NGINX Ingress Controller®

Ingress-Egress 트래픽에 대한 프로덕션급 (Production-Grade) 제어

Kubernetes 애플리케이션의 보호, 강화 및 확장

CNCF(Cloud Native Computing Foundation)의 2020년 설문조사에 따르면 응답자의 91%가 Kubernetes를 사용하며, 이들 중 83%는 운영 환경에서 사용하고 있는 것으로 나타났습니다. 즉, Kubernetes는 컨테이너화된 애플리케이션을 관리하기 위한 사실상의 표준이 됐습니다.

그러나, 운영 환경에서 Kubernetes를 적용하는 경우, 업무에 치명적인 영향을 미치는 많은 문제들을 겪게 됩니다. 가장 심각한 문제는 문화, 복잡성, 그리고 보안입니다.

이러한 이슈를 해결하는 첫 단계가 프로덕션급 Ingress 컨트롤러 입니다.

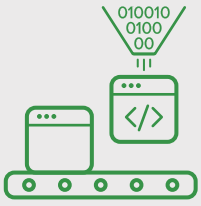
Ingress 컨트롤러는 전문 로드 밸런서 이상의 역할을 수행할 수 있습니다. 프로덕션급(production-grade)으로 평가받기 위해서는 다음과 같은 기능들을 갖추어야 합니다.

- 보안 간소화
- 복구력 증대
- 신속한 확장 실행

NGINX Ingress Controller는 신뢰할 수 있는 NGINX 소프트웨어 로드 밸런싱과 표준 Kubernetes Ingress 리소스 또는 커스텀 NGINX Ingress 리소스 기반의 단순화된 구성을 결합해 Kubernetes 클러스터에서 애플리케이션들이 안정적이고 안전한 방식으로 매우 빠르게 제공되도록 합니다.

왜 NGINX Ingress Controller를 사용해야 하는가?

NGINX에서 테스트를 완료했으며, 기업 고객들을 위해 24x7 지원을 제공하는 안정적이고 신뢰할 수 있는 Ingress Controller를 통해 확신을 가질 수 있습니다.



프로덕션급 특징들

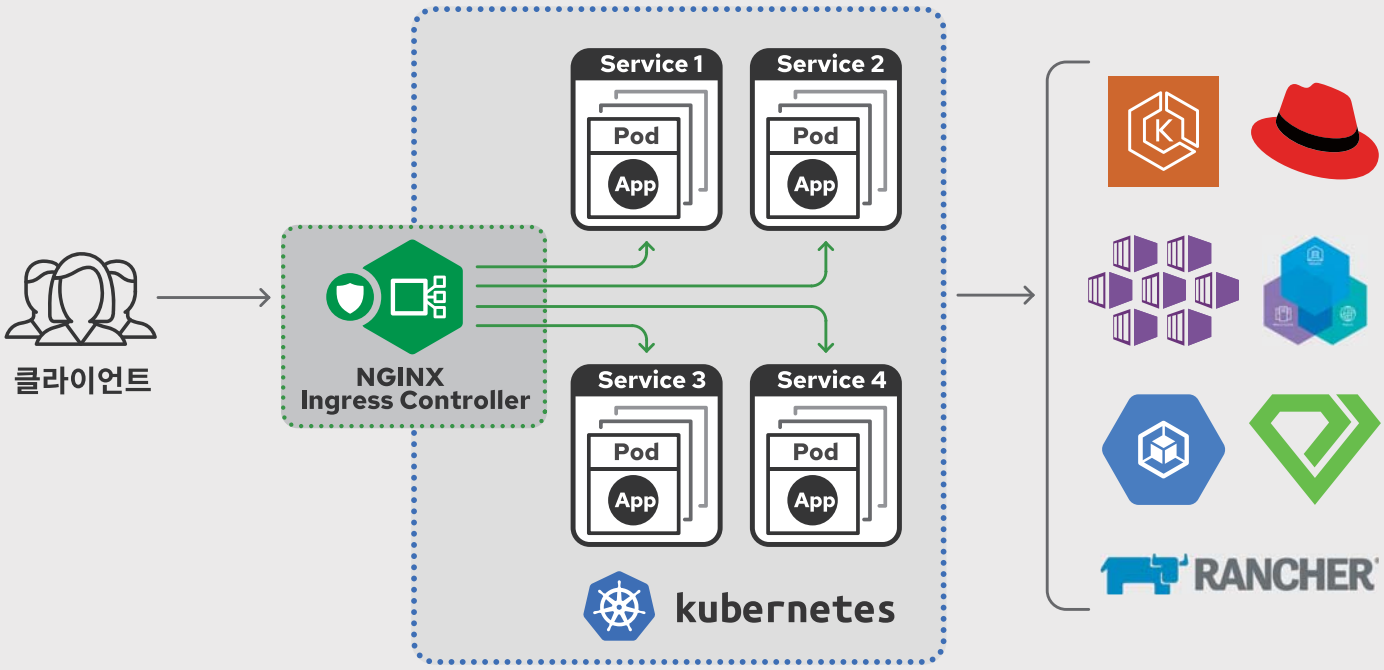
한층 향상된 애플리케이션 중심 구성, 가시성, 성능 모니터링 등을 통한 애플리케이션 강화 및 확장

컨테이너화된 애플리케이션 보안

인증, 권한 부여, 완전히 통합된 웹방화벽 등으로 보안에 대한 시프트 레프트(shift left) 실행

전체 트래픽 관리

ingress 및 egress 애플리케이션 트래픽을 한 번에 쉽고 지능적으로 관리



복잡성 감소

표준 Kubernetes Ingress 리소스를 사용해 구성하거나 NGINX Ingress resources를 활용하십시오. NGINX Ingress 리소스를 사용하면 서킷 브레이킹(circuit breaking), 라우팅 세분화, 헤더 조작(header manipulation), mTLS 인증, 웹방화벽 등과 같은 기능들을 단순화하는 네이티브, 타입 세이프(type-safe), 인덴티드(indented) 구성 스타일을 확보하게 됩니다. 또한, 이미 NGINX를 사용하고 있다면, NGINX Ingress 리소스를 통해 다른 환경의 기존 구성을 쉽게 조정할 수 있습니다.

복원력 향상

NGINX Ingress 리소스에서 사용할 수 있는 고급 로드 밸런싱 및 요청 라우팅 기능을 통해 blue-green 배포, canary 배포, A/B 테스트 및 서킷 브레이커(circuit breaker)를 지원합니다. 슬로우 스타트(slow-start) 기능을 통해 기본 및 OOB(Our-of-Band) 애플리케이션 상태 검사(가상 트랜잭션(synthetic transactions)으로도 알려짐)를 실행하여 서비스 중단없이 신규 서버와 복구된 서버를 로드 밸런싱된 그룹에 추가합니다. 무료로 제공되는 NGINX Service Mesh를 추가해 ingress 및 egress 애플리케이션 트래픽을 한 번에 원활하고 지능적으로 관리하십시오.

셀프 서비스 및 멀티 테넌시 제공

RBAC(role-based access control)와 셀프 서비스를 사용해 보안 가드레일(게이트 아님)을 설정하면, 애플리케이션을 안전하고 민첩하게 관리할 수 있습니다. 멀티 테넌시, 재사용성 및 간편한 구성 등을 지원합니다.

트래픽 통찰력 확보

애플리케이션 트래픽 흐름(NGINX Plus의 경우)에 관한 실시간 통계는 물론, 상세 로깅 기능, 그리고 네이티브 Prometheus 통합 및 Grafana 대시보드를 통해 제공되는 과거 기록 보기를 통해 Kubernetes의 가시성을 향상시킵니다.

컨테이너화된 애플리케이션 보안

설정 가능한 암호화(wildcard 인증서 포함)로 SSL/TLS 종단(termination) 성능을 최적화하고 JWT 인증 및 SSO(single sign-on)를 사용해 애플리케이션을 보호합니다. NGINX App Protect를 사용해 ingress 지점 또는 클러스터 내 다른 위치에 웹방화벽을 구축하십시오.

귀사에 적합한 NGINX Ingress Controller 버전을 알고 싶습니까? 옵션을 비교해 보십시오.

베어 메탈 서버를 위한 NGINX Ingress Controller 사이징 가이드

아래 표에서는 특정 서버 규모에서 실행되는 NGINX Ingress Controller로 달성할 수 있는 성능 수준이 요약되어 있습니다. 각 행에는 성능 수준 달성에 필요한 하드웨어 사양과 해당 하드웨어의 일반적인 비용이 자세히 설명되어 있습니다.

성능 값을 도출하기 위해 2개 베어 메탈 서버를 가진(기본 노드와 보조 노드) 클러스터에 Kubernetes 버전 1.13.1을 설치했습니다. 테스트하는 기본 노드는 Docker Hub에서 가져온 NGINX Ingress Controller 이미지를 실행합니다. 기본 노드에서 실행되는 다른 컨테이너는 없고, 전용 NGINX Ingress Controller 컨테이너에 사용할 수 있는 코어 수를 제한하는 방식으로 사이징을 도출했습니다. Flannel은 기본 노드를 보조 노드와 연결하기 위한 네트워킹 오버레이 스택으로서 사용됩니다. 보조 노드는 하나의 웹 서버 포드(pod) 전용입니다. 보조 노드에서 실행되는 다른 컨테이너는 없습니다.

NGINX는 하드웨어를 판매하지 않습니다. 여기에 제시된 비용은 소매 업체에서 구매할 때 지불할 것을 예상되는 평균적인 비용입니다.

하드웨어 비용[1]	하드웨어 사양	예상 성능
$1,400	2 CPU 코어[2] 8 GB RAM 2x10 Gbe NIC 1 TB HDD	74,000 RPS[3] 8,700 SSL TPS (RSA)[4] 9,100 SSL TPS (ECC)[5] 4 Gbps throughput[6]
$2,500	4 CPU 코어 8 GB RAM 2x10 Gbe NIC 1 TB HDD	150,000 RPS 17,400 SSL TPS (RSA) 17,600 SSL TPS (ECC) 8 Gbps throughput
$3,600	8 CPU 코어 16 GB RAM 2x10 Gbe NIC 1.2 TB HDD	300,000 RPS 30,000 SSL TPS (RSA) 33,000 ECC SSL TPS 8 Gbps throughput
$5,600	16 CPU 코어 32 GB RAM 2x10 Gbe NIC 480 GB SSD	340,000 RPS 55,000 RSA SSL TPS 57,000 SSL TPS (ECC) 8 Gbps throughput
$7,300	24 CPU 코어 32 GB RAM 2x10 Gbe NIC 480 GB SSD	340,000 RPS 58,100 SSL TPS (RSA) 58,500 SSL TPS (ECC) 8 Gbps throughput

1. 가격은 Intel NIC를 탑재한 Dell PowerEdge 서버를 기준으로 합니다
2. Intel® Xeon® Platinum 8168 CPU @ 2.70Ghz로 수행된 테스트
3. Keepalive 연결 시 1 KB 응답 사이즈
4. RSA 2048 bit, ECDHE-RSA-AES256-GCM-SHA384, OpenSSL 1.1.0g
5. ECC 256 bit, ECDHE-ECDSA-AES256-GCM-SHA384, OpenSSL 1.1.0g
6. 1 MB 응답 사이즈

성능 측정 지표 개요

RPS(Requests per second) – HTTP 요청을 처리하는 NGINX Ingress Controller의 성능을 측정합니다. 클라이언트는 keepalive 연결을 통해 요청을 보냅니다. NGINX Ingress Controller는 각 요청을 처리하고 별도의 Keepalive 연결을 통해 웹 서버로 전달합니다.

SSL TPS(SSL transactions per second) – 새로운 SSL/TLS 연결을 처리하는 NGINX Ingress Controller의 성능을 측정합니다. 클라이언트는 새로운 연결이 이루어질 때마다 일련의 HTTPS 요청을 보냅니다. NGINX Ingress Controller는 요청을 파싱하고 설정된 Keepalive 연결을 통해 웹 서버로 전달합니다. 웹 서버는 각 요청에 대해 0바이트의 응답을 반환합니다.

Throughput – HTTP를 통해 대량의 파일을 지원할 때 NGINX Ingress Controller가 처리할 수 있는 트래픽의 양을 초당 기가비트(Gbps) 단위로 측정합니다.

메모리 사이징

NGINX Ingress Controller 메모리 사용량은 동시에 활성화된 연결 수에 따라 천천히 증가합니다. 구성에 따라 차이가 있지만, 일반적으로 연결당 10~20KB 미만입니다.

캐싱(caching)이 enabled로 설정되면, NGINX Ingress Controller에 더 많은 메모리가 필요할 수 있습니다. 운영 체제 페이지 캐시에 핫 캐시 콘텐츠를 저장할 수 있는 충분한 여유 메모리가 있도록 메모리 사이즈를 지정합니다.

PFS(Perfect Forward Secrecy)

위에 제시된 SSL TPS 수치는 PFS(Perfect Forward Secrecy)를 적용한 SSL/TLS에 대해 산출한 것입니다. PFS는 프라이빗 키가 노출되는 경우에도 현재 캡쳐된 암호화된 트래픽이 추후에 복호화될 수 없도록 합니다. PFS는 현재 보안 상황에서 최대한의 보호와 사용자 프라이버시를 제공하기 위해 권장됩니다.

PFS는 컴퓨팅 성능에 대한 요구가 더 높기 때문에, 결과적으로 전반적인 TPS가 더 낮습니다. 대부분의 다른 벤더들은 PFS를 사용하고 있는지 여부를 밝히지 않았습니다. 비교 시 이 점을 유념하십시오.

기술 사양 – 다음을 포함해 모든 Kubernetes 플랫폼에 배포합니다

- Red Hat OpenShift
- Amazon Elastic Kubernetes Service
- Azure Kubernetes Service (AKS)
- Google Kubernetes Engine (GKE)
- IBM Private Cloud
- Diamanti

보다 자세한 기술 사양과 기능 및 모듈 목록은 full technical specifications을 참조하십시오.

NGINX이 어떻게 귀사를 지원할 수 있는지에 대한 자세한 내용은 nginx.com에서 확인해 보십시오.

NGINX
Part of F5