

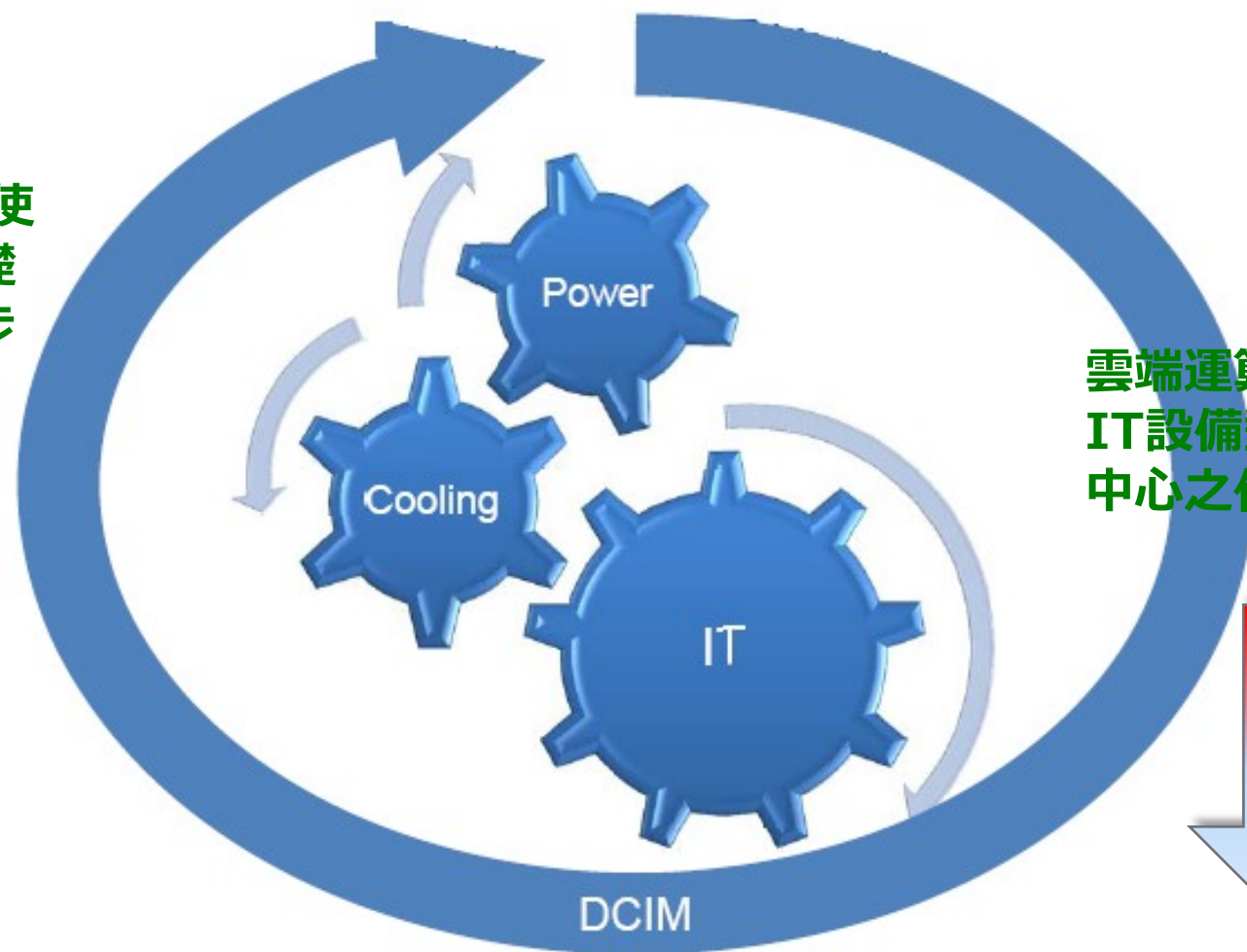
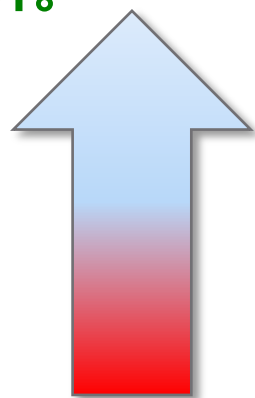
VMware校園授權方案介紹及實 際應用案例分享

vmware®

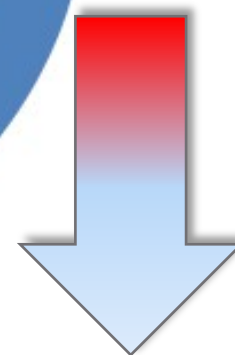
虛擬化及雲端運算對資料中心帶來的影響

資料中心四大基本組成：IT設備, 電力, 冷卻, DCIM

雲端運算成熟, 使得資料中心基礎架構重要性逐步提升。



雲端運算成熟, 造成IT設備對整體資料中心之佔比逐漸下滑。



資料中心提供的兩大服務類型：

電腦教學應用



電腦應用教學常見問題：

- 特殊軟體教學（如3D繪圖）：
現有電腦配備不足需添購較高等級PC
- 擴充更多間電腦教室：
- ✓ 現有電腦教室間數無法滿足排課需求。
- ✓ 學校購置之授權軟體數量少，僅能
安裝於少數教室，無法彈性排課。
- 傳統PC耗電量高

資訊服務應用

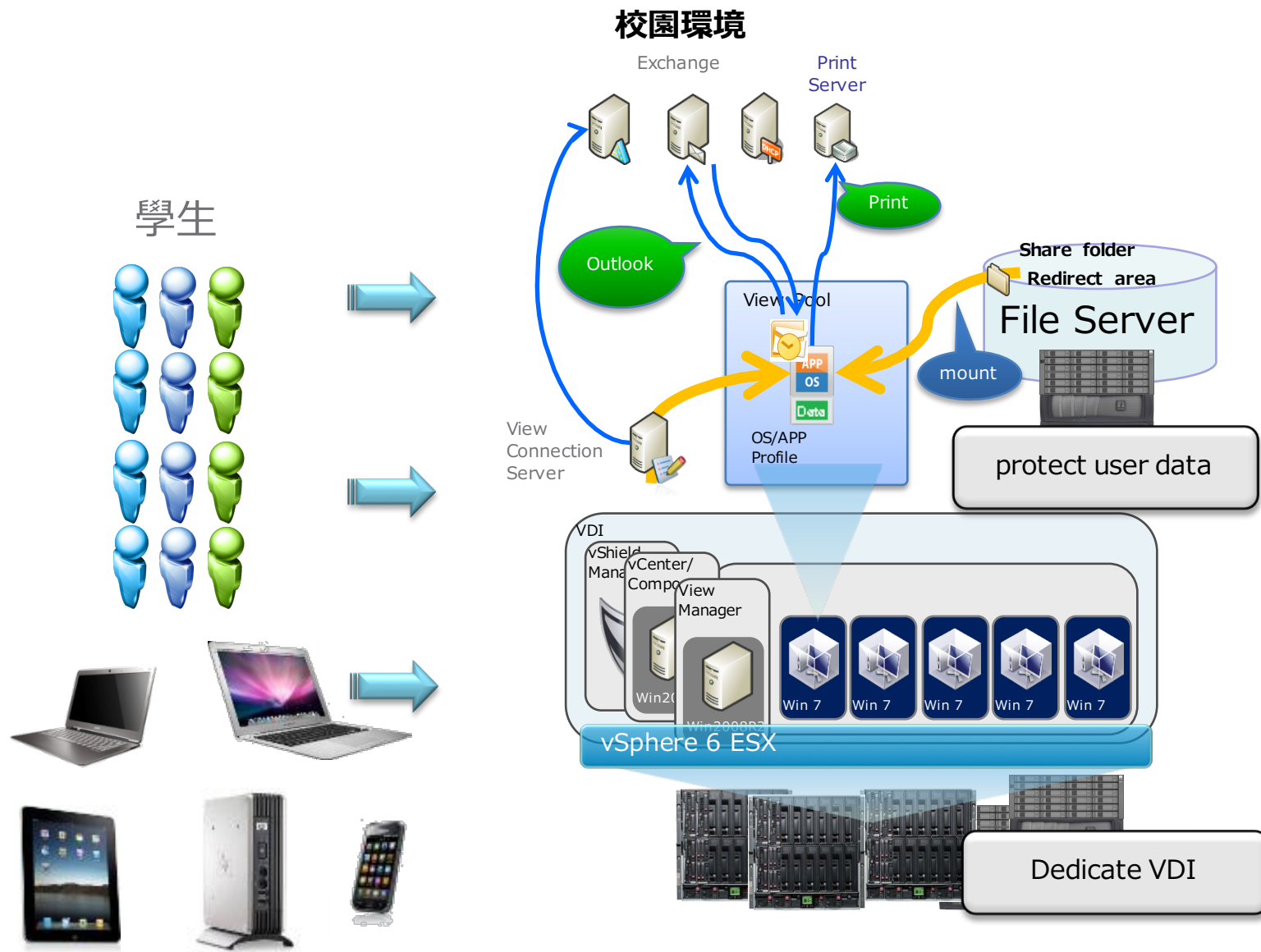


資訊服務應用的資源消耗之常見因素：

- 單一應用服務佔用一台主機：
常因不同專案需求，購置專屬該專案
的資訊設備
- 老舊伺服器仍在運行：
因無法在新型設備上安裝既有軟體：
(如：公文簽核)，而無法汰換舊設備

雲端電腦教學教室

電腦教學教室示意圖



電腦教學教室規劃方向

Approach



方便管理的終端顯示裝置



集中管理的學生上課環境

工具

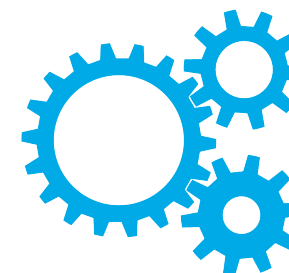


適當的解決方案
管理裝置與上課環境

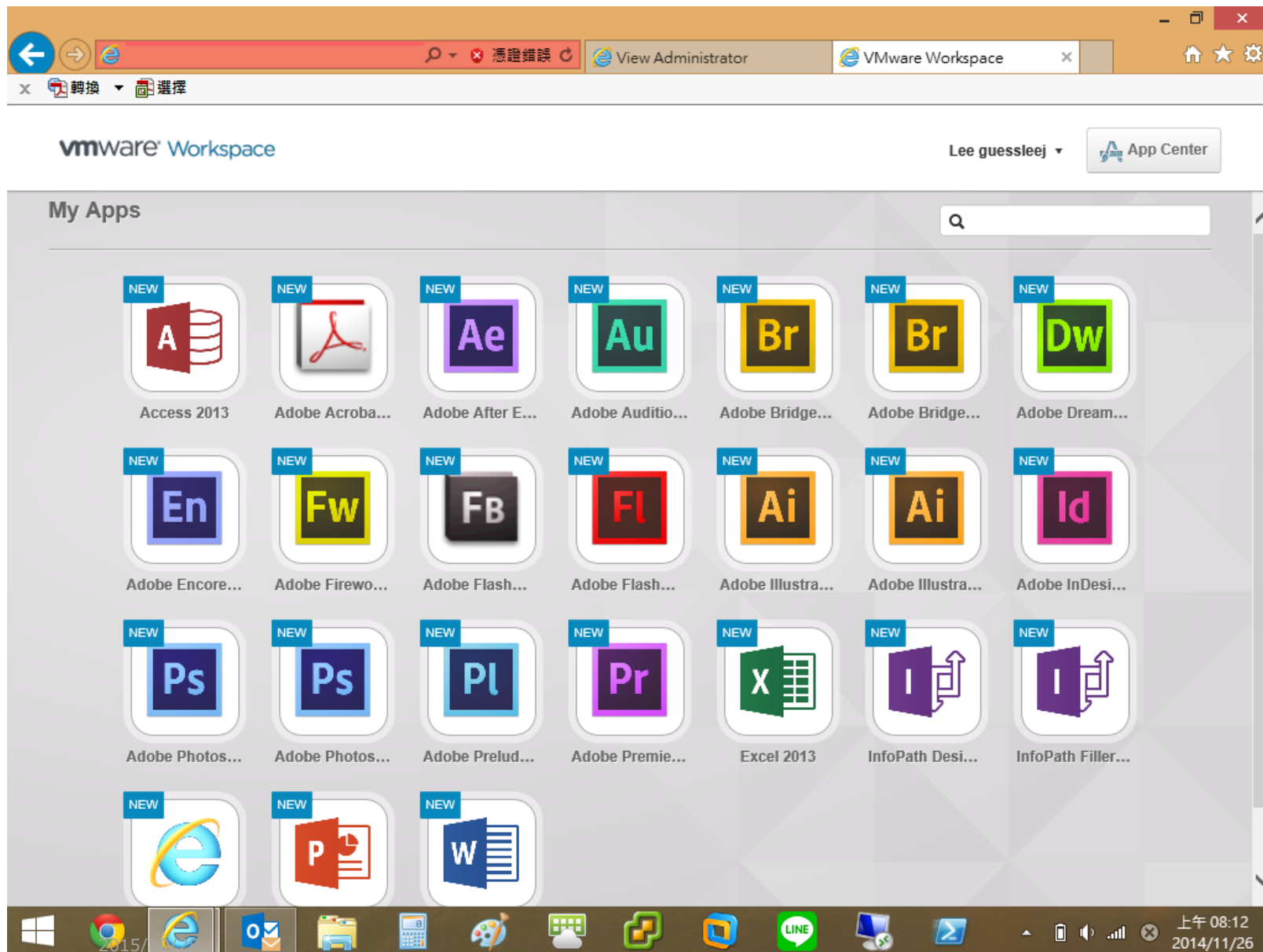
軟體資源與 內容管理



管理政策與 機制



將軟體進一步整合至虛擬桌面打造雲端教室



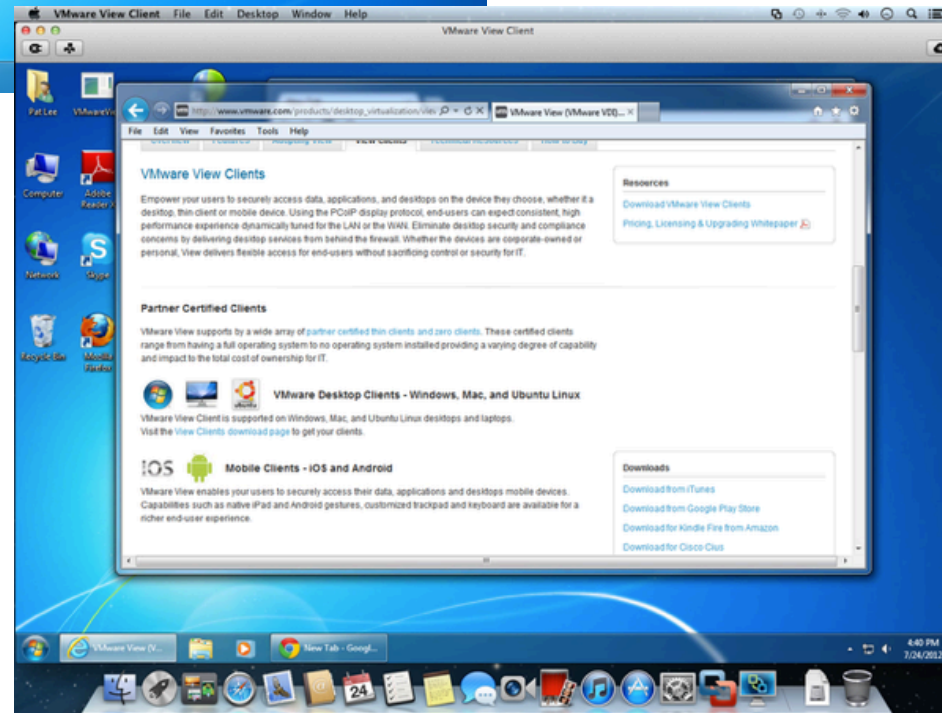
同樣的Windows 桌面可在任何設備上使用



Smartphone



平板

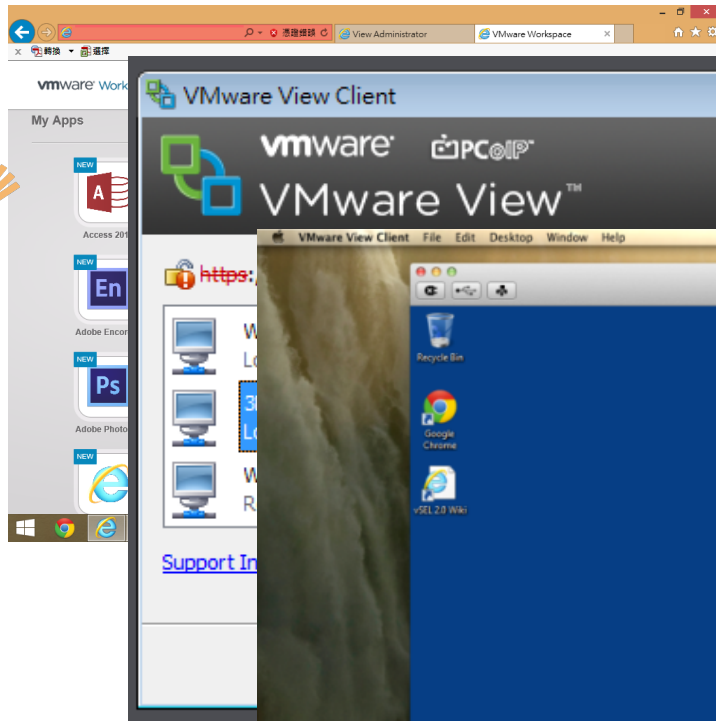


Mac Desktop

導入雲端教室，學生可以...

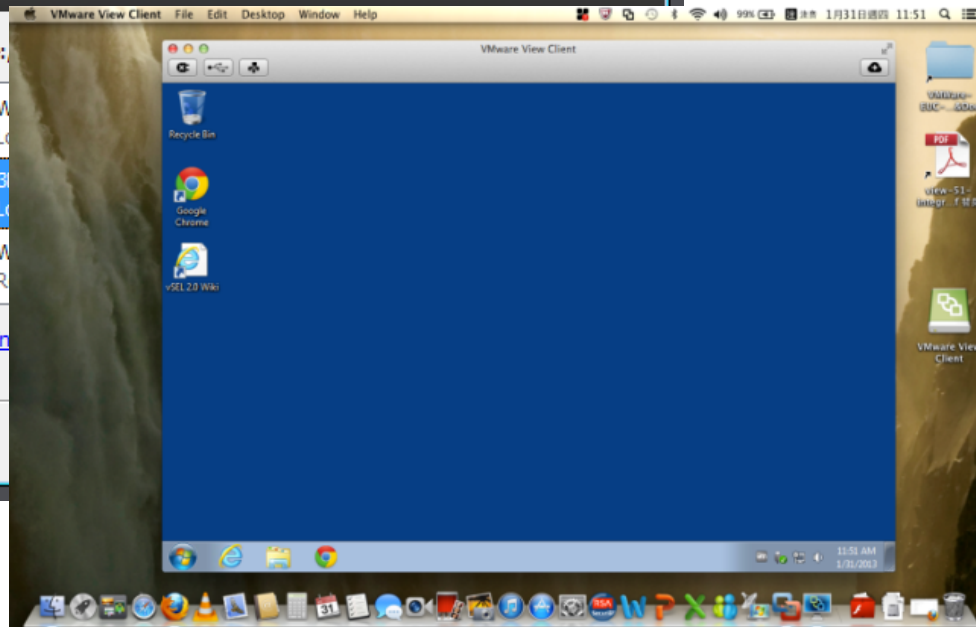
上課時：

① 學生登入網站，僅能看到跟自己修的課有關的課程軟體



② 並選擇該堂課的軟體環境

③ 開始上課



下課前：將課程檔案儲存於
個人專屬雲端空間

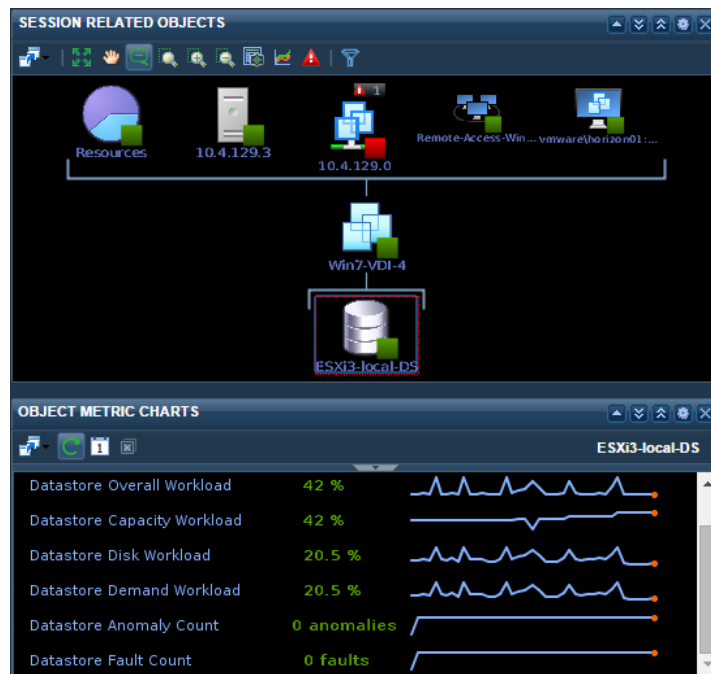
vmware®



雲端電腦教學教室效益

易於管理的電腦教室

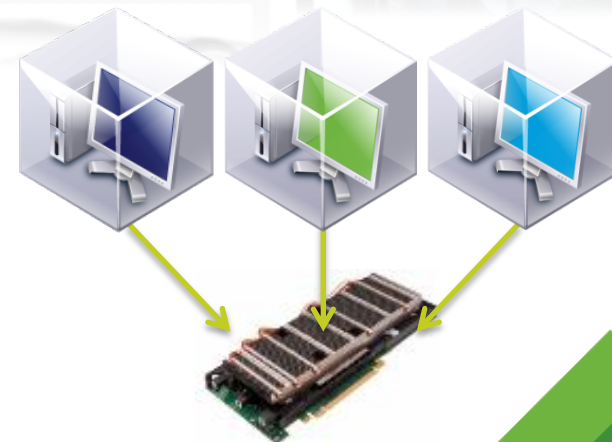
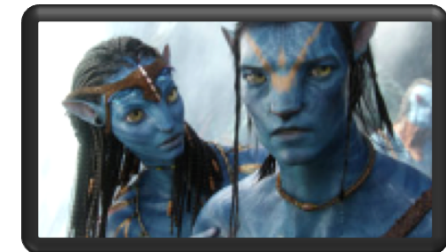
- 獨立設備與環境以**桌面虛擬化**方案建立標準化電腦教室，搭配Zero-Client方案提供用戶終端顯示
- 教師可集中依據課程進行作業環境更新或轉換
- 標準環境，快速進行硬體設備維護與更換



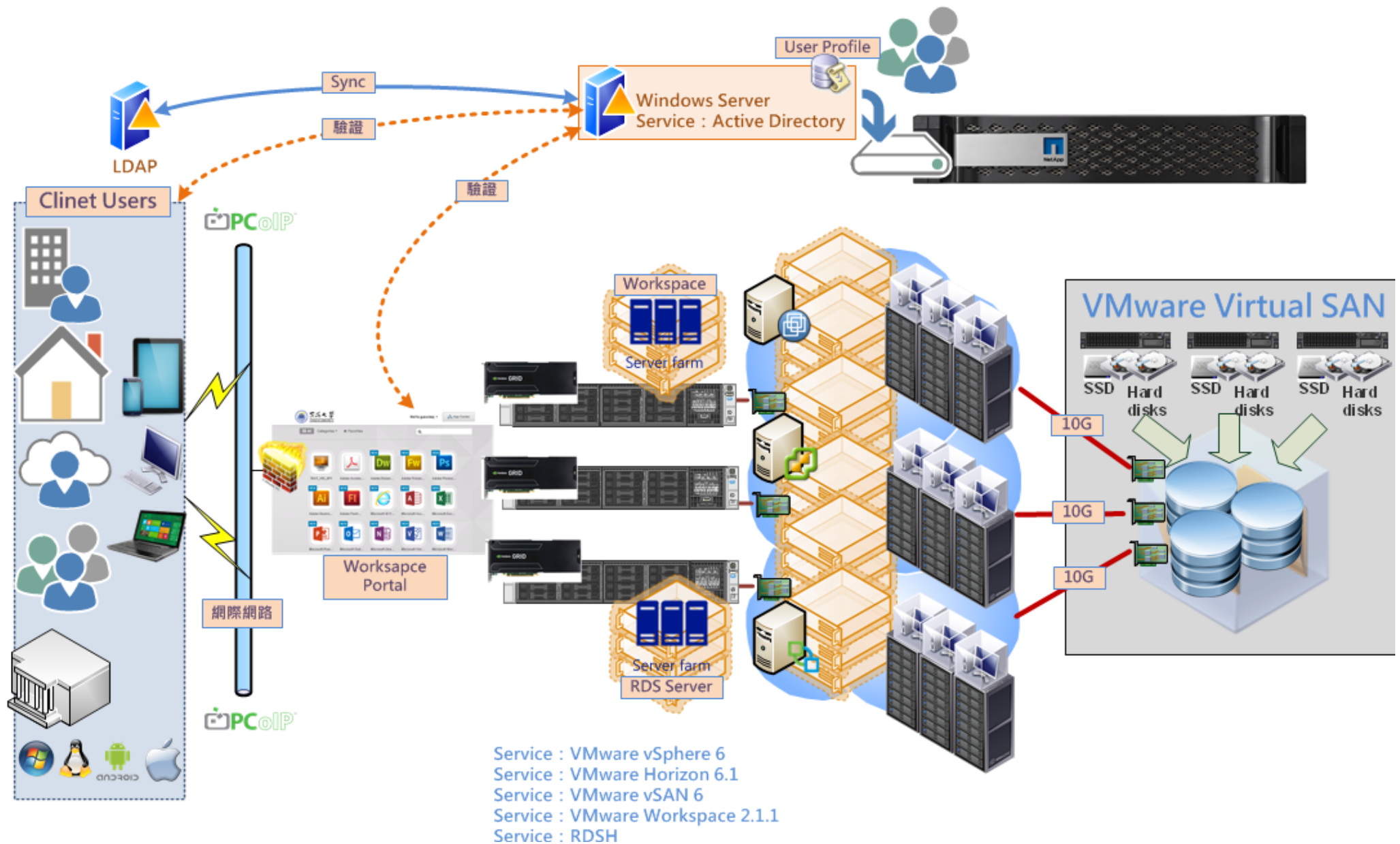
vmware®

多媒體應用教學

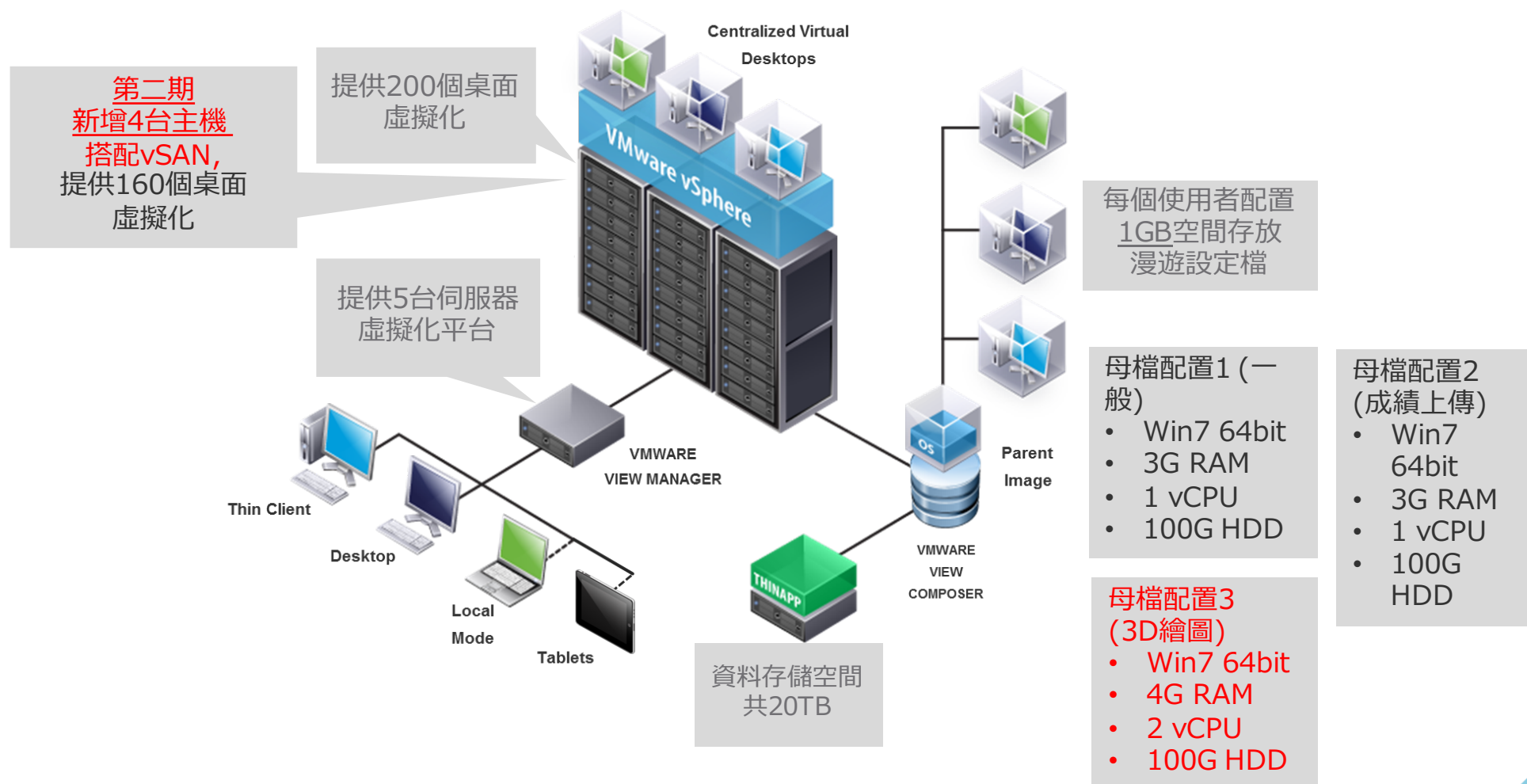
- **桌面虛擬化**方案支援以專屬或共享的方式讓用戶虛擬機器使用GPU資源。已支援各種主流CAD / CAM與多媒體應用軟體，提供教師各種多媒體與3D應用軟體的教學平台



某大學虛擬應用軟體雲端服務 - 3D VACS架構圖



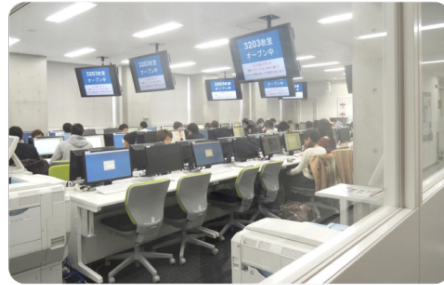
某大學桌面軟體雲建置架構



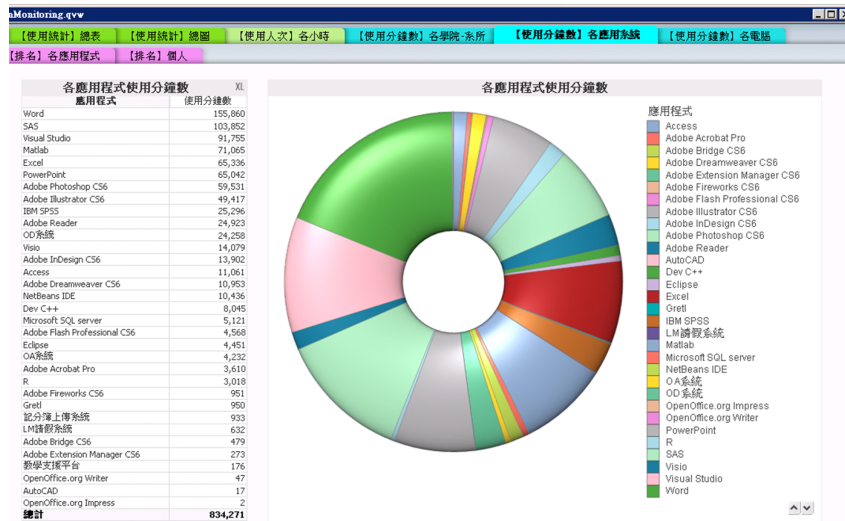
導入雲端教室，老師可以...

上課時：

- ① 選擇任何一間電腦教室，無需因受限設備等級而產生教學效能問題

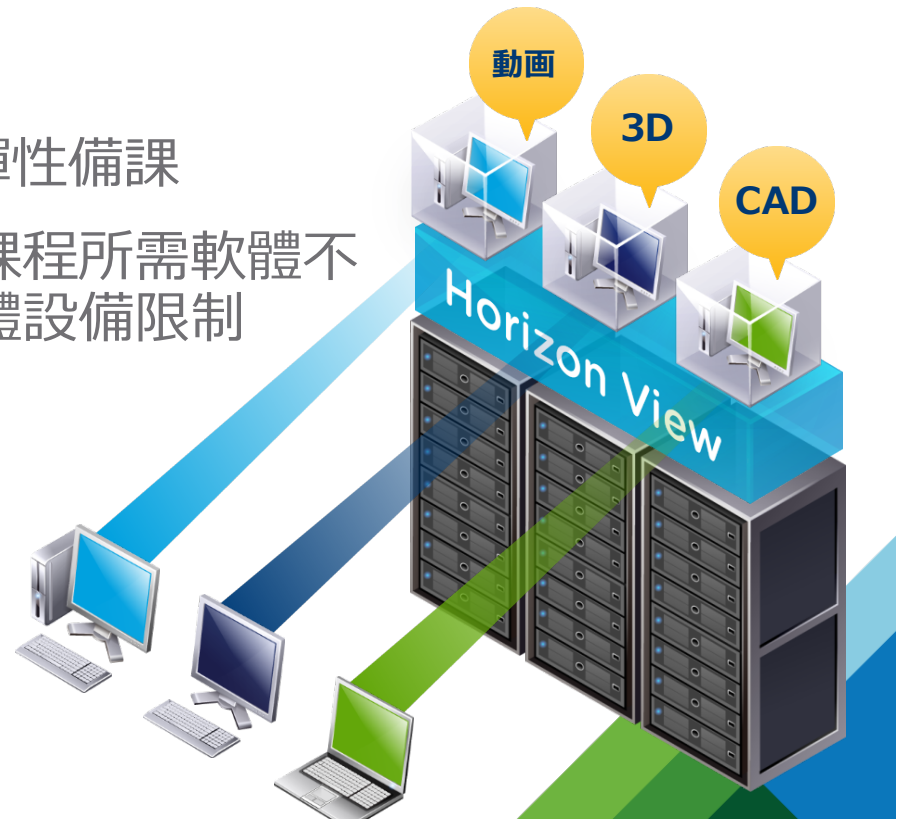


- ② 透過客製報表取得學生的學習歷程資訊



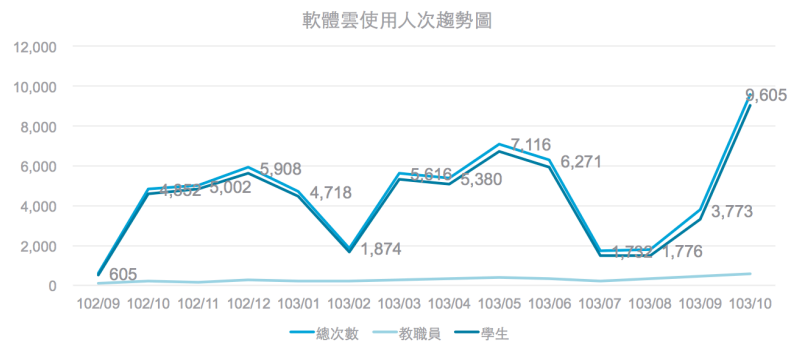
- ③ 彈性備課

新增課程所需軟體不受實體設備限制



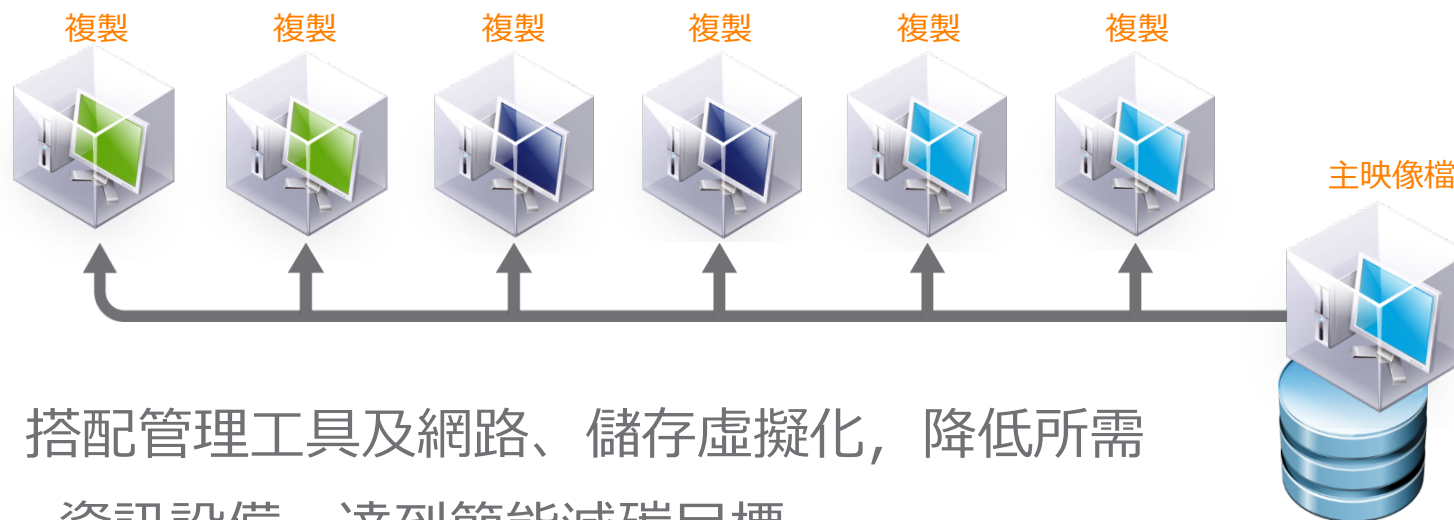
導入雲端教室，計中管理人員可以...

- ① 了解軟體使用頻率，評估授權軟體購買需求及效益（客製報表）



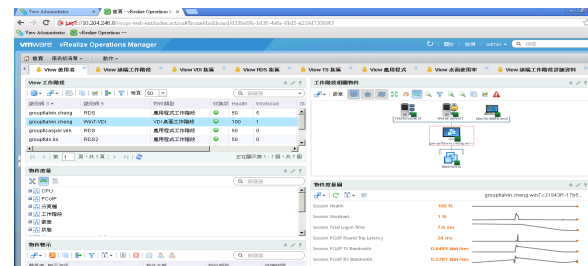
各應用程式使用分鐘數		XL
應用程式	使用分鐘數	
Word	155,860	
SAS	103,852	
Visual Studio	91,755	
Matlab	71,065	
Excel	65,336	
PowerPoint	65,042	
Adobe Photoshop CS6	59,531	
Adobe Illustrator CS6	49,417	
IBM SPSS	25,296	
Adobe Reader	24,923	
OD系統	24,258	
Visio	14,079	
Adobe InDesign CS6	13,902	

- ② 課程所需相關軟體一次安裝，無須浪費時間更新版本或補丁



- ③ 搭配管理工具及網路、儲存虛擬化，降低所需資訊設備，達到節能減碳目標

vmware®



在桌面集區如何找到問題

第一步、針對alvin.cheng去查詢正在使用的Win7 VDI 工作階段

識別碼 3	識別碼 5	物件類型	收集狀	Health	Workload
grouptalvin.cheng	RDS	應用程式工作階段	●	50	5
grouptalvin.cheng	Win7-VDI	VDI 桌面工作階段	●	100	1
grouptcasper.yeh	RDS	應用程式工作階段	●	50	0
grouptds.lin	RDS2	應用程式工作階段	●	50	0

第二步、圖像化清楚呈現與這台虛擬桌面所有相關的管理連線角色分佈

第三步、清楚條列這台VDI 虛擬桌面連線相關資訊，如連線負載、登入花費時間、PCoIP頻寬傳送大小

Session Health: 100 %

Session Workload: 1 %

Session Total Logon Time: 7.6 sec

Session PCoIP Round Trip Latency: 24 ms

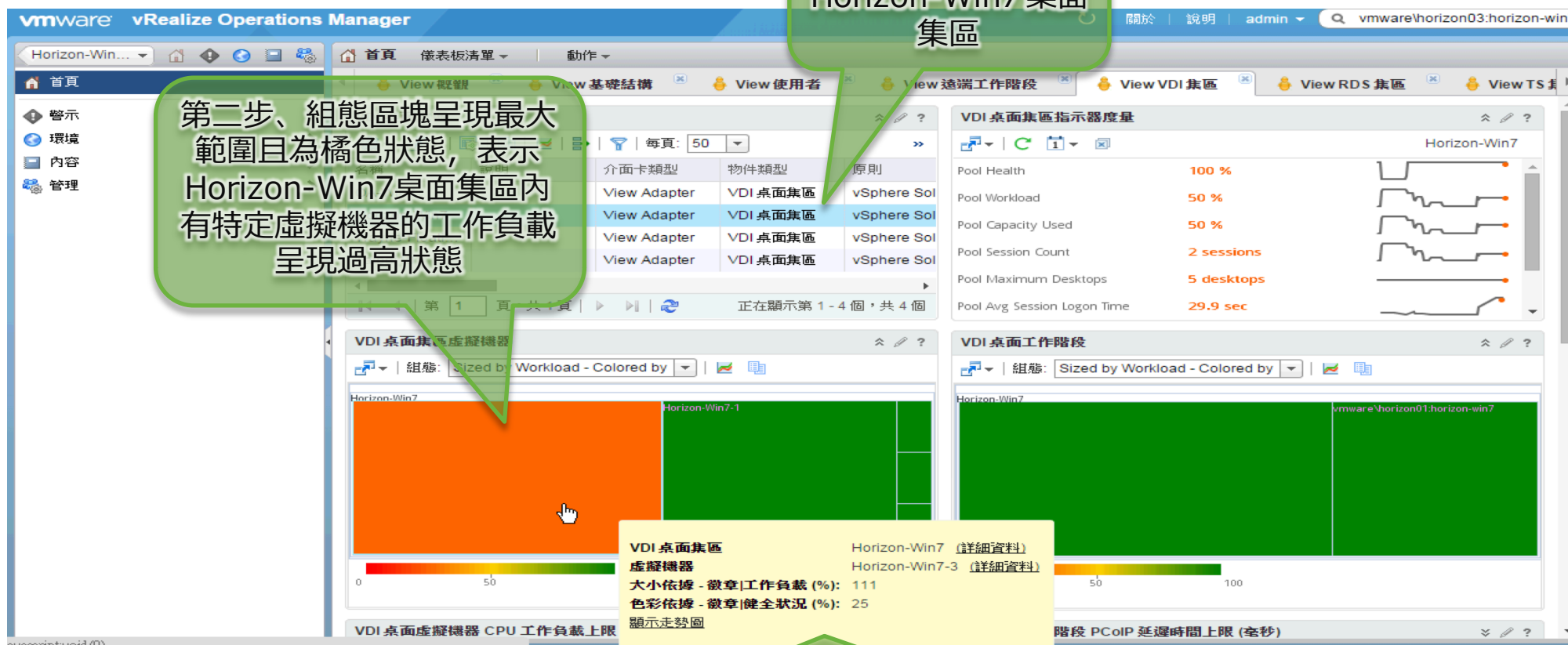
Session PCoIP TX Bandwidth: 0.6483 kbit/sec

Session PCoIP RX Bandwidth: 0.5781 kbit/sec

在桌面集區發現特定虛擬桌面負載過高

第一步、選擇這位使用者所屬於在的 Horizon-Win7 桌面集區

第二步、組態區塊呈現最大範圍且為橘色狀態，表示 Horizon-Win7 桌面集區內有特定虛擬機器的工作負載呈現過高狀態



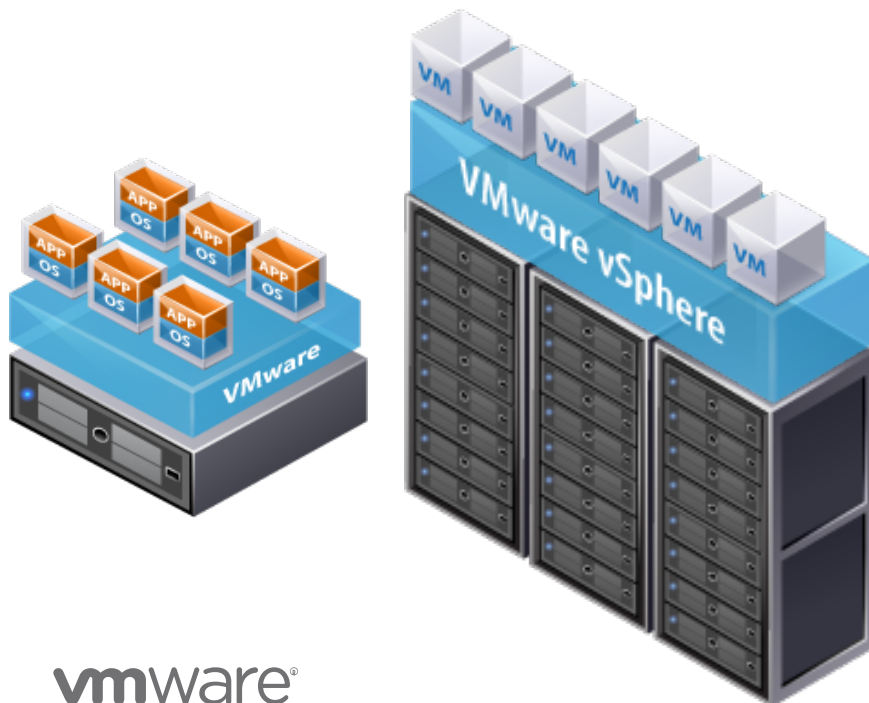
第三步、滑鼠移過去，隨即顯示出 Horizon-Win7 桌面集區中的 Horizon-Win7-3 虛擬機器出現嚴重工作負載問題

資訊應用場景

資訊服務應用效益

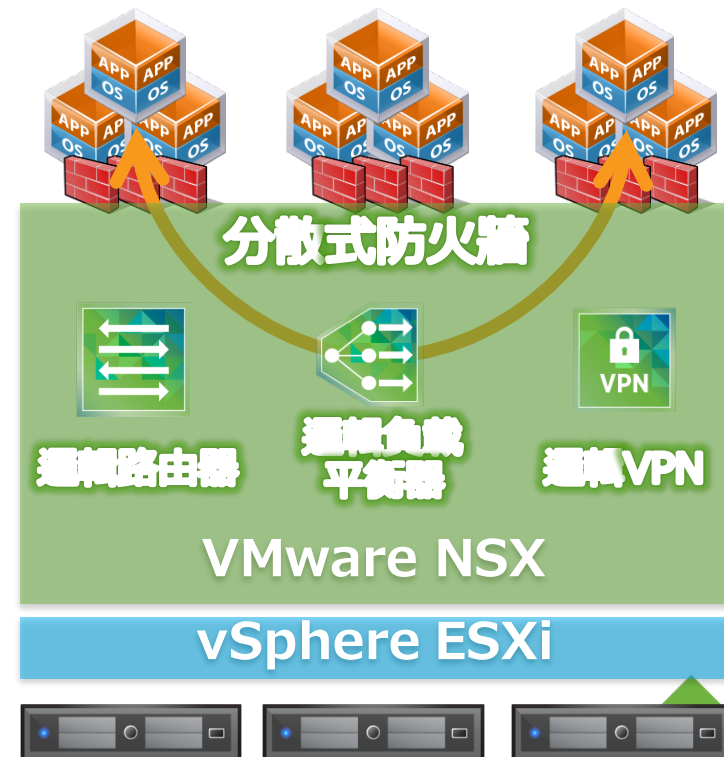
現有資訊系統虛擬化

- 虛擬化技術已經成熟，關鍵校務資訊系統上虛擬化能善用機房資源
- 在硬體發生非計劃損壞時即時保護
- 透過虛擬平台管理工具能有效掌握機房運算與儲存資源，並即時回應運作與效能問題



在軟體層實現網路和安全服務

- 資料中心內網路的功能，以內建於Hypervisor或虛擬機器的方式，跑在x86平台上
- 虛擬層直接提供安全功能。簡而言之，每個虛擬機器前，都有一台防火牆（安全設備）



永續運作並提供能源運用效率最佳化的資料中心

自動化資源確保

- > 平衡工作負載
- > 有效使用規劃硬體資源
- > 能及時進行最佳化

業務連續性

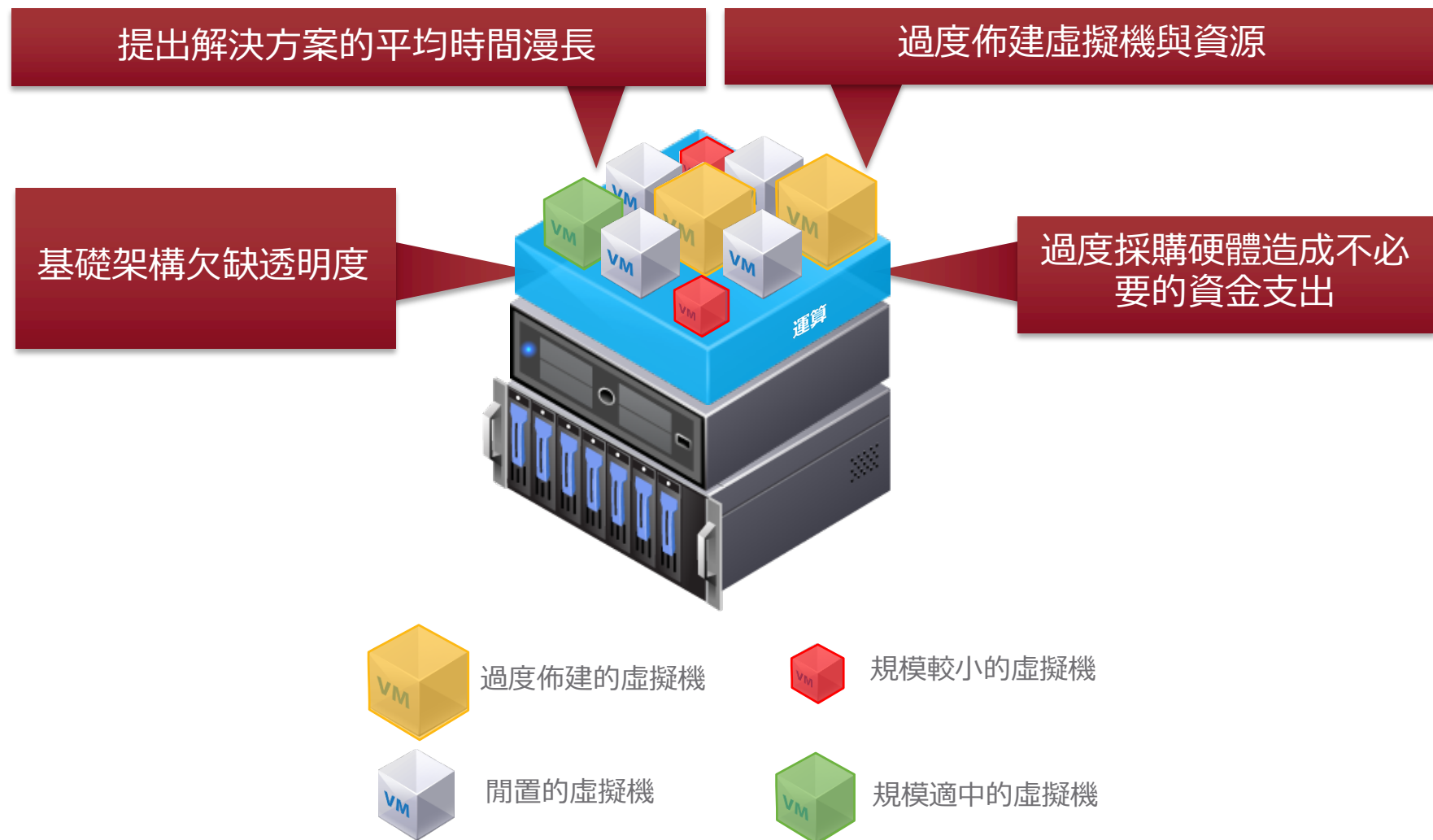
- > 當硬體或作業系統故障能立即重新啓動
- > 保護所有應用

隨需擴充的容量

- > Scale without disruption
- > Reconfigure on the fly
- > Save time



簡化及自動化的資料中心營運



簡化及自動化的資料中心營運

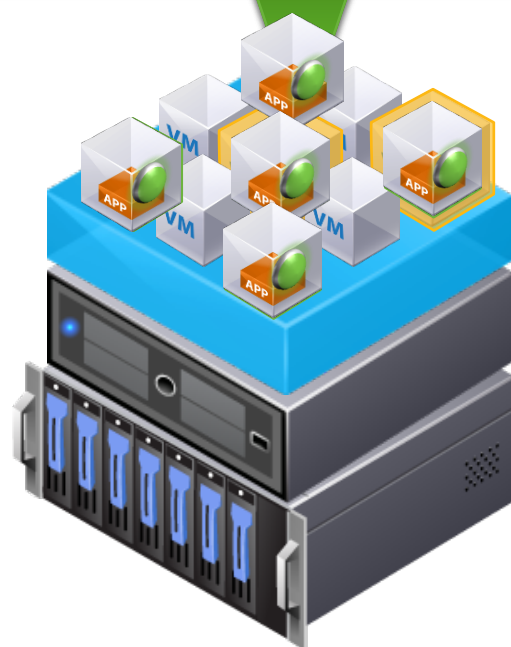
有效率的作業可降低 IT 管理的營運成本

提升效能並避免中斷服務

統一管理基礎架構和
應用程式

提出解決方案的平均時間更快

自動化的工作流程與
原則實行



過度佈建的虛擬機



規模較小的虛擬機



運作狀況良好



運作狀況不良



閒置的虛擬機



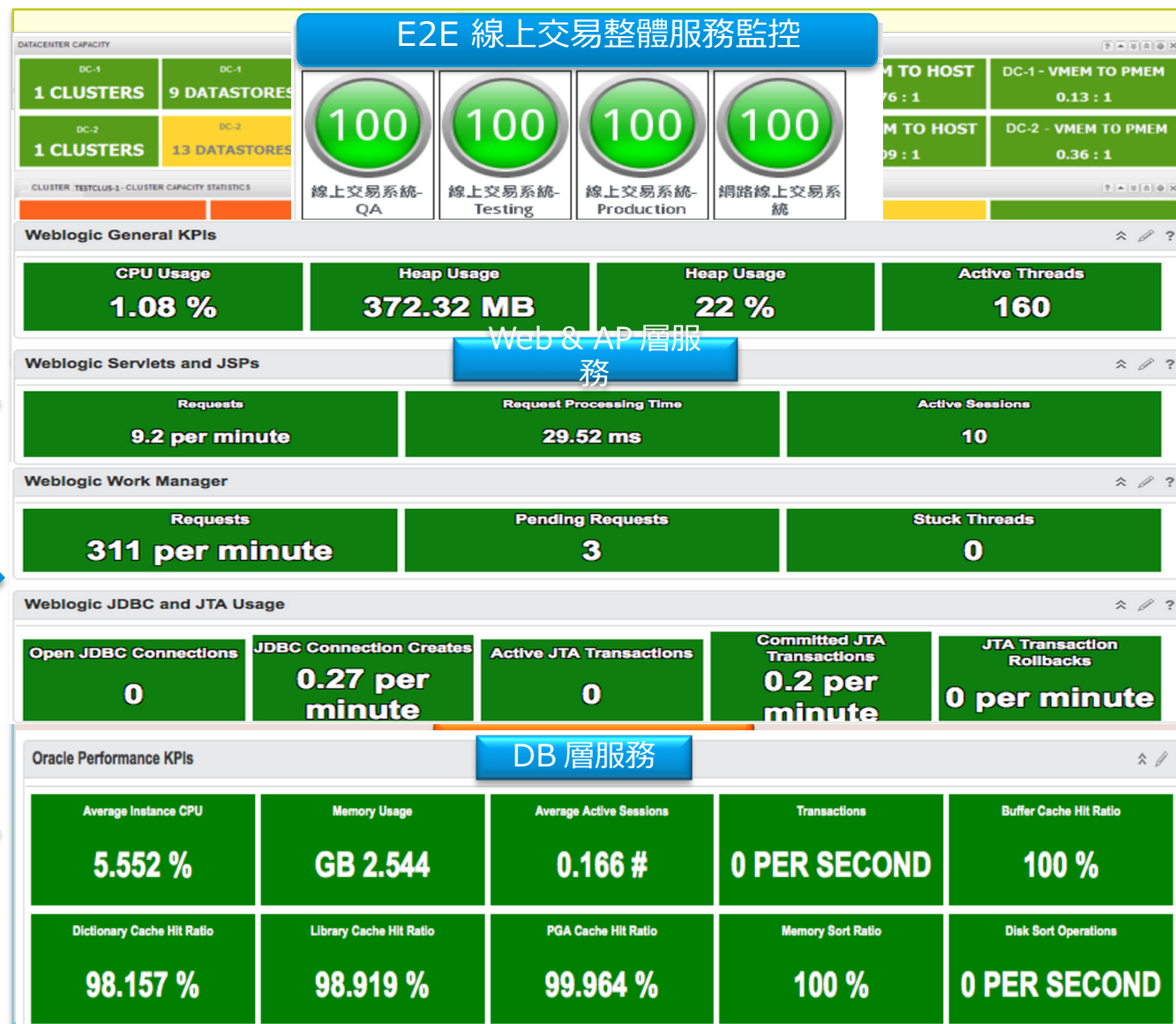
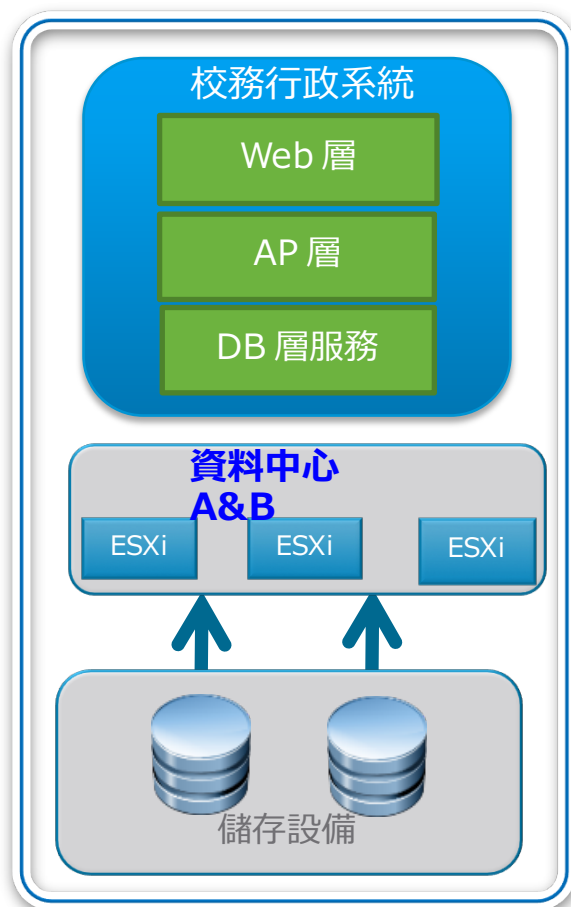
規模適中的虛擬機



運作狀況異常

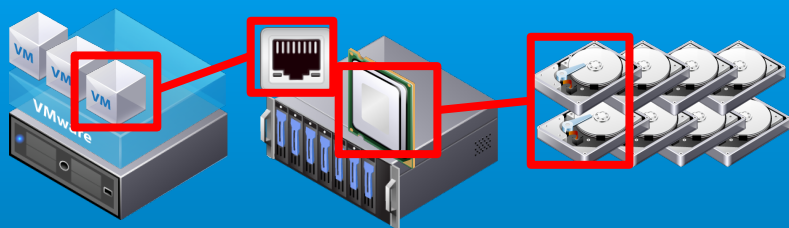


維運管理自動化

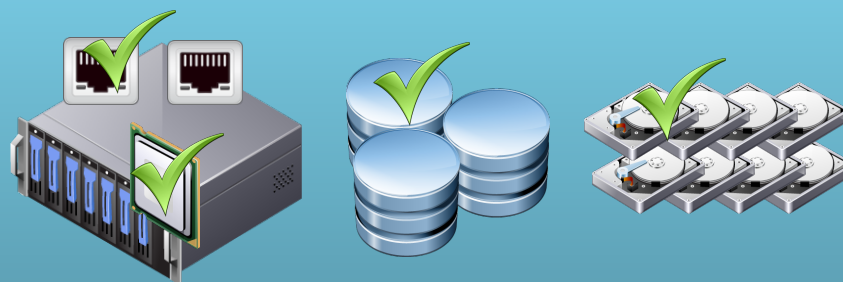


整體虛擬化環境可以透過集中管理達到整合綜效

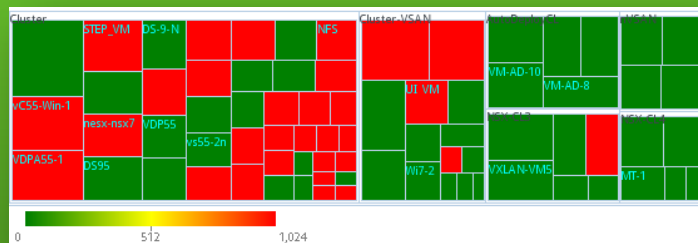
實體－虛擬環境連動



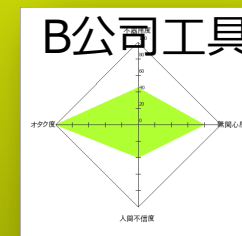
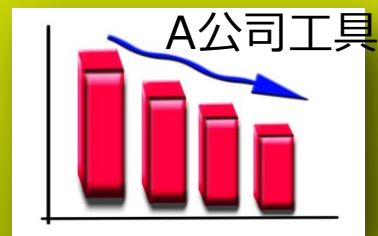
取得硬體層面相關效能指標



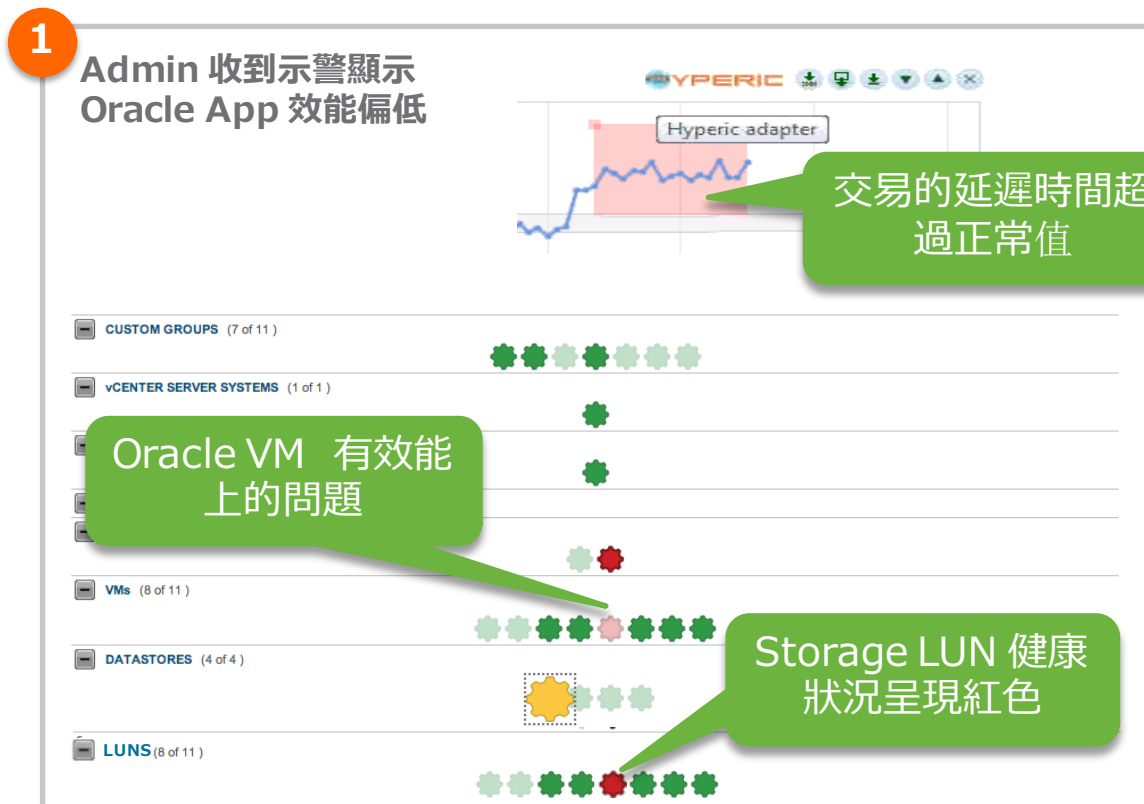
透過多維度色彩熱圖呈現問題



並且不需要同時使用特定的工具



使用情境：從應用程式，虛擬機，以及儲存整體環境進行故障排除



主動協助容量預估與警示分析



依照過去使用分析
記憶體預計12天後用完

	可用容量	無壓力值	剩餘時間
▶ CPU	199.58 vCPU 已設定 (包括過度認可)	153.44 vCPU 全部的 76.88 %	91.0 天
▶ 記憶體	280.58 GB 已設定 (包括過度認可)	268.39 GB 全部的 95.65 %	12.0 天
▶ 磁碟空間	7.64 TB 已設定	3.23 TB 全部的 42.26 %	>1 年
▶ vSphere 組態限制	1,536 台虛擬機器 已設定	84.2 台虛擬機器 全部的 5.48 %	>1 年

依照過去使用分析
其他資源使用剩餘時間

不含 認可的專案: 此為不考慮認可容量專案時的剩餘時間



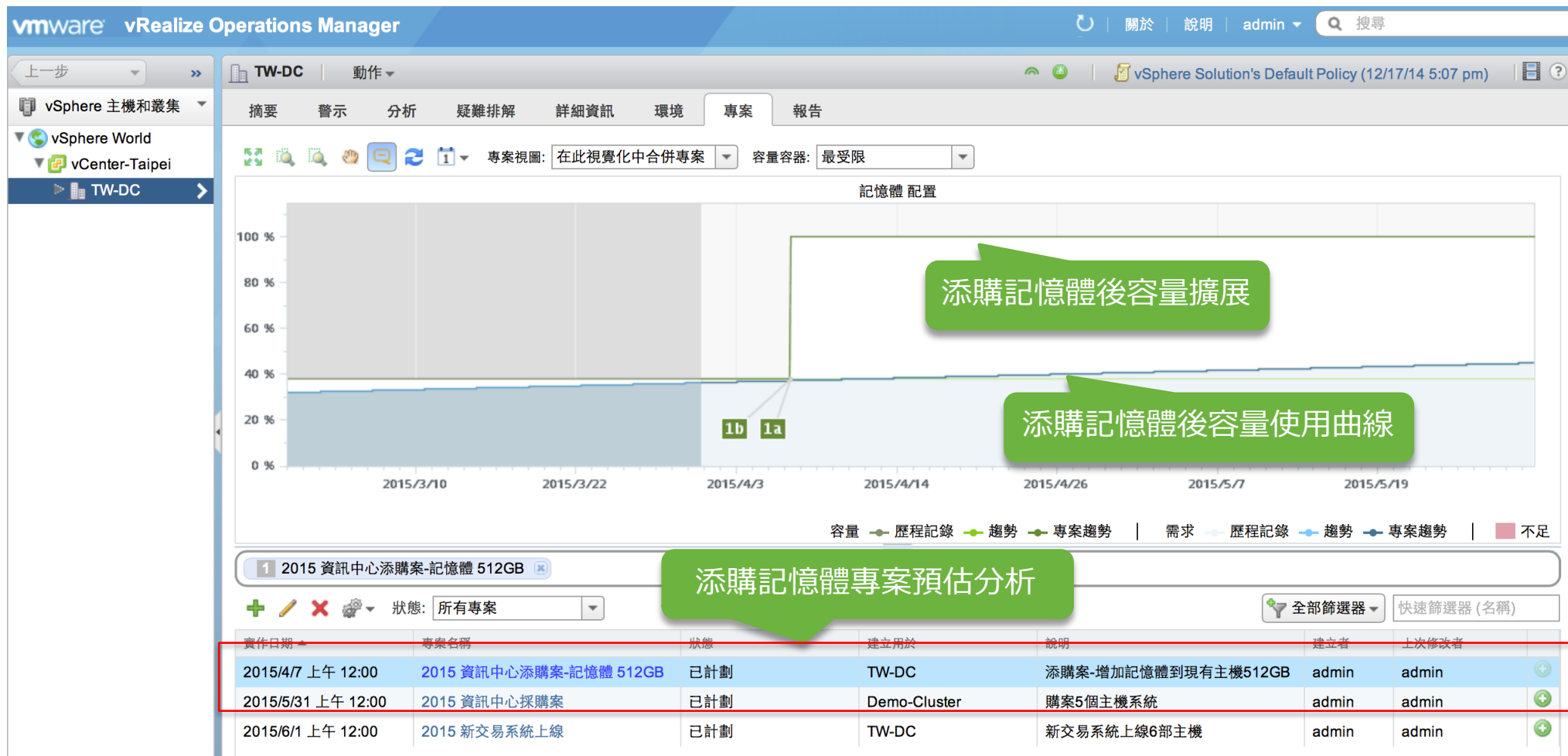
記憶體 12 天

CPU 91 天 磁碟空間 >1 年

vSphere 組態限制 >1 年

資訊中心應立即採購記憶體
提供採購依據與精準投資(CAPEX)

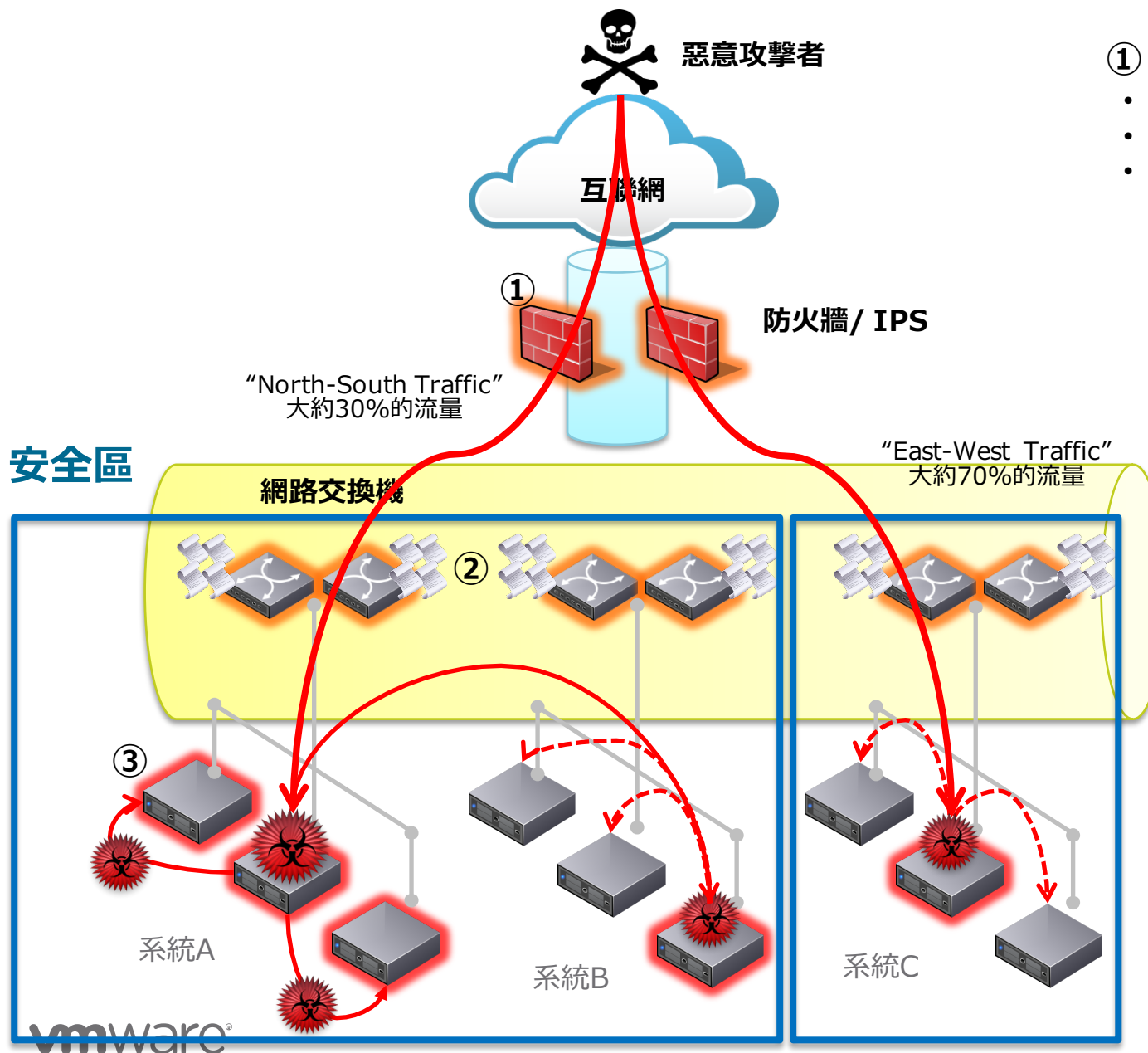
協助預估採購硬體配備及數量



協助預估新系統上線的影響



IT基礎設施的網路安全現狀和挑戰



① 防火牆之邊界安全極限

- 防禦入侵型安全機制
- 不可能防範所有的威脅
- 只能防禦進出互聯網的流量



② 實體網路的限制 (對操作帶來較大的負擔)

- 由網路交換機進行ACL設置提高管理複雜度
- 需要對每個安全區域進行配置管理
- 發生問題時追蹤能力有限



③ 增加擴散的風險

- 難以防止在安全區內擴散
- 資料中心內近七成網路流量是彼此互連的交通



VMware NSX

以虛擬機為單位的網路安全機制

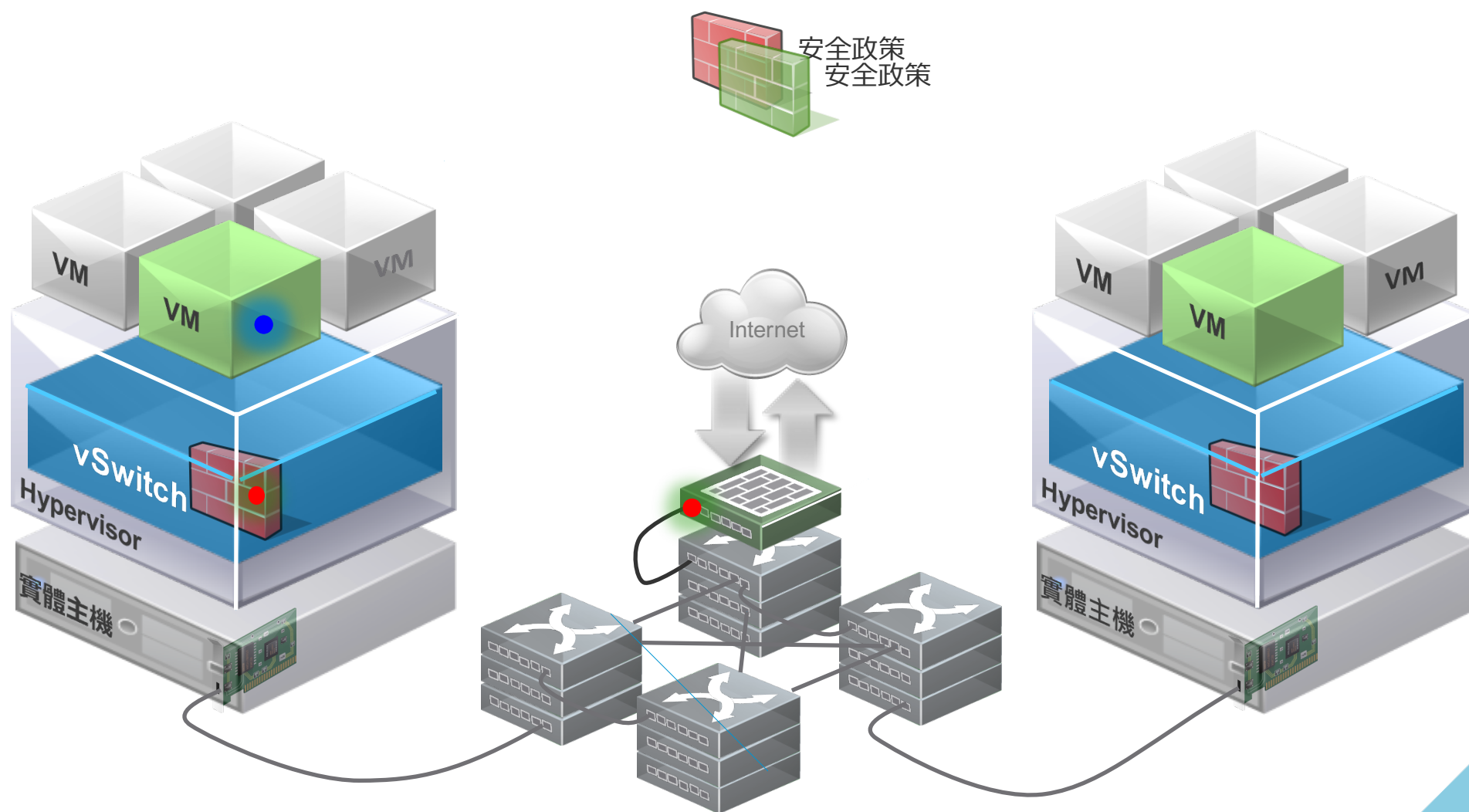


「零信任」

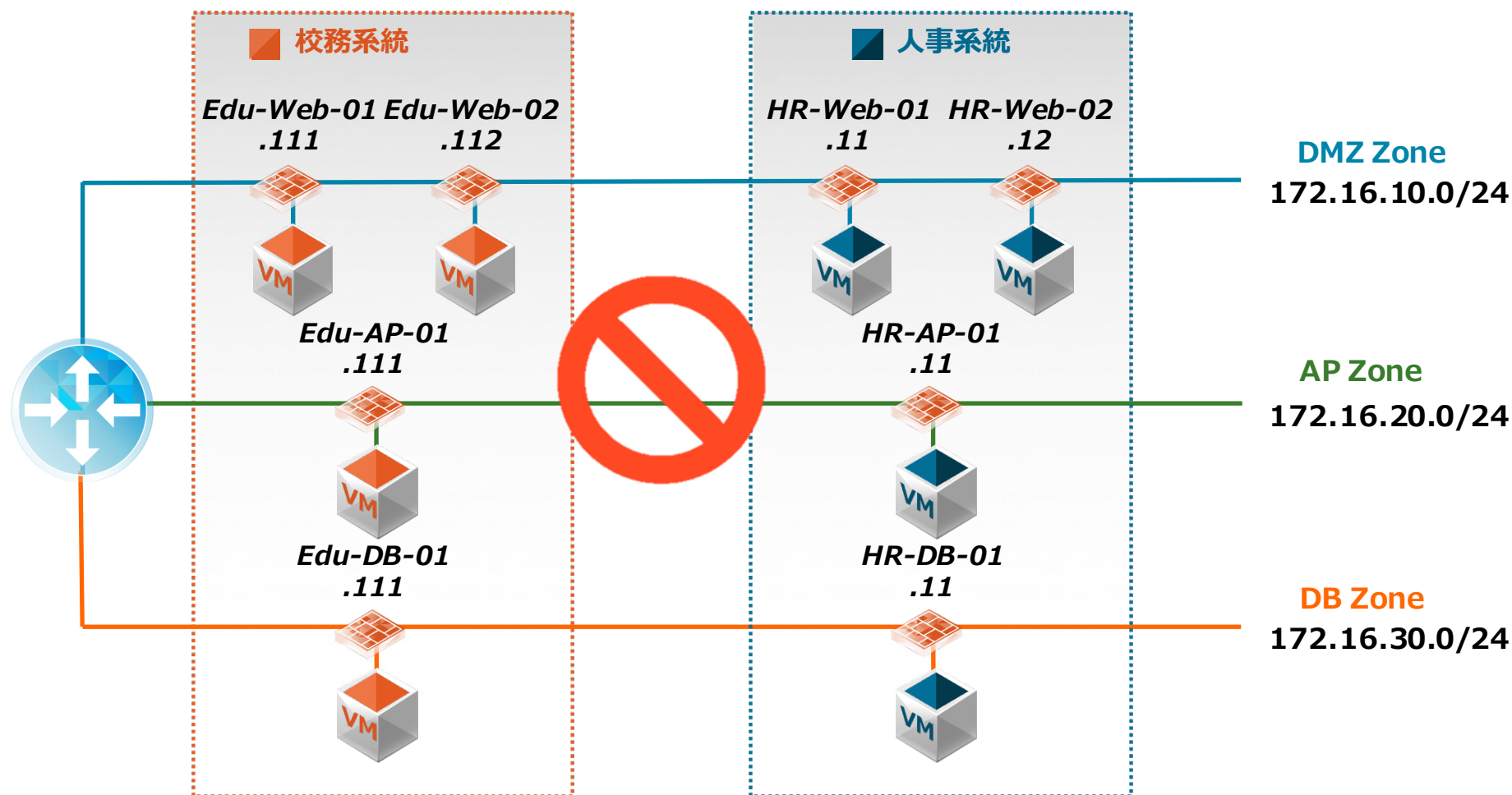
「防止擴散」



中央集中控管虛擬機的安全政策並能跟隨虛擬機移動

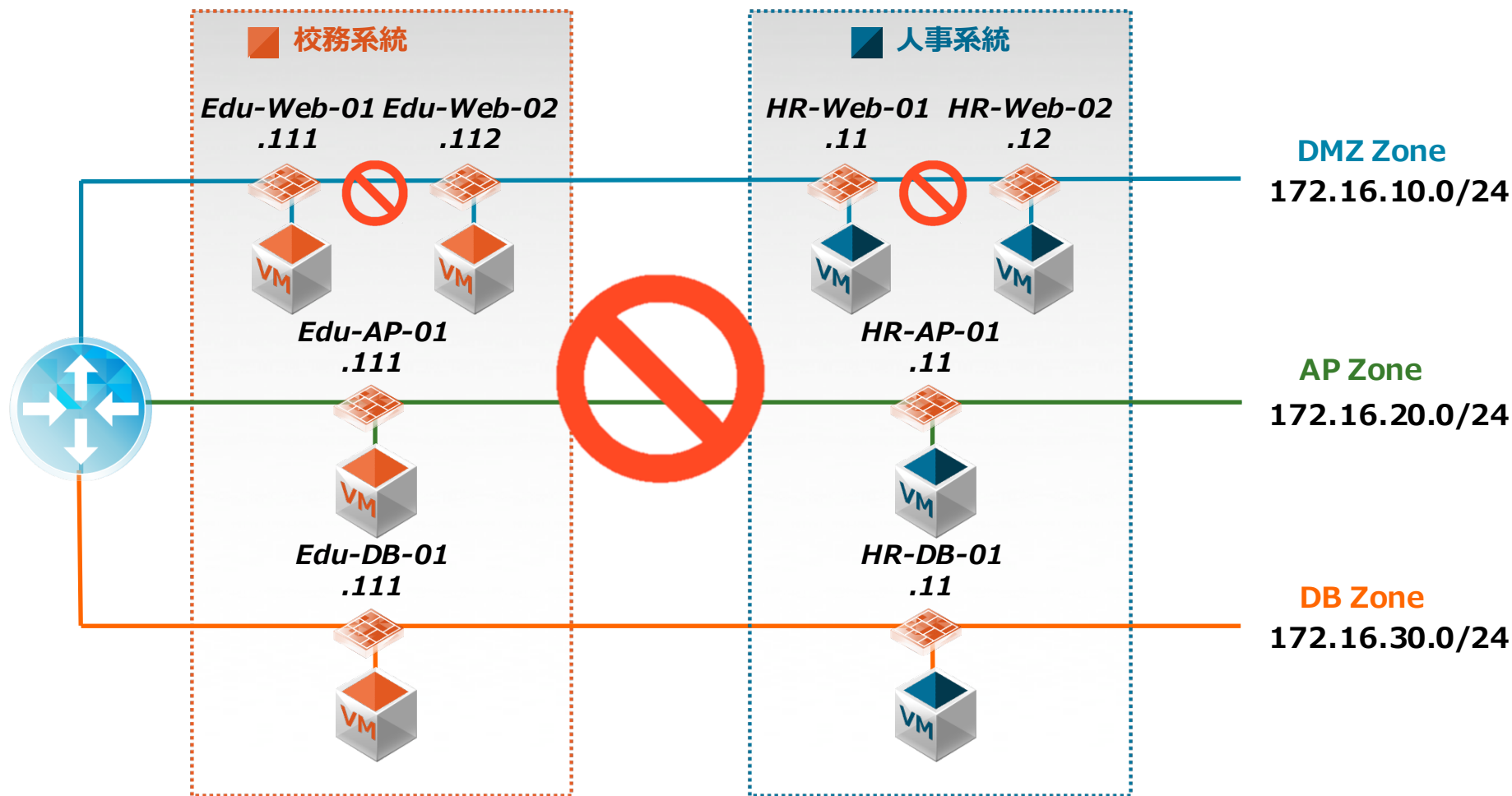


安全需求情境一：阻擋不同系統間之網路連線



校務系統與人事系統間沒有網路連線需求，
透過NSX防火牆阻止連線

安全需求情境二：阻擋DMZ網段內的相互連線



同樣位於DMZ Zone內的多台Web Server沒有相互連線需求，阻擋同網段內的相互連線



VMware 解決方案著墨於滿足大專院校現在與未來的資訊規劃需求

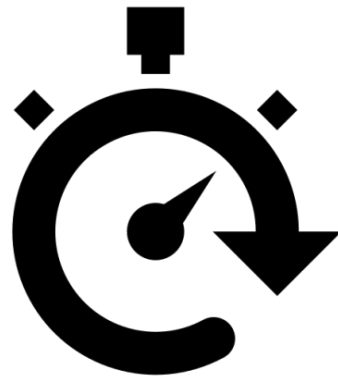
提升整體電子化校園的品質

VMware的技術使學校實現校園資訊化並因應新世代多樣性設備的資源存取



快速佈建與維護雲端環境

在時間緊迫與有限的人員/預算的狀況下，VMware的方案協助學校在很短的時間部署雲端框架與營運的能力



對現有投資提供保障

學校可以充分利用現有的基礎設施，在滿足當前需求的同時，並將它們轉化為滿足未來環境的平台環境



Thank You!

vmware