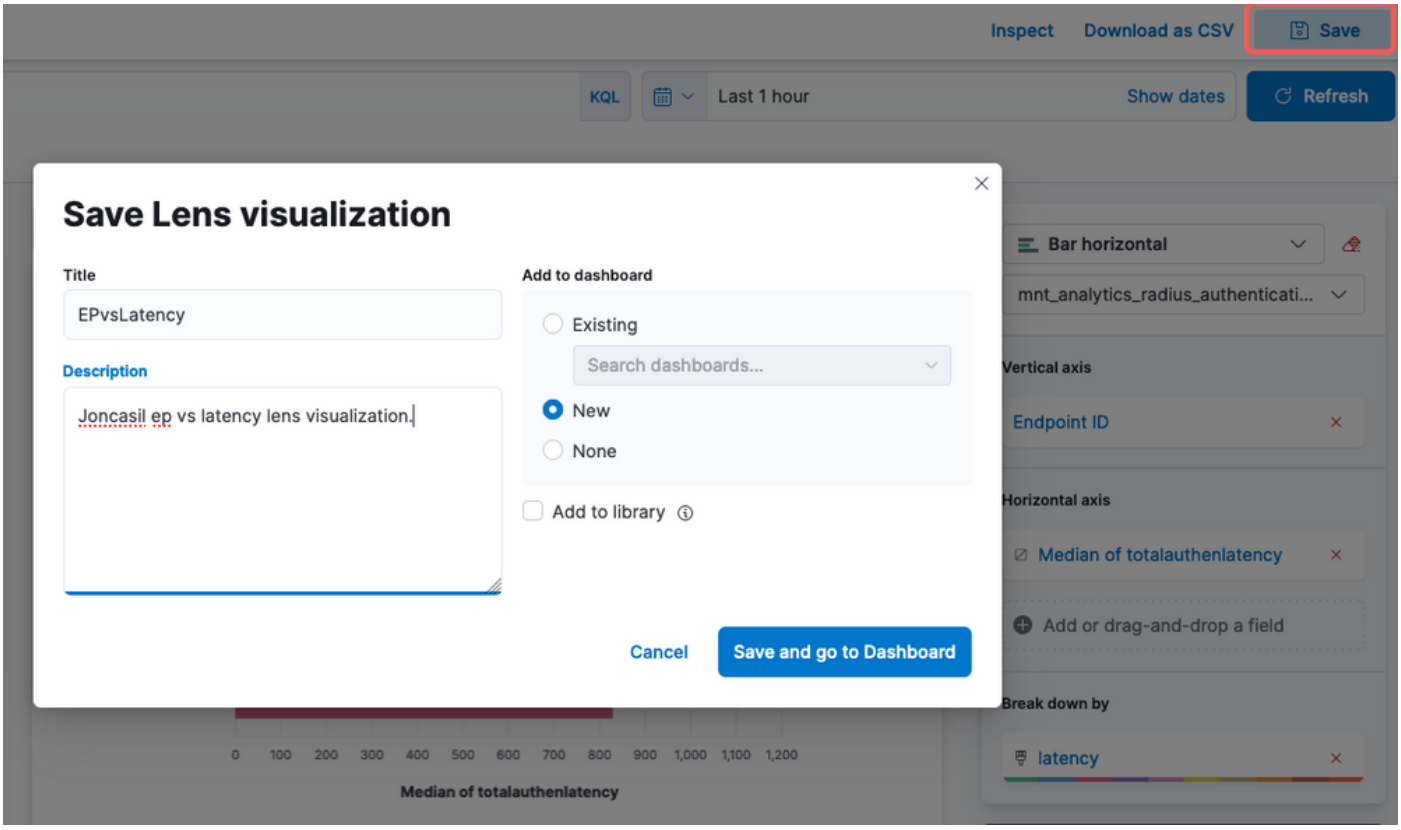


렌즈 시각화

Cisco 버그 ID CSCwh48057로 인해 왼쪽 패널에 사용 가능한 필드가 표시되지 않습니다. 그러나 오른쪽에서 필수 필드와 다이어그램 스타일을 선택할 수 있습니다. 이 예에서는 인증 레이턴시가 일반적인 관심 주제이므로 인증 레이턴시와 엔드포인트 ID를 시각화하기 위해 그래프를 구축합니다.



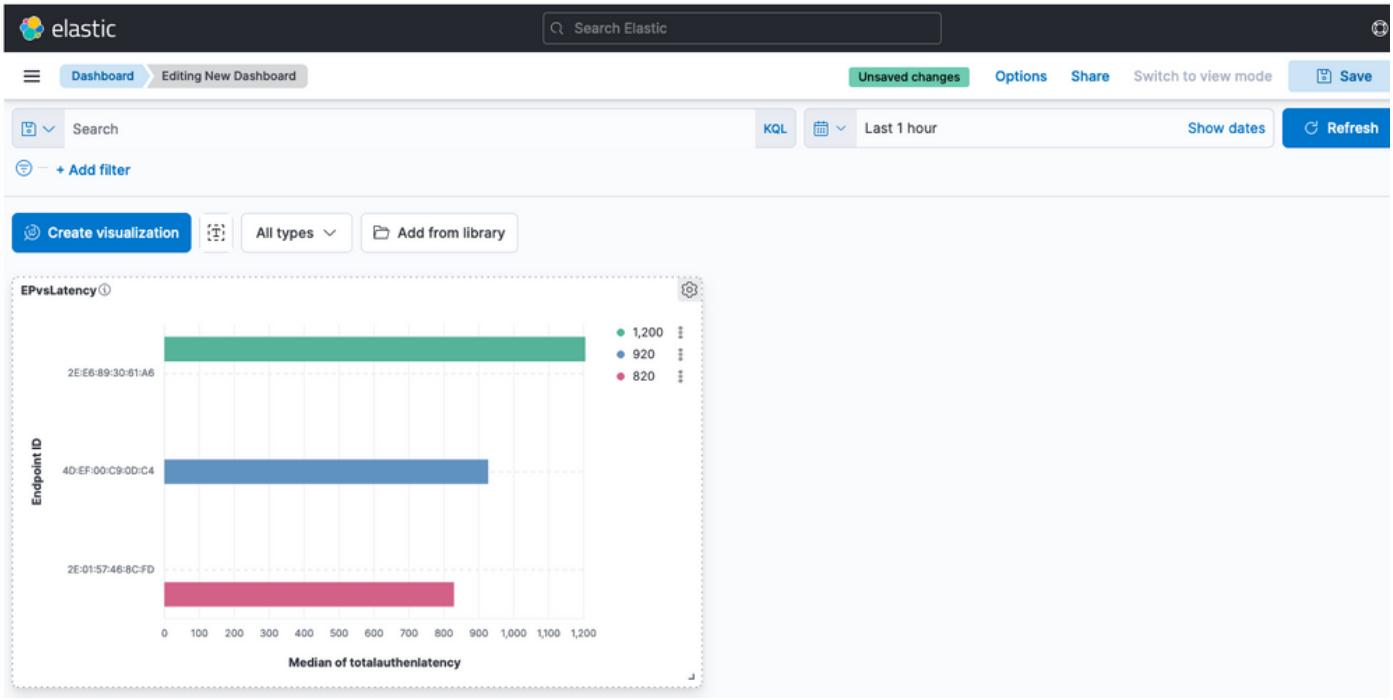
작업을 마치면 Save 오른쪽 구석에 있는 단추를 클릭합니다.



시각화 저장

3단계. 대시보드 만들기

새 시각화는 자동으로 새 대시보드에 추가됩니다. Kibana Dashboards를 사용하면 Elasticsearch 인덱스에 저장된 데이터를 기반으로 대화형 시각화 및 보고서를 만들고, 사용자 지정하고, 공유할 수 있다는 점을 기억하십시오.



새 대시보드

문제 해결

- MNT에서 ELK 스택 서비스가 실행 중인지 확인합니다.
- Kibana, Logstash 및 Elasticsearch가 컨테이너에서 실행되므로 로그는 다음 위치에서 찾을 수 있습니다.

```
admin#show logging application ise-kibana/kibana.log
admin#show logging application ise-logstash/logstash.log
admin#show logging application mnt-la-elasticsearch/mnt-la-elasticsearch.log
```

관련 정보

- ISE 3.3 관리 설명서
- 키바나 문서
- Cisco 기술 지원 및 다운로드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.