컨트롤 플레인-노드 간 통신

이 문서는 API 서버와 쿠버네티스 클러스터 사이에 대한 통신 경로의 목록을 작성한다.

이는 사용자가 신뢰할 수 없는 네트워크(또는 클라우드 공급자의 완전한 퍼블릭 IP)에서 클러스터를 실행할 수 있도록 네트워크 구성을 강화하기 위한 맞춤 설치를 할 수 있도록 한다.

노드에서 컨트롤 플레인으로의 통신

쿠버네티스에는 허브 앤 스포크(hub-and-spoke) API 패턴을 가지고 있다.
노드(또는 노드에서 실행되는 파드들)의 모든 API 사용은 API 서버에서 종료된다.
다른 컨트롤 플레인 컴포넌트 중 어느 것도 원격 서비스를 노출하도록 설계되지 않았다.
API 서버는 하나 이상의 클라이언트 인증 형식이 활성화된 보안 HTTPS 포트(일반적으로 443)에서 원격 연결을 수신하도록 구성된다.

특히 익명의 요청 또는 서비스 어카운트 토큰이 허용되는 경우, 하나 이상의 권한 부여 형식을 사용해야 한다.
노드는 유효한 클라이언트 자격 증명과 함께 API 서버에 안전하게 연결할 수 있도록 클러스터에 대한 공개 루트 인증서로 프로비전해야 한다.
kubernetes 서비스(default 네임스페이스의)는 API 서버의 HTTPS 엔드포인트로 리디렉션되는 가상 IP 주소(kube-proxy를 통해)로 구성되어 있다.

컨트롤 플레인에서 노드로의 통신

컨트롤 플레인(API 서버)에서 노드로는 두 가지 기본 통신 경로가 있다.
1) API 서버에서 클러스터의 각 노드에서 실행되는 kubelet 프로세스
2) API 서버의 프록시 기능을 통해 API 서버에서 모든 노드, 파드 또는 서비스에 이르는 것

API 서버에서 kubelet으로의 통신

API 서버에서 kubelet으로의 연결은 다음의 용도로 사용된다.

- 파드에 대한 로그를 가져온다.
- 실행 중인 파드에 (보통의 경우 kubectl을 통해) 연결한다.
- kubelet의 포트-포워딩 기능을 제공한다.