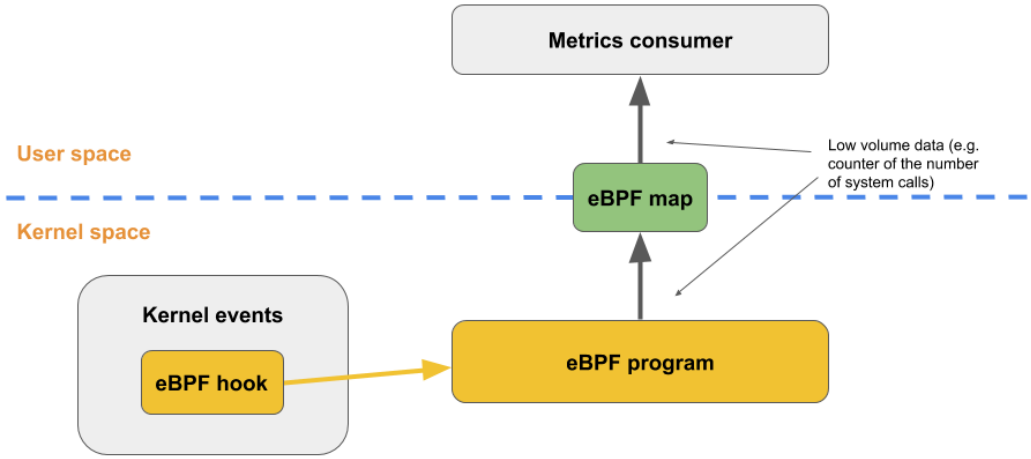
# Sysdig - Kubernetes 安全防護者

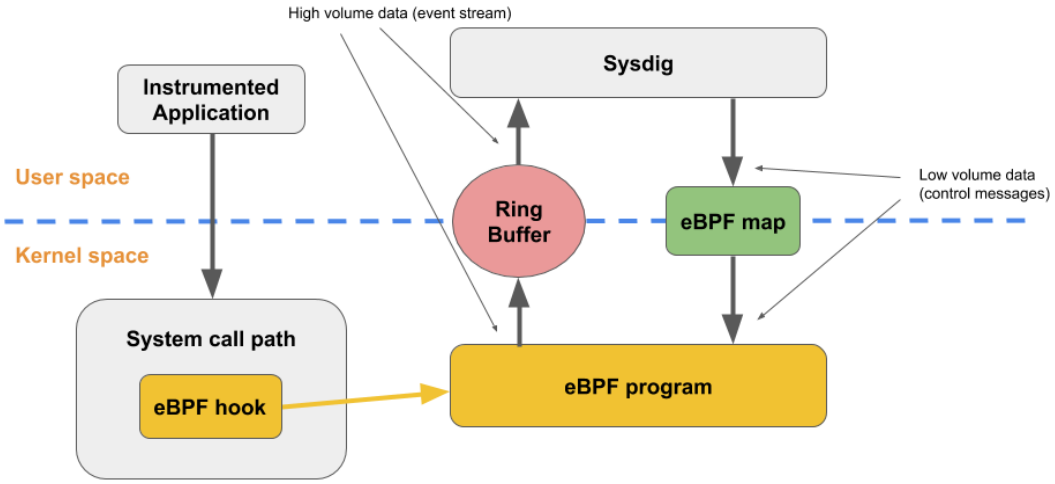
Sysdig 是一個針對 Kubernetes Cluster 的監測工具，它會探索與記錄 Kubernetes Cluster 中所有的運算執行機器節點的系統狀態與運作活動，並且將收集到的相關資訊加以保存並透過 Dashboard 以圖形化方式呈現所監測到的運作狀態與效能數據，即時呈現當下 Kubernetes Cluster 整體、各個運算機器節點的資源使用狀況和各 Pods 即時的運作狀況，讓管理者可以輕鬆地掌握整個 Kubernetes Cluster 環境。

## Sysdig 架構

eBPF(Extended Berkeley Packet Filter)是一套全新且功能強大的 Linux Kernel 功能，它適用於監測探索整個 Linux 系統的狀態與執行在 Linux 上的網路和所有各項程式執行活動狀況，如下圖(一)所示；Sysdig 是實作 eBPF 技術，它透過 eBPF 技術來追蹤與監控 Kubernetes Cluster 中所有運算執行機器節點與部屬在執行機器節點上的所有 Pods 的狀態與運作狀況，如下圖(二)所示。




圖(一)　eBPF 架構



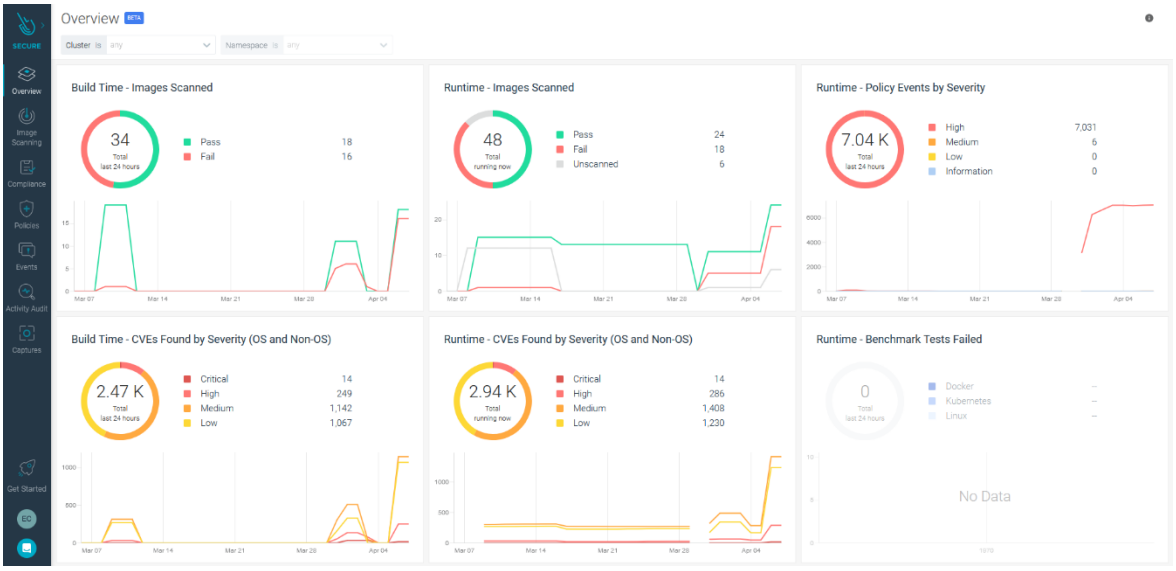

圖(二)　Sysdig 架構

## Sysdig 主要的系統功能

Sysdig 提供許多 Kubernetes Cluster 環境的安全監控機制，接下來列出幾項 Kubernetes Clusters 環境中重點且有用的功能做簡單的介紹說明：

## 詳細的儀表板

Sysdig 提供一個內容詳盡的數位儀表板，如下圖(三)所示；在儀表板上呈現所有被監控的 Kubernetes Cluster 的匯整或是個別的資訊，並且完整呈現當下安全性弱點的數據與各項安全描的結果，讓管理者可以清楚了解企業當下整個 Kubernetes Cluster 系統運作平台的健康狀況。

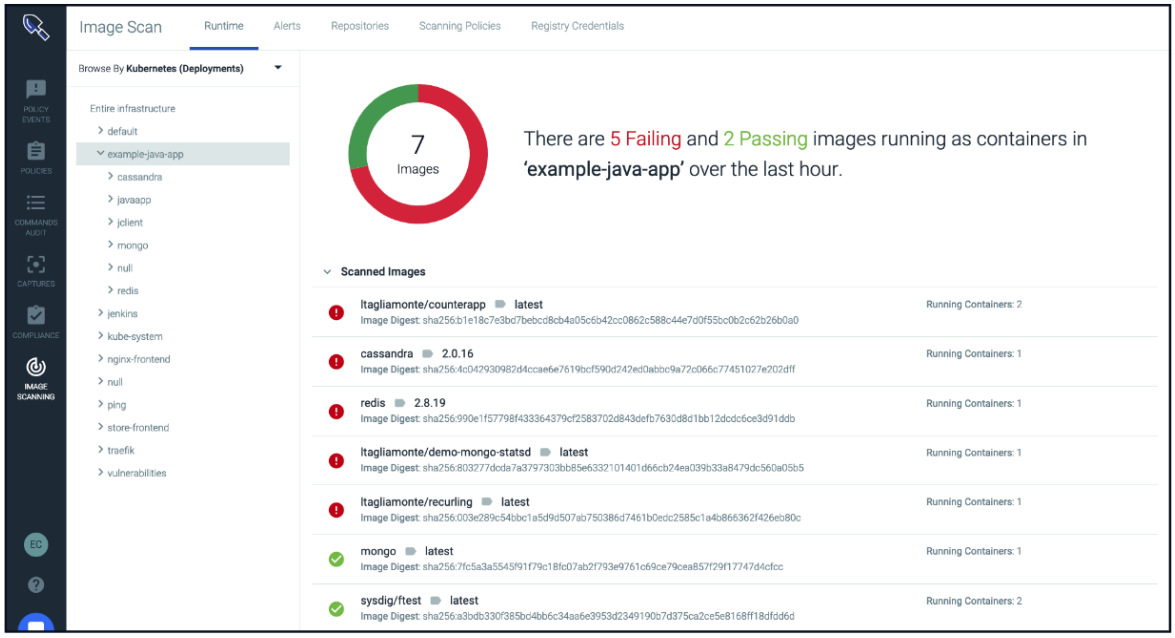



圖(三) 數位儀表板

## Image 弱點探測

所有的應用程式皆打包成 Image，應用程式 Image 裡面所打包的函式庫，若有安全性漏洞則會影響到應用程式的正常運作，嚴重可能會導致整個 container crash 造成服務中斷，或是影響 Kubernetes Cluster 環境運作造成其他應用程式運作異常；因此能夠在應用程式弱點曝露前，發現應用程式 Image 的安全性弱點，並且及早修復才確保應用程式的運

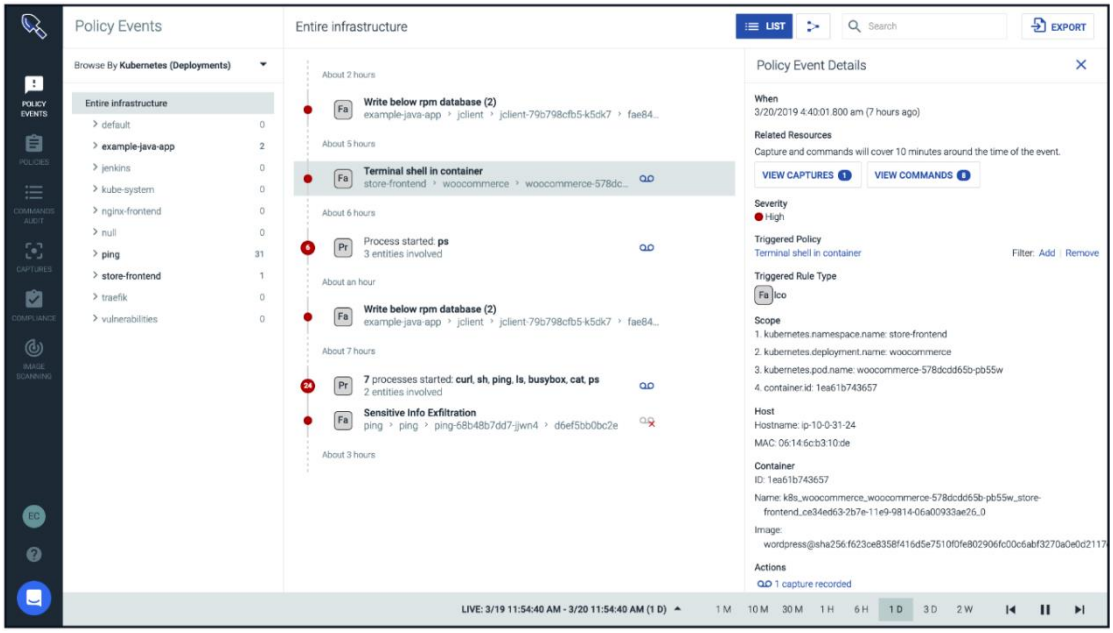
作正常，Sysdig 提供探測 Image 安全性弱點的功能，如下圖(四)所示；可以針對正在執行中或是未被執行的 Image 做完整呈現整弱點的探測，並且列出相關訊息與違反的安全規則項目，讓管理者可以知道該做何種修來排除此問題，以防範此弱點造成系統運作異常。




圖(四)　Image Scan

## Container runtime 安全機制

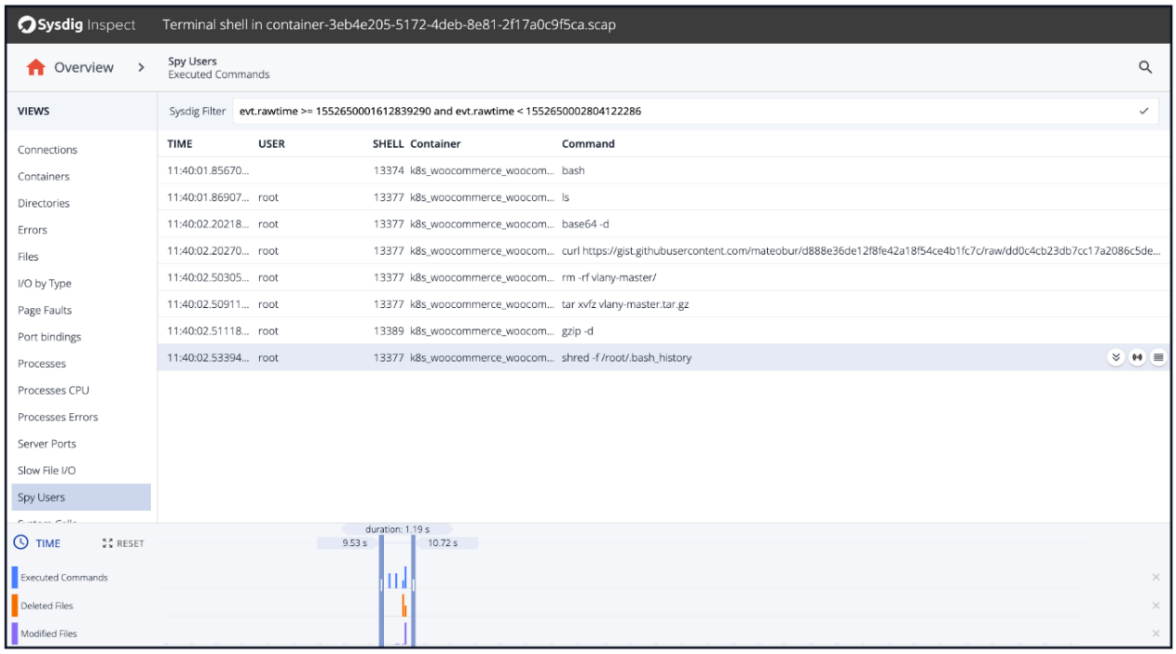
Sysdig 針對當 container 執行的指令操作違反定義的安全性規則時，Sysdig 可以限制該 container 後續的操作並且將其整個的運作狀況紀錄下來，然後將異常 container 運作視為一個安全事件，在儀表板上按照時間列出異常的 container 所違反的規則與所造成的影響，然後將其運作的動作做詳細的紀錄下來，如下圖(五)所示；針對當下發生異常的 container 可以呈現出其當下執行的指令資訊，以確認此異常的操作為行。




圖(五)　Container Runtime

## Container 故障排除

當 Container 運作異常時，Sysdig 可以把 Container 的異常操作動作記錄下來，然後按照時間呈現於儀表板上呈現出來，如下圖(六)所示；以清楚呈現問題發生當下的操作動作，用以釐清 Container 故障問題主因，以快速排除 Container 故障讓服務回復正常運作。




圖(六) Container Inspact

## 結語

Sysdig 是一套對 Kubernetes Cluster 環境開發出來的安全監測工具，其是實作 Linux Native Module 來監控 Kubernetes Cluster 環境，它可以提供完善對 Kubernetes Cluster 環境的安全監控，並提供易讀的圖形化儀表板介面，便於掌握環境所管理的 Kubernetes Cluster 的安全狀況。

想要了解更多 Sysdig 功能，可以到官網 sysdig.com 參考相關說明，有需要諮詢協助的地方，可直接聯絡：

Java 服務部

協理 陳金生 Edward Chen

02-27316868 分機 820

edwardchen@mpinfo.com.tw