結合雲端虛擬化叢集式架構與網路入侵偵測系統的網頁主機之可用性和安全性研究探討

Combined with cloud virtualization cluster architecture and web intrusion detection system Research on High Availability and Security

黃朝曦 張怡祥

Chao-Hsi Huang Yi-Shing Chang

宜蘭大學 宜蘭大學

資訊工程學系 資訊工程學系

副教授 研究生

chhuang@niu.edu.tw fastman9009@gmail.com

摘 要

本論文是基於『雲端時代』所做的探討，由於雲端虛擬化技術的成熟，業界中大量的運用虛擬技術來架設伺服主機。使用虛擬主機技術可以節省資訊基礎建設的成本，且可將有限的資源做彈性且充份的利用。但是現在越來越多種類的資安入侵攻擊行為，對於使用雲端虛擬化的平台也形成極嚴重的威脅。我們在虛擬化伺服主機裡，架設主機式的入侵偵測系統（Hosts based , IDS, Intrusion Detection System），可將實體機(Host VM)與虛擬機(Guest VM)的網路行為做全面性的偵測過濾。我們利用虛擬機器的快照技術 Snapshot，快速的建構起高可用(HA , High Availability)的叢集架構，避免(Host VM)因硬體故障或維修造成的服務中斷。在研究中;我們分析了[爆量式]的網站交量行為，虛擬環境中可以輕易的使用網頁式叢集架構(Web Based Cluster)與負載平衡技術(Load Balancer)，便可以在短時間處理大量的連線工作使得系統運作順暢。

關鍵詞：Cloud、KVM、IDS、RHCS、Web cluster

Abstract

This paper is based on the "cloud based" made by the discussion, Due to the maturity of cloud virtualization technology, The industry uses a lot of virtual technology to setup the server host. The use of virtual hosting technology can save the cost of information infrastructure . Can be limited resources to make flexible and full use. But now more and more types of security intrusion attacks, For the use of cloud virtualization platform also poses a very serious threat. We are in the virtualized host,Setup host-based intrusion detection system, Can be a physical machine (Host VM) and virtual machine (Guest VM) network behavior to do a comprehensive detection filter. We use snapshots of virtual machine. Quickly build a high availability cluster architecture. To avoid service interruption due to downtime. In the study, We analyzed the [huge amount] of the website traffic behavior, Virtual environment can be easily used Web-based cluster architecture and load balancing technology, It can be a short time to deal with a large number of connection work makes the system running smoothly.

1. 研究背景與動機

雲端時代:現今科技發展日新月異，無論是人工智慧、機器學習，或是虛擬實境、物聯網許多科技上的突破，無一不是與『雲端服務』密切結合。我們的生活正劇烈且迅速地被各種竄起的新技術與創新的概念大幅改變中。美國國家標準技術研究院 NIST [1]將雲端架構與特性定義，提出企業使用雲端服務的優勢，可節省掉資訊設備的建置成本。也可依企業本身的維運需求，自由選擇雲端的服務或調整所需的資源。在企業使用所選取服務後，取用的服務資源可以得到監測與評核，並以作為使用者使用以及供應商計費的標準依據。在雲端網路的服務之下，隨取可得十分的方便。

雲端資安的威脅:網路資訊服務越多元化，使用者越便利;然而，隨著網路資訊服務的快速擴展、延伸，系統、軟體的弱點堆疊起來，使得防火牆已不足抵擋來自四面八方的攻擊。前不久 Wanna-cry 橫掃全球，南韓的主機代管商 Nayana 也因客戶的主機遭受到攻擊，在無計可施之下，付出鉅額的贖款。雲端資訊產業界裡明顯的感受到威脅也明顯昇高。

總結; 在享受雲端服務的好處時，是否也造成企業身處資訊不安全的危機呢？雲端運算勢必為企業帶來新的資訊安全挑戰。

2. 研究目的

因此評估導入雲端服務(SaaS、IaaS 、PaaS)時，都必需考量「安全性」、「高可用性」、「雲端管理自動化」、「雲端效能調校」的問題，避免服務中斷可能造成的損失。另外;因網際網路應用發展快速，爆量「突波」式的交易活動造成系統的延遲(latcncy)問題[2]，本論文針三個議題進行研究探討。

1. **安全性:** 傳統的資訊安全防禦機制，不能有效保護雲端環境的安全，實體的資訊安全設備亦不能監控雲端環境所發生的事件，更不能於發生問題時，提供有效的防禦機制，因此需要導入新穎雲端資安技術，提供即時偵測及阻擋，以立即保護所有雲端虛擬主機。
2. **高可用性:** 雲端服務必需提供高可用性(HA,High Availability)信賴指標給使用客戶，服務中斷將造成使用用戶對雲端服務的不信任，使用叢集技術可避免因硬體故障，或維修所造成的服務中斷。
3. **爆量式的網頁交易:** 因爆量式的網頁交易;透過單台強大的伺服器處理運作是不夠的，雲端中可以輕易的使用叢集架構與負載平衡技術，便可以在短時間處理大量的連線工作使得系統運作順暢。

因此;本論文的研究目的，提供給自行架設私有雲的中小企業，一個「低成本」兼具「高可用性」叢集架構、且具「安全性」的解決方案。

3. 文獻的探討

本章節為整理國內外相關文獻研究結果，以作為本研究之實作根據。共分為 5 個小節，3.1 節介紹入侵偵測系統(Intrusion Detection System,IDS)，3.2 節則是介紹 OSSEC 主機式入侵偵測系統，3.3 節介紹基於核心層級的虛擬機器(Kernel-based Virtual Machine，KVM)，3.4 節介紹(RHCS, RedHat Cluster Suit)叢集架構，3.5 節對跟本研究的相關研究文獻做一個總結。

3.1 入侵偵測系統之介紹

在網路安全機制中，最廣為人知的，應屬防火牆。傳統防火牆提供三種機制-封包過濾(Packet Filter)、應用服務匝道(Application Gateway)及網路位址代轉(Network Address Translation)，主要是進行通訊封包的過濾分類，但是;無法防範精心設計規避的有心黑客。而入侵偵測系統(IDS,Intrusion Detection System)則是一種網路安全偵測系統，加強傳統防火牆所不足之處，透過比對主機上的「行為」、「安全日誌 Audit Log」、「稽核軌跡」或「入侵特徵資訊」，進行研判與比對，檢測出入侵企圖或疑似系統被入侵的異常行為，並且對於偵測到攻擊系統的行為，給予回應以維護系統的安全。

Mohd, Zuhairi, Shadil, and Hassan (2016)將入侵偵測系統(IDS,Intrusion Detection System)依偵測原理與偵測的架構[3]，做了以下的分類。

依偵測的方式可分:

1. **Anomaly-Based 異常偵測** :由於惡意軟體更新的速率越來越快速，異常偵測主要用來偵測未知的攻擊。通常會建立正常行為的標準值，當超過門檻時會觸發告警，通常採正面表列，即不在正常範圍內的行為均視為異常。缺點為導入期間需經長時間磨合期調校，合法的系統維護行為也可能被視為誤判造成假警報(False Postive)的情況。

2. **Signature-Based 特徵比對** (類防毒軟體偵測) : 透過偵測攻擊特徵(patterns) 尋找被入侵的跡象，例如檔案位元異動、異常網路流量或已知的惡意攻擊特徵，建立起入侵偵測系統的資料庫。這個偵測方式源自防毒軟體，可輕易偵測已知的攻擊。例如: /bin、/sbin 常用的指令被置換掉。缺點為無法偵測新型態(0 Day attack)的入侵攻擊，因沒有特徵值可參考，且進行大量特徵比對時，可能造成系統負荷過重。

依偵測的架構可分:

1. **主機型入侵偵測系統**(Host-based Intrusion Detection System,HIDS): 主要是針對單一伺服主機上的檔案、程式、日誌檔(Log files)及呼叫的指令等等，進行持續性的監控，如檔案刪除或修改權限、程式的異常行為，以及異常的系

統程式的呼叫，HIDS只要檢測判定為惡意行為時便會發出警告來通知網管人員，使其做出相對應的處理。

2. **網路型入侵偵測系統**(Network-based Intrusion Detection,NIDS)：主要藉由監控埠來監測來自網路的攻擊行為，針對網路封包的內容及標頭來進行分析以及流量管控，進一步根據分析的結果來判別封包的好壞以及流量是否正常。

3. **應用系統入侵偵測系統**(Application Intrusion Detection System,APIDS): 藉由監測在系統上的事件日誌中分析數據封包，查找特定的應用程序事件在日誌中記錄異常行為。例如:監測 Web Service 與Data Base之間的通訊與程序上的行為。

Network Based	*Host Based*	*Application Based*
analyze data packet in real-time	analyze Operating System event log to look for aberrant patterns in the system	analyze the application event log to look for aberrant pattern
Operate at Network node	Operate at Host node	

表1 IDS的分類

3.2 OSSEC 主機式入侵偵測系統

本研究採用 OSSEC 來建置入侵偵測系統，OSSEC(Open Source HIDS SECurity)是一套開源開放原始碼(Open Source)的主機型入侵偵測系統[6]。包括了日誌分析、系統檢測、rook-kit 檢測。作為一款 HIDS，OSSEC 安裝在一台實施監控的 Linux 系統之中。若有多台主機僅需安裝了 OSSEC 的 Agent，那麼就可以採用 Clinet 端/Server 模式來運行。Clinet 端透過客戶端 Agent 程序 將系統活動日誌發回到 OSSEC Server 端進行分析。

OSSEC 是依照特徵資料庫進行網路封包比對與行為的分析，當符合特徵資料庫中的紀錄時，就會發出相關的訊息。當特徵資料庫所搜集的特徵資料越多時，能夠偵測出來的異常網路行為就更廣泛。入侵偵測系統的目的，是希望能夠即時透過監控找出異常的狀態。馬上通知網路管理人員提醒資安事件的發生，且提供有效的資訊或是主動執行相關防護措施，以避免危害災情繼續的擴散。Tirumala(2015)研究中，將免費且為開放原始碼的入侵偵測系統做分析，其中在伺服主機上安裝 OSSEC Agent 幾乎不影響原有的效能，且提供了相當程度的保護措施[4]。

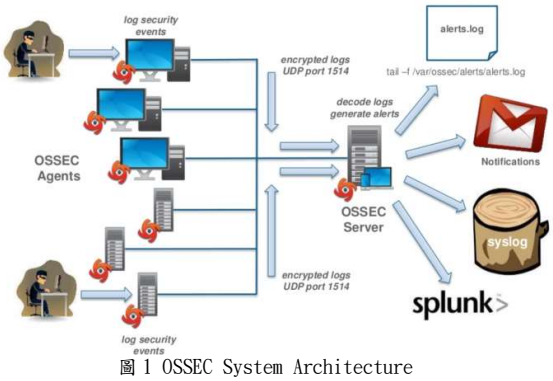

圖 1 OSSEC System Architecture

3.3 KVM(Kernel-base Virual Machine)

(Kernel-based Virtual Machine,KVM)基於核心技術的虛擬機器，是一種在 Linux Kernel 中的虛擬化基礎技術，透過載入模組將 Linux 系統轉換為 Hypervisor。KVM 在 2007 年 2 月被導入 Linux 2.6.20 核心中。KVM 需在具備 Intel VT 或 AMD-V 功能的 x86 平台上運行。KVM 目前由 Red Hat 廠商開發，對 CentOS/Fedora/RHEL 等 Red Hat 系列的支援度非常的高，Kourai 等人在 2016 年在研究中，提出在 Linux KVM 上的使用效能分析，說明 KVM 是中小企業導入虛擬化環境的良好方案[8]。

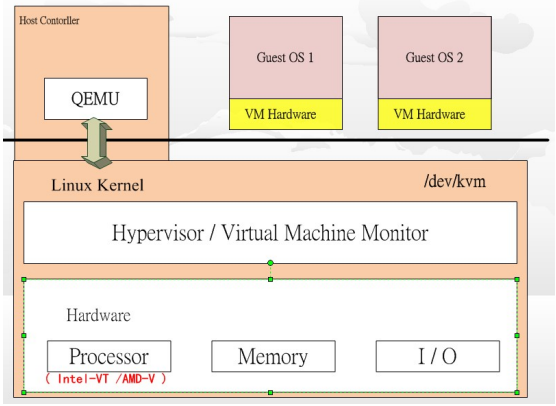

圖 2 KVM 架構

KVM 的架構(如圖 2)所示可區分成幾個部分，包含實體機器上所提供的硬體資源，如 Input/Ouput 的硬體裝置與 CPU 以及記憶體等等的硬體層(Hardware Layer)、運行在虛擬機器上的作業系統及應用程式的客戶層(Guest Layer)，以及負責管理硬體層資源及分配資源給客戶層虛擬機器的 Hypervisor/VMM 層。由於 KVM 必需要 CPU 支援虛擬化技術才能運行，而 Hypervisorr/VMM 負責控管所有虛擬機器的系統資源分配，KVM 的運行必須借助 QEMU 來虛擬硬體環境以及管理虛擬機器。在 QEMU 虛擬出硬體環境後，會在目錄/dev 底下建一個名為 KVM 的物件，QEMU 會將每個 Guest OS 的資訊存放在在個別的 KVM 容器裡，並且提供虛擬化的硬體空間讓每 Guest OS 都能擁有獨立，且不受其他 VM 干擾的空間。

3.4 RHCS, RedHat Cluster Suit 叢集

RHCS (RedHat Cluster Suit)是 Redhat 公司在 Linux 提供高可用叢集功能的解決方案[13] [14]。藉由消除單點失敗、將失效的服務可從無法使用的節點移往另一個叢集節點，高可用性的叢集提供無間歇的服務。通常高可用性的叢集會讀、寫資料(透過可讀寫、掛載的檔案系統)。因此，高可用性叢集必須維持資料的完整性，因為一個節點會接手另一個節點的服務。高可用性叢集外的使用者，並不會察覺節點失效。Red Hat Cluster Suite 透過「高可用性服務管理」(High-availability Service Management)元件，提供高可用性的叢集。

RHCS 透過 LVS（Linux Virtual Server）來提供負載平衡叢集(Load Balance Cluster)如(圖 3)，LVS 是開放原始碼、功能強大用於 IP 的負載平衡技術上，LVS 由負載調度器和服務訪問節點組成，通過 LVS 的負載調度功能，可以將用戶端請求平均的分配到各個服務節點，負載平衡叢集會分派網路服務的需求，送到多個叢集節點，好將負載平均分配到叢集的節點上。如果負載平衡叢集中的節點無法運作，那麼負載平衡的軟體會偵測到這問題，然後將需求導向至其他的叢集節點。對叢集外的 Clinet 端來說，並不會注意到叢集裡有個節點失效。

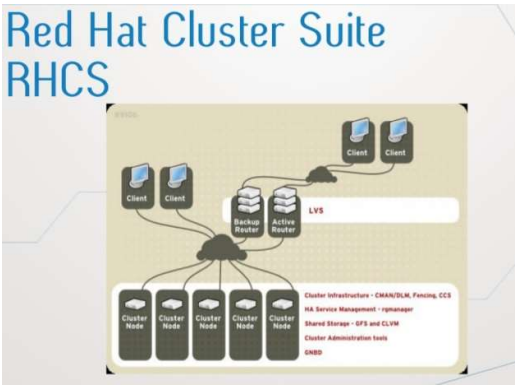

圖 3 RHCS Architecture

3.5 相關的研究文獻

3.5.1 VMM-IDS

陳陽昇(2016) Linux 核心層級入侵防禦系統反應機制的研究與實作之研究中;提出因網路技術的快速發展，駭客的攻擊方式也日新月異，保護系統安全最有效的防禦方法為入侵偵測系統(IDS)，它是一種網路安全偵測系統，對攻擊系統的行為進行偵測及回應以維護系統的安全。在其研究的實驗中結果中，顯示們實作的系統確可以有效地偵測且防禦惡意攻擊[21]。

蔡秉任(2014)在未知攻擊辨識之混合式入侵偵測系統之研究中;針對未知攻擊辨識之混合式入侵偵測系統，將自我學習機制套用在入侵偵測系統上，並由實驗結果可看到，系統對於未知攻擊的偵測能力有顯著性的改善，而在加強偵測能力的同時，其誤判率僅為些許的上升，整體的偵測精確性也是呈現上升的狀況[22]。

Mahajan and Peddoju (2017)針對雲端環境 Openstack 環境之下，提出惡意用戶可能從外部侵入危及雲端環境之安全問題。因此對雲端的服務的安全性持懷疑態度。所以他檢測各種攻擊模式應該有有不同的部署 IDS 入侵檢測系統的場景和檢測方法提出資安的疑慮與說明，並且在實驗中証明 OSSEC 在雲端架構之下確實有其重要性[5]。

Wang, Z 與 Zhu, Y(2017)針對雲端服務統容易受到威脅各種網路攻擊。 因此，入侵檢測系統（IDS）對於雲計算系統來說是非常必要的。主機式的入侵偵測系統 HIDS 可能消耗虛擬主機大量的系統資源。但是;在 OSSEC IDS 幾乎不用擔心這個問題，所以他檢測安裝過 OSSEC Agent 的機器，驗証系統資源上的變化而做出的結論[23]。

3.5.2 VMM-based Cluster

吳和融(2015)在研究中，提出如何有效率地提升伺服器的負載能力，使用伺服器叢集 (Server Cluster) 來提供網頁服務無疑是較好的選擇，研究中將使用 LVS 負載平衡器 (Load Balancer)的有效率網頁叢集伺服器 (Web Cluster)，能夠有效率地根據使用者所發出的應用層資料請求，平均分散負載至後端的伺服器來提供服務[19]。

Alagic, D., & Arbanas(2016)在雲端環境的研究中，提出雲端系統將越來越複雜。如何實現更高的系統可用性、可擴展性，建構所謂的 Storage Cluster 或 Web Cluster，在雲端環境中;可以用很低成本的方式建構叢集架構[9]。

杜睿嚴(2014)在雲端環境中資料儲存負載平衡之研究中，針對在叢集的研究裡，將叢集雲的網路拓撲，透過佛洛伊德演算法(Floyd-Warshall)取得每個客戶端對所有服務節點的最短距離。再收集所有客戶端對檔案的存取次數及各服務節點的負載狀況，依照取得的資訊，應用在所設計的負載平衡演算法中，計算出每個檔案最有利於客戶端存取的節點，以實驗證明所研究策略，可縮短每個客戶端存取所需檔案的延遲時間[20]。

3.5.3 突波式需求之網頁伺服器負載平衡架構

池至欽(2004)在其研究中，針對短時間內網路流量爆量所面臨網頁伺服器過載不敷使用及當機等狀況，提出大量網頁交易服務不太容易僅透過一台伺服器來單獨提供服務。叢集架構較能應付短時間大量的網頁伺服器連線服務。另外; 在系統負載吃緊時也可以機動地調派新的伺服器加入服務，而於負載較輕時，也可輕易地卸載部分伺服器而不致影響正常作業[16]。

4. 研究方法

4.1 研究的流程

首先確認研究的方向，其次;進行搜集背景技術與相關文獻資料。再以實作的方式建置 KVM 核心基礎虛擬技術(Kernel-based Virtual Machine) 的私有雲端主機，利用虛擬主機資源可彈性運用的特性，安裝 RHCS (RedHat Cluster Suit)用以建置 Linux 的高可用性(High Availability)及負載平衡（Load Balancing）的集群 Web 平台。並且架設 OSSEC 主機型入侵偵測系統，監控此平台的每一台虛擬主機(Guest OS)，以達到高可靠、穩定性、高安全性及永續不間斷服務的網頁伺服器，研究中;我們進行探討 OSSSEC 與虛擬化下叢集結合的可能性。並設計實驗的計畫，經由實驗得出實驗的結果，以驗證我們所導出結論(如:圖 1)。

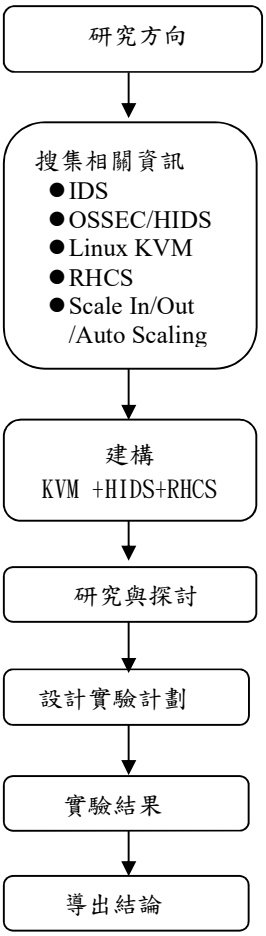

圖 4 研究流程

4.2 VMM-IDS

VMM-IDS 是針對虛擬機器執行環境所設計與實作的主機式的入侵偵測系統，它使用了 Linux Kernel 系統上的日誌記錄檔進行行為的分析，將所有經由網卡進入伺服器系統後，欲執行虛擬機器或實體主機系統服務的行為進行全面性檢測。都能夠經由 VMM-IDS 攔截且進行檢測，因此系統能夠同時保護本機及虛擬機器的安全。

4.2 .1 VMM-HIDS Architecture

在研究中;我們將 OSSEC HIDS 安裝在一台實施監控的 Linux 系統之中。另外在多台主機上安裝了 OSSEC 的 Agent，在虛擬化的環境上就可以採用 Clinet /Server 模式來運行(如圖 5)，Clinet 端透過安裝的 Agent 程序 將系統活動日誌(Log Files)發回到 OSSEC Server 端進行分析。可在一台主機上對多個系統進行監控稽核，對於網路的管理人員是非常實用的。因主機式入侵偵測系統是透過行為模式進行偵測的，所以安裝在虛擬化主機端上，也同樣兼具網路式入侵偵測系統的優點。

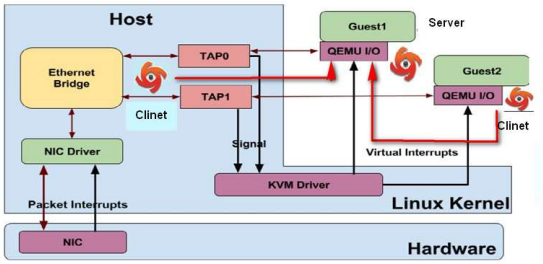

圖 5 WMM-HIDS Server/Client Architecture

4.2 .2 VMM-HIDS OSSEC 功能說明

OSSEC 可偵測主機上未經授權檔的案屬性變更（File Integrity checking）、網路上對主機的存取行為、監控主機上的各種日誌檔案（Log Monitoring）、監控主機上系統設定檔（Rootkit detection）進行比對入侵的行為，在發現異常事件後可主動執行相關防護措施以避免影響擴散（Active response）。

File Integrity checking	檢查檔案屬性，偵測未經授權的變更
Log Monitoring	監控各種日誌檔案，協助重要訊息監看
Rootkit detection	偵測潛伏系統的惡意軟體/後門程式
Active response	發現異常事件後可主動執行相關防護措施避免影響擴散

表 2 OSSEC 四大功能

OSSEC Agent 的運作說明:

1. (Syschenkd) :保護系統程序檢查配置的文件，以檢驗是否超過權限進行修改。
2. (Rootcheckd) :檢測可能的 rootkit 安裝與日誌分

析和完整性檢查引擎。

3. (Logcollector):系統日誌收集器。
4. Agent 將收集來的監測資訊，發送至 OSSEC Server 端的(Remoted)接收，再進入分析處理引擎(analysisd)。Server 端可透過(monitod)隨時知道 Client Angent 的健康狀況。

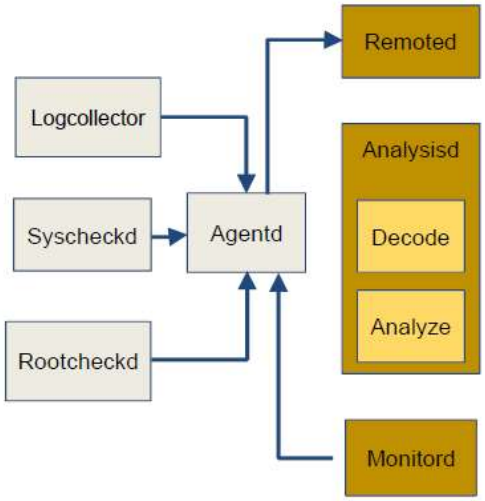

圖 6 Agent function

4.2.3 OSSEC Wazuh 的 ELK 分析平台

若有多台電腦都安裝 OSSEC Agent 後，就可採用用戶端/伺服器模式來運行。OSSEC 可另外再安裝 Wazuh 套件，Piazza, M (2016)針對 ELK 套件做以下的說明[7]，ELK(Elasticsearch, Logstash, Kibana)日誌管理平台,可透過 Kibana 的管理介面，將已部屬 OSSEC agent 的電腦系統進行弱點掃瞄，建構起符合(PCI-DSS) 網站應用程式的防護規範，客戶端通過用戶端程式將資料傳回到 OSSEC 伺服器端上的 Logstash 進行日誌的收集，通過 OSSEC 的 ElasticSearch 的資料搜尋分析系統，使用者便可使用 Kibana Web 視覺化的操作畫面進行資安分析與查詢日誌，Kibana 提供視覺化的圖表畫面，讓使用者很輕易的操作使用，並提供系統上的資安防禦的建議。在一台電腦上對多個系統進行監控對於中小企業來說都是相當方便的。

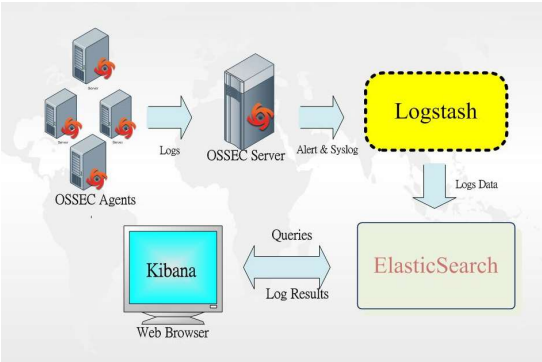

圖 7 Wazuh ELK Architecture

4.3 VMM-Web Based Cluster

若系統服務是由一台伺服器所提供，當此台伺服器發生故障時，對外服務就會中斷，即存在著單點失效的問題。目前有許多的應用程式、服務、交易系統都必須一天 24 小時不間斷的運轉，如各大網站、電商交易、數據中心、金融交易、軍事或醫療系統的監測儀器。對這些應用系統而言，短暫的停機都將導致數據的遺失或是災難性的後果。『高可用性的叢集』系統正是提供此問題解決方案，實現對外的永不間斷服務。

4.3.1 叢集介紹

Cluster 叢集主機群[10]的概念是指多台電腦透過某些技術或架構運作成單一系統，共同提供服務，多台電腦互相為備援，以維持伺服器與應用程式運作時間，確保服務的高可用性(HA, High Availability)指標。提供服務的多台主機，叢集主機會安裝相同的應用程式及設定以共同提供服務；依運用程式的架構不同，叢集主機可能會同時一起提供服務經由(Load Balance)派送工作、或由其中一台主機提供服務，當該主機因故無法提供服務 Failover 時 (例如故障或關機維修)，另一台主機會自動接替該主機執行服務(Active/Standby)，叢集主機群運行時會透過 HeartBeat 相互監視軟硬體狀態；在叢集架構中我們常以節點(Node)來稱呼叢集主機。

叢集架構中共用磁碟是很重要的，所有的服務資料都會儲存在共用磁碟中，所有的叢集主機也會存取相同的共用磁碟並看到相同的資料，以確保服務在節點之間轉移時的正確性，服務在移轉前後不會有資料遺失或不一致的情形發生。

4.3.2 Web based Cluster 介紹

Alagic 與 Arbanas, K (2016)在 Web Based Cluser 研究中[9]，將多台網頁伺服器組成 Cluster 叢集主機群後，用以提供一個不中斷的、可靠的、高流量的網站服務，當 Web Cluster Group 的 Load Balancer 接收到不同使用者的網站要求連線時，這些被要求的服務會被分散，交由 Web Farm 的叢集主機成員來處理。因此可提高網頁的存取效率，若成員中有網頁伺服器故障、無法提供服務，會有其他仍然正常運作的伺服器來繼續對使用者來提供服務(如圖 8)。

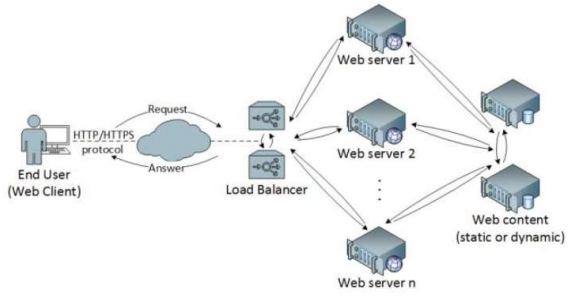

圖 8 Web base Cluster Architecture

目前主要的 Linux 發行版本基本都有提供高可用叢集(HA, High Availability Cluster)元件，主要

要的高可用叢集決方案，例如:SUSE 所使用的（High Availability Clustering）與（Geo Clustering）與 Redhat 所用的 RHCS(RedHat Cluster Suit)採用的，本論文所使用的 Linux 版本為 Redhat 與 CentOS，所以我們選擇以 Redhat 的 RHCS(RedHat Cluster Suit)做為研究叢集與負載平衡的最佳方案。相關研究如:陳建宏(2003) [11]與 Suntae, H, & Naksoo, J. (2002) [12]。

4.4 網頁式爆量式交易

很多人都曾經發生在網路上訂票一票難求的問題，整個網路卡到一個不行，等到自己連線進網站之後，卻發現票卻被一掃而空的現象[17]。例如:熱門演唱會門票(如圖 9)，對於; 爆量的交易量是無法光靠一台超級電腦處理的，池至欽(2004)的研究中提出[16]，雲端中可以輕易的使用『叢集架構』與『負載平衡技術』進行分散處理交易，便可以在短時間處理大量的連線工作，使得系統運作順暢。

圖 9 突波式交易爆量的問題

雲端服務供應商提供的解決方案為，虛擬機器自動擴增機制（auto-scaling mechanism）。當現有伺服器的負載過重，它會自動新增伺服器數，來分散負擔工作量。反之亦然，當伺服器大部分都在閒置時，則將工作集中，減少伺服器，以避免資源浪費，降低營運成本。這類的服務在亞馬遜的 EC2、微軟的 Azure、Google 以及其它供應商的解決方案都可以見到。

4.4.1 Scale-Up / Scale-In /Auto Scaling

以往在面對伺服器主機系統效能不夠時，按照傳統 Scale-up 的觀念，解決方案就是購買更新穎的主機硬體設備，更快速的運算能力，更高容量的存儲空間來更換，那麼難免面臨數據遷移的問題，用戶必需停機遷移數據，意味著服務的中斷。在 Cloud 雲端虛擬化的時代，高彈性的架構克服了這個問題。用戶按需新增一台主機，或是存儲硬磁陣列，系統無須停機遷移數據，且服務的不會中斷[15]。

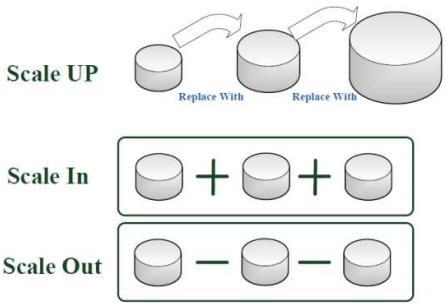

圖 10 Scale Up / Scale In /Scale Out

在傳統機房裡 scale up 是很常見的，但很少人會談到 scale down 的這個現象。原因;系統伺服器主機上硬體資源資源不足時，我們才會去考慮購買新的硬體資源去做硬體上的昇級動作。當在採買伺服器主機時，為了耐用度使用年限的延長，又必須放棄 Suitability『適合』目前使用所需硬體資源，而必需選擇較高規格的硬體需求。造成建置成本的增加，也形成了資源的閒置的情況(如圖 11)。所以;因為系統資源過度的閒置，而將伺服器主機換成較低硬體規格較差的情況，在傳統機房裡『scale down 並不存在』。

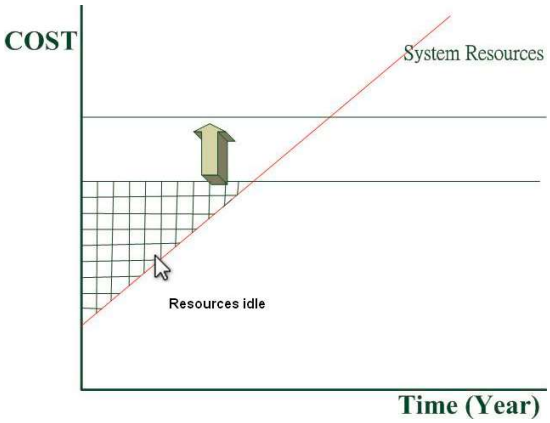

圖 11 傳統機房成本與資源的閒置

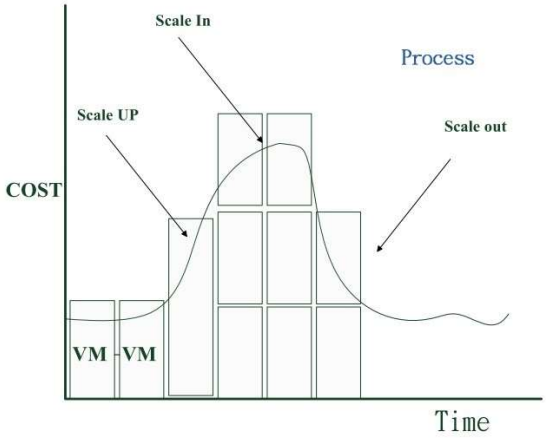

圖 12 Cloud Platform On-Demand

在雲端機房虛擬化後的主機(如圖 12)，可輕易的使用 Scale Up/Scale Down 或是 Scale In/Scale Out，為運作的系統的伺服主機，量身訂製適合且適量所需的硬體規格資源。雲端機房是採用 On-Demand Self-Service，依使用需求狀況自行使用隨時調節雲端服務。On-Demand 的精神為使用多少資源就支付多少費用，企業可以降低IT成本，也不再需要自己投資建製一個機房，減少資源閒置狀況。

以下以 Amazon 雲端機房的運作說明 Auto-Scaling:

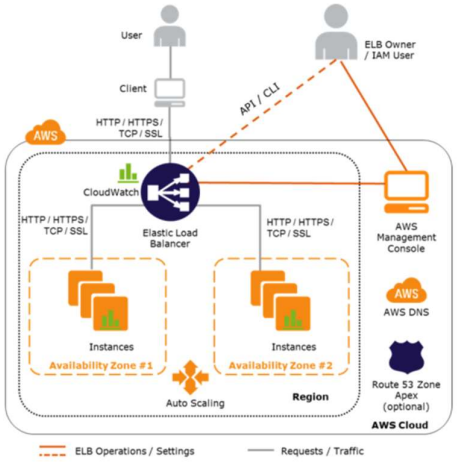

圖 13 Auto-scaling 與 ELB(Elastic Load Balancer)

AWS(Amazon Web Service) Auto Scaling 的原理 (Amazon) [18]：

(一)AWS 利用 Cloudwatch 偵測 Elastic Load Balance 控管下的每一台機器的繁忙程度(是依據 CPU 或記憶體、網路負載流量)。

(二)(scale-In)如果繁忙程度超過我們設定的上限，並且尚未超過設定的最大機器數，那麼就自動啟動一台機器，並將啟動完成的機器，自動配置到 Load Balance 下執行服務。

(三)(scale-out)如果繁忙程度低於我們設定的下限，並且尚未達到設定的最小機器數，那麼就關閉最閒的機器，以節省資源。

(四)在 ELB 的叢集環境架構下，Route 53 所負責的工作為 DNS 的指向工作。

本章節中; 我們研究與分析 Scale-in 與 Auto-Scaling，在叢集群分散式處理的目的與方法。並了解 web server 叢集群的應用，叢集可用以解決『突波式』的交易爆量的問題。而做出一個想法，我們利用 Linux OpenSource 的 RHCS 實作，建置高可用性叢集(HA, High-availability Cluster)應用，並以實驗驗証我們的假設。

5. 結論

市場上有許多的雲端供應商，提供著各式各樣的雲端服務。雲端服務對現在企業來說，固然給予、便利性、隨取使用、高彈性,等等的好處，但是;對雲端安全性仍有存疑保守心態的部份使用者，會以自行建置的私有雲，做為其公司的資訊基礎建設。

本論文的研究目的，提供給自行架設私有雲的中小企業，一個「低成本」兼具「高可用性」叢集架構、且具「安全性」的解決方案。

參考文獻:

[1] NIST, *The NIST Cloud Computing Project* (2017 年 9 月 23 日)，取自 https://csrc.nist.gov/CSRC/media/Events/Cyber-Maryland-Summit-(2010)/documents/posters/cloud-computing.pdf

[2]楊劍銘 (2017)IT,s 通訊，取自 http://newsletter.ascc.sinica.edu.tw/news/read_news.php?nid=2385

[3]Mohd, R. Z. A., Zuhairi, M. F., Shadil, A. Z. A., & Hassan, D. (2016). *Anomaly-based NIDS: A review of machine learning methods on malware detection*. Paper presented at the 2016 International Conference on Information and Communication Technology (ICICTM)

[4]Tirumala, S. S., Sathu, H., & Sarrafzadeh, A. (2015, 12-15 July 2015). *Free and open source intrusion detection systems: A study.* Paper presented at the 2015

[5]Mahajan, V., & Peddoju, S. K. (2017). *Deployment of Intrusion Detection System in Cloud: A Performance-Based Study*. Paper presented at the 2017 IEEE Trustcom/BigDataSE/ICESS

[6] OSSEC 官網 https://ossec.github.io/

[7]Piazza, M., Fernandes, J., Anderson, J., & Olmsted, A. (2016). *Cloud payment processing without ritualistic sacrifices reducing PCI-DSS risk surface with thin clients*. Paper presented at the 2016 International Conference on Information Society (i-Society)

[8]Kourai, K., & Nakamura, K. (2014). *Efficient VM Introspection in KVM and Performance Comparison with Xen*. Paper presented at the 2014 IEEE 20th Pacific Rim International Symposium on Dependable Computing.

[9]Alagic, D., & Arbanas, K. (2016, 2016). *Analysis and comparison of algorithms in advanced web clusters solutions.* Paper presented at the 2016 39th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO).

[10]國立台灣大學計算機中心及資訊網路中心，叢集技術與雲端服務。2017 年 9 月 23 日，取自 http://www.cc.ntu.edu.tw/chinese/epaper/0015/20101220_1505.htm

[11]陳建宏 (2003)。伺服器叢集系統的允入控制與負載平衡機制。(碩士)，國立中山大學，高雄市。

[12] Suntae, H., & Naksoo, J. (2002, 17-20 Dec. 2002). *Dynamic scheduling of Web server cluster*.

Paper presented at the Ninth International Conference on Parallel and Distributed Systems, 2002. Proceedings.
[13]壹讀網，解析 RHCS 高可用集群 HA 及負載均衡集群 LB 的實現方法，2017 年 9 月 23 日，取自 https://read01.com/ANBNR3.html
[14] Redhat Linux 官網，*Red Hat Cluster Suite 概論* 2017 年 9 月 23 日，取自 https://access.redhat.com/documentation/zh-TW/Red_Hat_Enterprise_Linux/5/html/Cluste,r_Suite_Overview/ch.gfscs.cluster-overview-CSO.html
[15]Programming4.,*Scale-up vs. scale-out storage*, 2017 年 10 月 07 日取自 http://programming4programming4.us/enterprise/18762.aspx
[16]池至欽（2004）。突波式需求之網頁伺服器負載平衡架構。(碩士)，大同大學，台北市。
[17]IThome 官網，【當系統遇上爆量搶票】百倍人潮擠爆系統，2017 年 9 月 24 日取自 http://www.ithome.com.tw/news/94531
[18]Amanzon 官網,*What is Amanzon Autoscaling,* 2017 年 9 月 23 日，取自，dhttp://docs.aws.amazon.com/zh_cn/autoscaling/latest/userguide/WhatIsAutoScaling.html
[19]吳和融 (2015)。支援需求內容分配與 TCP 快速開啟的有效率網頁叢集伺服器的設計與實作。(碩士)國立暨南國際大學，南投縣。
[20]杜睿嚴 (2014)。在雲端環境中資料儲存負載平衡之研究。(碩士)，大葉大學， 彰化縣。
[21]陳陽昇 (2016)。Linux 核心層級入侵防禦系統反應機制的研究與實作。(碩士)，國立暨南國際大學, 南投縣。
[22]蔡秉任 (2014)。針對未知攻擊辨識之混合式入侵偵測系統。(碩士)，國立交通大學，新竹市。
[23] Wang, Z., & Zhu, Y. (2017). *A centralized HIDS framework for private clou*d. Paper presented at the 2017 18th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD).