NGINX Ingress Controller®

IngressとEgressのトラフィックをプロダクショングレードで制御

Kubernetesアプリケーションの保護、強化、拡張

2020年のCloud Native Computing Foundation（CNCF）による調査で回答者の91%が使用していると答え、そのうち83%が実稼働環境で使用していると答えていることからも分かるように、Kubernetesは、コンテナ化されたアプリケーションの管理における事実上の業界標準となっています。

しかし、Kubernetesを実稼働環境で運用することは、ビジネスクリティカルな問題を伴います。特に、文化、複雑さ、セキュリティが最も深刻な問題です。

これらの問題を解決するための第一歩となるのが、プロダクショングレードのIngressコントローラです。

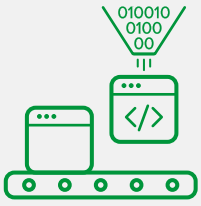
Ingressコントローラが単なる一部に特化したロードバランサではなく、プロダクショングレードとなるためには、以下のような機能が必要です。

- セキュリティの合理化
- 耐障害性の向上
- 迅速なスケーラビリティの実現

NGINX Ingress Controllerは、信頼できるNGINXソフトウェアのロードバランシングと、標準のKubernetes Ingressリソースまたはカスタム NGINX Ingressリソースに基づくシンプルな構成を組み合わせ、Kubernetesクラスタのアプリケーションが確実かつ安全に、高速で配信されることを保証します。

NGINX Ingress Controllerを使用すべき理由とは？

NGINXによってテストされ、24x7の商用サポートが提供される、安定して、信頼性に優れたIngress Controllerは、安心してご利用いただけます。



プロダクショングレードの機能

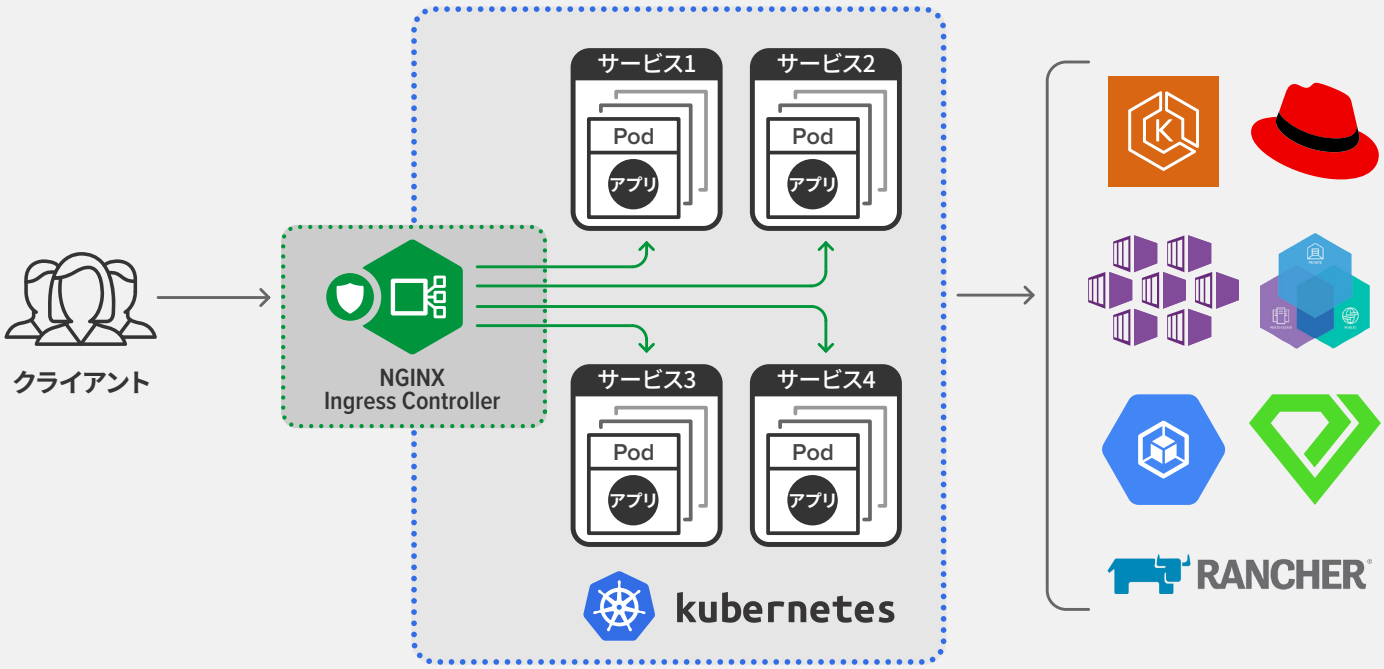
アプリケーション中心の高度な設定、可視化、パフォーマンス監視により、アプリを強化および拡張します。

コンテナ化されたアプリケーションの保護

認証、認可、完全統合されたWAFによりセキュリティをシフトレフトします。

総合的なトラフィック管理

IngressとEgressのアプリトラフィックを簡単かつインテリジェントに一括管理します。



複雑さを軽減

標準的なKubernetesのIngressリソースを使用して設定するか、NGINX Ingressリソースを活用できます。NGINX Ingressリソースを使用すると、ネイティブでタイプセーフな、インデントされた設定スタイルにより、サーキットブレーキング、高度なルーティング、ヘッダー操作、mTLS認証、WAFなどの機能を簡素化できます。さらに、すでにNGINXを使用している場合、NGINX Ingressリソースを使用することで、他の環境から既存の設定を簡単に適応させることができます。

耐障害性を向上

NGINX Ingressリソースで利用可能な高度なロードバランシングとリクエストルーティング機能により、ブルーグリーンデプロイメント、カナリアリリース、A/Bテスト、サーキットブレーカをサポートします。基本的な帯域外アプリケーションのヘルスチェック（合成トランザクションとも呼ばれる）を実行し、スロースタート機能を使用して、新規サーバーやリカバリされたサーバーをロードバランスされたグループに最小限の影響で追加します。無料で利用できるNGINX Service Meshを追加して、IngressとEgressのアプリケーショントラフィックをシームレスかつインテリジェントに一括管理できます。

セルフサービスとマルチテナンシーを提供

ロールベースのアクセス制御（RBAC）とセルフサービスを使用して、セキュリティガードレール（ゲートではない）を設定することで、チームはアプリを安全かつ俊敏に管理できます。マルチテナンシー、再利用性、シンプルな設定なども可能です。

トラフィックインサイトを取得

アプリケーションのトラフィックフローに関するリアルタイム統計（NGINX Plusの場合）と、詳細なログ機能による履歴表示、さらにPrometheusのネイティブ統合とGrafanaダッシュボードにより、Kubernetesの可視化を強化します。

コンテナ化されたアプリケーションを保護

設定可能な暗号化（ワイルドカード証明書を含む）によりSSL/TLSターミネーションのパフォーマンスを最適化し、JWT認証とシングルサインオン（SSO）を使用してアプリケーションを保護します。NGINX App Protectを使用して、Ingressまたはクラスタ内の他の場所にWAFを導入します。

組織に適したNGINX Ingress Controllerのバージョンについては、こちらのオプション比較を参考にしてください。

NGINX Ingress Controllerのサイジングガイド

ベアメタルサーバー

以下の表は、特定のサーバーサイズで動作するNGINX Ingress Controllerで得られるパフォーマンスレベルの概要を示しています。各行には、各パフォーマンスレベルを得るために必要なハードウェアの仕様と、そのハードウェアの一般的なコストが記載されています。

これらのパフォーマンス数値は、2台のベアメタルサーバー（プライマリノードとセカンダリノード）で構成されるクラスタにKubernetesバージョン1.13.1をインストールして算出しました。テスト対象のプライマリノードは、Docker Hubから取得したNGINX Ingress Controllerのイメージを実行しています。プライマリノードでは、他のコンテナは実行されていません。サイジングでは、NGINX Ingress Controller専用コンテナに利用できるコア数を制限しました。プライマリノードとセカンダリノードを結合するためのネットワーキングオーバーレイスタックとしてFlannelを使用しています。セカンダリノードは、1つのWebサーバー専用のPodです。セカンダリノードでは、他のコンテナは実行されていません。

NGINXはハードウェアを販売していません。ここに記載されているコストは、小売業者から購入する場合に想定される一般的なコスト例です。

ハードウェアコスト(例)[1]	ハードウェア仕様	想定パフォーマンス
$1,400	2 CPUコア[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スループット[6]
$2,500	4 CPUコア 8 GB RAM 2x10 Gbe NIC 1 TB HDD	150,000 RPS 17,400 SSL TPS (RSA) 17,600 SSL TPS (ECC) 8 Gbpsスループット
$3,600	8 CPUコア 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スループット
$5,600	16 CPUコア 32 GB RAM 2x10 Gbe NIC 480 GB SSD	340,000 RPS 55,000 RSA SSL TPS 57,000 SSL TPS (ECC) 8 Gbpsスループット
$7,300	24 CPUコア 32 GB RAM 2x10 Gbe NIC 480 GB SSD	340,000 RPS 58,100 SSL TPS (RSA) 58,500 SSL TPS (ECC) 8 Gbpsスループット

1. 価格は、Intel NICを搭載したDell PowerEdgeサーバーを基準とします。
2. Intel® Xeon® Platinum 8168 CPU @ 2.70GHzでのテストです。
3. レスポンスサイズ1 KB、キープアライブ接続
4. RSA 2048ビット、ECDHE-RSA-AES256-GCM-SHA384、OpenSSL 1.1.0g
5. ECC 256ビット、ECDHE-ECDSA-AES256-GCM-SHA384、OpenSSL 1.1.0g
6. レスポンスサイズ1 MB

RKE ベアメタル

以下の表は、NGINX Ingress Controller と Rancher Kubernetes Engine（RKE）（マネージド Rancher Kubernetes サービス）で得られるパフォーマンスレベルの概要と、そのハードウェアを小売業者から購入した場合の一般的なコスト例を示しています。

コア[1]	RPS[2]	SSL TPS (RSA)[3]	SSL TPS RSA、HyperThreading 使用	ハードウェアコスト(例)
1	24,000	900	1,000	$750
2	48,000	1,750	1,950	$750
4	95,000	3,500	3,870	$1,300
8	190,000	7,000	7,800	$2,200

1. Intel® Xeon® CPU ES-2690 v3 @2.60GHzでのテストです。
2. レスポンスサイズ1 KB、キープアライブ接続
3. RSA 2048ビット、ECDHE-RSA-AES256-GCM-SHA384、OpenSSL 1.0.2k-fips（TLS v1.2）

Amazon EKS

以下の表は、NGINX Ingress Controller と Amazon Elastic Kubernetes Service（EKS）（AWS のマネージド Kubernetes サービス）を使用して、特定の AWS インスタンスタイプで得られるパフォーマンスレベルの概要と、想定される月間総所有コスト（TCO）を示しています。

AWS インスタンスタイプ	コア	RPS[1]	SSL TPS (RSA)[2]	平均月間 TCO[3]
c5n.large	1	45,000	6,700	$100
c5n.large	2	80,000	12,600	$100
c5n.xlarge	4	135,000	23,000	$200
c5n.2xlarge	8	175,000	40,000	$400
c5n.4xlarge	16	237,000	68,500	$795
c5n.9xlarge	32	290,000	88,800	$1,790
c5n.9xlarge	36	300,000	92,800	$1,790

1. レスポンスサイズ1 KB、キープアライブ接続
2. RSA 2048ビット、ECDHE-RSA-AES256-GCM-SHA384、OpenSSL 1.0.2k-fips（TLS v1.2）
3. AWSインスタンス価格ページを参考に算出しています。

パフォーマンスメトリクスについて

1秒あたりの処理リクエスト数（Requests per second、RPS）：NGINX Ingress ControllerがHTTPリクエストを処理する能力を測定します。クライアントは、キープアライブ接続を介してリクエストを送信します。NGINX Ingress Controllerは、各リクエストを処理し、別のキープアライブ接続を介してWebサーバーに転送します。

1秒あたりのSSLトランザクション数（SSL TPS）：NGINX Ingress Controllerが新しいSSL/TLS接続を処理する能力を測定します。クライアントは、一連のHTTPSリクエストをそれぞれ新しい接続で送信します。NGINX Ingress Controllerは、リクエストを解析し、確立されたキープアライブ接続を介してWebサーバーに転送します。Webサーバーは、各リクエストに対して0バイトのレスポンスを返します。

スループット：NGINX Ingress ControllerがHTTPで大きなファイルを提供するときに維持できるトラフィックの量を1秒あたりのギガビット数（Gbps）で測定します。

メモリサイジング

NGINX Ingress Controllerのメモリ使用量は、同時にアクティブになる接続の数に応じて徐々に増加します。設定により異なりますが、通常は接続ごとに10～20 KB未満増加します。キャッシングが有効な場合、NGINX Ingress Controllerが必要とするメモリはさらに多くなる可能性があります。ホットキャッシュされたコンテンツをオペレーティングシステムのページキャッシュに保存するために十分な未使用メモリを確保できるように、メモリのサイズを設定してください。

Perfect Forward Secrecy

上記のSSL TPSの数値は、Perfect Forward Secrecy（PFS）を使用したSSL/TLSの数値です。PFSは、秘密鍵が漏洩した場合でも、暗号化トラフィックを傍受して後から解読できないようにします。PFSは、現在のセキュリティ状況において、最大限の保護およびユーザープライバシーを提供するために推奨されています。

PFSを使用すると、計算量が多くなり、結果として全体的なTPSが低くなります。他のほとんどのベンダーはPFSを使用しているかどうかを明記していません（したがって、おそらく使用していません）。そのため、比較検討にはこの点に注意してください。

技術仕様：あらゆるKubernetesプラットフォームに導入可能です。

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

その他の技術仕様および機能やモジュールの一覧については、技術仕様書をご覧ください。

NGINXの詳細については、nginx.co.jpをご覧ください。

NGINX
Part of F5