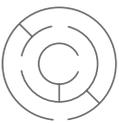




SECURE SERVICE MESH

マイクロサービスアーキテクチャに基づいた
アプリケーションのセキュリティと可視性を強化

アプリケーションがマイクロサービスベースのアーキテクチャに移行するにつれて、コンテナとKubernetesの採用が増えてきました。これらの技術の使用は、パブリックおよびプライベートクラウドでもデータセンターでも急速に増大しています。これらのアプリケーションが本番環境に導入されてその規模が拡大するにつれて、従来のツールがKubernetesに合わなくなっています。アプリケーションの配信やセキュリティも含めたあらゆるアプリケーションサービスにおいて、エンタープライズクラスのKubernetes向けソリューションを求める需要が増大しています。A10 Secure Service Meshは、このようなニーズを満たすために設計されたソリューションであり、Kubernetes環境に導入されたマイクロサービスを対象とした高度なアプリケーションロードバランシング/トラフィック管理、統合されたセキュリティ、トラフィック分析、および実用的な知見を提供します。



課題

Kubernetes環境内のアプリケーションを適切に管理するには、以下の課題に対処できる新しい統合ソリューションが必要です。

1. マイクロサービス向けのセキュリティおよびポリシーを適用できるようにする。
2. マイクロサービスの最適な稼働状態を維持するために必要な可視化と分析機能を提供する。
3. コンテナベースのワークロードの一貫した可用性を確保するために、「スマート」なロードバランス機能とトラフィック管理機能を提供する。

課題

マイクロサービスベースのアプリケーションがKubernetes環境に導入されていくにつれて、ノード間のEast-Westトラフィックの可視化とセキュリティが大きな課題になってきます。他の環境でこれらの課題に対処している従来のソリューションでは、ユニークなアーキテクチャを持つKubernetes環境には適しません。

ソリューション

A10のSecure Service Meshソリューションは、エンタープライズクラスのセキュリティとロードバランシング機能、トラフィック管理機能を包括的なアプリケーションの可視化、及び分析機能と統合するための（アプリケーションに変更を加えることなくアプリケーションのライフサイクル全体を通じて）、簡単に自動化された手段を提供します。

特長

- トラフィック管理を改善し、操作を簡素化します
- トラフィックのマイクロセグメンテーションと各マイクロサービス間の分離によって、セキュリティを向上させます
- 全ノードでマイクロサービス間のトラフィックを自動的に暗号化します
- サービスディスカバリの負荷を個々のマイクロサービスから中央のロードバランサーに移します
- 実用的な知見を得ることでITのアジリティを向上させます

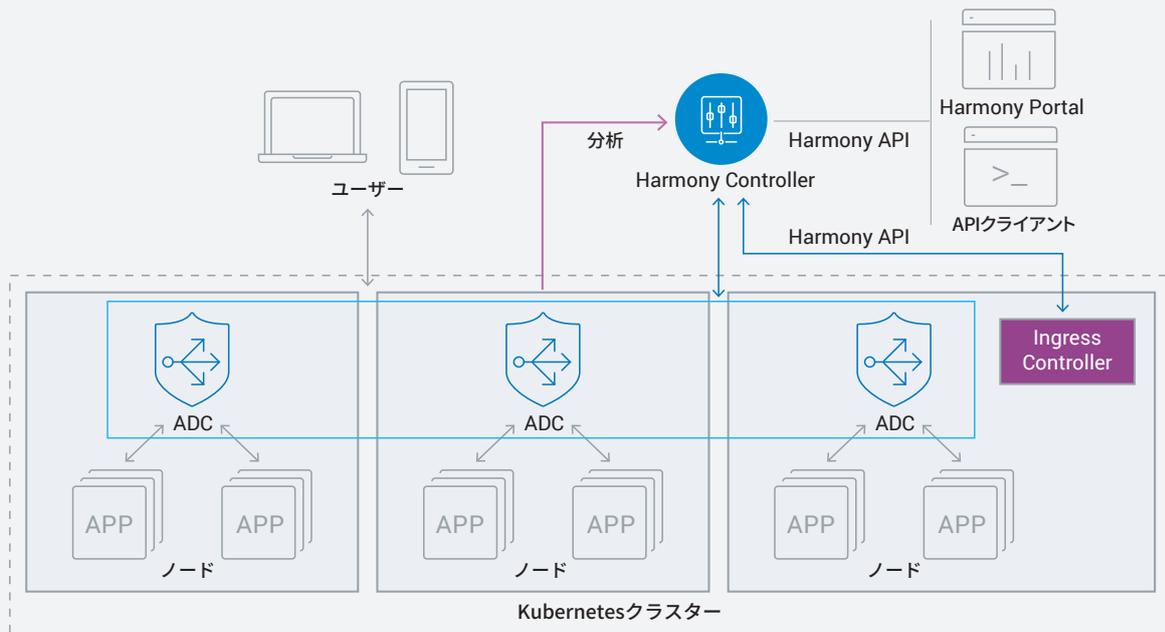


図1: Secure Service Meshソリューションの導入アーキテクチャ

A10 Secure Service Mesh ソリューション

A10 Secure Service Meshは、マイクロサービスとコンテナベースのアプリケーションに対応したソリューションです。この統合ソリューションは、高い拡張性を備えたSoftware-definedな分散アーキテクチャを提供します。そのアーキテクチャは、A10 Lightning ADC、A10 Ingress Controller、A10 Harmony Controllerという3つの主要コンポーネントで構成されています。

このアーキテクチャでは、データプレーン要素としてLightning ADCをKubernetes環境内にデプロイし、Harmony Controllerで管理を行います。Ingress Controllerは、HarmonyのAPIを使用してIngressリソースと連携し、アプリケーションを自動的に作成します。また、ロードバランシングやコンテンツスイッチングのルールも作成し、アプリケーション配信およびセキュリティポリシーを設定して、アプリケーションをLightning ADCクラスターに追加します。Ingress Controllerは、アプリケーションサービスコンテナを監視し、変化があればそれをHarmony Controllerを通じてLightning ADCに通知することで、ADCの構成とインフラストラクチャを常に同期した状態に保ちます。

機能と特長 柔軟な拡張性

Lightning ADCは、Kubernetesデーモンセットとしてデプロイされます。トラフィックが増大してKubernetesクラスターにノードが追加されるのに合わせて、A10 Lightning ADCクラスターも自動的にスケールアウトします。新しく追加されたADCインスタンスは、自動的にHarmony

Controllerに接続して設定情報を取得し、手動による設定作業なしでトラフィックを処理できる準備を整えます。

サービスのオートディスカバリ

Kubernetesは、ノード、ポッド、サービスなどを簡単に拡張できる手段を提供します。さらに、稼働中のコンテナを常時監視して、コンテナに障害が起きた場合は新しいものと置き換えます。このため、サービスコンテナのIPアドレスは、変化し続けます。このような動的な環境では、アプリケーションサービスが相互に通信する際、通信しようとしているサービスのIPアドレスがわからなくなるという問題を引き起こします。

Secure Service Meshは、動的なKubernetes環境内で変化するマイクロサービスのIPアドレスを自動的に追跡し、マイクロサービス間の通信を容易にします。

マイクロセグメンテーションと、 マイクロサービス間の安全なトラフィック

Lightning ADCは、マイクロサービス間のトラフィック (East-Westトラフィック) をインターセプトするように設定することができます。トラフィックがLightning ADCを通過し始めると、適切なセキュリティポリシー (マイクロセグメント用に設定されたもの) がトラフィックに適用されるようになります。マイクロセグメンテーションにより、各マイクロサービスを互いに分離して、各マイクロサービスを個別に保護できるようになります。これにより、さらにきめ細かいセキュリティを実現することができます。アプリケーションサービスコンテナのIPアドレスが時間の経過につれて自動的に変更されるため、アクセスポリシーはIPアドレスではなくサービスラベルに基づいて適用されます。

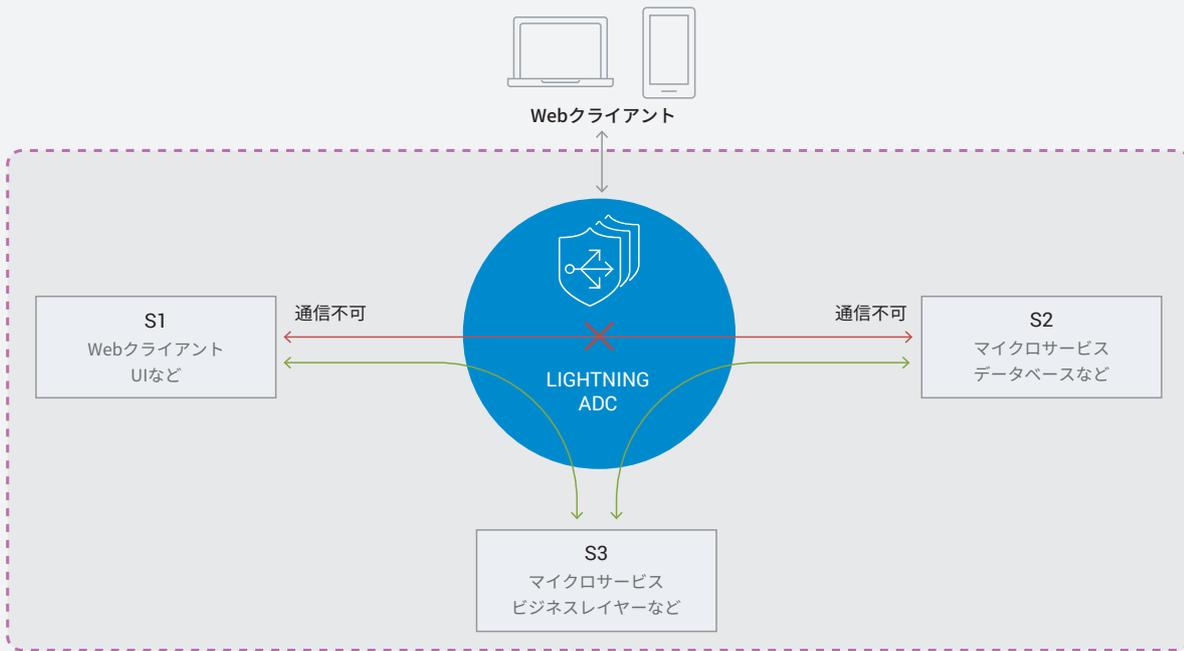


図2: Lightning ADCによるNorth-South及びEast-Westトラフィックへのセキュリティポリシー適用

ノード間トラフィックの自動暗号化

このソリューションは、トラフィックがノードを越えて出て行くときにそのトラフィックを自動的に暗号化し、目的のノードに到着してマイクロサービスに配信される前に復号します。これにより、アプリケーションに小さい変更を加えずにSSL/TLSセキュリティを強化できます。

アプリケーションの集中管理とAPIによる自動化

Kubernetesのような柔軟で分散化した環境では、ADCの個別管理が大きな課題となります。Harmony Controllerを使用すれば、論理アプリケーションレベルで設定を定義し、それを適切なADCインスタンスに対してインテリジェントにプッシュできるので、構成を簡単に維持管理できます。さらに、すべての管理機能と分析機能はHarmony APIと呼ばれるREST APIを通じて公開されます。これにより、アプリケーション配信機能を最適化するための高度な自動化が可能になります。

サービスごとの分析と知見

従来のADC環境では、アプリケーションレイヤーのトラフィックがほとんど(あるいはまったく)見えないため、問題のトラブルシューティングに必要なデータの収集が困難です。A10のADCは、リアルタイムでメトリクスを収集して分析エンジンにプッシュし、分析エンジンはそれらに基づいて実用的な知見を提供します。ユーザーはこの情報に基づいてアプリケーションやインフラストラクチャをきめ細かく調整でき、トラブルシューティングを迅速化できます。

ソリューションのコンポーネント 動作の仕組み

A10 Lightning ADC

- Kubernetes環境に導入されたマイクロサービス向けのトラフィック管理、柔軟かつ高度なロードバランシング、セキュリティ、分析機能などを含む、革新的なレイヤー4-7機能を提供します
- トラフィックのマイクロセグメンテーションと、North-South及びEast-Westトラフィックへのきめ細かいポリシー適用を可能にします
- CI/CDアプリケーション環境向けのBlue-Green/カナリアデプロイメントをサポート
- 運用を効率化し、煩雑な作業やリスクを軽減します

A10 Harmony Controller

- マルチクラウド環境でアプリケーションサービスのセキュリティを確保するための管理、オーケストレーション、および分析機能を提供します
- ADCを通過するトラフィックについて情報を収集し、分析し、レポートを生成して、サービスごとの可視化、分析機能、アラートを提供します
- IT部門によるアプリケーションサービスの導入および運用の自動化を可能にし、その結果として運用のアジリティを向上させ、分散化したサービスの管理を簡素化し、トラブルシューティングの時間を短縮して、TCOを削減します

A10 Ingress Controller

- アプリケーションサービスコンテナとIngressリソースを監視し、何か変化が生じた場合はそれをHarmony Controllerに通知して、Lightning ADCと即座に同期できるようにします

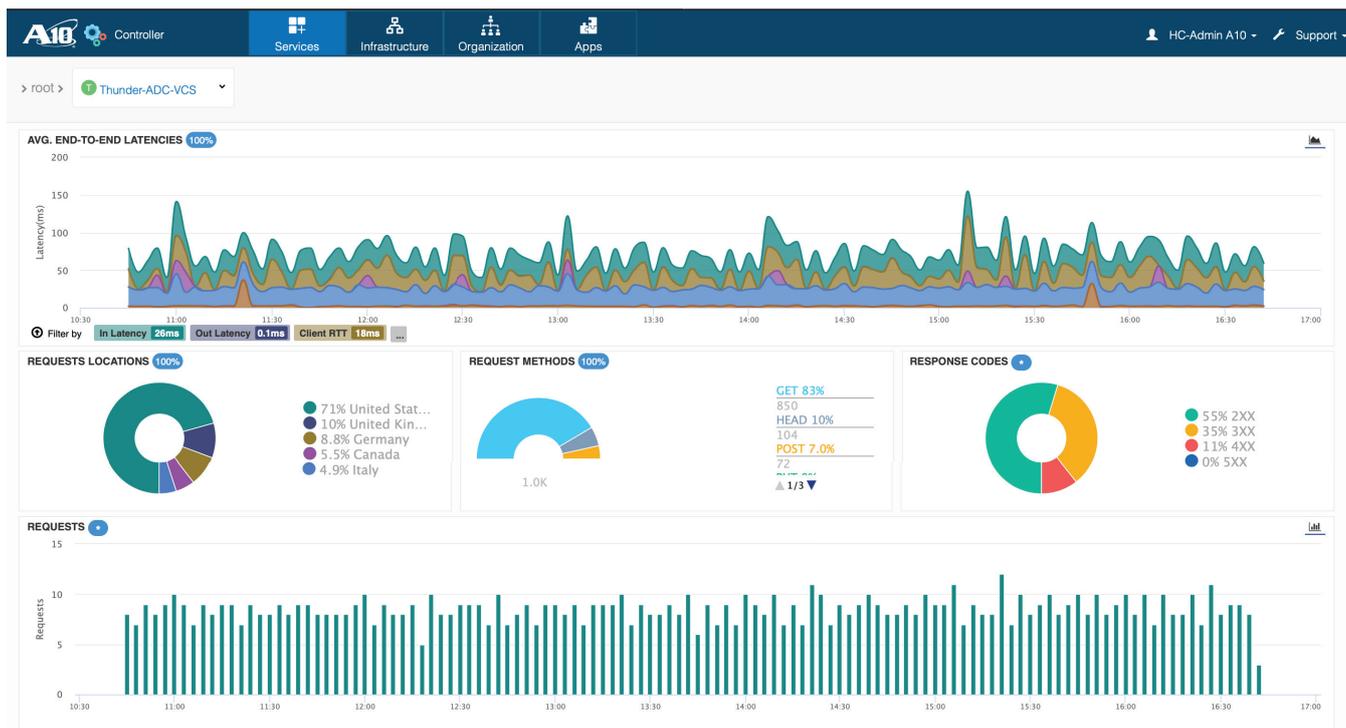


図3: Harmony Controllerが提供する分析結果の例

Kubernetes環境に導入されたアプリケーションに最適なアプリケーション配信とセキュリティを提供

A10 Secure Service Meshは、運用の簡素化、マイクロサービスの優れたパフォーマンス、そしてすべてのアプリケーショントラフィックの詳細な可視化と分析に加えて、Kubernetes環境に導入されたアプリケーションのアプリケーションレイヤーでのセキュリティも提供します。このセキュリティ機能は、North-SouthトラフィックとEast-Westトラフィックの両方を対象としています。実用的な知見と優れたトラブルシューティング機能により、Kubernetes環境でのアプリケーション配信管理の負荷を最小化できます。

無料体験版のご案内

A10 Secure Service Meshソリューションは、無料でお試しいただけます。[Lightning ADCの無料体験版](http://www.a10networks.co.jp/)をお申し込みいただき、Kubernetes環境向けのソリューションをご検討されていることを弊社にお知らせください。

A10 Networks / A10ネットワークス株式会社について

A10 Networks (NYSE: ATEN) はセキュアアプリケーションサービスにおけるリーディングカンパニーとして、高性能なアプリケーションネットワークワーキングソリューション群を提供しています。お客様のデータセンターにおいて、アプリケーションとネットワークを高速化し可用性と安全性を確保しています。A10 Networksは2004年に設立されました。米国カリフォルニア州サンノゼに本拠地を置き、世界各国の拠点からお客様をサポートしています。

A10ネットワークス株式会社はA10 Networksの日本子会社であり、お客様の意見や要望を積極的に取り入れ、革新的なアプリケーションネットワークワーキングソリューションをご提供することを使命としています。

詳しくはホームページをご覧ください。

URL: <http://www.a10networks.co.jp/>

Facebook: <http://www.facebook.com/A10networksjapan>

LEARN MORE

ABOUT A10 NETWORKS

お問い合わせ:

a10networks.co.jp/contact

A10ネットワークス株式会社

www.a10networks.co.jp

©2019 A10 Networks, Inc. All rights reserved. A10 Networks, A10 Networks ロゴ, ACOS, A10 Harmony は米国およびその他の各国におけるA10 Networks, Inc. の商標または登録商標です。その他の商標はそれぞれの所有者の資産です。A10 Networks は本書の誤りに関して責任を負いません。A10 Networks は、予告なく本書を変更、修正、譲渡、および改訂する権利を留保します。製品の仕様や機能は、変更する場合がございますので、ご注意ください。

商標について詳しくはホームページをご覧ください。 www.a10networks.com/a10-trademarks

Part Number: A10-SB-19195-JA-01 FEB 2019