

SECURE SERVICE MESH

提升基於微服務架構的應用程式安全性 與可視性

隨著越來越多應用程式轉為基於微服務的開發架構，容器技術與 Kubernetes 的使用率也跟著增加。在跨公有雲、私有雲以及資料中心環境中，對於使用這些技術的需求大幅成長。當應用程式部署到正式環境並達到一定規模時，傳統工具並不足以適用於 Kubernetes。所有針對企業級和 Kubernetes 專用解決方案的應用程式服務（包括應用程式交付與安全性）需求都在增長。

A10 Secure Service Mesh 專為解決這些需求而打造，替部署在 Kubernetes 環境的微服務提供進階應用程式負載平衡、流量管理、整合式安全、流量分析與可用資訊。



關鍵挑戰

想要在 Kubernetes 環境中成功管理應用程式，需要一個嶄新、統一的解決方案來解決以下關鍵挑戰：

1. 提供微服務安全性與強制執行政策。
2. 提供使微服務保持最佳運行狀態所需的深入可視性和深度分析。
3. 提供「智慧」負載平衡與流量管理，以確保基於容器的工作負載 (container-based workloads) 的一致可用性。

挑戰

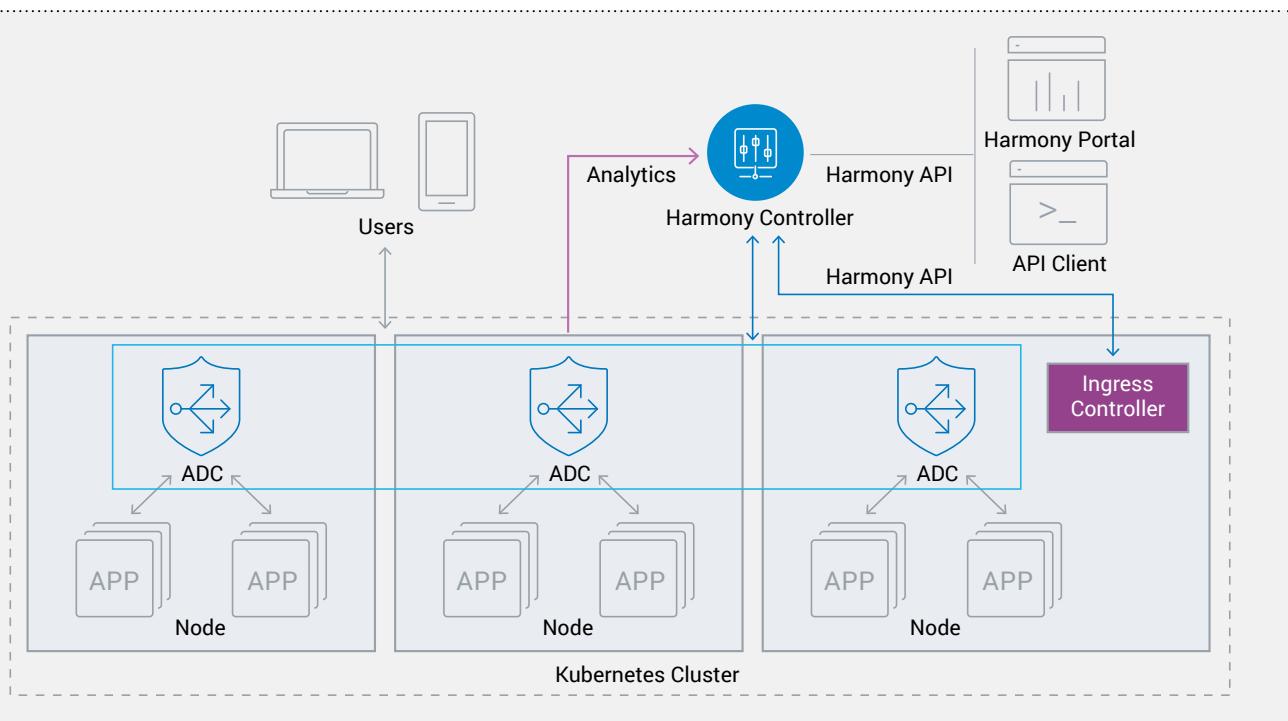
以微服務為基礎的應用程式開始在 Kubernetes 部署時，東西向流量的可視性及安全性便成為了關鍵挑戰。因 Kubernetes 的獨特架構，傳統適用於其他環境的解決方案無法於此架構中完整解決這些挑戰。

解決方案

A10 Secure Service Mesh 解決方案提供了一種簡單，自動化的方式，可將企業級安全性和負載平衡/流量管理與全面的應用程式可視性和分析功能整合在一起——在整個生命週期間皆無須更動應用程式。

優勢

- 改善流量管理以及簡化操作
- 透過流量微分段和微服務彼此隔離來提高安全性
- 自動加密跨節點的微服務間的流量
- 將服務發現 (Service discovery) 從獨立的微服務卸載至中央負載平衡器
- 獲取可執行的分析與洞察，以提升 IT 敏捷度



圖表 1: Secure Service Mesh 解決方案部署架構

A10 SECURE SERVICE MESH 解決方案

A10 Secure Service Mesh 是專為現代化微服務，以及以容器為基礎的應用程式所打造。這個統一的解決方案提供了高度可擴展、軟體定義的分散式系統架構，其中包含三個關鍵要素：A10 Lightning ADC、A10 Ingress Controller 和 A10 Harmony Controller。

此架構讓 Lightning ADC（資料層元素）輕量化，並且能部署於 Kubernetes 環境中； Harmony Controller 則負責管理。 Ingress Controller 運用 Ingress Resource，利用 Harmony API 自動創建應用程式。此外，Ingress Controller 還可建立負載平衡與內容切換規則，配置應用程式交付與安全政策，並將應用程式附加到 Lightning ADC 叢集。 Ingress Controller 也監控應用程式服務容器，透過 Harmony Controller 將任何變更通知 Lightning ADC，讓 ADC 的配置與基礎架構始終保持同步。

特性與優勢

靈活擴展

Lightning ADC 以 Kubernetes Daemonset 部署。隨著流量增加以及額外的節點加入 Kubernetes 叢集，A10 Lightning ADC 叢集也會跟著自動增加。新的 ADC 實例會自動與 Harmony controller 連接，以獲取配置資訊，並準備好接管流量，無須手動配置。

自動化服務發現

Kubernetes 提供簡單的方式來擴展 nodes, pods 和服務等。此外，它還能持續監控運作中的容器，並在容器發生錯誤時更換新的容器。因此，這些服務容器的 IP 位置會不斷變動。如此動態的環境在應用程式服務想要互相聯繫時，會因為無法找到目前運作應用程式的 IP 位置而成為問題。

Secure Service Mesh 會自動追蹤在動態 Kubernetes 環境中變動的微服務 IP 位置，方便微服務間的聯繫。



圖表 2: Lightning ADC 執行東西向流量與南北向流量的安全政策

微服務之間的微分段與安全流量

Lightning ADC 可配置為攔截微服務之間的流量（即東西向流量）。一旦流量開始通過 Lightning ADC，為了微分段所採取的適當安全政策就會開始控管流量。微分段准許微服務相互隔離，並受到個別保護。目的在於使安全性更緊密。由於應用程式服務容器的 IP 位置隨著時間自動改變，因此存取政策是基於服務標籤，而不是 IP 位置。

自動加密節點間流量

此解決方案在流量離開節點邊界時自動加密，並在傳送到微服務前對目標節點解密，藉此加強 SSL 安全性，且無須變更應用程式。

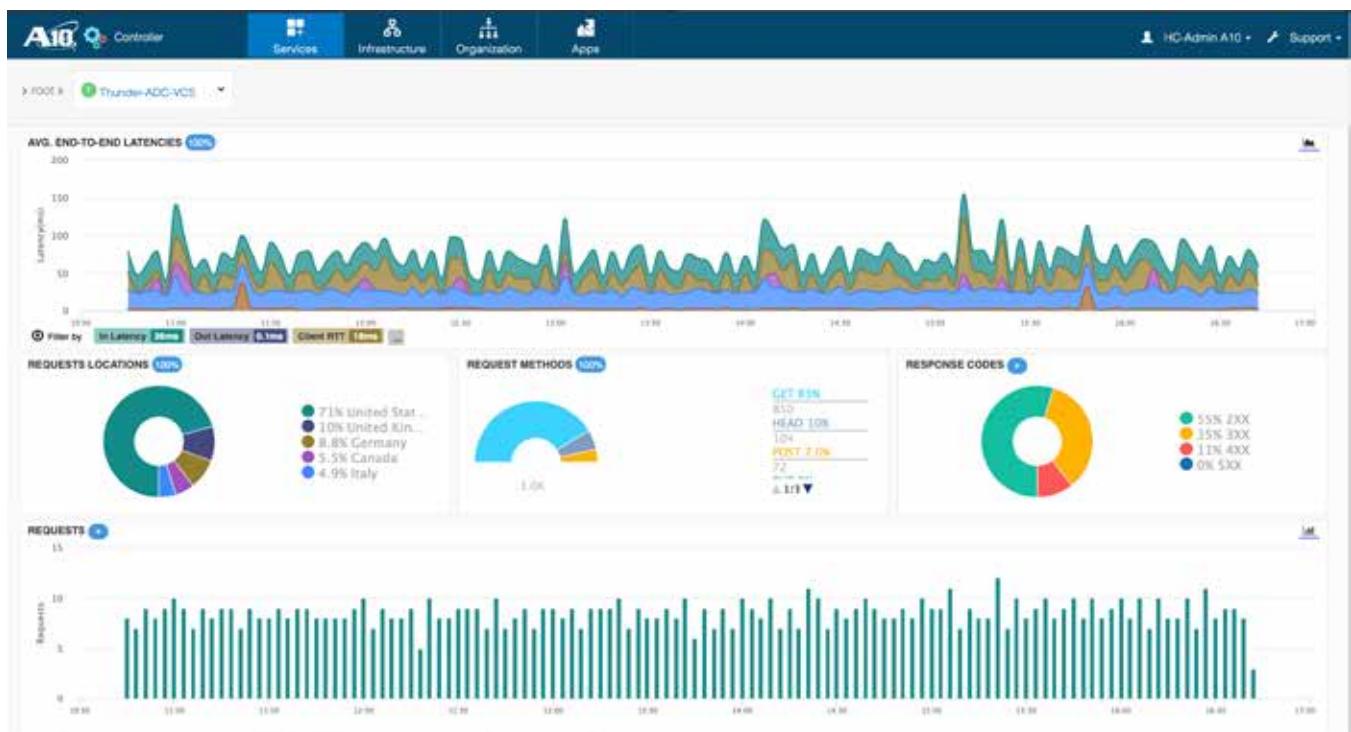
集中化應用程式管理與 API 驅動的自動化

在 Kubernetes 如此彈性且分散的環境中，單獨管理 ADC 成為最大的挑戰。運用 Harmony Controller，維護配置很容易，因為控制器准許定義邏輯應用程式級別的配置，並會聰明地將其推向相應的 ADC 實例。

此外，所有的管理與分析功能都可透過 Harmony APIs（基於 REST APIs）而看得一清二楚。這可實現高度自動化，並優化應用程式交付功能。

各服務 (PER-SERVICE) 的分析與洞察

傳統的 ADC 環境中，應用層中的流量幾乎沒有可視性，造成收集排除故障的資料相對困難。A10 ADC 能即時收集指標數據，並送往分析引擎，該引擎負責生產可用資訊，為使用者提供情報，藉此調整應用程式與基礎架構，也能更快速地排除故障。



圖表 3: Harmony Controller 提供的分析樣本

解決方案要素

如何運作

A10 LIGHTNING ADC

- 提供創新的 4 到 7 層功能，包括流量管理、先進靈活的負載平衡，以及部署於 Kubernetes 微服務的安全性與分析
- 准許流量微分段，以及應用於南北向和東西向流量的細分政策
- 支援 CI/CD 應用程式環境的 Blue-Green/Canary 部署
- 提升操作效率，減少繁雜任務與風險

A10 HARMONY CONTROLLER

- 為多雲端環境中的安全應用程式服務提供管理、編排與分析
- 收集、分析與報告經過 ADC 的流量，並為各項服務提供可視性、分析與警報
- 讓 IT 能自動部署與操作應用程式服務，進而提升操作靈活度，簡化分散式服務的管理，縮短排除故障時間，以及減少總體持有成本

A10 INGRESS CONTROLLER

- 監控應用程式服務容器和 Ingress Resources，並在發生變更時，通知 Harmony Controller 並立即與 Lightning ADC 進行同步處理

為您在 KUBERNETES 容器環境中的服務部署最佳應用程式交付與安全性解決方案

除了操作簡單，卓越的微服務性能，以及對所有應用程式流量的詳細可視性和分析之外，A10 Secure Service Mesh 還專為部署於 Kubernetes 環境的應用程式提供了應用層安全性。安全性可兼顧南北與東西向流量。可用資訊與出色的故障排除能力可大幅降低 Kubernetes 環境中應用程式交付管理的負擔。

與我們聯繫

想瞭解更多有關 A10 Secure Service Mesh 解決方案，歡迎申請 [Lightning ADC 免費試用版](#) 或與您的 A10 Networks 窗口聯繫，並讓我們知道您在尋找 Kubernetes 環境適用的解決方案。

關於 A10 NETWORKS

A10 Networks (NYSE: ATEN) 以 Reliable Security Always™，提供一系列高性能應用網路解決方案，協助企業確保其資料中心及跨雲端環境應用和網路保持高可用性、加速性和安全性。A10 Networks 成立於 2004 年，總部位於美國加州聖荷西市，並在世界各地設有辦事處為全球客戶提供服務。更多資訊請瀏覽：a10networks.com

LEARN MORE ABOUT A10 NETWORKS

與我們聯絡

a10networks.com/contact

©2018 A10 Networks, Inc. 版權所有，保留所有權利。A10 Networks、A10 Networks 標誌、ACOS、A10 Thunder、A10 Lightning、A10 Harmony 和 SSL Insight 是 A10 Networks, Inc. 在美國及其他國家/地區的商標或註冊商標。所有其他商標之所有權分屬於各自所有者擁有。A10 Networks 對本文件中的任何錯誤概不負責。A10 Networks 保留未經通知即變更、修改、轉讓或修訂本出版品之權利，恕不另行通知。如需完整商標清單，請造訪: www.a10networks.com/a10-trademarks

文件編號: A10-SB-19195-TW-01 2018年12月