雲端技術及台大區網服務簡介

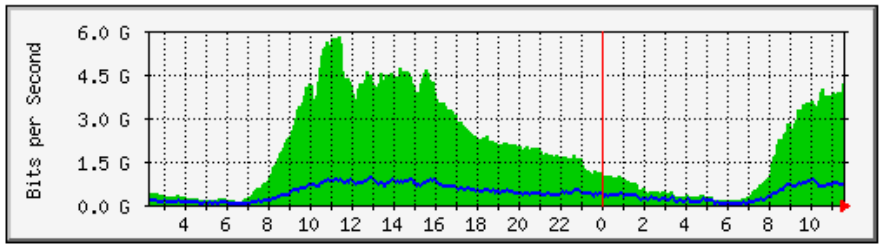
臺灣大學 計算機及資訊網路中心
網路組 曾保彰

為何需要雲端服務?

- 學術網路要節省頻寬
  - 師生常用的服務都在雲端
- 節省費用
  - 電力空調、網路、UPS等基礎建設
  - 主機、軟體、工程師的費用
- 資訊安全
  - 異地備援、主機每日備援
  - 防火牆、WAF 、IPS 、源碼檢測、滲透測試

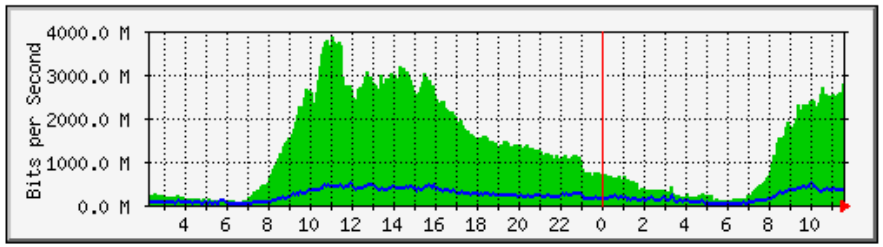
NBA 西區第七戰

GGC total

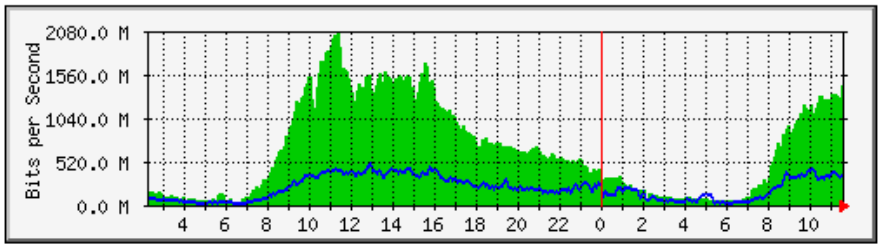


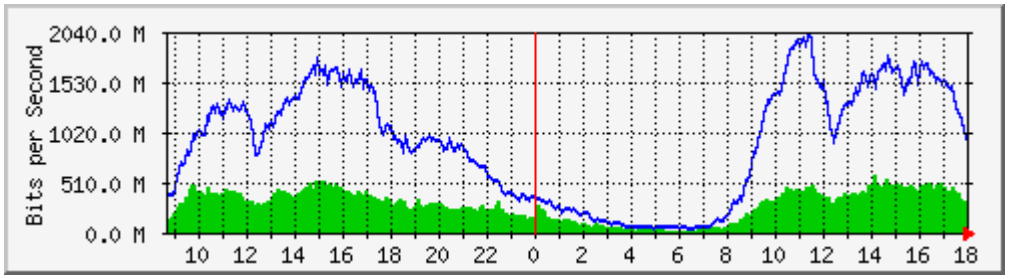
<a href="//video.udn.com/nba/510810" class="youtube" title="LeBron James總冠軍列戰好球" style="pointer-events: none; cursor: default;">

GGC1



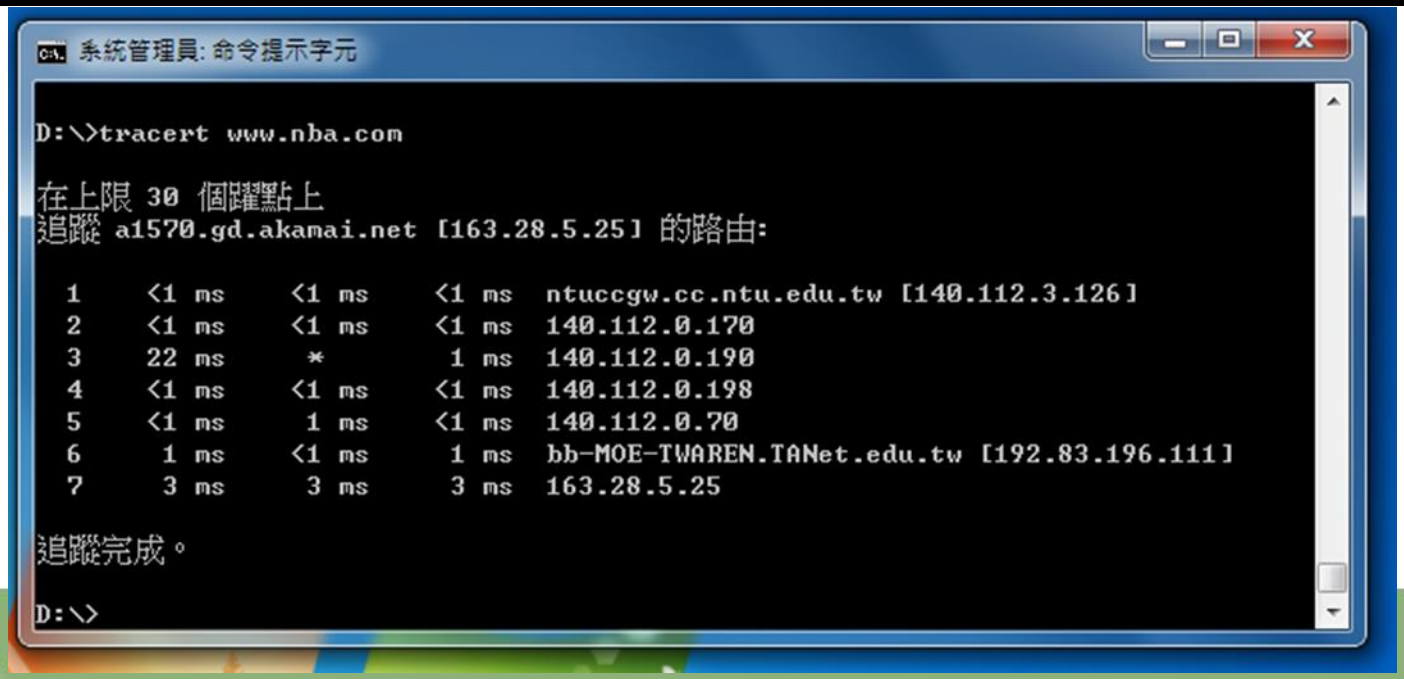
GGC2





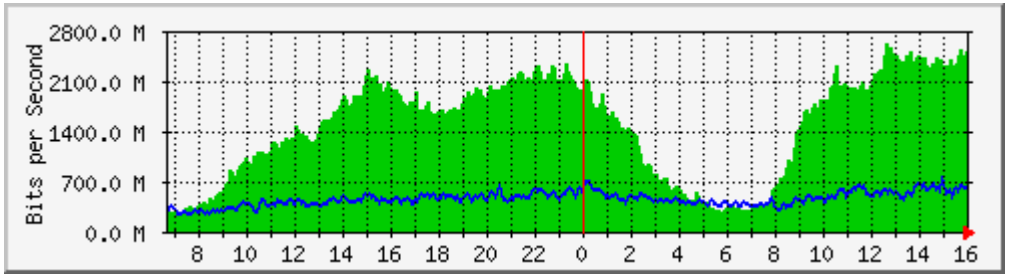
服務師生的重要服務在那?

```
C:\Users\bjtseng>tracert www.appledaily.com.tw

在上限 30 個躍點上
追蹤 a1085.w19.akamai.net [163.28.5.10] 的路由:

  1    <1 ms    <1 ms    <1 ms  ntuccgw.cc.ntu.edu.tw [140.112.3.126]
  2     1 ms     1 ms     1 ms  140.112.0.210
  3    <1 ms    <1 ms    <1 ms  140.112.0.186
  4    <1 ms    <1 ms    <1 ms  140.112.0.198
  5     1 ms     1 ms     1 ms  140.112.0.70
  6    <1 ms    <1 ms    <1 ms  bb-MOE-TWAREN.TANet.edu.tw [192.83.196.111]
  7     4 ms     3 ms     3 ms  163.28.5.10

追蹤完成。
```



Why at MOE

- PROXY service ?
  - https://www.google.com
  - https://tw.yahoo.com
- AMAZON CDN (CONTENT DELIVERY NETWORK)
  - spanning more than 175,000 servers in over 100 countries
- NTU TWGATE
- TP1RC GCC



AWS DATA CENTER

全球基礎設施

Amazon CloudFront

AWS 節點

以下 AWS 節點提供 Amazon CloudFront、Amazon Route 53 與 AWS WAF 服務：

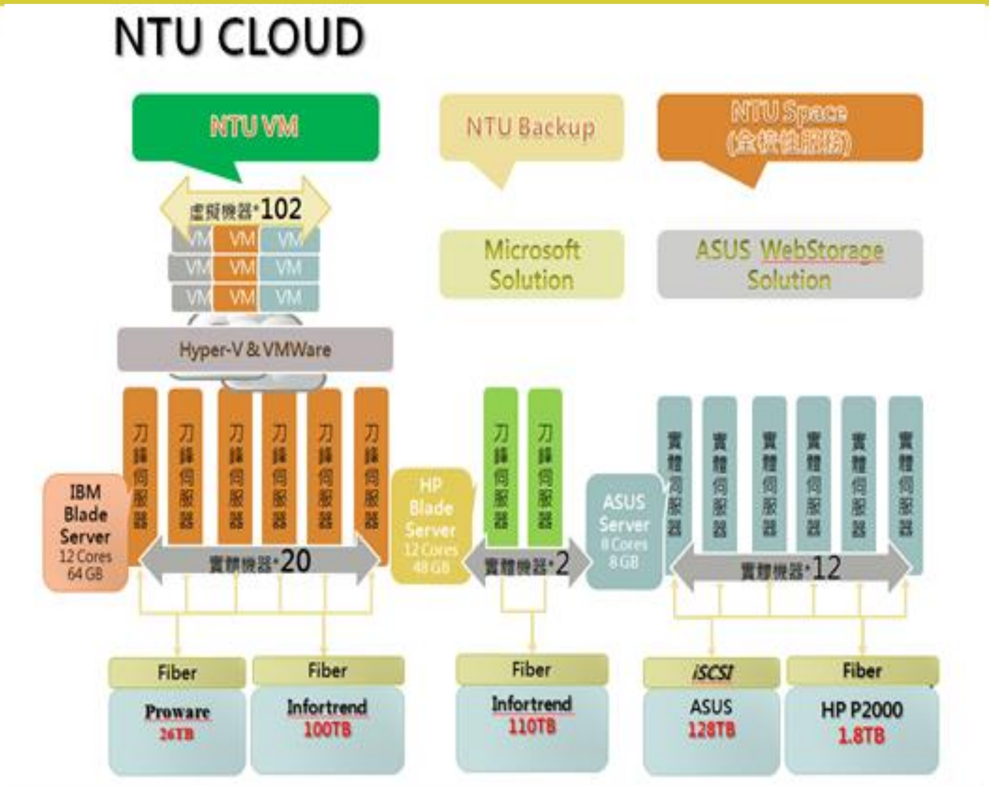
北美洲	南美洲	歐洲/中東/非洲	亞太區域
喬治亞州亞特蘭大	巴西里約熱內盧	荷蘭阿姆斯特丹 (2)	印度清奈
維吉尼亞州阿什伯恩 (3)	巴西聖保羅	愛爾蘭都柏林	中國香港 (2)
伊利諾州芝加哥		德國法蘭克福 (3)	菲律賓馬尼拉
德州達拉斯/沃思堡 (2)		英國倫敦 (3)	澳洲墨爾本
加州海沃德		西班牙馬德里	印度孟買
佛羅里達州傑克遜維爾		法國馬賽	日本大阪
加州洛杉磯 (2)		義大利米蘭	韓國首爾 (2)
佛羅里達州邁阿密		法國巴黎 (2)	新加坡 (2)
紐約州紐約 (3)		瑞典斯德哥爾摩	澳洲雪梨
紐澤西州紐渥克		波蘭華沙	台灣台北
加州帕羅奧圖			日本東京 (2)
加州聖荷西			

台大區網

- HINET 10G
- 和信 1Gbps
- 遠傳 2Gbps
- 台固 1Gbps
- 教育部 6G
- 台北市網 3.5G

- 未來教育部100G 其餘順勢升級

臺大觔斗雲 (2010 ~)



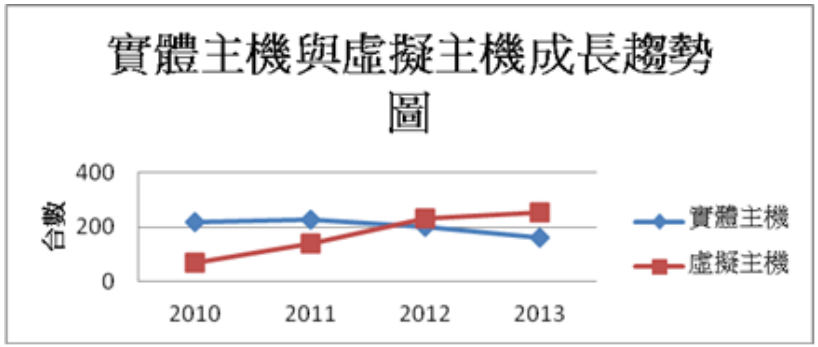
57 Servers、 485 TB 、 275 VM

EXAMPLE: mail 1.0 and mail 2.0 differences

臺大: 實體主機 vs. 虛擬主機

年度	計資中心採購伺服器量	其他單位採購伺服器量	全校總計
2010	19	199	218
2011	17	208	225
2012	15	185	200
2013	11	149	160
2014 上半年	11	57	68

年份	虛擬主機數目(累進)
2011 年 1 月-2012 年 12 月	140
2013 年 1 月-2013 年 12 月	231
2014 年 1 月-2014 年 8 月	251



2010至2013年臺大實體主機與虛擬主機成長趨勢圖

NTU Cloud: 一站搞定 = 運算 + 軟體 + 資料

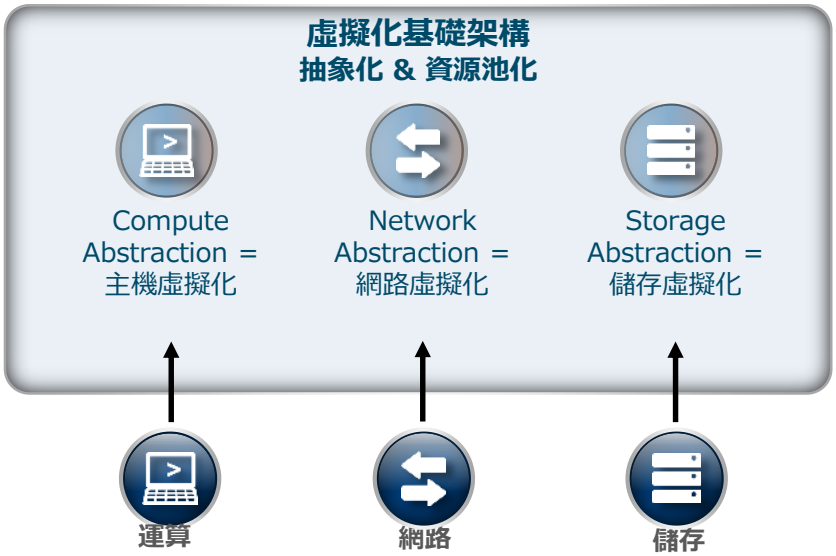
美國學網案例

- 美國國家科學基金會(NSF)於2014年8月花了2千萬美金，在全國各大學，成立"Chameleon"及"CloudLab"二個雲端測試平台，分別提供了650個nodes(含5PB的儲存空間)及15000 processing cores(1PB的儲存空間)，分別作不同的雲端服務測試，其中包括100G及SDN等最先進的網路架構。
- http://nsf.gov/news/news_summ.jsp?cntn_id=132377

為何要虛擬化?

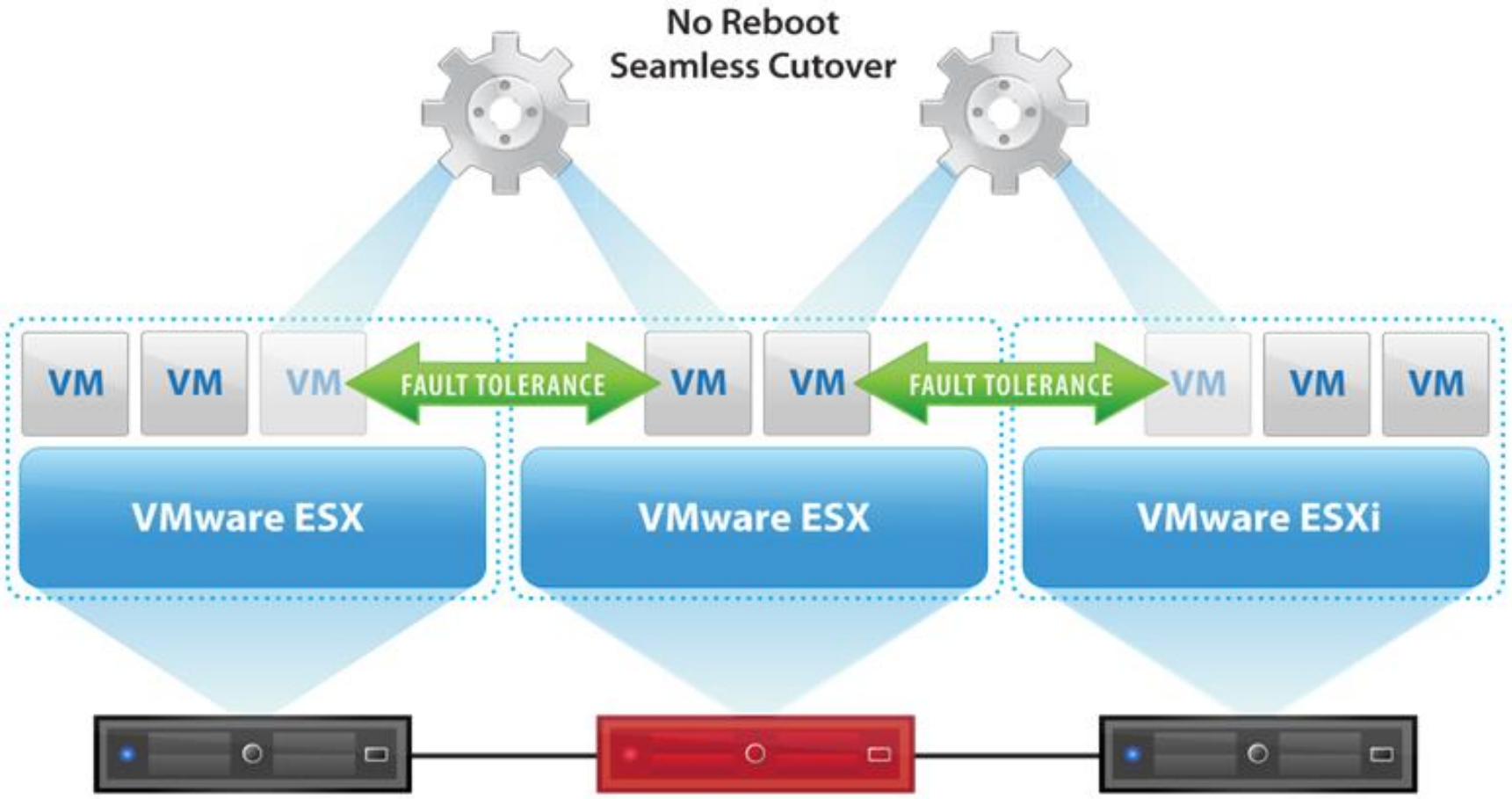
- 硬體愈來愈強,虛擬化的效能就逐漸被接受
- 主機虛擬化
  - 節能, 實體機:虛擬機=1:20,實體機:VDI=1:33
  - 備援, VDP備30天, DEDUP及COMPRESS
- 網路虛擬化
  - NSX, Nicira Network Virtualization Platform
  - SDN, Open flow 1.3
- 資料虛擬化
  - VSAN

虛擬化基礎架構

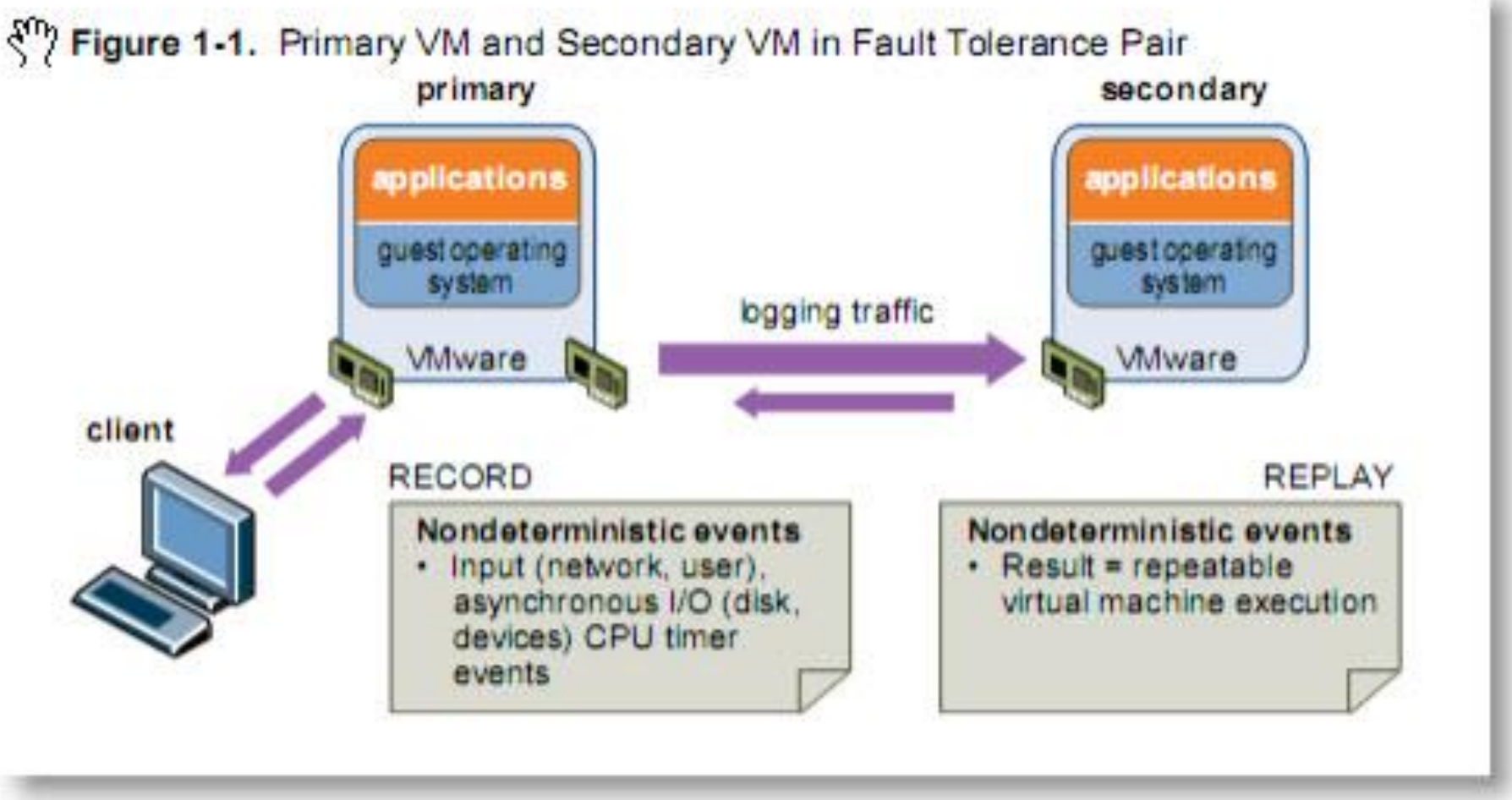

虛擬化基礎架構
抽象化 & 資源池化
Compute
Abstraction =
主機虛擬化
Network
Abstraction =
網路虛擬化
Storage
Abstraction =
儲存虛擬化
運算
網路
儲存

主機虛擬化好處

VMware Fault Tolerance



Fault Tolerance

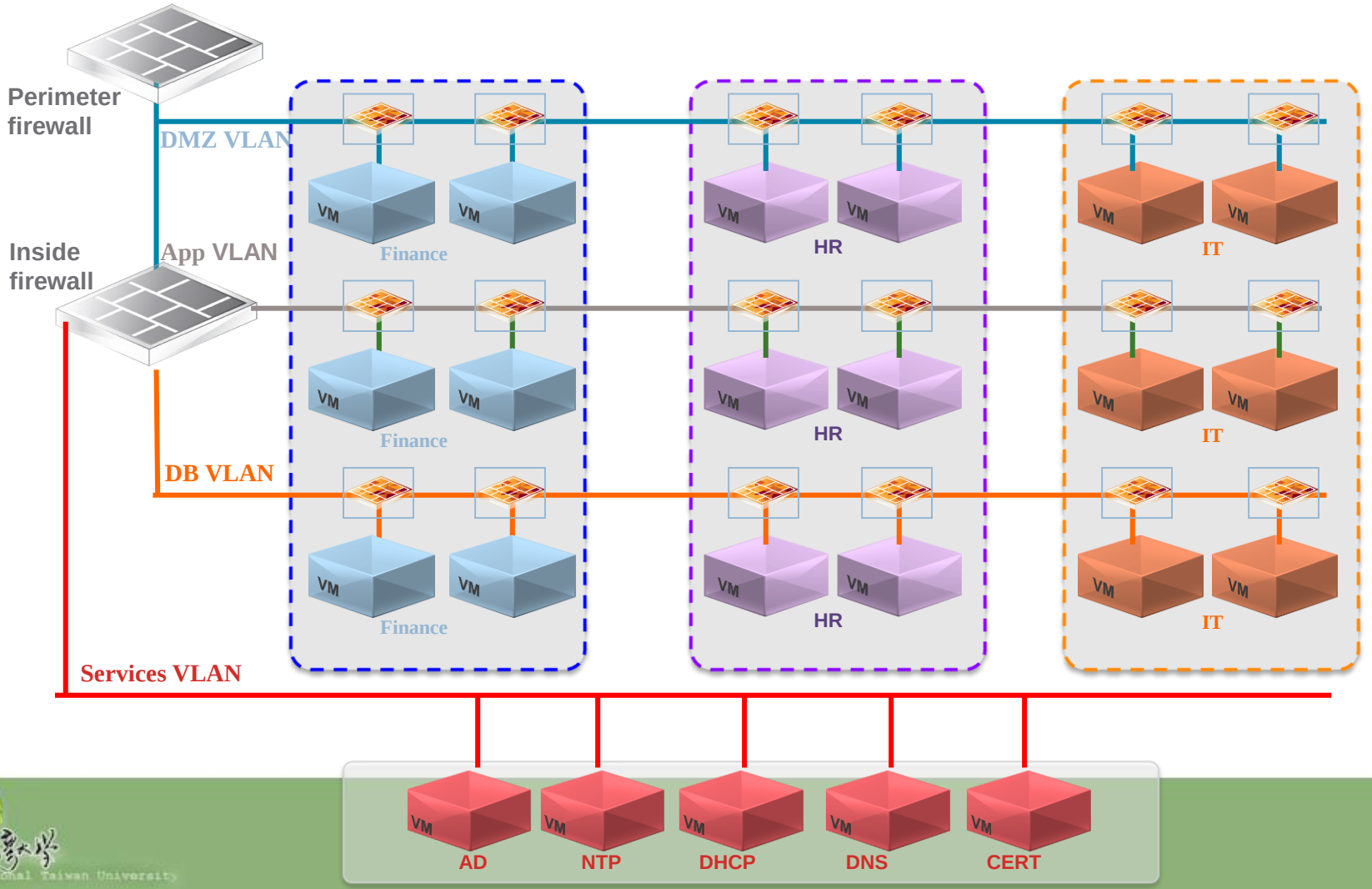


VMware NSX 簡介

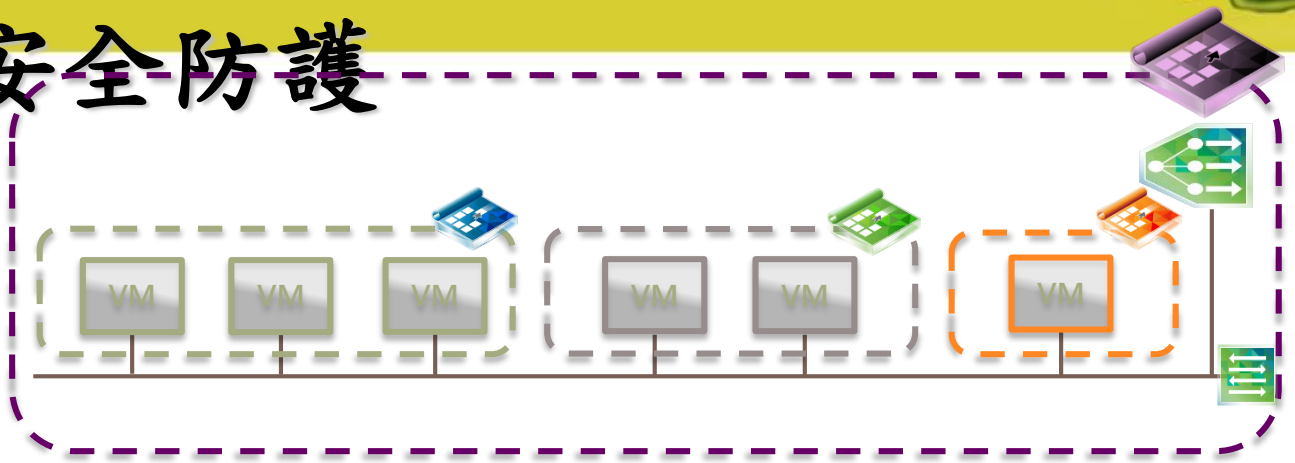
- 依據業務需求，隨取所需提供VM-Base
  防火牆、負載平衡器、VPN、路由器功能

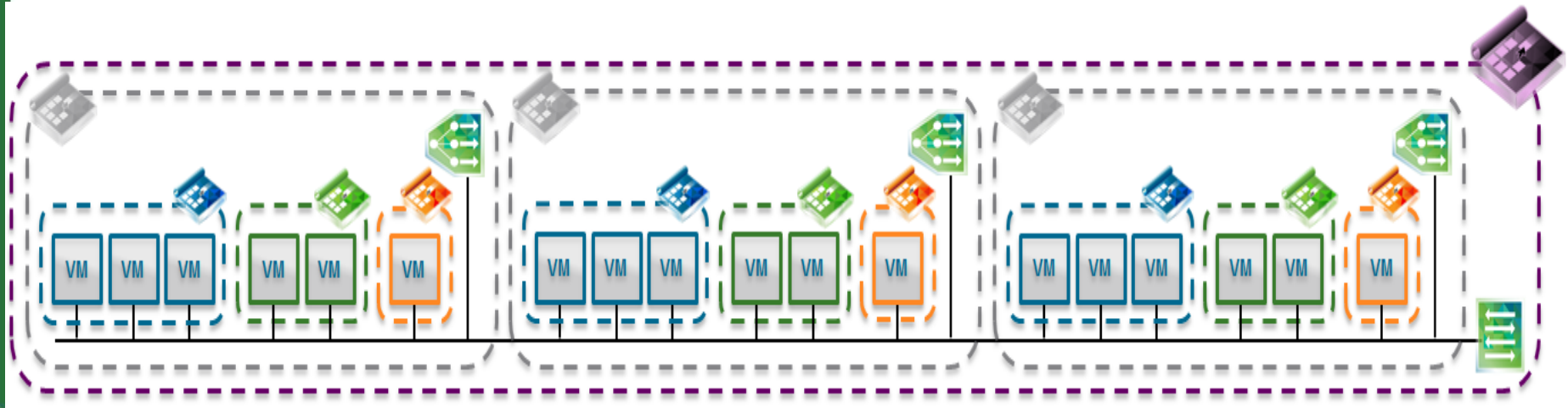
Use case: 資料中心內的業務細部隔離控制

- 無須區隔網段或占用實體網路介面，NSX DFW可以做到非常細部的虛擬環境服務或業務組合



Use case: 大型運營商或製造業的同網段內安全防護



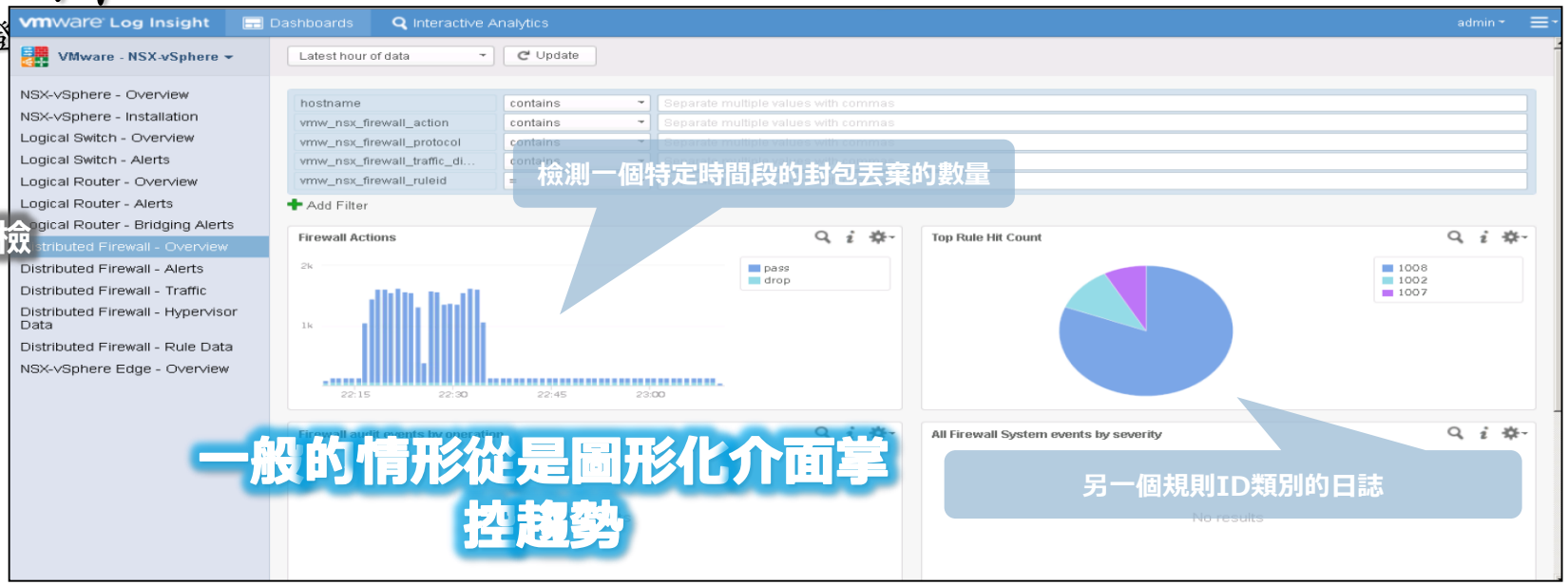


每日/每週定期檢測和執行情況的詳細分析

審[illegible]詐登

每日/每週例行檢測 or 示警

緊急情況下詳細分析

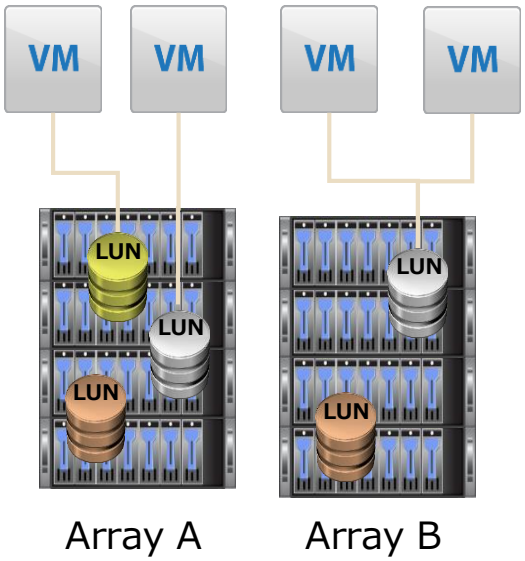


VSAN

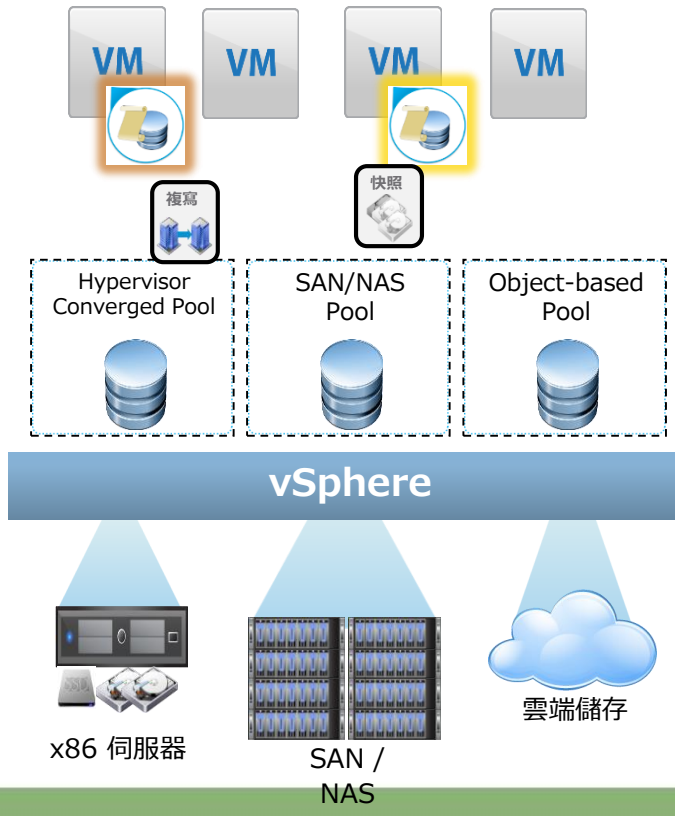
- VMware Virtual SAN儲存虛擬化方案
  打造軟體定義的儲存

利用虛擬中介層我們可以轉換儲存

今日



軟體定義儲存

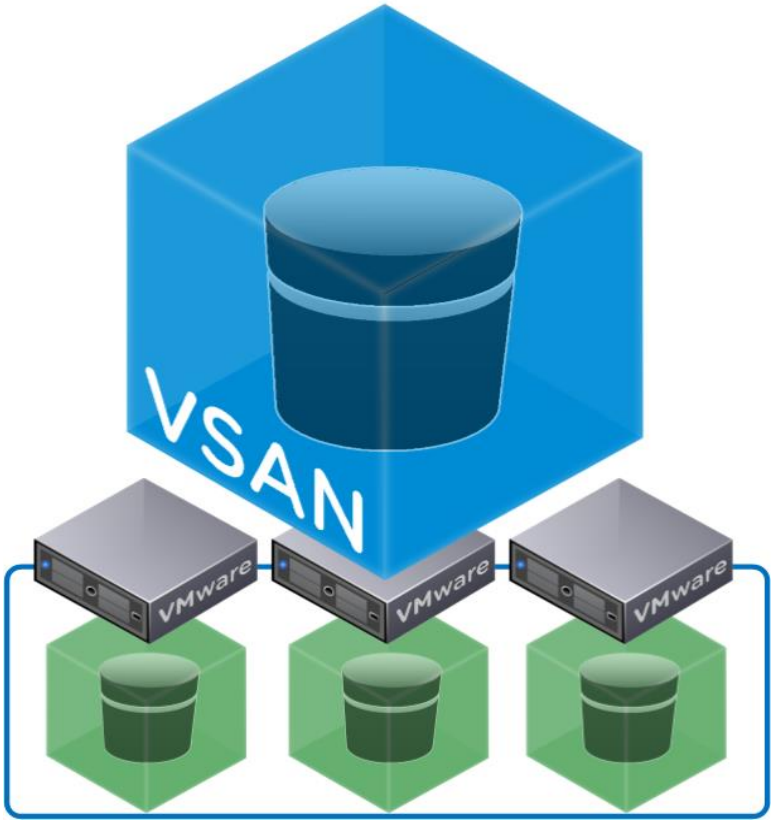


透過以虛擬機為中心的政策達成自動化SLAs *(Policy-based Control Plane)*

虛擬機層級資料服務 *(Virtual Data Services)*

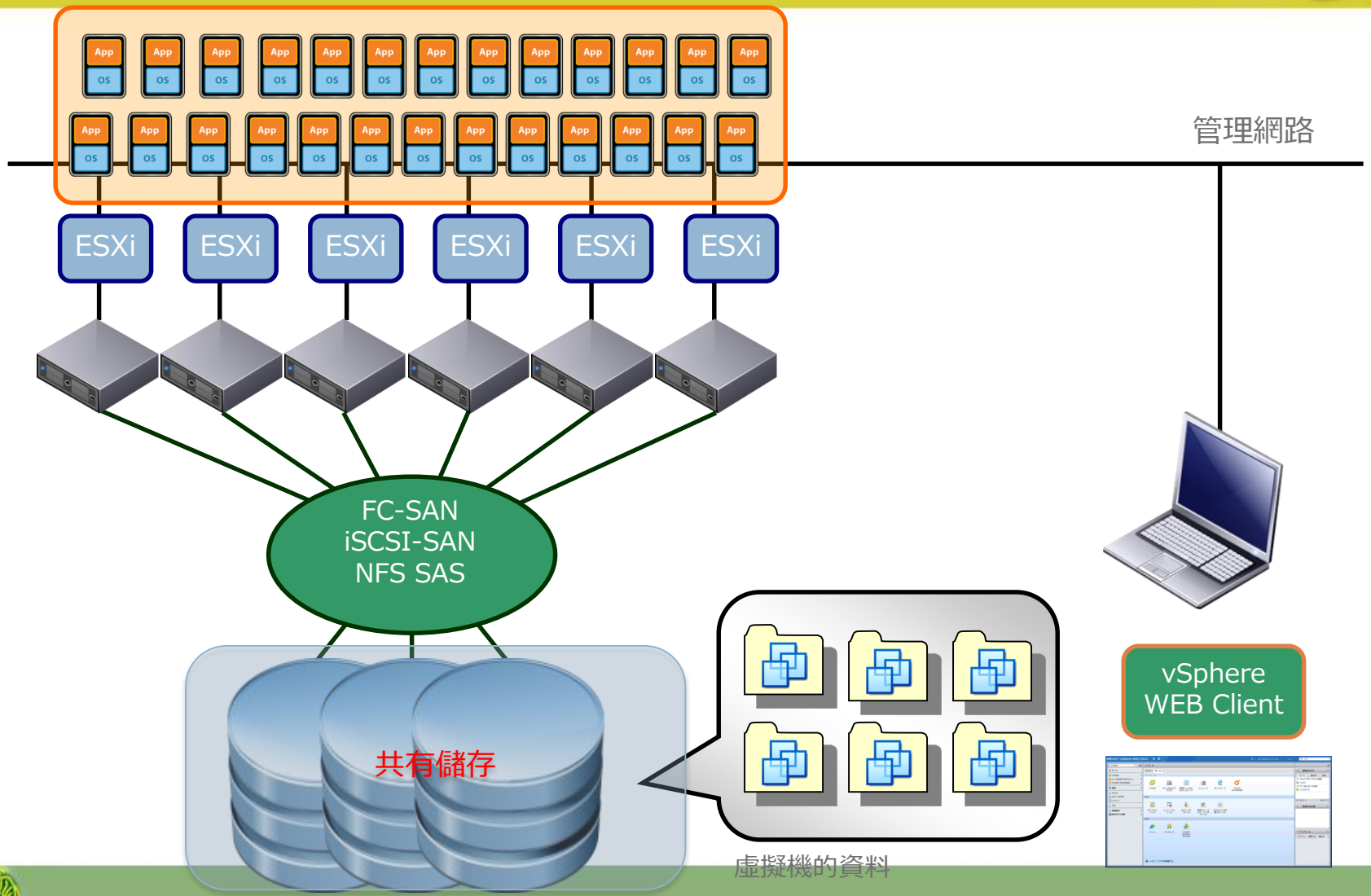
抽象化與資源池化 *(Virtualized Data Plane)*

Virtual SAN 概述

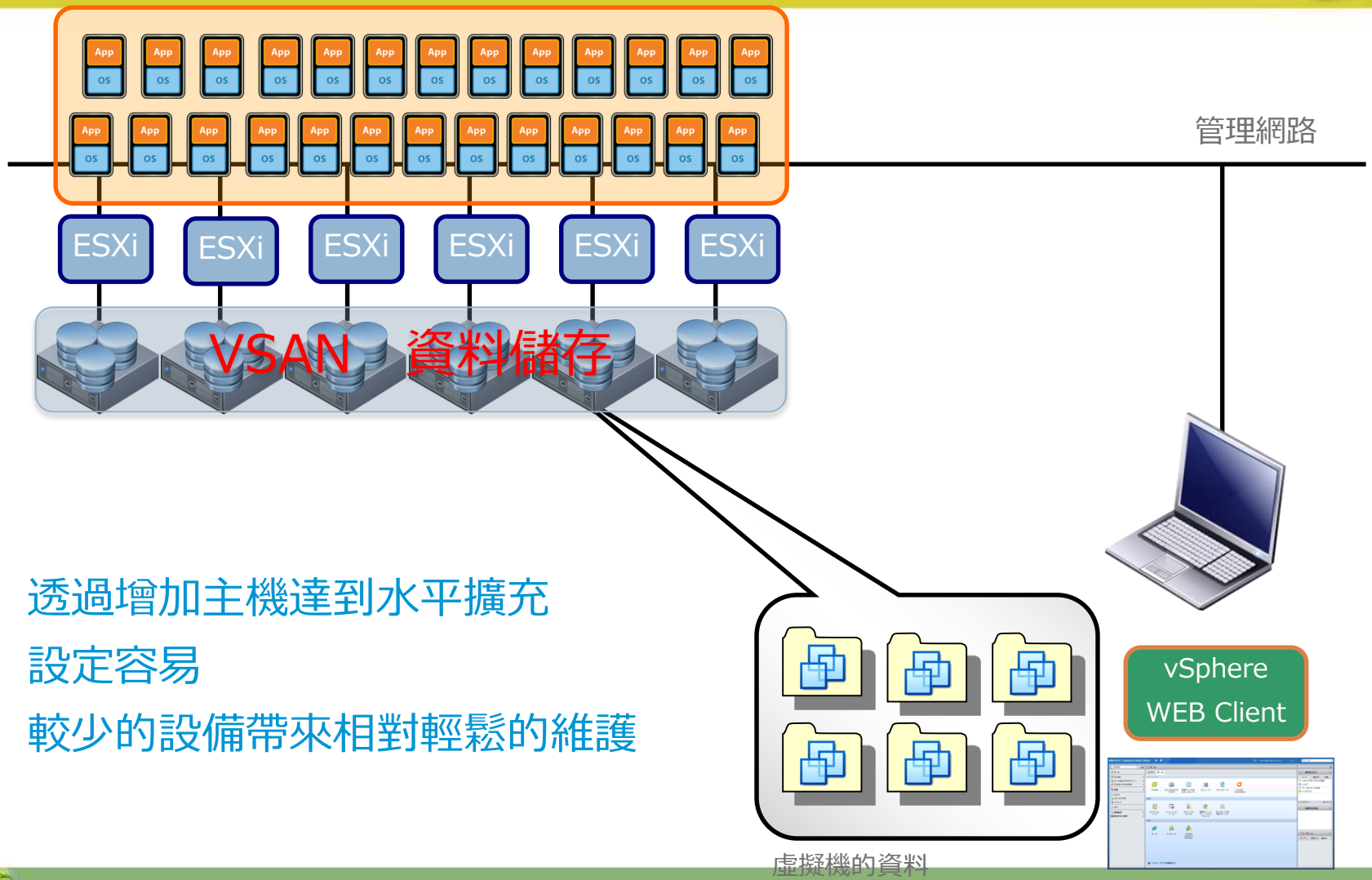


- 將各台伺服器本地接取之低成本儲存結合為一個虛擬的外接儲存叢集
- 專為VMDK儲存設計的物件儲存方案
- 利用SSD/Flash提供讀寫校能優化
- 基於高速網路建置之分散式RAID架構, 無單點失效
- 易於垂直或水平擴充的彈性架構
- 基於業務政策導向的設計
- 支援絕大部分的虛擬化儲存功能
- 完全整合入 vSphere ESXi 核心

虛擬環境示意圖(沒有VSAN)

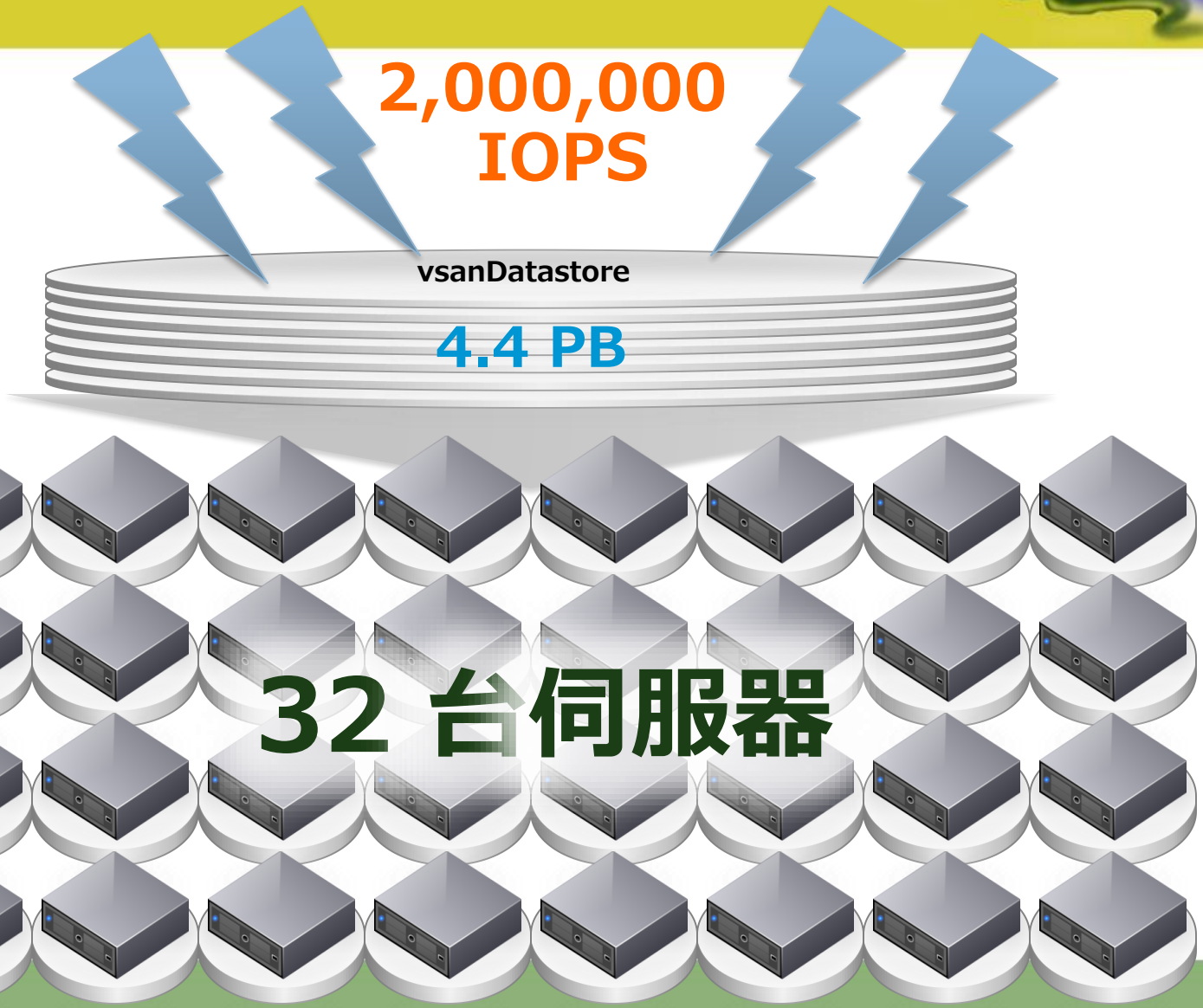


虛擬環境示意圖(有VSAN)



- 透過增加主機達到水平擴充
- 設定容易
- 較少的設備帶來相對輕鬆的維護

VSAN擁有卓越的可擴展性

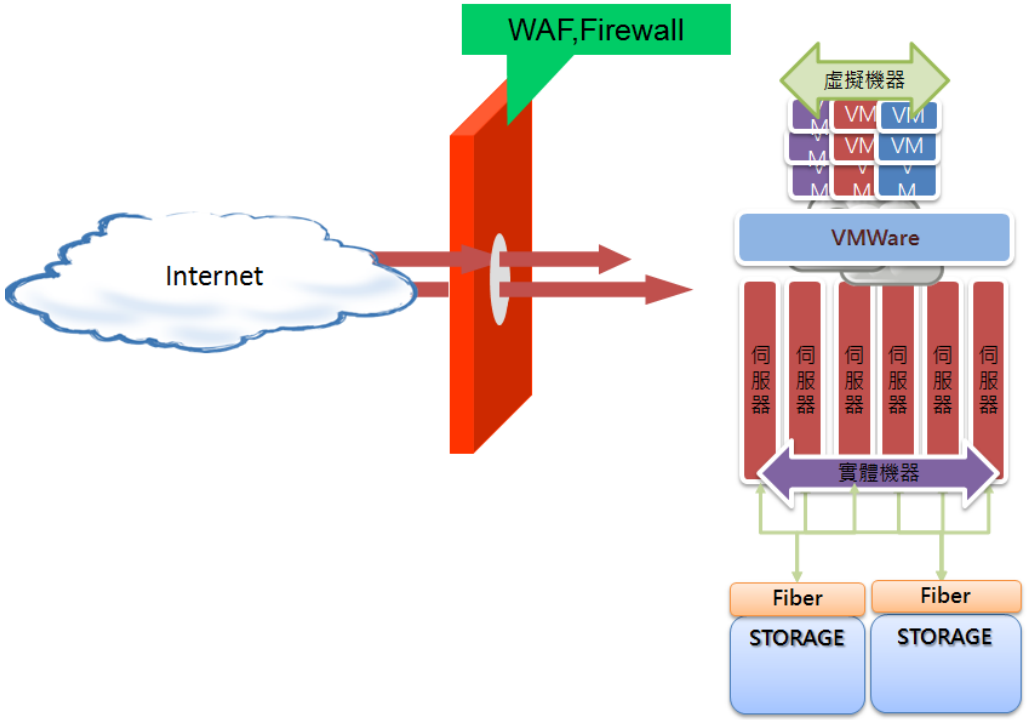


IOPS

- IOPS（Input/Output Operations Per Second）是一個用於電腦儲存裝置（如硬碟（HDD）、固態硬碟（SSD）或儲存區域網路（SAN））效能測試的量測方式，可以視為是每秒的讀寫次數。
- 7,200 RPM SATA硬碟機 硬碟機 ~75-100 IOPS SATA 3 Gbit/s
- 10,000 RPM SATA硬碟機 硬碟機~125-150 IOPS SATA 3 Gbit/s
- 10,000 rpm SAS硬碟機 硬碟機 ~140 IOPS SAS
- 15,000 rpm SAS硬碟機 硬碟機 ~175-210 IOPS SAS
- 英特爾Intel X25-M G2（MLC）SSD ~8,600 IOPS SATA 3 Gbit/s
- 英特爾 Intel X25-E (SLC) SSD ~5,000 IOPS SATA 3 Gbit/s

- ALL FLASH ARRAY 500K IOPS = 4KB X 500K X 8 = 16Gbps
- 10G SWITCH是DATA CENTER的標準規格

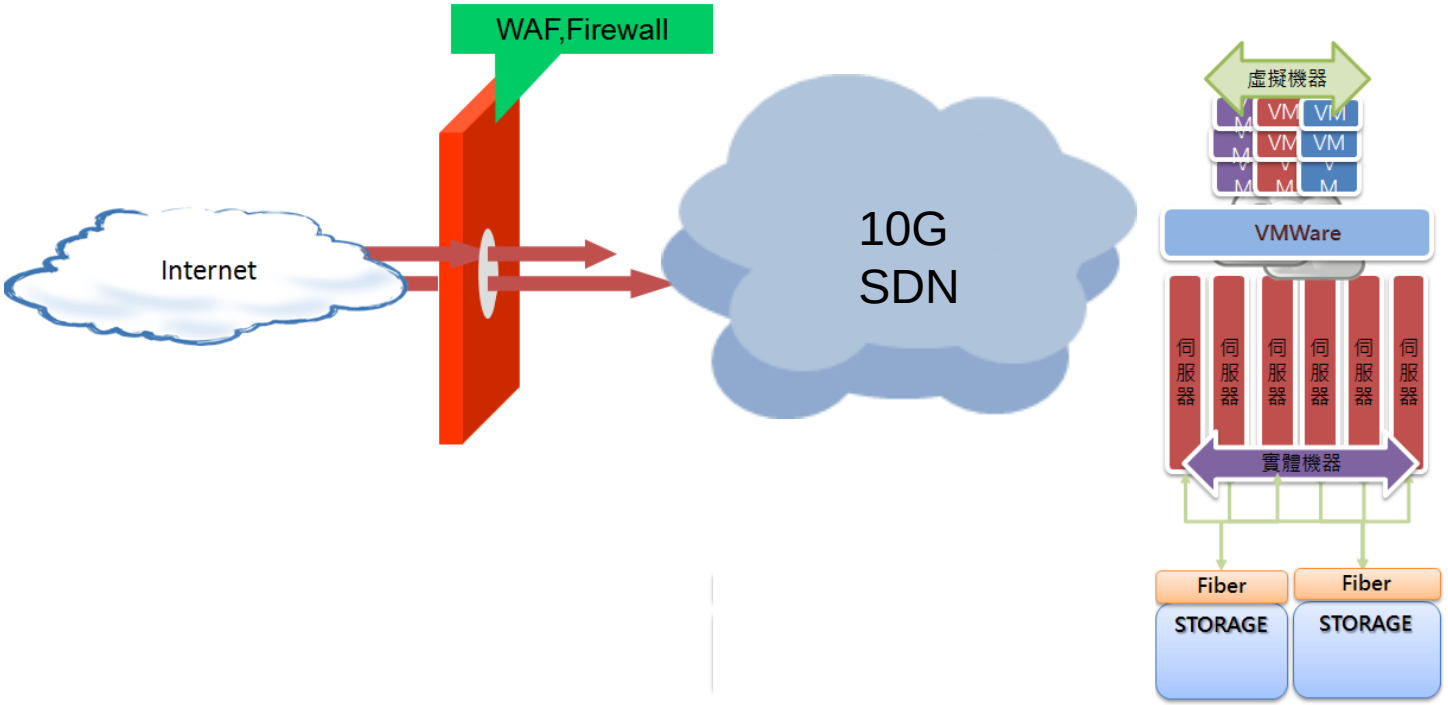
台北區網雲端環境建置(第一年)



8 Servers、 180 TB 、 149 VM、19單位

台北區網雲端環境建置(第二年)

- 新增SDN & VDI(之後再介紹)



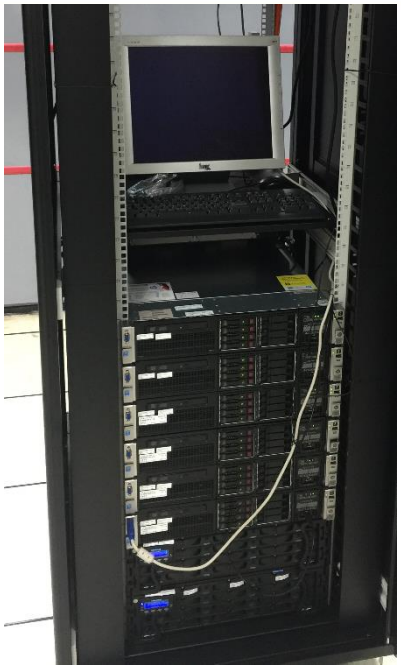
計畫亮點(酷課雲在臺大區網雲端)

- 2015-07-28 14:33:06 聯合新聞網 綜合報導
  - 台北市教育局籌備已久的「台北酷課雲」正式上線，（7/25）於建國中學舉辦第一階段成果發表會。
  - 酷課雲目前已使用臺大區網雲端 61個VM，持續增加中 。

經濟效益與社會影響

某國小機房
（約十台實體主機）

透過虛擬化轉化為

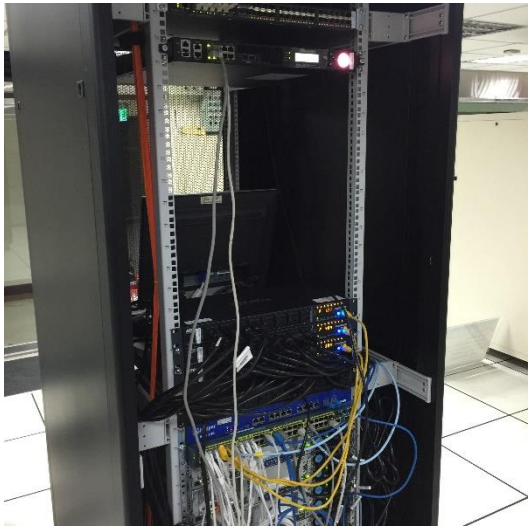


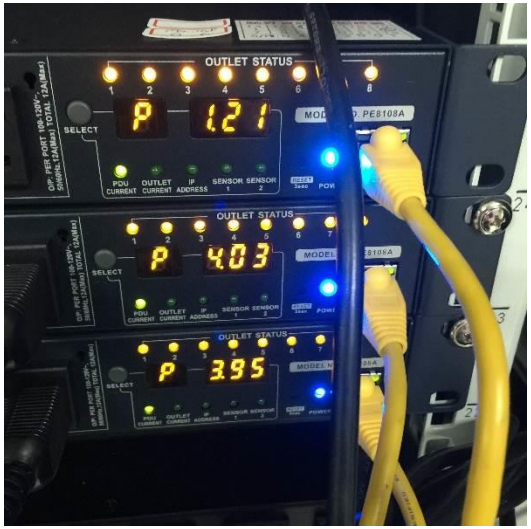
區網雲虛擬主機

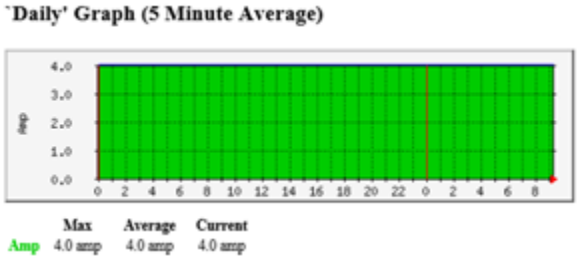
雲端研討會
目前已辦四場

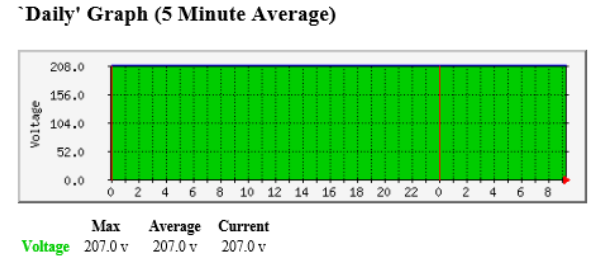
臺大機房機櫃耗能量測

可量測總耗能
及各別插座的耗能

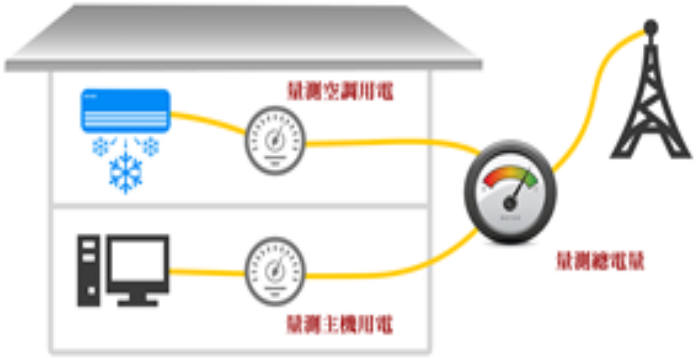






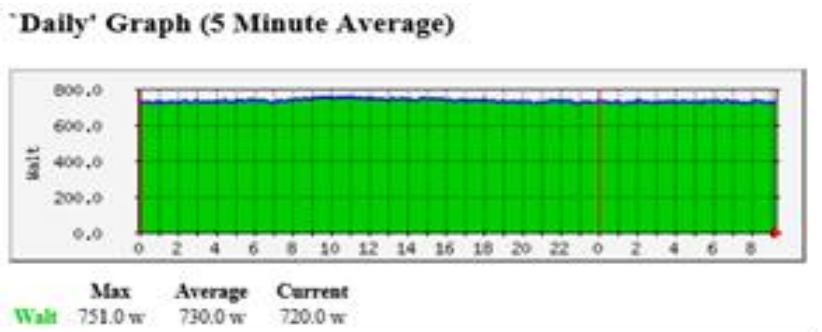


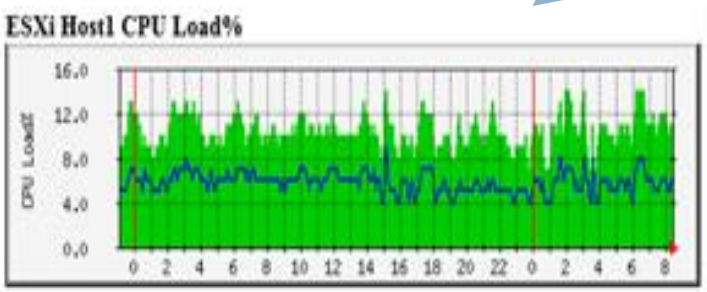
中小學機房耗能量測

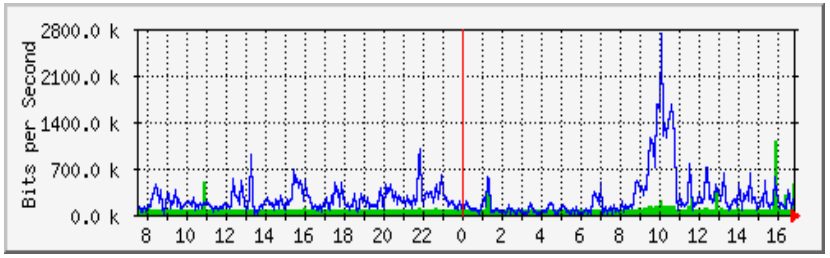


技術創新

- 計畫管理網頁 http://nepcloud.tp1rc.edu.tw
  - 虛擬主機總數
  - 即時電力量測
  - 即時網路流量
  - VM效能監控





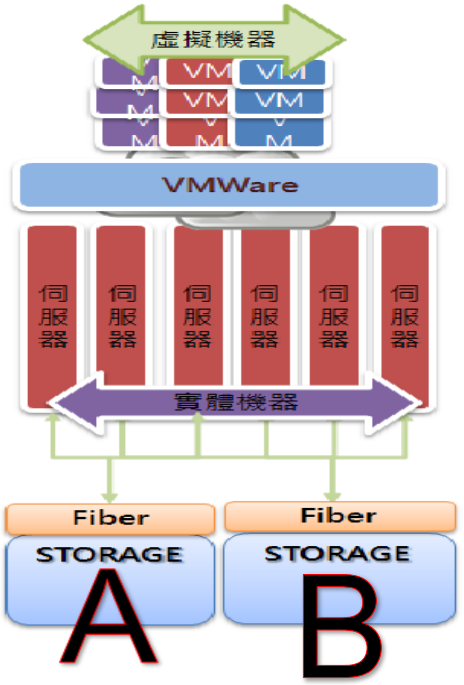


台大計中環境及雲端技術

- 停電
  - UPS+發電機
- 主機故障（自動轉到其他主機）
  - VMWARE HA CLUSTER
- 回覆多天前的主機
  - VMWARE VDP
- 儲存設備故障
  - VSAN
- 資安
  - WAF、 IPS、 FORTIFY

vSphere Data Protection

- 簡稱ＶＤＰ
- 建立虛擬機器的快照。
- 備份30天,每天備一份
- A備到Ｂ、Ｂ備到Ａ



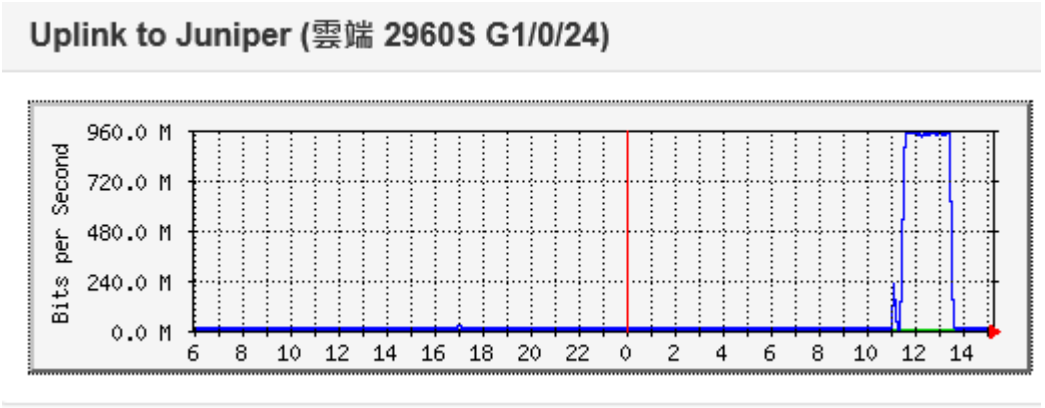
NSX & VSAN

- Virtual SAN
  - 使用大容量的SSD來作為讀取與寫入快取。
  - 磁碟Stripe(寫二份檔案)
  - 預計今年會導入
- NSX
  - 結合SDN

監控案例說明

- 案例:upload file server ，一上架CPU就100%, 已作了二台SERVER

- 流量異常偵測



WAF 能幫什麼?

SQL INJECTION example from speed.ntu.edu.tw

←T→	id	IP	SelectCity	SelectZone	speed	satisfied	suggestions	daytime
	2947	218.65.12.200	???..	???..	??	???	test	2015-05-25 13:04:41
	2948	218.65.12.200	???..	???..	??	???	test	2015-05-25 13:04:48
	2949	218.65.12.200	???..	???..	??	???	test	2015-05-25 13:04:49
	2950	218.65.12.200	???..	???..	??	???	test	2015-05-25 13:04:49
	2951	218.65.12.200	???..	???..	??	???	test	2015-05-25 13:04:50
	2952	218.65.12.200	???..	???..	??	???	test	2015-05-25 13:04:50
	2953	218.65.12.200	???..	???..	??	???	test	2015-05-25 13:04:54
	2954	218.65.12.200	???..	???..	??	???	test' and '1'='1	2015-05-25 13:05:03
	2955	218.65.12.200	???..	???..	??	???	test' and '11'='11	2015-05-25 13:05:04
	2956	218.65.12.200	???..	???..	??	???	test' and '1'='11	2015-05-25 13:05:04
	2957	218.65.12.200	???..	???..	??	???	test' and '%'='	2015-05-25 13:05:04
	2958	218.65.12.200	???..	???..	??	???	test' and '11%'='11	2015-05-25 13:05:08
	2959	218.65.12.200	???..	???..	??	???	test' and '1%'='11	2015-05-25 13:05:08
	2960	218.65.12.200	???..	???..	??	???	test	2015-05-25 13:05:08
	2961	218.65.12.200	???..	???..	??	???	test	2015-05-25 13:05:09
	2962	218.65.12.200	???..	???..	??	???	test	2015-05-25 13:05:09
	2963	218.65.12.200	???..	???..	??	???	test	2015-05-25 13:05:09
	2964	218.65.12.200	???..	???..	??	???	test	2015-05-25 13:05:13
	2965	218.65.12.200	???..	???..	??	???	test	2015-05-25 13:05:16
	2966	218.65.12.200	???..	???..	??	???	test	2015-05-25 13:05:40
	2967	218.65.12.200	???..	???..	??	???	test	2015-05-25 13:05:41
	2968	218.65.12.200	???..	???..	??	???	test	2015-05-25 13:05:50
	2969	218.65.12.200	???..	???..	??	???	test	2015-05-25 13:05:51
	2970	218.65.12.200	???..	???..	??	???	test	2015-05-25 13:05:51
	2971	218.65.12.200	???..	???..	??	???	test	2015-05-25 13:05:52
	2972	218.65.12.200	???..	???..	??	???	test	2015-05-25 13:05:59
	2973	218.65.12.200	???..	???..	?? and '1'='1	???	test	2015-05-25 13:06:04
	2974	218.65.12.200	???..	???..	?? and '11'='11	???	test	2015-05-25 13:06:07
	2975	218.65.12.200	???..	???..	?? and '1'='11	???	test	2015-05-25 13:06:11
	2976	218.65.12.200	???..	???..	?? and '%'='	???	test	2015-05-25 13:06:11

The Open Web Application Security Project
OWASP top 10

- A1 Injection (高中就在改成績)
- A2 Broken Authentication and Session Management (was formerly 2010-A3)
- A3 Cross-Site Scripting (XSS) (was formerly 2010-A2) 留言版最常發生
- A4 Insecure Direct Object References
- A5 Security Misconfiguration (was formerly 2010-A6)
- A6 Sensitive Data Exposure (2010-A7 Insecure Cryptographic Storage and 2010-A9 Insufficient Transport Layer Protection were merged to form 2013-A6)
- A7 Missing Function Level Access Control (renamed/broadened from 2010-A8 Failure to Restrict URL Access)
- A8 Cross-Site Request Forgery (CSRF) (was formerly 2010-A5)
- A9 Using Components with Known Vulnerabilities (new but was part of 2010-A6 – Security Misconfiguration)
- A10 Unvalidated Redirects and Forwards

區網雲端SOP

- 服務監控:
  - 流量異常,找到原因,通知申請單位
  - 主機異常,主動EMAIL通知申請單位
  - 重大的事件簡訊及電話通知
  - 資安事件,主動EMAIL通知申請單位(開發中,但要導入WAF)

今年研發重點

- 中華電信 或 安碁
  - 7X24
- 台大區網
  - 5X8
- AWS 或 ASURE
  - 0X0 信用卡->帳密-> VM ,FIREWALL ..全自動化
- 利用LOG結合SDN設自動防火牆

雲端服務(部份參考共同契約)

- 虛擬主機服務
- 雲端電腦教室(VDI)
  - 已建置完成
- 雲端會議
  - 本校去年已建置完成
  - http://ccnet.ntu.edu.tw/adobe_connect/video.html
- 網路直播
  - 預計今年建,使用WOWZA
- 影音DRM保護
  - Digital Right Management

虛擬桌面基礎結構 (VDI)

- WHY?
- Windows update ?
- 軟體授權?
- 行動通訊?

- VM -> PC ：多人共用一個OS ,
  - DATA & OS 分開

提供軟體雲服務平台 Horizon

- EX:
  - 30套 PDF writer
  - 給大於30人使用,
  - 但同時只有30台機器運作,解決授權問題

WINDOW 遠端桌面

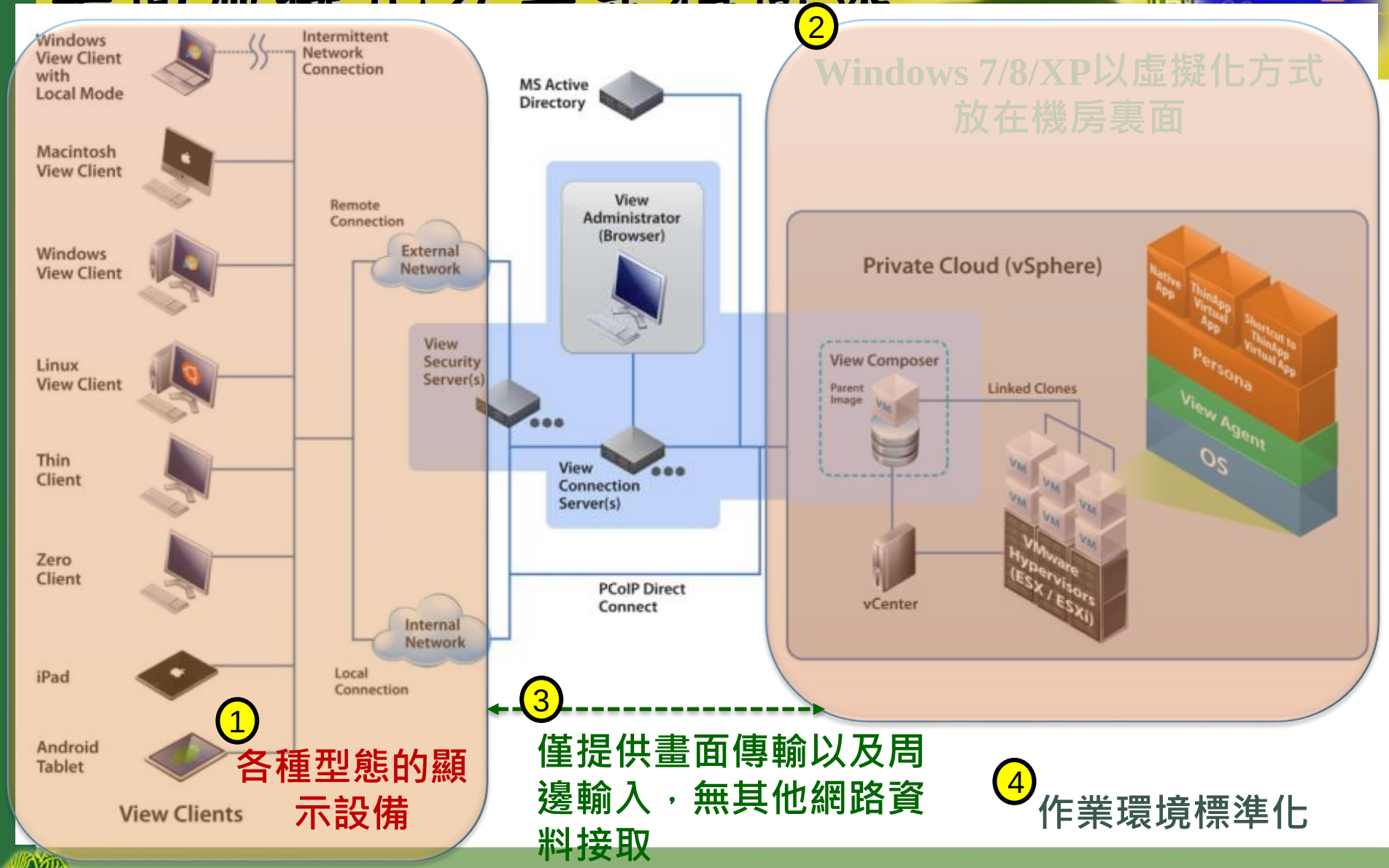
桌面虛擬化（Virtual Desktop Infrastructure）
機敏資料保護、行動化支援、集中管理

管理集中化虛擬桌面平台

- 機敏資料保護
- 行動化隨處存取
- 集中化管理
- 各種行動設備支援
- 節省營運成本

使用者可從各種裝置進行遠端存取

桌面虛擬化方案架構簡述



VDI規劃需求

導入範圍

- 電腦教室(校內、校外)
- 各種行動裝置(NB、平版、手機

需求環境

- MATLAB、SAS、MS VS 2015、Eclipse、SPSS、Adobe、RGui Microsoft Office、Flash Dreamweave、Illustrator Photoshop、Java 和其他一般教學用軟體等共計48種。

需求條件

- 初期VDI導入200U
- 儲存使用Virtual SAN架構
- VDI使用帳號能整合AD
- 電腦教室需提供共用帳號及各別帳號使用

VDI效益

共享軟體

提供本校教職員工、學生等以用戶端連接或以瀏覽器直接操作雲端桌面，使用本校授權軟體，免除設定環境和安裝軟體等步驟。節省軟體成本。

節能

雲端虛擬桌面服務收容數比為1:33，一年可節省988,416度電。
及師生在家使用VDI，節省交通往返。及節省計中電腦教室空調。

課表

雲端電腦桌面預計全年支援10種課程以上。

DEMO

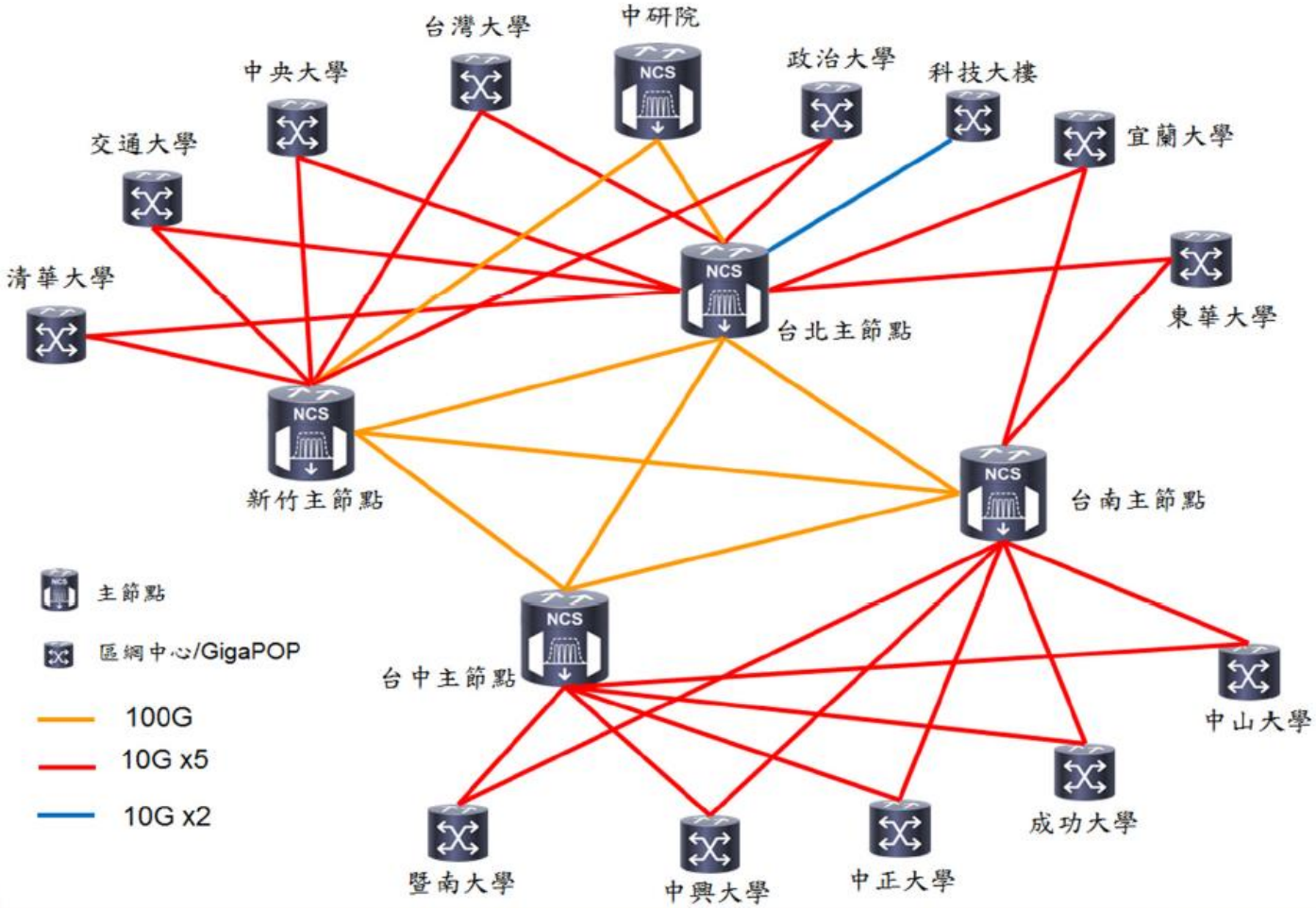
VDI

COOC

TWAREN 100G頻寬建置架構

NARLabs

承諾·熱情·創新



主機出租服務

VPS主機

智邦生活館「虛擬實體主機」(Virtual Private Server)服務採用國外最盛行的 Xen 軟體，將一台主機的資源分配給數十位客

主機規格

A方案

硬碟容量： 50G
每月流量： 160G
網站數量： 5個
首次設定費：NT$ 1,500

立即購買

NT$ 20,000/年

B方案

硬碟容量： 100G
每月流量： 400G
網站數量： 5個
首次設定費：NT$ 1,500

立即購買

NT$ 40,000/年

不限流量主機

硬碟容量： 50G
每月流量： 不限流量
網站數量： 1個
首次設定費：NT$ 1,500

立即購買

NT$ 36,000/年

經銷商主機

網站空間： 50G
每月流量： 50G
網站數量： 35個
首次設定費： **

加入經銷商

加入經銷商

共同契約

	中華電信	安碁
CPU:2 Core RAM:2GB HD:100GB 作業系統:Linux	2095	2091
Memory增加2GB	1170	231
Memory增加4GB	2339	463
Memory增加8GB	4678	926
CPU增加2	2924	926
CPU增加4	5848	1852
Firewall服務10條Policy	335	335
儲存空間硬碟擴充100GB	487	487
儲存空間硬碟擴充1TB	4873	4873
儲存空間硬碟擴充500GB	2437	2437
儲存空間硬碟擴充50GB		865

歡迎租用

敬請指教