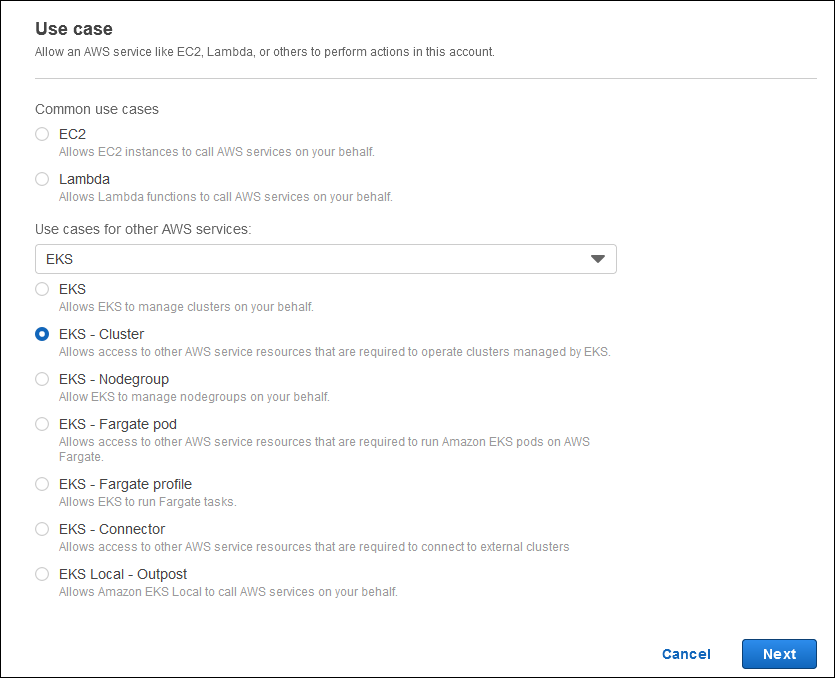
우선 EKS Cluster의 역할을 생성해준다.

 텍스트이(가) 표시된 사진

자동 생성된 설명

텍스트이(가) 표시된 사진

자동 생성된 설명

그리고 Role을 생성해준다. 이제 Control Plane 보안그룹을 생성해주자. (규칙은 나중에 Cluster, Control Plane, Worker Node 보안 그룹들이 모두 생성되고나서 규칙을 작성해줄 것이다.)

텍스트이(가) 표시된 사진

자동 생성된 설명

그리고 EKS Cluster를 생성해주자.

텍스트이(가) 표시된 사진

자동 생성된 설명 텍스트이(가) 표시된 사진

자동 생성된 설명 텍스트이(가) 표시된 사진

자동 생성된 설명

Private Subnet을 선택하고 아까 생성한 control-plane 보안그룹을 선택해준다.

텍스트이(가) 표시된 사진

자동 생성된 설명

그리고 Cluster를 생성해준다. (생성하는데 꾀 많은 시간이 소요된다.)

이제 Kubernetes 서비스 계정에 IAM 리소스에 액세스할 수 있도록 OIDC라는 것을 생성해주자.

우선 EKS Cluster로 가서 OIDC Provider URL을 복사해준다.

텍스트이(가) 표시된 사진

자동 생성된 설명

그리고 IAM으로 이동 후 Identity providers를 추가해주자.

텍스트이(가) 표시된 사진

자동 생성된 설명

텍스트이(가) 표시된 사진

자동 생성된 설명

아까 복사한 OIDC Provider URL을 붙여 넣은 뒤에 Get thumbprint를 눌러서 유효한지 확인해준다.

그리고 Provider를 추가해준다.

이제 Node Group을 생성해주자. 우선 VPC CNI Plugin에 대한 IAM 역할을 생성해줘야한다.

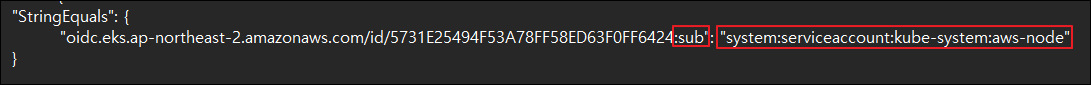
텍스트이(가) 표시된 사진

자동 생성된 설명텍스트이(가) 표시된 사진

자동 생성된 설명텍스트이(가) 표시된 사진

자동 생성된 설명

그리고 아래와 같이 Trusted Entities를 수정해준다.



기존 aud": "sts.amazonaws.com"을 위와 같이 sub": "system:serviceaccount:kube-system:aws-node"로 수정

※ aud와 sub와 같은 형식을 OpenID Connect Core라고 한다. 종류는 아래와 같다

|  |
| --- |
| 1. iss: ID Token을 발급한 ID Provider(example: Google, Facebook) 2. sub: Client 측에서 End-user를 식별할 수 있는 고유한 식별자 3. aud: ID Token이 어떤 Client를 위해 발급된 것인지 4. exp: 만료시점 5. iat: 발급시점  <https://openid.net/specs/openid-connect-core-1_0.html#IDToken> |

이제 EKS 콘솔로 이동해서 서비스 계정에 우리가 만든 CNI 역할을 붙여준다.

텍스트이(가) 표시된 사진

자동 생성된 설명

그리고 업데이트한다.

이제 Node에 대한 IAM 역할을 생성해주자.

텍스트이(가) 표시된 사진

자동 생성된 설명텍스트이(가) 표시된 사진

자동 생성된 설명텍스트이(가) 표시된 사진

자동 생성된 설명

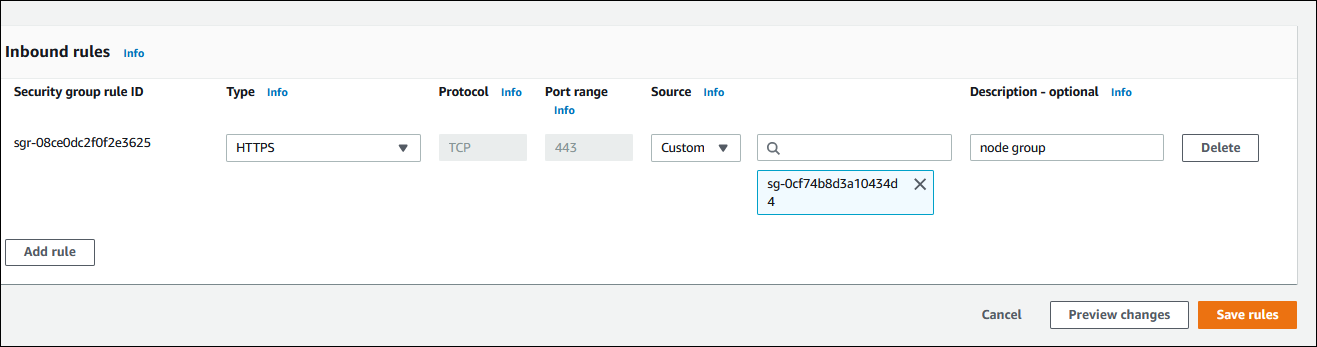
그리고 Node 보안그룹도 생성해준다.

텍스트이(가) 표시된 사진

자동 생성된 설명

이제 보안그룹에 대한 설정을 해주자.

우선 Control Plane에는 아래와 같은 인바운드 규칙을 작성해준다.



그리고 Node Group의 보안그룹에는 아래와 같이 규칙을 작성해준다.

텍스트, 스크린샷, 실내이(가) 표시된 사진

자동 생성된 설명

모든 Node들의 보안그룹에 대해 all로 열고, Control Plane에 대해 443, 1025-65535를 열어준다.

<https://docs.aws.amazon.com/ko_kr/eks/latest/userguide/sec-group-reqs.html>

위 사이트를 참고하여 방화벽을 구성하면 된다.

그러면 이제 Node Group을 생성해보자.

텍스트이(가) 표시된 사진

자동 생성된 설명텍스트이(가) 표시된 사진

자동 생성된 설명텍스트이(가) 표시된 사진

자동 생성된 설명텍스트이(가) 표시된 사진

자동 생성된 설명텍스트이(가) 표시된 사진

자동 생성된 설명

그리고 Node Group을 생성해준다.

이제 Bastion을 통해서 접근이 가능하도록 Cluster 보안그룹에 Bastion에 대한 443 포트를 열어준다.