DATA SHEET

# A10 Harmony 控制器

## 適合多雲環境的敏捷管理、自動化及分析功能

A10 Harmony® 控制器提供集中的敏捷管理、自動化及分析功能，適用於部署在各種基礎架構的 A10 安全應用程式服務，範圍涵蓋資料中心、私有雲、公有雲乃至於混合雲。

### 敏捷管理及分析功能適合任何應用程式部署

A10 Harmony 控制器提供集中管理及分析功能，適用於任何網路或雲端環境中以 A10 Thunder® ADC、SSLi®、CFW 及 CGN 部署的 A10 安全應用程式服務，協助進行服務配置及原則執行。

Harmony 控制器提供整合式的應用程式交付及安全解決方案，有助於收集、分析及回報通過 A10 Thunder ADC 的應用程式流量。

針對 A10 SSL Insight、CGNAT、Gi/SGI 防火牆及 GTP 防火牆的集中分析，能夠以整合式儀表板具體呈現安全態勢，協助提升營運效率。

Harmony 控制器可協助組織高效地自動部署及運作應用程式服務、提升營運效率及敏捷度、強化終端使用者體驗及降低 TCO、簡化管理分散式應用程式服務，乃至於大幅縮短疑難排解時間、接收有關效能或安全異常的警示、加強容量規劃及最佳化 IT 基礎架構和雲端環境。

SaaS

Harmony SaaS

自助管理

aws

Microsoft Azure

Google Cloud

ORACLE CLOUD

vmware

redhat

CentOS

與 A10 交談

A10networks.com/harmony

# 功能與優勢

Harmony 控制器可簡化應用程式服務作業，提升營運團隊的敏捷度。這款控制器是針對 A10 安全應用程式服務提供的集中管理解決方案，能夠以 API 進行自動配置及控制，協助支援 DevOps/SecOps 工作流程。控制器可做為單一整合點，與組織內部使用的編排系統整合。其中也提供全方位的基礎架構和每個應用程式的見解、效能及安全性分析、異常偵測及加速疑難排解等功能。

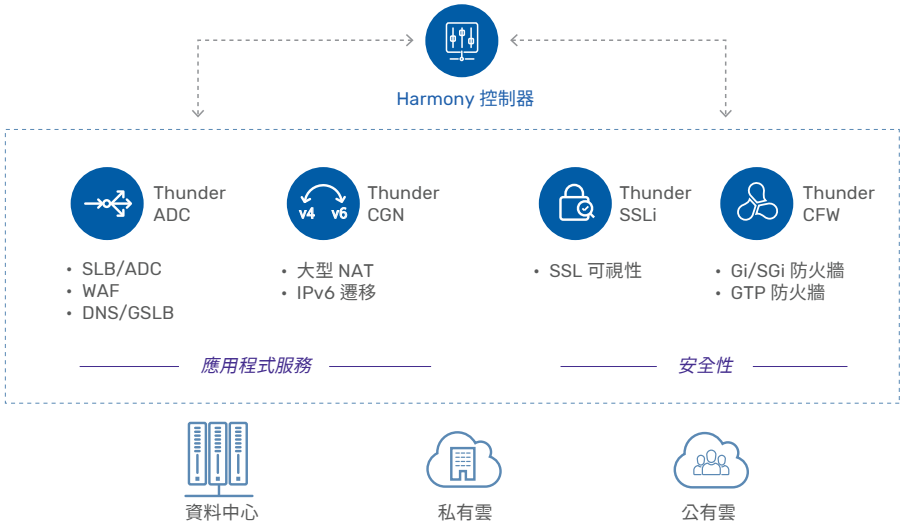


圖 1：Harmony 控制器是集中管理解決方案，可在多個資料中心與雲端環境實現應用程式服務分析及自動化。

## 集中管理

集中管理功能適用於 A10 各式各樣的安全應用程式服務產品組合，包括 Thunder ADC、SSLi、CFW 及 CGN。您可輕鬆管理及監控裝置和配置原則，範圍涵蓋部署於資料中心、私有雲及公有雲的應用程式。

## 應用程式流量和安全性分析

取得可視性及可行見解，協助掌握應用程式流量。Harmony Apps 可協助分析收集到的資料，以偵測異常趨勢，並可存取情境式資料和記錄，協助簡化疑難排解。作業人員可依據各種指標和自訂欄位，透過電子郵件或 Web-hook URL 取得警示，實現自動化的快速行動。

## 多租戶和自助服務

每個 Thunder 裝置叢集的 L3V 或服務分區都會對應至租戶，代表在該分區內執行的一組應用程式服務。Harmony 控制器的階層式租戶模型可於任何資料中心及雲端環境實現多租戶作業，並讓每個應用程式團隊及服務負責人能夠管理本身原則，有助於提升敏捷度。

## 裝置生命週期管理

集中的裝置生命週期管理，適用於 A10 硬體設備或虛擬執行個體。您可套用共同範本，輕鬆管理大量裝置。此外還能備份及還原配置，並執行排程的軟體升級作業。

## API 驅動自動化

全方位 API 能夠與 DevOps 工具鏈整合，例如 Ansible、Chef 和 Jenkins，也能與各種編排系統整合，例如 VMware VRO/VRA、Cisco Cloud Center、Microsoft Azure、Google Cloud Platform、Amazon Web Services 等等。REST API 可用於應用程式配置、裝置運作及存取分析資料。

## 跨平台安裝

Harmony 控制器是以容器為基礎的微服務架構，可讓控制器部署於各種 Linux 機器環境中，包括裸機、虛擬化伺服器以及公有或私有雲。

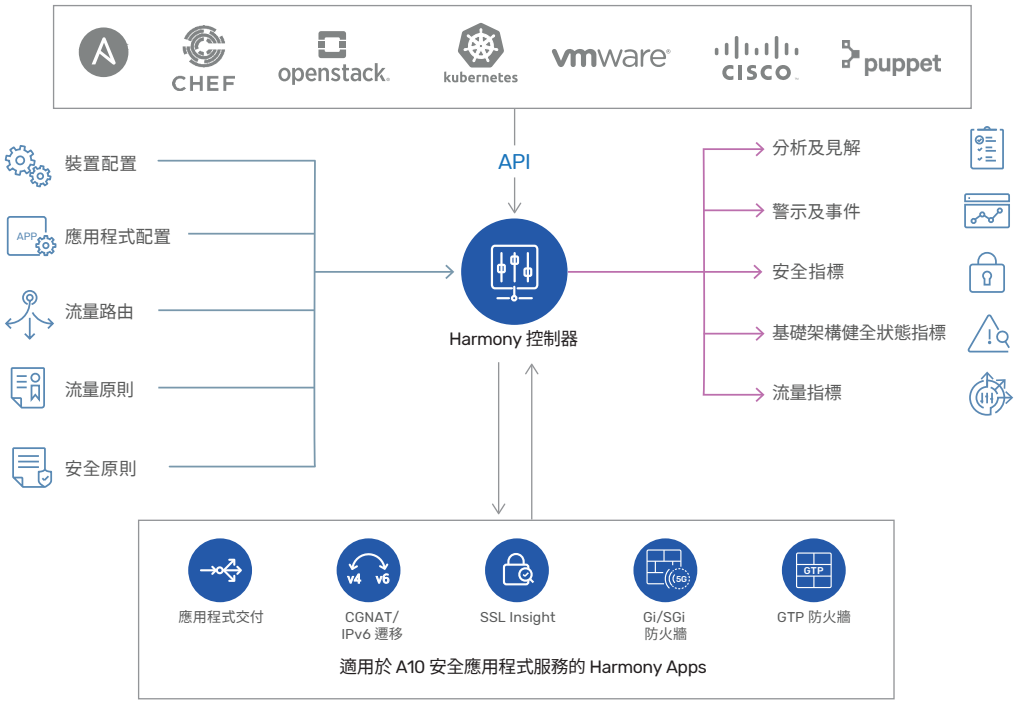


圖 2：Harmony 控制器可在任何及多雲環境中簡化和自動化應用程式管理及作業。

# Harmony 控制器使用者介面

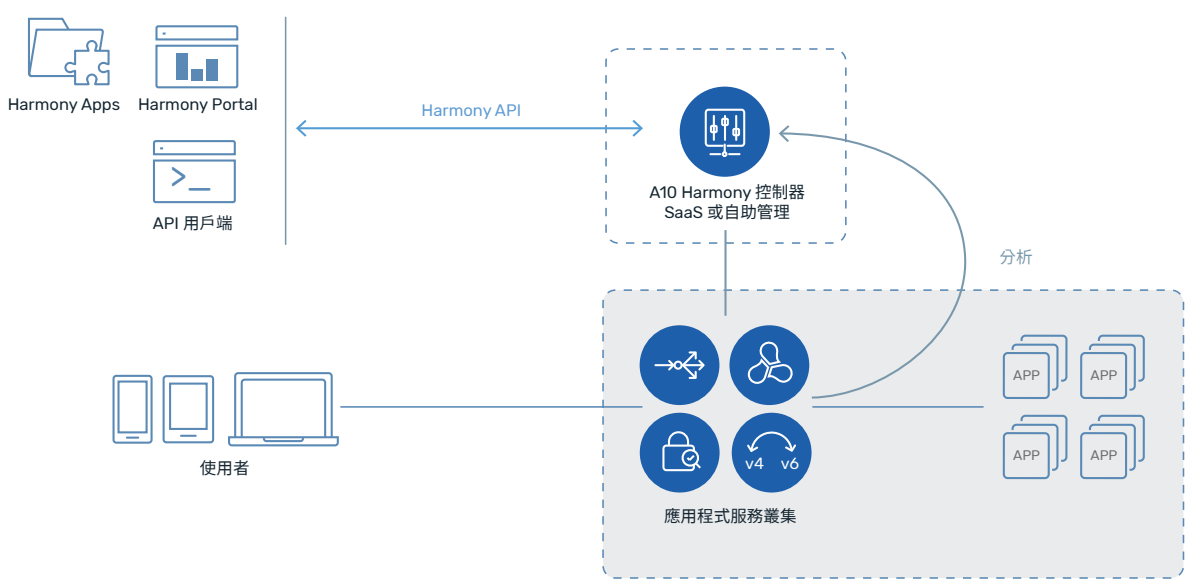


圖 3：Harmony 控制器可管理各種應用程式服務、用戶端 API 及管理功能。這項部署模型可協助組織在中央位置配置所有原則，不受應用程式部署地點影響。

## Harmony Portal

Portal 是可直覺操作的圖形使用者介面，以每個應用程式為基礎，透過角色型存取控制 (RBAC) 管理應用程式服務基礎架構及相關原則。Harmony Apps 提供以每個應用程式為基礎的可視性和見解，作業人員可於 Portal 挑選及啟用。其自助服務功能讓中央 IT 管理員無須設定及配置每個應用程式的基礎架構，從而達到最高的敏捷度及顯著減少營運成本，以支援多個應用程式團隊。

## Harmony API

這些 API 能夠進行編排和配置。所有應用程式服務功能都可透過 RESTful 介面提供。API 可與 Chef、Puppet 及 Ansible 等部署自動化工具整合，也可與 Jenkins 等 CI/CD 工具整合。分析 API 也可存取每個應用程式的指標和記錄，並可與第三方工具整合，或協助建構自訂儀表板。

# 部署模型

## SaaS — 由 A10 管理

雲端型 Harmony 控制器以「即服務」形式提供，由 A10 完全管理及監控。應用程式團隊可直接在 SaaS Harmony 控制器取得「租戶」帳戶，或是由組織 IT 團隊取得「供應商」帳戶，用於管理各自的內部或外部租戶。

只有控制訊息、指標及遙測資料會經由安全的 TLS 加密通道，在控制器和 A10 Thunder 裝置等服務執行個體之間傳送。應用程式流量不會通過控制器。這樣可以確保資料留在客戶網路內部。

控制器是以強化作業系統為基礎建構而成，以高可用性配置安裝，並託管於公有雲供應商。A10 Networks 授權人員會操作及執行定期安全掃描與稽核作業，檢查是否存在安全漏洞。控制器提供多層級安全性，並接受審核以確保安全性及法規遵循。其中使用通過 VPN 及多因素驗證 (MFA) 所驗證的內部跳板伺服器，限制登入存取雲端資源。

安全清單及網路安全群組則用於控制通往資源的封包層級流量，並限制公共網際網路存取應用程式允許的連接埠。IP 表格用於在所有執行個體強化作業系統。子系統內部的資料交換會以強密碼及類似機密資料的密碼進行加密；SSL 私密金鑰會以強加密技術處理並儲存於資料庫中。外部存取一定要透過業界標準的 TLS 通訊進行。

## 自助管理 — 內部部署及雲端

控制器也可在客戶資料中心或雲端等環境內部，部署為由客戶管理的可擴充軟體解決方案或硬體設備，包括裸機伺服器、以 Hypervisor 為基礎的 VM、Amazon Web Services、Google Cloud Platform 及 Microsoft Azure。

自助管理控制器可安裝於執行 CentOS 或 RHEL 7.4 以上版本作業系統的任何實體或虛擬機器執行個體。控制器採用內部微服務架構，可讓控制器達到最高的可用度。此外這項架構也能在控制器與應用程式服務之間連線中斷時，確保絕對不會發生流量中斷的情況。

## Harmony 控制器軟體系統要求

Harmony 控制器可於任何裸機、Hypervisor 或雲端執行個體的 Linux 機器 (CentOS 或 RHEL) 以獨立或高可用性 (HA) 形式安裝。HA 支援三節點部署 ( 例如虛擬機器或裝置 )，可在節點故障時提供恢復能力。微服務及控制器的資料儲存會分散在三個節點之間。

實際的資源需求取決於受管理裝置的數量和所需分析。安裝 Harmony 控制器時並不需要準備特殊或高規格硬體，可使用任何等級的伺服器硬體。SSD ( 固態硬碟 ) 儲存裝置因具備高 IOPS 值而成為首選。如需深入瞭解系統需求及安裝控制器的先決條件，請參閱最新產品文件或聯絡 A10 銷售代表。

# 授權

控制器軟體訂閱的價格是根據受管理裝置使用的頻寬單位。前述頻寬單位稱為受管理頻寬單位 (MBU)。每個 Thunder 裝置都有固定的 MBU 值。頻寬單位集區可彈性靈活運用，以管理頻寬單位不一的不同受管理裝置。訂閱套裝方案提供一年或三年方案。所有訂閱方案都隨附金級 (Gold) 支援。A10 Thunder 裝置授權需另行購買。

## 支援的 A10 平台

### A10 Thunder ADC

A10 Thunder® ADC 為高效能的進階負載平衡解決方案，可確保應用程式高度可用、加速且安全無虞。

### A10 Thunder SSLi

SSL Insight® 功能是全方位的 SSL/TLS 解密解決方案，可協助安全裝置高效分析所有企業流量，同時確保法規遵循及隱私，並大幅提升 ROI。

### A10 Thunder CFW

A10 Thunder Convergent 防火牆具備資料中心防火牆、站台對站台 IPsec VPN、Gi/SGi 防火牆、GTP 防火牆及安全網路閘道，搭配 ADC 及 CGN 功能，是服務供應商和企業的理想選擇。

### A10 Thunder CGN

A10 Thunder® CGN 提供高效能及透明的網路位址，以及通訊協定轉換功能，協助服務供應商及企業延展 IPv4 連線並轉換為 IPv6 標準。

# Harmony 控制器功能清單

| Harmony Portal | |
|---|---|
| 裝置庫存 | 提供多種形式的完整裝置庫存，例如個別裝置檢視、實體叢集檢視和邏輯叢集檢視等。 |
| CLI 命令公用程式 | 可將單一或批次 CLI 命令同時推送至多個裝置分區。 |
| 裝置升級 | Thunder 裝置可由 Harmony Portal 於遠端進行升級。 |
| 監控裝置健全狀態 | Harmony 控制器可監控連網裝置的健全狀態，並提供可直覺操作的儀表板，包括每項租戶服務的系統使用率、裝置位置、事件及警示資訊。 |
| 裝置配置備份及還原 | Thunder 是全狀態 (state-full) 裝置，其配置可由 Harmony Portal 備份，並於需要時還原。 |
| 裝置管理及分析 | Thunder 裝置可跨不同地理區域部署在各種網路及雲端環境中，提供詳細的裝置層級分析功能。 |
| 集中配置工具 (Objects Explorer) | Object Explorer 可進行應用程式服務層級配置，適用於 ADC、GSLB、CGNAT、Gi/SGi FW、WAF 及其他應用程式和安全功能。此工具也能從連網的 Thunder 裝置掃描現有配置。 |
| 在雲端自動佈建 Thunder | Harmony 控制器能與私有雲/公有雲基礎架構環境互相操作，以便自動啟動及管理虛擬 Thunder 裝置。其中包括 AWS、Micrsoft Azure VMware ESXi、Kubernetes 及其他環境。 |
| **作業** | |
| RESTful API | Harmony API 可用於執行每項作業，包括裝置管理、應用程式配置及讀取分析資料等。這些 API 可達成任何整合或自動化。 |
| 比較多租戶與供應商租戶模型 | 管理功能在供應商與租戶之間分割。Harmony 控制器能夠託管多個供應商。每個供應商都有多個租戶及多個使用者。管理實體 (供應商、租戶或使用者) 數量無任何限制或授權，可依據需求建立 500 個以上管理實體。 |
| 多因素驗證 (MFA) | MFA 可確保帳戶存取安全無虞。SaaS Harmony 控制器可協助供應商管理員為供應商的所有使用者啟用 MFA。 |
| 角色型存取控制 | 具備適當權限的供應商、租戶或裝置層級使用者，只能存取自己獲得授權的區域。多個使用者可同時登入並管理各自的區域。 |
| 警示 | 從 ADC 收集的指標會依據使用者定義規則建立關聯及評估，以便提出警示。這類警示可透過電子郵件傳送以採取手動行動，或透過 Webhook 傳送，並使用 Slack 及 Microsoft Teams 等協作工具實現自動化。 |
| 外部驗證 | 供應商可為其使用者選擇驗證供應商。除了本機使用者驗證以外，任何以 LDAP、Radius 或 TACACS 為基礎的伺服器均可使用。 |
| 配置備份 | Harmony 控制器配置可透過排程定期備份進行備份並於外部儲存。 |
| 排程報告 | 可排程各種報告 (PDF 格式) 以進行定期管理。此外任何分析頁面也能輸出為 PDF。 |
| **安裝及維護** | |
| 跨平台安裝 | Harmony 控制器軟體可安裝於實體或虛擬 Linux 機器等任何環境。 |
| 自我修復的微服務型架構 | 控制器內部包含多項微服務。如果微服務停止運作，架構會自動讓微服務恢復運作。 |
| 透過 API 進行配置 | 控制器本身的配置作業，可透過控制器公開的 API 進行監控及變更。 |
| 災難復原 | 主動式及被動式控制器可部署於不同地理區域，以便在任何災害事件造成主要位置無法使用時快速恢復。 |

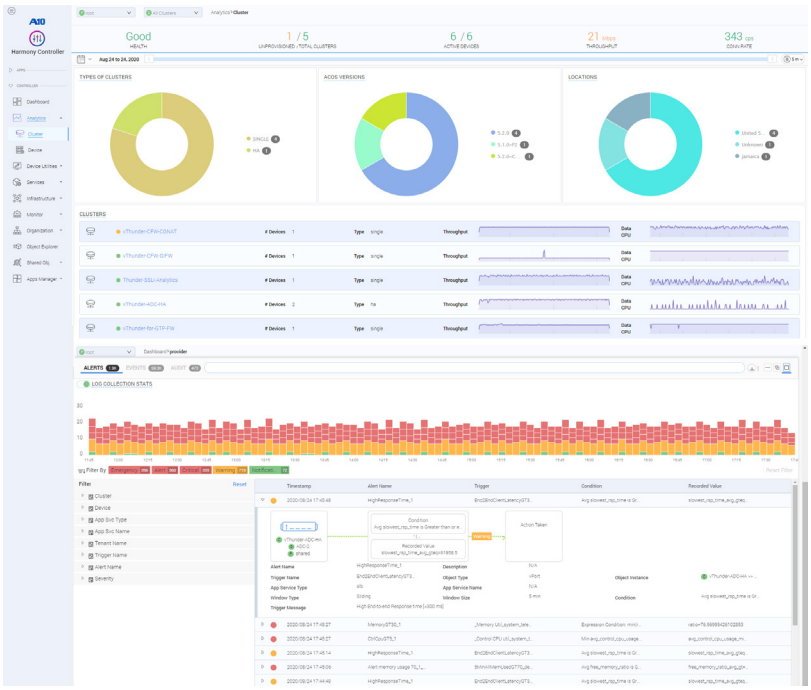

圖 4：Harmony Portal 提供完整的儀表板及分析功能，顯示安全應用程式服務基礎架構的健全狀態和事件。範例顯示裝置狀態及詳細的警示見解。

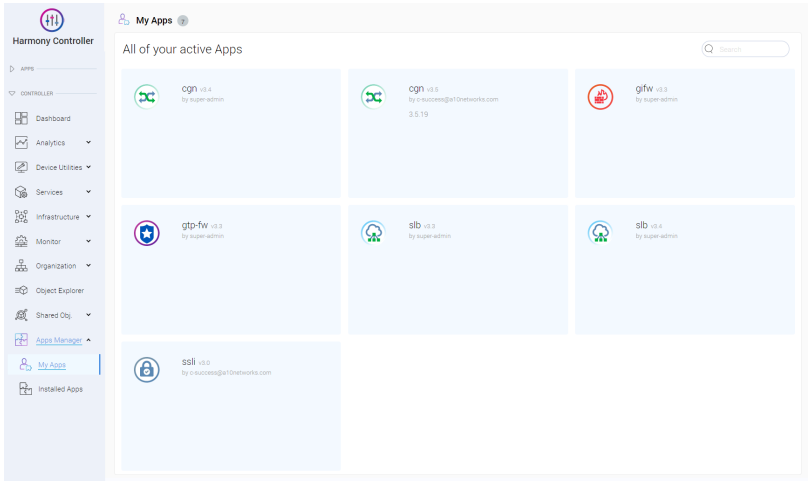


圖 5：Harmony Apps 集合。Harmony Apps 以每個應用程式為基礎提供完整可視性及分析，適用於 SLB/ADC、CGNAT、SSL Insight、Gi/SGi 防火牆、GTP 防火牆等等。

# Harmony Apps 功能清單

| ADC/SLB 應用程式 | | |
|---|---|---|
| 分析及見解<br>(服務通訊埠層級) | 用戶端 | • 使用者請求見解 - 請求方法、回應代碼及時間序列請求統計資料<br>• 平均端對端延遲可顯示用戶端在每個區段體驗的回應時間 (用戶端 - ADC - 應用程式伺服器)<br>• 用戶端見解 - 地理區域分佈、用戶端屬性 (包括作業系統、裝置、瀏覽器類型)<br>• 依據請求和處理量的主要用戶端 |
| | 網際網路 | • 依據地理位置的應用程式流量分析，協助掌握延遲時間、請求數 (HTTP/HTTPS) 及處理量 |
| | WAF | • WAF 原則違規見解，包括違規類型分佈、HTTP 閾值違規及通訊協定違規<br>• 依據類型的時間序列 WAF 違規統計資料<br>• 時間序列 WAF 請求處理及事件統計資料<br>• Cookie 安全見解<br>• 接收請求觸發 WAF 原則違規的主要來源 |
| | DNS | • 每秒 DNS 查詢 (QPS) 的時間序列圖表，依據查詢類型分組，例如 A、AAAA、CNAME 等<br>• 每秒 DNS 回應的時間序列圖表，依據回應代碼分組，例如 NOERROR、NXDOMAIN 等<br>• DNS 健全狀態、平均延遲及平均大小 (查詢/回應) 的時間序列圖表<br>• 格式錯誤 DNS 查詢率的時間序列圖表<br>• 產生查詢及造成 NXDOMAIN 回應的主要 DNS 網域名稱<br>• DNS 流量的主要來源 (IPv4/IPv6)，以及依據查詢數量、NXDOMAIN 回應、查詢大小及回應大小的分佈情形<br>• 依據唯一用戶端 IP 位址的 DNS 流量時間序列圖表<br>• 依據回應來源 (DNS 快取、DNS 伺服器、GSLB 等) 分析 DNS 回應 |
| | ADC 服務 | • 連線數及回應數在各個應用程式伺服器之間分佈的時間序列圖表<br>• 時間序列應用程式流量處理量 (上行鏈路/下行鏈路)<br>• 平均逆向及正向延遲的時間序列圖表<br>• 含回應代碼 3xx、4xx 及 5xx 的錯誤流量數的時間序列圖表<br>• HTTP2 見解 – HTTP 流量時間序列，包含 Proxy 連線統計資料、流量、關閉的串流、傳送至用戶端的框架類型等<br>• TLS/SSL 見解 – 用戶端側及伺服器側的 TLS 連線時間序列<br>• RAM 快取使用率及壓縮使用情形的 HTTP 加速見解 |
| | 應用程式和應用程式伺服器 | • 時間序列應用程式效能，包括回應時間及端對端延遲<br>• 應用程式服務見解，包括造訪最多的 URL/網域、最慢的 URL 等<br>• 時間序列後端伺服器見解，包括伺服器健全狀態、回應時間、新連線及現有連線 |
| | Thunder Cluster | • ADC 裝置/叢集系統使用率 (CPU、記憶體) 及處理量 (峰值及平均值)<br>• 部署位置世界地圖<br>• 雙向 (傳入及傳出) 處理量及作用中工作階段的時間序列叢集流量圖表<br>• 時間序列服務分區層級延遲見解 (正向、逆向、第一個位元組時間 (TTFB)、最後一個位元組時間 (TTLB)) |
| | 延遲深入研究 | • 延遲分析概觀<br>• 完整請求回應週期的時間序列平均端對端延遲 |
| ADC 服務儀表板<br>(全域) | | • ADC 服務層級 KPI (關鍵效能指標) 列，包含全域即時 ADC 流量統計資料，其中包括處理量、目前連線、連線速率及錯誤流量率<br>• 服務庫存資訊，包含服務連接埠統計資料及狀態、全域部署位置、事件記錄及警示<br>• 全域 (租戶層級) ADC 流量見解儀表板，顯示流量模式、特性、平均端對端延遲及前 20 名應用程式服務 |
| 集中 ADC 配置工具 | | • 共用物件可集中管理原則及範本，適用於 ADC 服務範本、WAF 規則、安全原則、aFleX 指令碼、健全狀態監控範本等，並可在多個裝置之間共用<br>• 服務物件提供可直覺操作的 ADC 虛擬伺服器 (VIP) 配置工具，將共用物件之中建立的服務範本、安全原則及其他物件建立關聯 |
| 工作階段記錄<br>深入研究 | | • 詳細的 ADC 交易記錄提供用戶端資訊 (IP、位置、裝置等)、ADC 服務資訊 (例如 VIP、服務連接埠、通訊協定)，以及包含請求和回應詳細資料的交易詳細資料<br>• 回應時間分佈代表各個請求及回應階段的工作階段延遲 (RTT)<br>• WAF 事件的詳細交易記錄可提供違規詳細資料 (類型、類別、WAF 原則及行動)<br>• 易於使用的搜尋及篩選功能可支援加速 ADC 服務疑難排解<br>• 指出網路及應用程式層的潛在問題/瓶頸 |

## 用戶端和 WAF 視圖

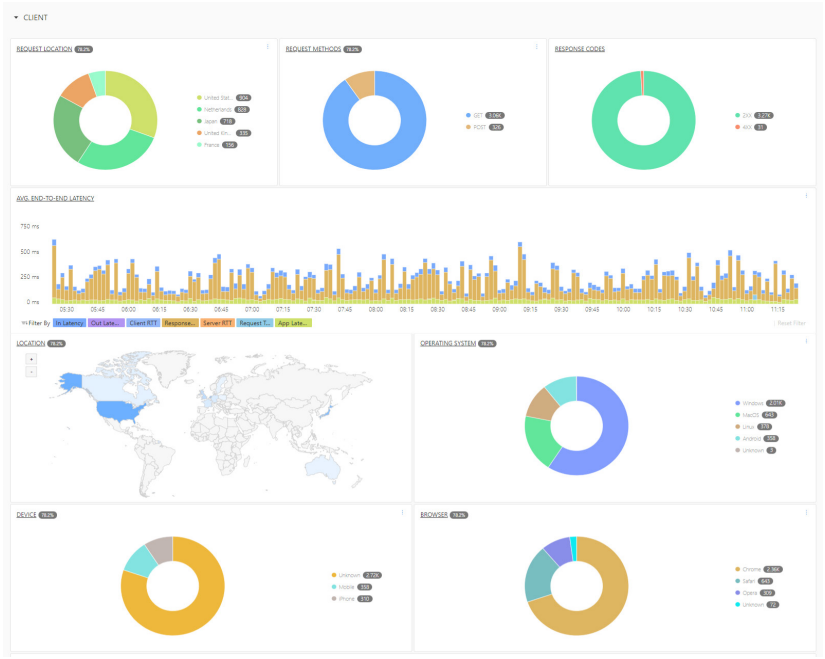


圖 6：ADC Harmony 應用程式可提供多層面的應用程式分析及見解，包括用戶端 (範例)、網際網路、ADC 服務、應用程式、應用程式伺服器等。

## 回應時間詳細資料

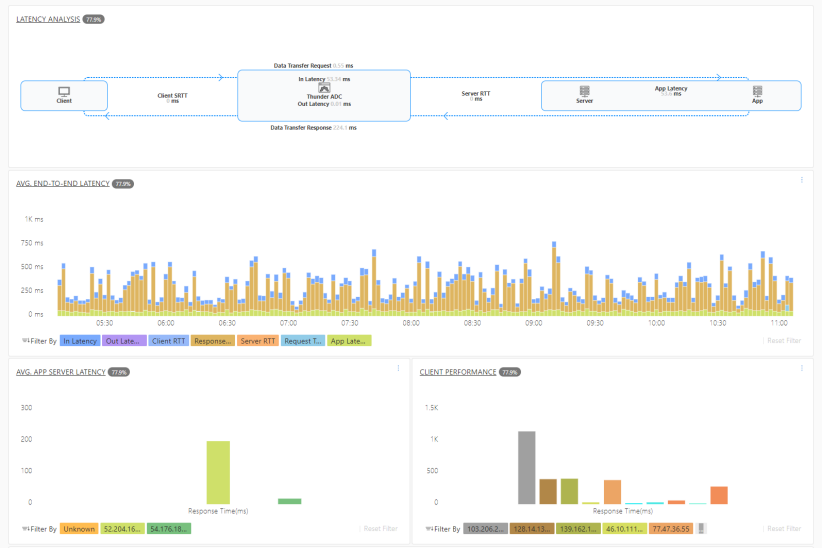


圖 7：延遲深入研究分析可提供完整請求回應週期的時間序列平均端對端延遲。這有助於疑難排解延遲回應時間相關的應用程式效能問題。

| SSL Insight 應用程式 | | |
|---|---|---|
| 分析及見解 | 流量見解 | • TLS 檢測狀態可依據連線及流量提供總數及時間序列圖表<br>• TLS 密碼分析可依據用戶端及伺服器連線用於分析金鑰交換方法及 TLS 版本<br>• 依據連線及流量提供通訊協定和區段的時間序列流量分佈<br>• 每秒及依據流量的時間序列 TLS 連線<br>• 依據連線及流量提供主要的 TLS 解密來源 IP |
| | 應用程式見解 | • 依據連線及流量的主要應用程式<br>• 依據連線及流量的主要 SaaS 應用程式<br>• 依據連線及流量的主要高風險應用程式<br>• 應用程式流量分配<br>• 成長的主要應用程式及類別<br>• 列出觀察到的所有應用程式通訊協定 |
| | URL 見解 | • 依據連線及流量的主要 URL 類別<br>• 依據生產力、敏感度、IT 資源及隱私群組的 URL 類別見解<br>• 依據連線的可疑 URL 類別<br>• 可疑類別群組的時間序列連線圖表<br>• 前 5 大 URL 類別的時間序列連線圖表 |
| | 來源及目的地見解 | • 依據連線及流量使用桑基圖進行來源和目的地 IP 分析<br>• 依據連線及流量進行來源和目的地 IP 的帕雷托分析<br>• 依據連線及流量的主要目的地國家/地區 |
| | 威脅見解 | • 依據威脅類別篩選的時間序列偵測威脅圖表<br>• 依據各個類別連線及主要 IP 的威脅類別分佈<br>• 依據流量及連線的威脅分佈國家/地區地圖 |
| | Threat Investigator | • 這款威脅情報研究及調查工具能夠迅速查看及調查個別網際網路物件的潛在風險，包括 IP、URL、檔案及應用程式。 |
| | 觀察清單 | • 依據 URL 及應用程式類別監控 TLS 流量<br>• 建立自訂應用程式清單，於時間序列圖表監控使用者流量<br>• 建立自訂 URL 類別清單，於時間序列圖表監控使用者流量 |
| 裝置管理及配置工具 | | • SSL Insight 服務層級 KPI (關鍵效能指標) 列包含裝置群組健全狀態、即時 SSLi 流量統計資料、服務可用性、錯誤率等<br>• 部署精靈提供直覺引導的配置功能，適用於各種部署選項 (單一或雙重設備、包含或不含高可用性、L2 或 L3)，並提供建議的安全原則<br>• 站台群組及站台拓撲支援眾多主要的部署拓撲。在相同站台群組新增新裝置/站台就和複製現有站台一樣簡單<br>• 支援單一裝置層級配置及管理，用於一般系統設定、介面及網路、附加安全授權<br>• 原則管理工具可實現集中 SSL Insight 服務及原則配置，適用於裝置群組內的所有裝置<br>• 共用物件是各種 SSLi 配置的抽象層，包括 ACL、原則範本、SSL 設定檔、URL 篩選、ICAP、AAM、G-suites、Office 365 等 |
| 工作階段記錄<br>深入研究 | | • 記錄檢視提供存取記錄、SSLi 連線記錄、錯誤記錄及系統記錄的擴展檢視和搜尋功能，協助進行疑難排解<br>• 搜尋含未分類 URL 的工作階段記錄 |
| 疑難排解工具 | | • 主動及引導的驗證測試，適用於系統、資源及端對端通訊<br>• 指標關聯可用於比較相同裝置的不同 KPI，以及比較不同裝置的相同 KPI |

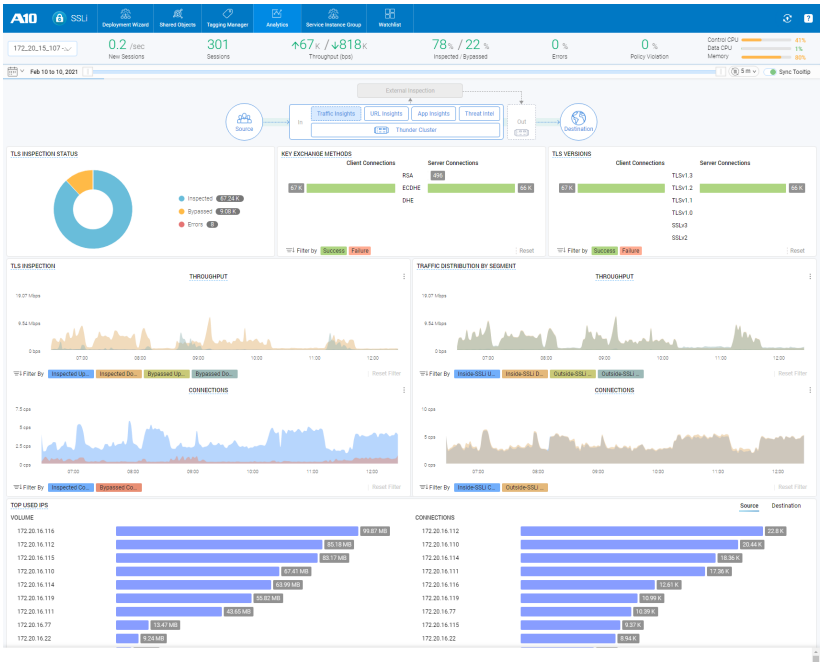

圖 8：SSL Insight 應用程式可針對 TLS 的應用程式流量提供全方位分析，此外還可進行集中原則控制，以及使用可直覺操作的精靈型配置工具。

圖 9：SSL Insight 分析可從 IP、TLS 流量模式、URL、應用程式類別、裝置及其他項目等各種層面，具體呈現各種流量見解。

## CGNAT 應用程式

| | | |
|---|---|---|
| 分析及見解 | 流量分析 | • CGNAT 服務層級 KPI (關鍵效能指標) 列包含即時流量統計資料及裝置健全狀態<br>• 主要訂閱用戶 (IPv4/IPv6) 和時間序列同時連線數及工作階段率<br>• 於上行鏈路和下行鏈路測量的訂閱用戶側時間序列總流量 (處理量及封包率)<br>• CGNAT 服務分析用於連接埠對應 (通訊協定)、時間序列工作階段統計資料 (使用者配額、Full-Cone 工作階段、EIM/EIF、Hairpin 連線)、NAT 集區、不當行為/錯誤流量統計資料<br>• CGN 裝置/叢集統計資料，以及網際網路 (上行鏈路) 側的流量統計資料和見解 |
| | 訂閱用戶連接埠使用情形 (適用於固定 NAT) | • 訂閱用戶連接埠使用關聯性 (TCP/UDP)<br>• 連接埠範圍內的訂閱用戶流量模式見解<br>• 有效訂閱用戶 |
| | 應用程式可視性 | • 主要應用程式圖表 (每個規則集)<br>• 依據連線及流量的應用程式流量分佈<br>• 依據類別/觀察清單的應用程式見解 |
| | SYN Cookie | • 回應 ACK 通過 SYN Cookie 檢查的 TCP SYN Cookie 數量，對比回應 ACK 未通過 SYN Cookie 檢查的 TCP SYN Cookie 數量<br>• 傳送的 TCP SYN Cookie 數量，依據通過/未通過/傳送的 ACK 等條件進行篩選 |
| | IP 異常 | • 比較正常封包與異常事件的見解<br>• 依據下行鏈路、上行鏈路、第 3 層及第 4 層等條件篩選<br>• 異常類型與層的分佈情形 |
| 儀表板 | | • 整體 CGNAT 服務租戶檢視，包括警示及事件、地理區域部署位置、CGNAT 服務 KPI 評分卡<br>• CGN 服務類型檢視提供 KPI 快照列及深入研究統計資料，包含訂閱用戶、目前工作階段數量及工作階段率、處理量 (bps)、封包率 (pps)、NAT 集區使用 (TCP/ UDP)、裝置狀態 (資料及控制 CPU、記憶體的使用情況) 等 |
| 集中 CGNAT 配置工具 | | • 集中配置 LSN/NAT44、NAT64 及 DNS64<br>• 物件用於定義類別清單、IP 清單、網域清單、記錄、NAT 集區 DDoS 防護、NAT 集區及 NAT 集區群組、範本 (HTTP ALG 及 PCP) |
| 疑難排解 | | • 下降分析可協助視覺化呈現鏈中封包下降發生的地方，以便迅速掌握問題及其根源<br>• 時間序列圖表會在時間軸上疊加警示和事件，協助使用者輕鬆建立與效能或錯誤的關聯性，迅速發現問題<br>• 異常偵測功能配置後可用於偵測任何時間序列資料的高峰並產生警示 |
| 工作階段記錄深入研究 | | • 詳細的 CGNAT 交易記錄可提供訂閱用戶資訊 (IP、MSISDN、IMEI、IMSI)、NAT 工作階段、連接埠對應、通訊協定、CGN 原則等<br>• 詳細錯誤交易記錄可提供訂閱用戶資訊、NAT 集區、通訊協定及原因/錯誤類型<br>• 易於使用的搜尋及篩選選項，適用於工作階段和錯誤記錄 |


圖 10：CGNAT 應用程式提供全方位的可視性及見解，協助以每個 CGNAT 服務為基礎掌握訂閱用戶流量。

| GTP 防火牆應用程式 | | |
|---|---|---|
| 分析及見解 | 流量見解 | • GTP FW 服務層級 KPI (關鍵效能指標) 列包含即時流量統計資料及裝置健全狀態<br>• 漫遊地理位置檢視以 GTP 工作階段數為基礎，適用於漫入及漫出<br>• GTPv0-C、GTPv1-C、GTPv2-C 及 GTP-U (上行鏈路/下行鏈路) 的時間序列 GTP 流量見解<br>• 以下項目的時間序列 GTP 流量分佈及比較圖表：<br>- 訊號閘道 (SGW) 及訊號閘道安全網路 (SGSN)<br>- 封包資料網路閘道 (PGW) 及閘道 GPRS 支援節點 (GGSN)<br>- 存取點名稱 (APN)<br>• GTP 工作階段的時間序列 CFW 叢集流量統計資料 |
| | 原則違規 | • GTP 防火牆原則行動時間序列統計資料，以及依據違規類別的原則違規見解<br>• 以下項目的時間序列 GTP 防火牆原則違規分析 (使用違規類型分佈及比較)：<br>- 訊號閘道 (SGW) 及訊號閘道安全網路 (SGSN)<br>- 封包資料網路閘道 (PGW) 及閘道 GPRS 支援節點 (GGSN)<br>- 存取點名稱 (APN)<br>• 防火牆規則效能分析及舊型規則指標 |
| | 漫入 | • GTP 漫入工作階段統計資料，以其在世界地圖檢視中的來源國家/地區為依據<br>• 依據記錄數、MMC 及 MNC 的漫遊來源國家/地區清單 |
| | 漫出 | • GTP 漫出工作階段統計資料，以其在世界地圖檢視中的目的地國家/地區為依據<br>• 依據記錄數、MMC 及 MNC 的漫遊目的地國家/地區清單 |
| 工作階段記錄深入研究 | | • 詳細的 GTP 防火牆工作階段記錄，提供來源/源頭、目的地、訊息類型、工作階段詳細資料 (通訊協定、使用者位置資訊 (LUI)、QoS 等)、記錄原因及防火牆規則/行動資訊<br>• 易於使用的搜尋及篩選選項，使用 GTP 通訊協定類型、IP、TEID 等 |

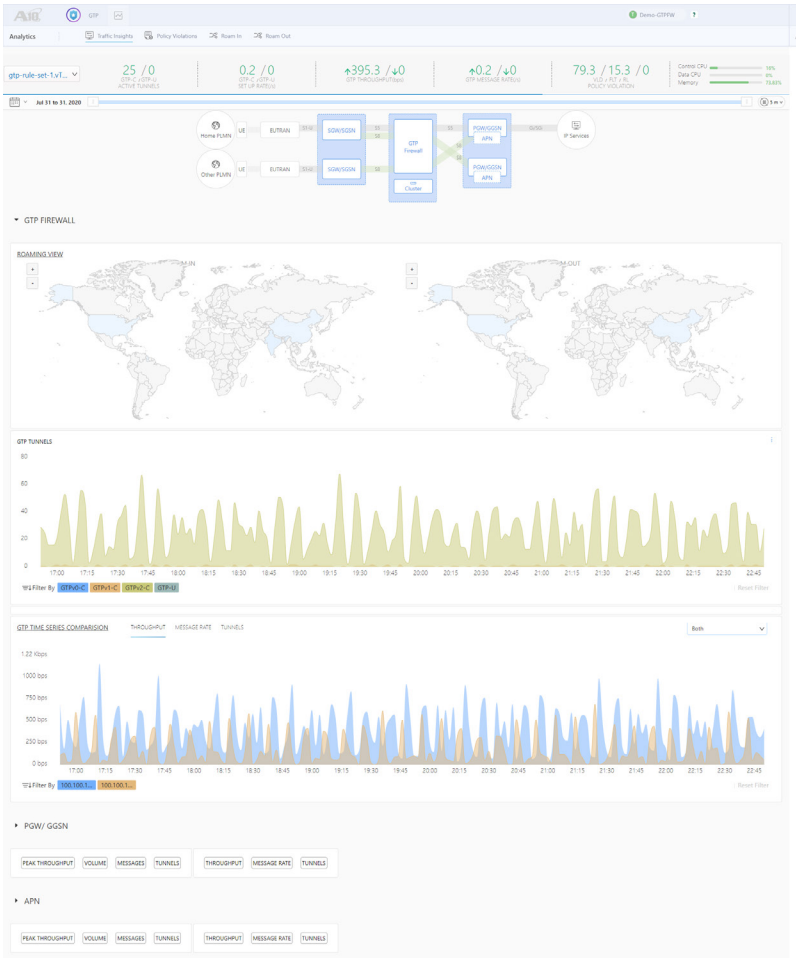


圖 11：GTP 防火牆應用程式為漫遊流量提供全面檢視及分析功能，其中使用時間序列 GTP 流量見解、GTP FW 服務層級 KPI、漫遊 (漫入 / 漫出) 工作階段統計資料、詳細工作階段記錄等。

| Gi/SGi 防火牆應用程式 | | |
|---|---|---|
| 分析及見解 | IP 流量 | • CGN 與 GiFW 服務層級 KPI (關鍵效能指標) 列包含即時流量統計資料、防火牆規則統計資料及裝置健全狀態<br>• 工作階段總數及工作階段率<br>• 總時間序列流量統計資料 (處理量及封包率)<br>• 依據處理量、工作階段及來源和目的地通訊協定 (IPv4/IPv6) 以前 K 名 IP 進行流量分析 |
| | 防火牆 | • 依據防火牆規則行動的時間序列流量見解<br>• 依據相符規則與下降流量的流量模式統計資料<br>• 各項行動防火牆規則的流量分佈<br>• 防火牆規則效能評分卡及舊型規則指標<br>• 依據流量、封包及工作階段 (IPv4/IPv6) 的主要訂閱用戶 |
| | CGN | • 以通訊協定為基礎的連接埠對應見解<br>• 時間序列連接埠對應統計資料<br>• 時間序列連接埠錯誤及超出配額統計資料<br>• 時間序列 NAT 集區使用率 (基於連接埠、基於 NAT IP、每 NAT IP 的訂閱用戶) |
| | 應用程式可視性 | • 主要應用程式圖表 (每個規則集)<br>• 依據連線及流量的應用程式流量分佈<br>• 依據類別/觀察清單的應用程式見解 |
| | 叢集 | • CFW 裝置/叢集系統使用率 (CPU、記憶體) 及頻寬<br>• 部署位置世界地圖<br>• 依據處理量及作用中工作階段的叢集流量見解 |
| 工作階段記錄深入研究 | | • 詳細的 CGNAT 交易記錄可提供訂閱用戶資訊、NAT 工作階段、連接埠對應、CGN 原則等<br>• 詳細的防火牆/透明工作階段記錄可提供訂閱用戶資訊、防火牆規則及行動、區域、進入/離開介面及工作階段狀態<br>• 易於使用的搜尋及篩選選項，適用於 NAT 和防火牆工作階段記錄 |

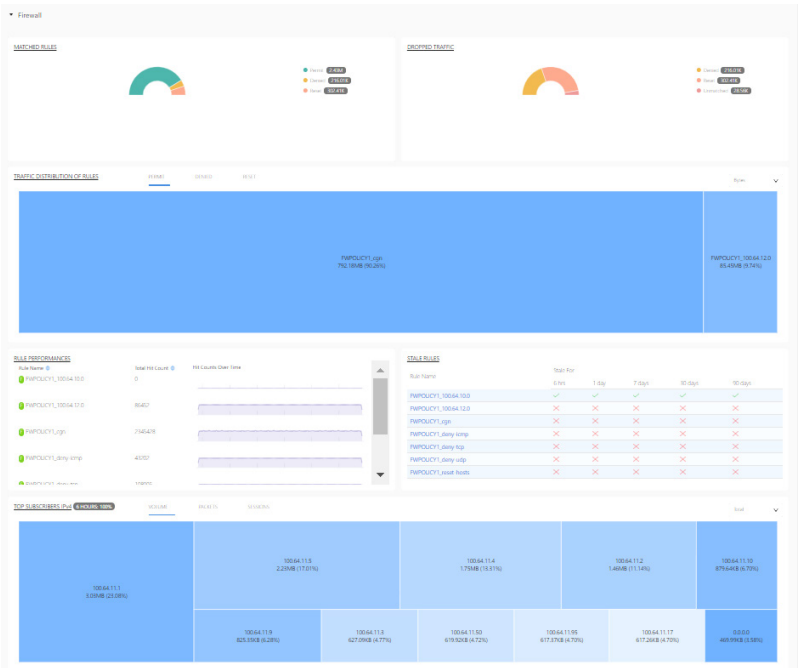

圖 12：Gi/SGi 防火牆應用程式可詳細分析使用者流量，提供時間序列流量見解、防火牆規則持久性、CGN 及 GiFW 服務層級 KPI 及許多其他項目。

## 深入瞭解

### 關於 A10 Networks

### 聯絡我們

APAC@a10networks.com



Part Number: A10-DS-15122-TW-15 April 2023