

AWS Elasticsearch 생성

Amazon ES 도메인을 만들려면(콘솔)

1. 배포 유형 선택

1. 배포 유형 : 개발 및 테스트

2. 버전 : 7.10 (latest)

Elasticsearch 도메인 생성

Step 1: 배포 유형 선택
Step 2: 도메인 구성
Step 3: 액세스 및 보안 구성
Step 4: 태그 추가 - 선택 사항
Step 5: 검토

배포 유형 선택

배포 유형은 사용 사례에 대한 공통 설정을 지정합니다. 도메인을 만든 후에 언제든지 이 설정을 변경할 수 있습니다.

배포 유형

- ☐ 프로덕션
동작한 성능을 위해 여러 가용 영역 및 전용 EC2 인스턴스
- ☒ 개발 및 테스트
Elasticsearch 엔드포인트로 필요한 경우 1개 가용 영역
- ☐ 사용자 지정
사용 가능한 모든 옵션에서 설정 선택

버전

도메인에 대한 Elasticsearch 버전을 선택합니다.

Elasticsearch 버전 7.10 (latest)

취소 다음

2. 도메인 구성

1. Elasticsearch domain name : managed-es

2. 사용자 지정 엔드포인트 : 비활성

3. 자동 튜닝 : 활성

Elasticsearch 도메인 생성

Step 1: 배포 유형 선택
Step 2: 도메인 구성
Step 3: 액세스 및 보안 구성
Step 4: 태그 추가 - 선택 사항
Step 5: 검토

도메인 구성

도메인은 Elasticsearch를 실행하는 데 필요한 리소스 모음입니다. 도메인 이름은 도메인 엔드포인트의 일부가 됩니다.

Elasticsearch 도메인 이름 managed-es

이름은 소문자로 시작해야 하며 3-28자여야 합니다. 유효한 문자는 a-z, 숫자, hyphen(-)입니다.

사용자 지정 엔드포인트

각 Amazon Elasticsearch Service 도메인은 자동 생성된 엔드포인트가 있지만 쉽게 참조할 수 있도록 사용자 지정 엔드포인트를 정의하고 AWS Certificate Manager(ACM)의 인증서를 링크할 수도 있습니다. 자세히 알아보기

사용자 지정 엔드포인트 활성화

자동 튜닝

자동 튜닝은 시간 경과에 따른 클러스터 성능을 분석하고 워크로드에 따른 최적화를 제안합니다. 언제든지 이러한 변경 사항을 배포하거나 기존 Amazon ES 설정으로 롤백하도록 선택할 수 있습니다. 자세히 알아보기

자동 튜닝

- ☐ 비활성화
클러스터에 대한 자동 변경 사항은 없습니다. Amazon ES는 클러스터 성능을 최적화하는 방법에 대한 권장 사항을 계속 전송합니다.
- ☒ 활성화
대기할 수 있는 크기 튜닝 등 자동 튜닝이 필요한 모든 EC2 인스턴스의 변경을 자동으로 수행합니다.

유지 관리 기간

- ☐ 유지 관리 기간 추가
일부 최적화에는 클러스터 성능에 영향을 줄 수 있는 플러그인 배포가 필요합니다. 자동 튜닝이 이러한 배포를 시작하려면 최적화가 낮은 시간을 지정합니다.

4. 데이터 노드

1. 인스턴스 유형 : r6g.large.elasticsearch

2. 노드 수 : 3

5. 데이터 노드 스토리지

1. 데이터 노드 스토리지 유형 : EBS

2. EBS 볼륨 유형 : 일반용(SSD)

3. 노드당 EBS 스토리지 크기 : 100

6. 전용 마스터 노드 : 비활성

데이터 노드

에플리케이션의 실행된, 메모리 및 스토리지 요구 사항에 해당하는 인스턴스 유형을 선택합니다. Elasticsearch 인덱스의 크기, 사드 및 복제본 수, 처리 유형 및 요청 볼륨을 고려합니다. 자세히 알아보기

인스턴스 유형 **r5g.large.elasticsearch (기본값)**
r5g.large.elasticsearch 인스턴스 유형은 EBS 스토리지가 필요합니다.

노드 수 **3**

데이터 노드 스토리지

데이터 노드의 스토리지 유형을 선택합니다. EBS 스토리지 유형을 선택한 경우 클러스터에서 사용 가능한 총 스토리지 크기 계산을 위해 노드당 EBS 스토리지 크기에 클러스터의 작업자 데이터 노드 수를 곱합니다. 스토리지 설정은 클러스터의 전용 마스터 노드에 적용되지 않습니다.

데이터 노드 스토리지 유형 **EBS**

EBS 볼륨 유형* **일반형(SSD)**

노드당 EBS 스토리지 크기* **100**
총 클러스터의 크기는 300GB입니다(EBS 볼륨 크기 x 인스턴스 수).

전용 마스터 노드

전용 마스터 노드는 도메인의 안정성을 향상시킵니다. 프로덕션 도메인의 경우 3개를 권장합니다.

☒ 전용 마스터 노드 ☐ 활성화

인스턴스 유형 **r5g.large.elasticsearch (기본값)**

3. 액세스 및 보안 구성

1. 네트워크 구성 : vpc 액세스

1. vpc, subnet, security group 설정

Elasticsearch 도메인 생성

Step 1: 배포 유형 선택
Step 2: 도메인 구성
Step 3: 액세스 및 보안 구성
Step 4: 태그 추가 - 선택 사항
Step 5: 검토

액세스 및 보안 구성

Amazon Elasticsearch Service는 세분화된 액세스 제어, IAM, SAML, Kibana용 Cognito 인증, 암호화 및 VPC 액세스를 비롯한 다양한 보안 기능을 제공합니다. 자세히 알아보기

네트워크 구성

인터넷 또는 VPC 액세스를 선택하십시오. VPC 액세스를 활성화하려면 기본적으로 보안을 제공하는 VPC의 프라이빗 IP 주소를 사용합니다. 보안 그룹을 사용하는 VPC의 네트워크 액세스를 제어합니다. 제한적 액세스를 적용하여 보안 계층을 더 추가할 수도 있습니다. 인터넷 엔드포인트에 공개적으로 액세스할 수 있습니다. 퍼블릭 액세스를 선택하면 특정 사용자의 IP 주소만 도메인에 액세스하도록 허용하는 액세스 정책으로 도메인을 보호해야 합니다.

☒ VPC 액세스 (권장)
☐ 퍼블릭 액세스

VPC **[선택된 VPC]**

서브넷 **[선택된 서브넷]**

보안 그룹 **하나 이상의 보안 그룹 선택**
[선택된 보안 그룹]

IAM 역할 **AWS::ServiceRole::AmazonElasticsearchService**

세분화된 액세스 제어 - Elasticsearch용 Open Distro 제공

세분화된 액세스 제어는 데이터 보안을 유지하는 데 도움이 되는 다양한 기능을 제공합니다. 이러한 기능에는 문서 수준 보안, 필드 수준 보안, 읽기 전용 Kibana 사용자 및 Kibana 태넌트를 포함합니다. 세분화된 액세스 제어에는 마스터 사용자가 필요합니다.

2. 세분화된 액세스 제어

1. 세분화된 액세스 제어 : 활성화

2. 마스터 사용자 생성 : 활성화

1. 마스터 사용자 이름 : elastic

2. 마스터 암호 : Bospin12!

IAM 역할 **AWS::ServiceRole::AmazonElasticsearchService**

세분화된 액세스 제어 - Elasticsearch용 Open Distro 제공

세분화된 액세스 제어는 데이터 보안을 유지하는 데 도움이 되는 다양한 기능을 제공합니다. 이러한 기능에는 문서 수준 보안, 필드 수준 보안, 읽기 전용 Kibana 사용자 및 Kibana 태넌트를 포함합니다. 세분화된 액세스 제어에는 마스터 사용자가 필요합니다.

ARN을 사용하여 IAM 계정에 마스터 사용자를 설정하거나, 마스터 사용자 이름 및 암호를 생성하여 Elasticsearch 내부 데이터베이스에 마스터 사용자를 저장합니다. 도메인이 설정된 후 Kibana 또는 REST API를 사용하여 사용자 및 권한을 추가로 구성할 수 있습니다. 자세히 알아보기

☒ 세분화된 액세스 제어 활성화

☐ IAM ARN을 마스터 사용자로 설정
IAM ARN을 마스터 사용자로 선택하면 도메인에서는 IAM 역할 및 사용자만 사용하여 인증합니다. Kibana가 액세스하려면 SAML 또는 Amazon Cognito 인증을 활성화해야 합니다.

☒ 마스터 사용자 생성
마스터 사용자를 생성하면 도메인의 내부 사용자 데이터베이스가 HTTP 기본 인증을 사용합니다.

마스터 사용자 이름 **elastic**
마스터 사용자 이름은 1-16자여야 합니다.

마스터 암호 *********
마스터 암호는 8자 이상이어야 하며 적어도 대문자 하나, 소문자 하나, 숫자 하나 및 특수 문자 하나를 포함해야 합니다.

마스터 암호 확인 *********

Kibana에 대한 SAML 인증

Kibana에 대한 SAML 인증
Kibana에 대한 SAML 인증을 사용하면 기존 자격 증명 공급자를 사용하여 Kibana에 대한 Single Sign-On을 제공할 수 있습니다. [자세히 알아보기](#)

☐ SAML 인증 준비

Amazon Cognito 인증
Kibana에 Amazon Cognito 인증을 사용하면 활성화합니다. Amazon Cognito는 사용자 인증-암호 인증을 위한 다양한 자격 증명 공급자를 지원합니다. [자세히 알아보기](#)

☐ Amazon Cognito 인증 활성화

액세스 정책
액세스 정책은 요청이 Amazon Elasticsearch Service 도메인에 도달할 때 수락 또는 거부되는지 여부를 제어합니다. 이 정책에서 계정, 사용자 또는 역할을 지정하는 경우 요청에 허용해야 합니다. [자세히 알아보기](#)

사용자 지정 정책 빌더는 최대 10개의 요소를 허용합니다. 요소가 10개를 넘는 정책을 정의하려면 JSON 정의 액세스 정책을 사용합니다.

도메인 액세스 정책 도메인에 대한 개방 액세스 허용
AWS 계정 ID, 계정 ARN, IAM 사용자 ARN, IAM 역할 ARN, IPv4 주소 또는 CIDR 블록의 의한 액세스를 허용하거나 거부합니다.

암호화
이러한 기능은 데이터를 보호하는 데 도움이 됩니다. 도메인을 만든 후에는 대부분의 암호화 설정을 변경할 수 없습니다.

암호화 ☒ 도메인으로 전송되는 모든 트래픽에 HTTPS 필요 ⓘ

☒ 노드 간 암호화 ⓘ

4. **Data nodes(데이터 노드)**에서 **c5.large.elasticsearch** 인스턴스 유형을 선택합니다. 기본값인 인스턴스 1개를 사용합니다.

5. **Data nodes storage(데이터 노드 스토리지)**에서 기본값을 사용합니다.

참고 자료