

OpenStack之「整合新興雲技術打造創新雲平台」專案

中華電信/工研院

105年07月12日



議程簡介



林建男
中華電信 工程師



Session Part 1(10分鐘)
專案計畫簡介



黃俊傑
工業技術研究院 資深工程師



Session Part 2(15分鐘)
軟體定義資料中心(SDDC)



簡士哲
中華電信 副理

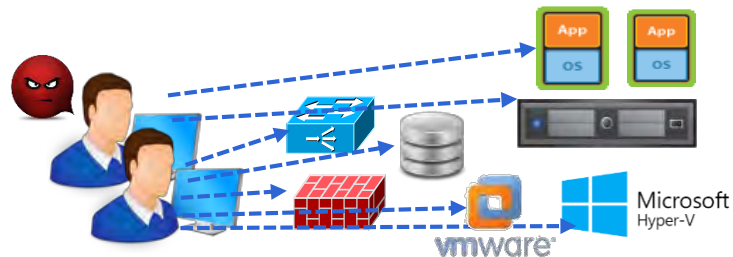


Session Part 3(15分鐘)
雲端整合管理平台介紹

企業資訊部門面臨的挑戰

維運管理複雜

當企業雲端建置規模變大時，因多機房/多設備/多虛擬平台，造成維運管理變得非常複雜



面臨複雜的維運管理流程

需要雲端服務自助管理平台

以人工受理並開通雲服務費時且維運複雜度高，導入自主管理平台有助提升效率



人工處理各方申請需求

服務開通流程未串整

中大型企業雲端環境複雜，當服務開通時，須在各別設備進行設定，才能完成開通



須分別設定各設備

雲端企業的新趨勢

66.9%企業採用私雲

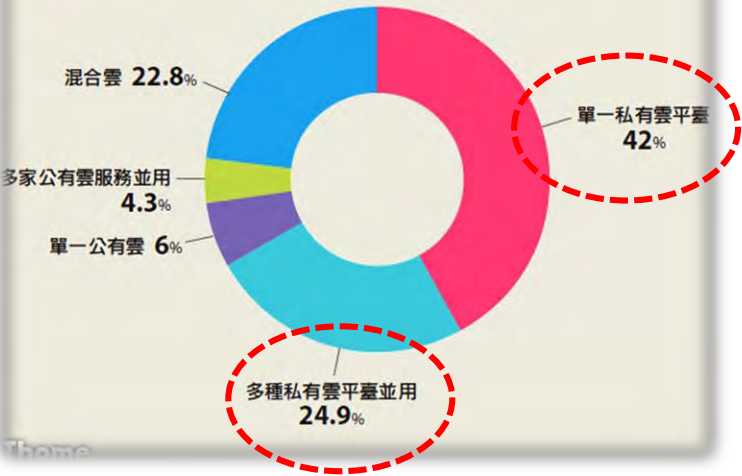
DevOps

SDN

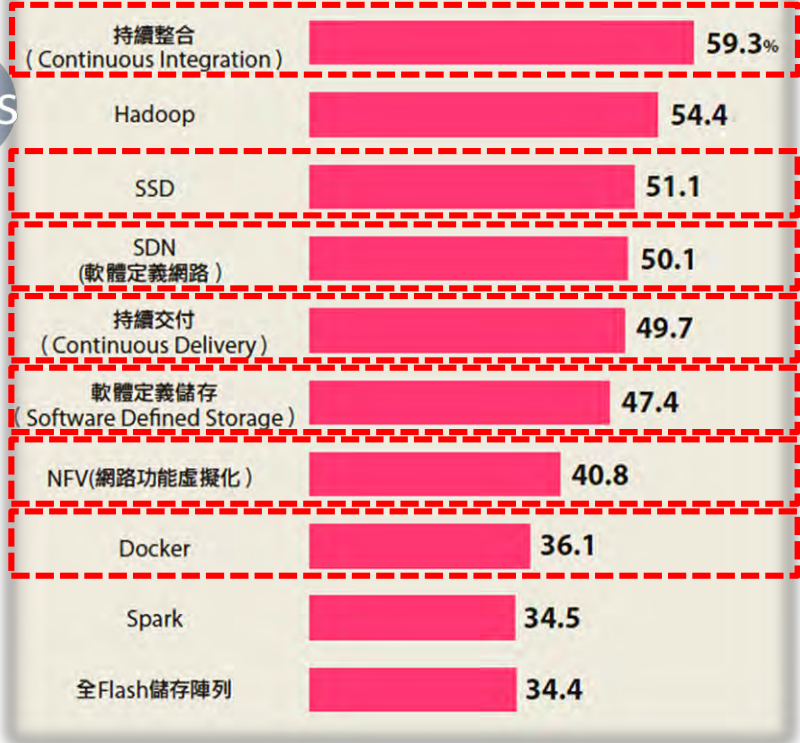
NFV



2016年上雲端企業的雲端建置模式採用率



2016年雲端企業導入新興技術Top10

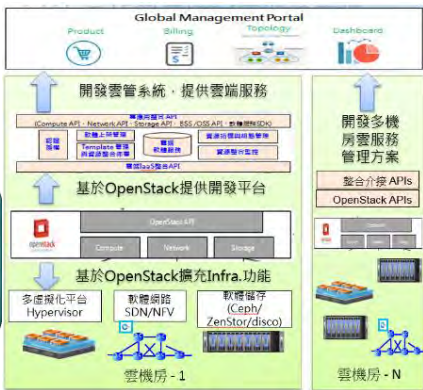


- 整合應用系統開發、部署與運流程，優化企業資源部門工作效率
- 彈性、開放的軟體式網路架構，節省企業建置與維護私雲基礎設施成本
- 導入輕量級虛擬化方案，提升雲資源池使用效率

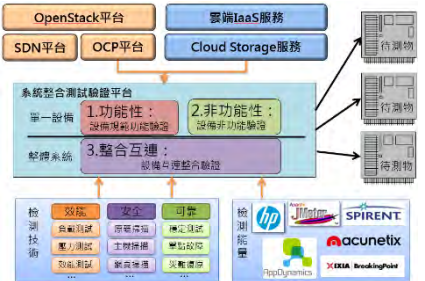
資料來源：iThome 2016年CIO大調查

專案開發內容規劃

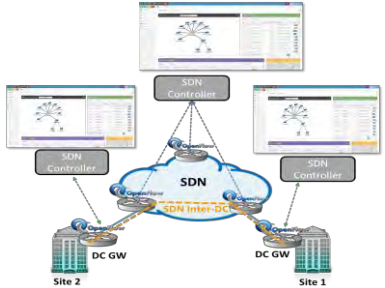
以OpenStack之隨選雲資源與儲存方案



國產軟硬體系統(含SSD)整合與驗證方案



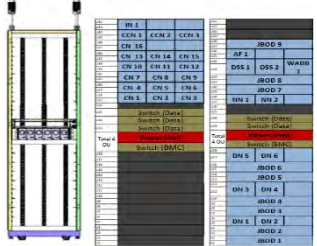
基於SDN之虛實整合網路隨選方案



全方位雲端安全縱深防護與管理方案



基於OCP綠能雲基礎環境之解決方案



三大目標執行重點



❖ 導入新技術，建構優質安全雲平台

- **創新**：導入**五項**重點技術，提供申裝與管理服務**自主性與彈性**
- **安全**：提供全方位**資安防護**，保障客戶
- **優質**：提供**優質高性價比**雲服務、網路/電路與增值選購服務

❖ 整合驗證機制，帶動雲端產業發展

- **整合**：結合**工研院、思銳、捷鼎**，並邀請國內雲端產業鏈廠商加入
- **提升**：建立**驗證機制**，提供單一設備與整合的驗證測試服務
- **場域**：通過驗證的產品**優先導入**政府相關雲計畫與中華電信機房

❖ 完備整廠輸出能量，行銷海外

- **參展**：參加**WCIT 2017**，展現台灣雲端實力與成就
- **市場**：以**東南亞**為首要海外輸出市場
- **壯大**：結合作夥伴，逐步擴展至**歐美市場**



分項計劃與目標

A. 新興雲技術發展分項

目標 研發OpenStack、SDN、OCP、SSD高速儲存等技術，完成雲端軟硬體系統創新研發

B. 整合驗證發展分項

目標 建置整合驗證所需之環境，研發從單一設備的功能與非功能品質到整體系統的整合運轉驗證

C. 雲服務營運發展分項

目標 研發新興雲資源管理系統，納入國產設備與系統，建置節能、高品質、彈性擴充雲資料中心

D. OCP與節能發展分項

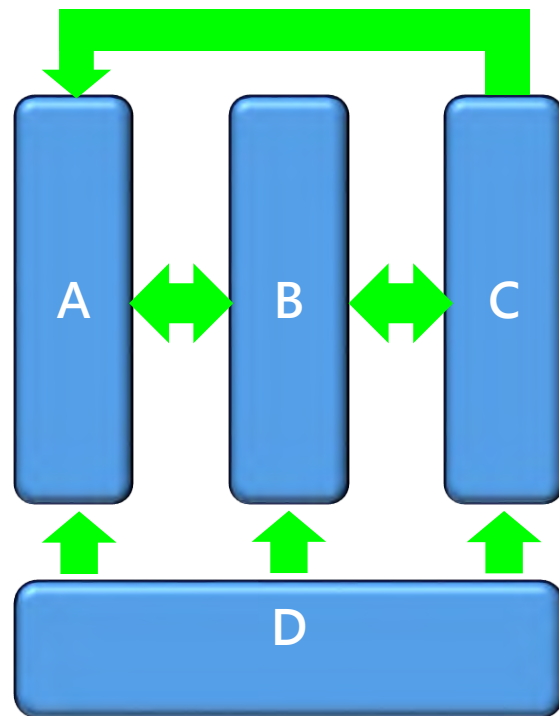
目標 建構以OCP為基礎的綠能雲基礎網路環境，提供本案其他分項使用，成為整廠輸出方案一環



系統
研發

功能
驗證

服務
上線



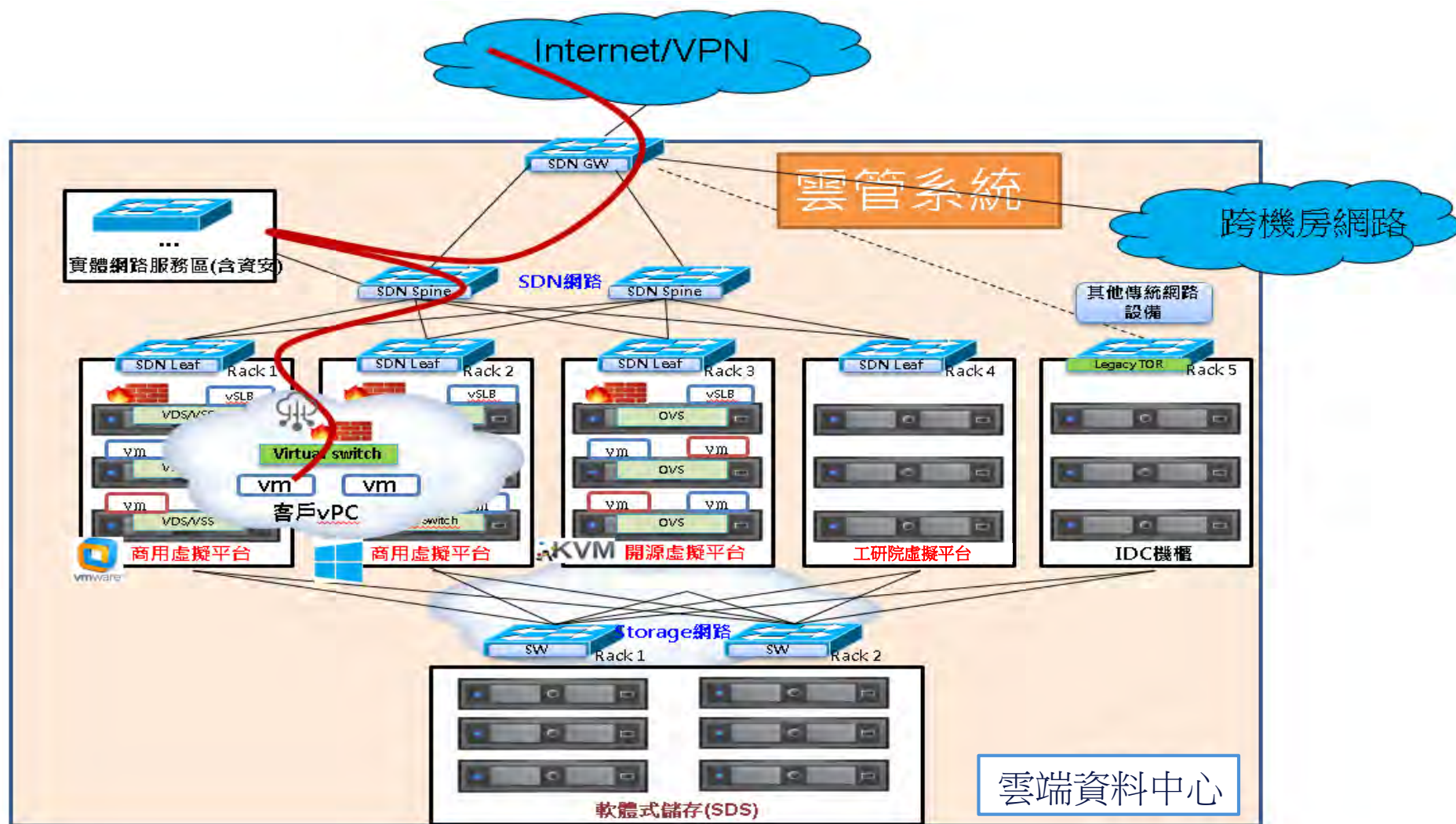
綠能雲基礎環境提供

團隊組成與相關產業鏈

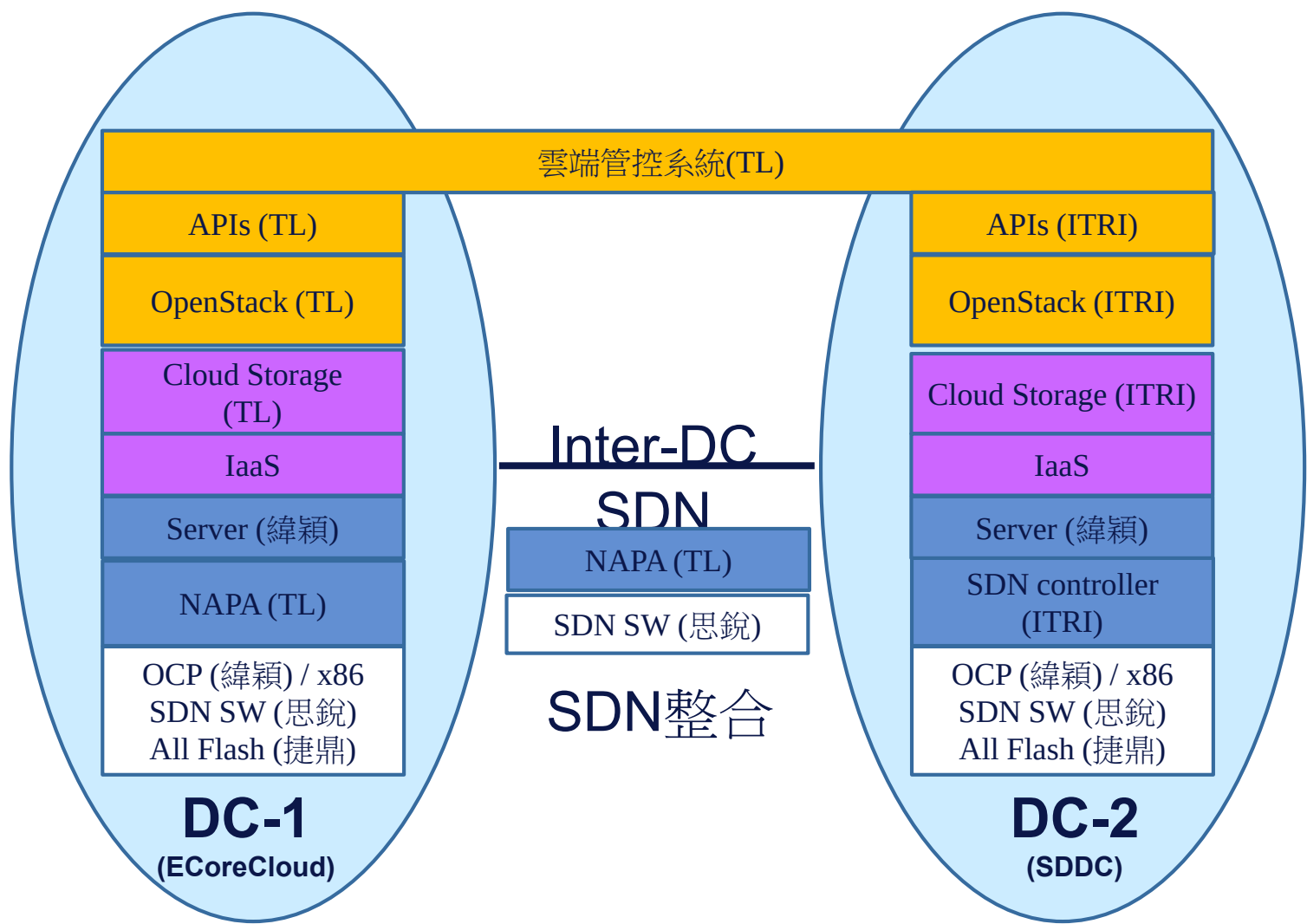
- ◆ 結合資通信、雲端、雲伺服器、儲存、節能與應用服務等頂尖成員組成全方位專業團隊，並由產學研全力支援



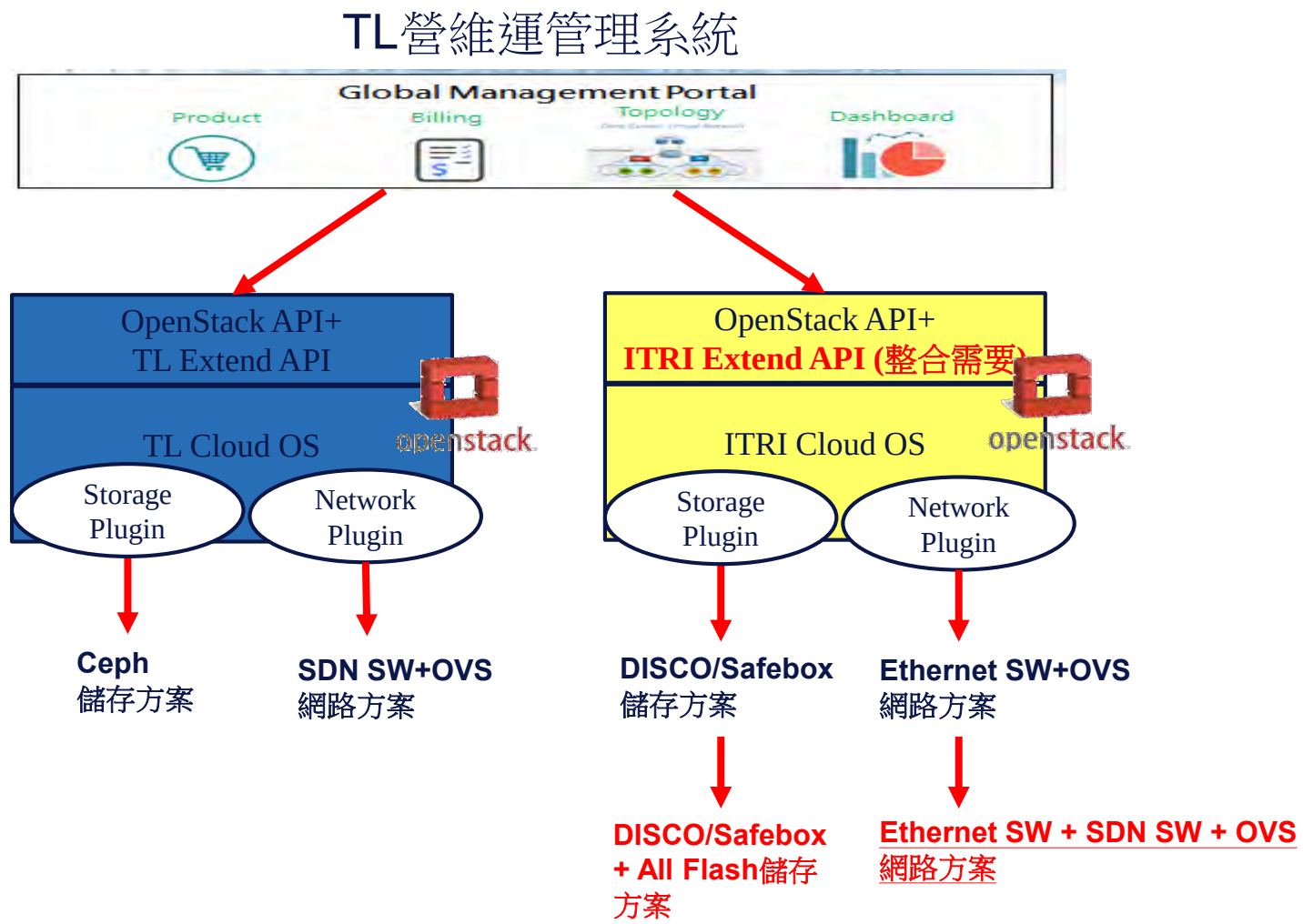
本專案架構示意圖



本專案DC-DC整體架構示意圖



本專案營維運整合架構



執行前後之國產化設備/系統比較

本計畫執行前

	執行前	是否使用國產品牌
虛擬層 (Hypervisor)	VMware	否
網路設備	Cisco、Juniper或其它相容網路設備	否
儲存設備	Netapp與其它相容儲存設備	否
伺服器	HP、Dell、緯創、廣達、英業達、台達電或相容伺服器	部分
Internet	中華電信	是
資安服務	HiNet 資安加值服務	部分
NFV防火牆	國外CheckPoint、FortiNet 虛擬防火牆與其它相容設備	否
NFV負載平衡	國外Citrix、F5、虛擬負載平衡器或其它相容設備	否
VPN提供	GSN、HiLink、IPVPN、IPSEC VPN	是
供裝系統	CHT雲寶供裝管理系統	是

本計畫執行後

	執行後	是否使用國產品牌	缺口
虛擬層 (Hypervisor)	KVM / ITRI OS (中華電信/工研院)	是	
網路設備	思銳科技國產SDN Switch	部分	高效能網路設備
儲存設備	緯穎Storage/捷鼎Flash Storage或相容之國產品	是	
伺服器	緯穎OCP、緯創、廣達、英業達、台達電或相容國產品	是	
Internet	中華電信	是	
資安服務	HiNet 資安加值服務	部分	高效能資安設備
NFV防火牆	本計畫研發之虛擬防火牆或其他相容之國產品	是	
NFV負載平衡	本計畫研發之虛擬負載平衡器或其他相容之國產品	是	
VPN提供	GSN、HiLink、IPVPN、IPSEC、SDN VPN	是	
供裝系統	CHT研發雲端供裝管理系統整合開源OpenStack技術	是	

■ 規劃優先使用國產設備提供服務，項目比例達85%

■ 缺口部分以高效能資安及高效能網路設備為主，仍待國內業者努力或尋求國際合作

議程簡介



林建男
中華電信 工程師



Session Part 1(10分鐘)
專案計畫簡介



黃俊傑
工業技術研究院 資深工程師



Session Part 2(15分鐘)
軟體定義資料中心(SDDC)



簡士哲
中華電信 副理



Session Part 3(15分鐘)
雲端整合管理平台介紹

Software define data center

Robert Huang
F Division / ICL / ITRI

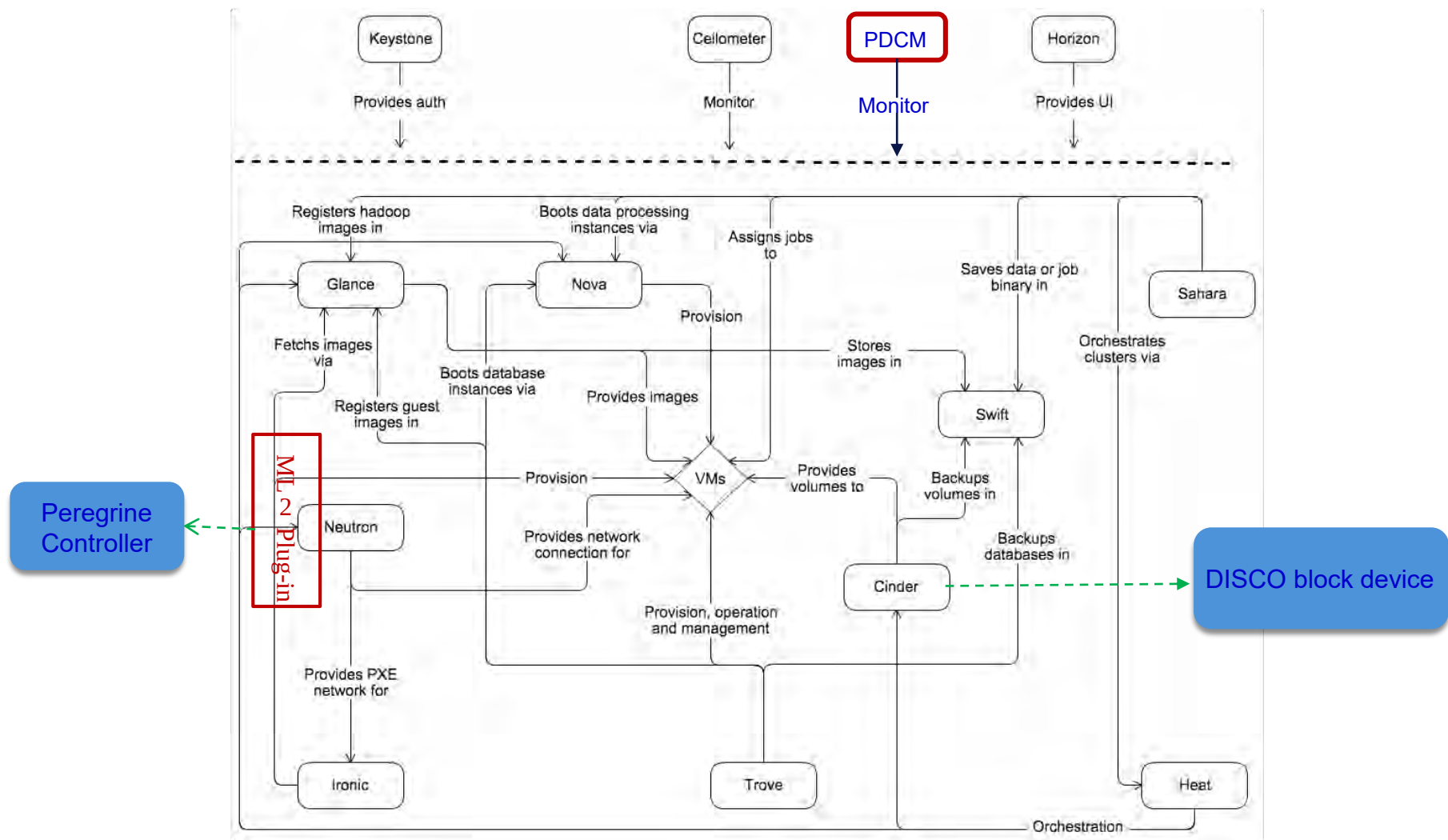


ITRI OpenStack Distribution

- What is ITRI OpenStack?
- What is missing in the OpenStack?
- ITRI OpenStack Distribution (IOD)
- DISCO
- SDN(Peregrine)
- PDCM



What is ITRI OpenStack?



Ref: http://docs.openstack.org/kilo/install-guide/install/apt/content/ch_overview.html

What is Missing in the OpenStack?

- Scalable and comprehensive bare metal provisioning
- HA support for every OpenStack system component
- Standard operating procedures (SOPs) and tools for change management
- Scalability for Internet-facing packet processing
- Overhead-minimizing network virtualization
- Physical data center administration tool
- PMLS (HaaS): Physical Machine (Hardware) Leasing Service)

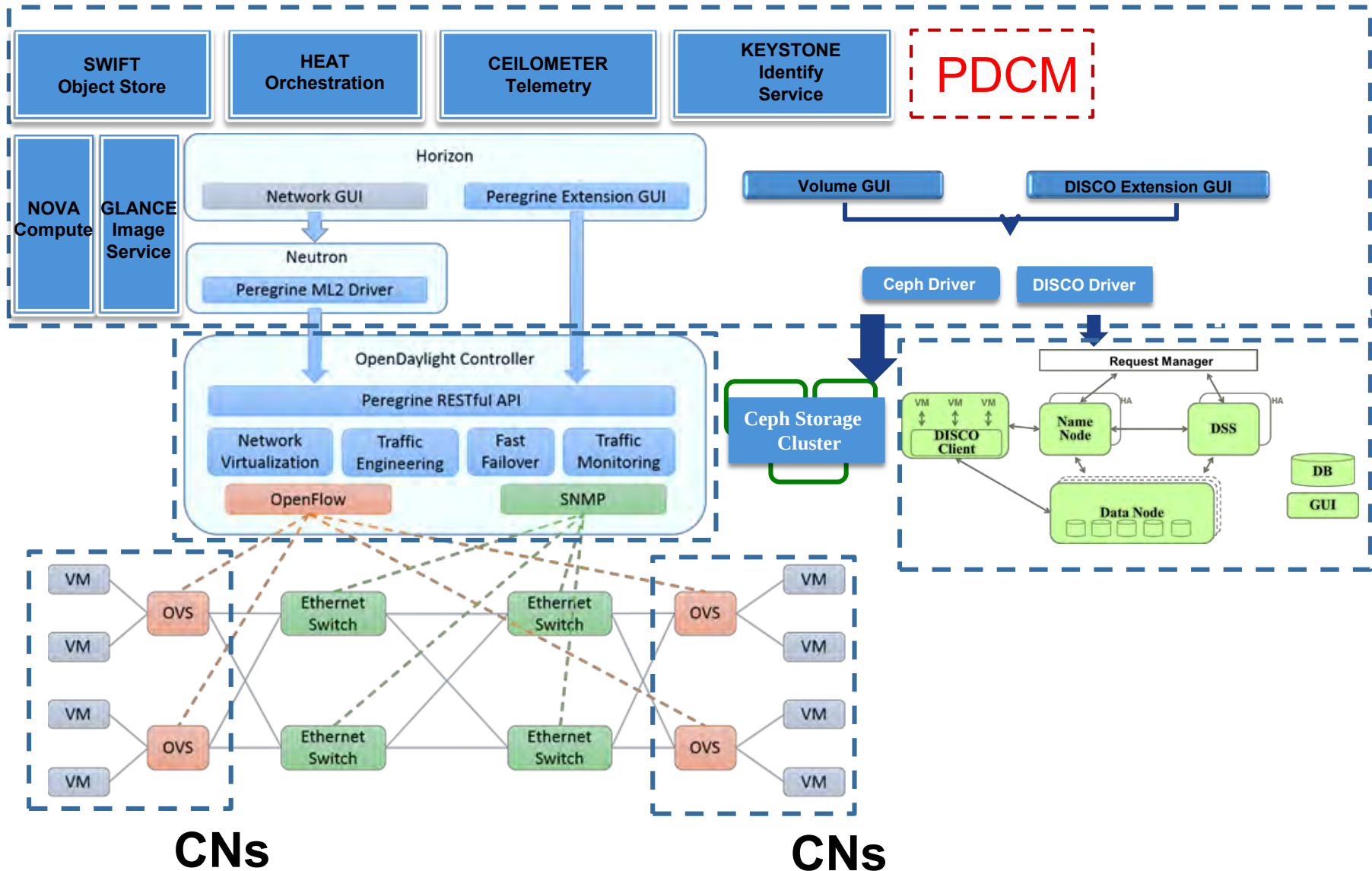


ITRI OpenStack Distribution

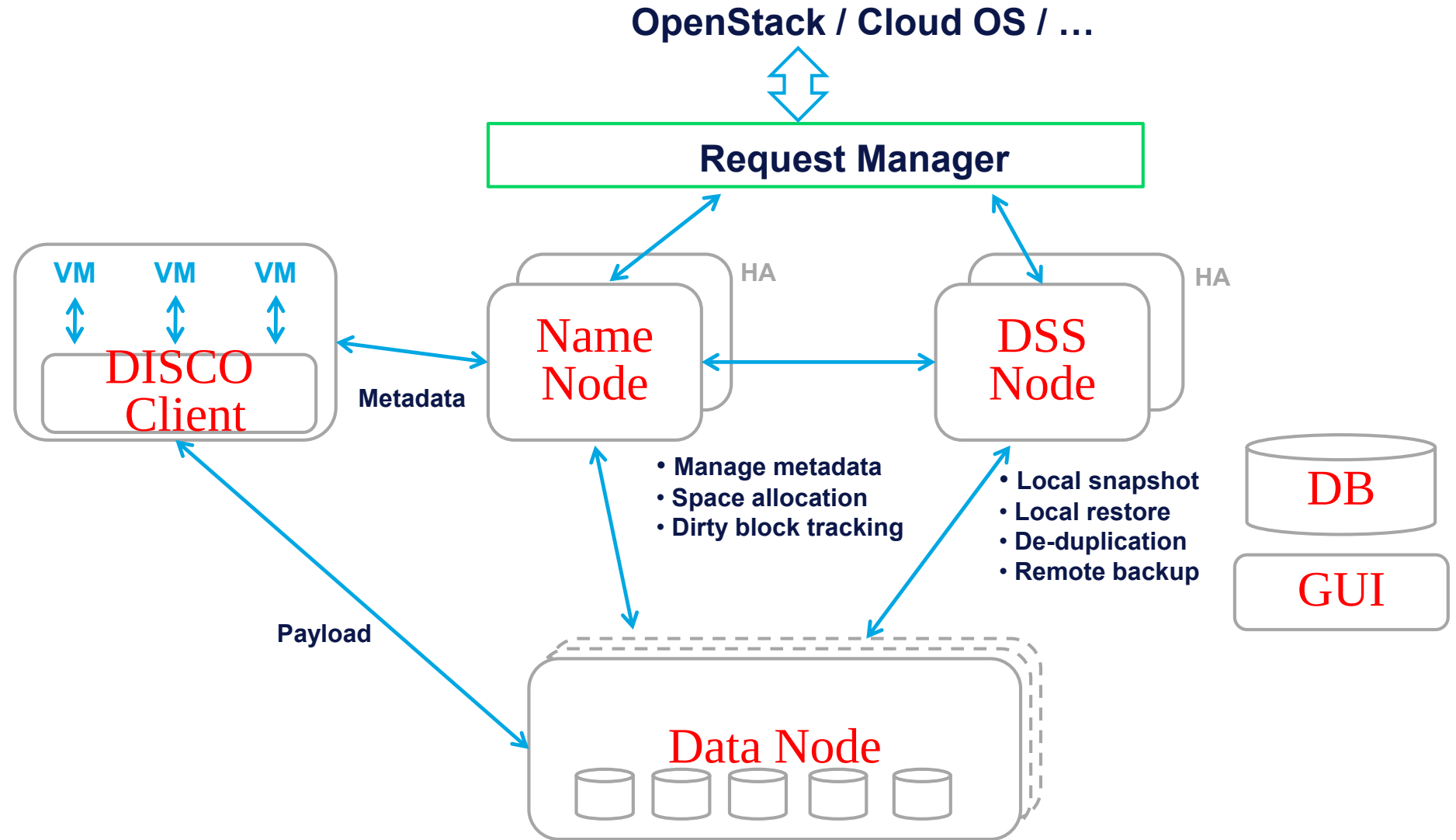
- Auto Deployment from Bare Metal
- ITRI OpenStack Components High Availability
- Dual Switch Protection
- Physical Data Center Monitor
- Cinder Plug-in
 - DISCO
- Neutron Plug-in
 - Peregrine
- Compute Node Failover
 - Move VMs from the broken Host to another healthy Host



ITRI OpenStack Distribution Stack



DISCO Isolation as a Cinder Plugin



Characteristics

Thin provisioning

Just use what you need,
Physical space is
allocated dynamically for
better efficiency.

Transparent data protection

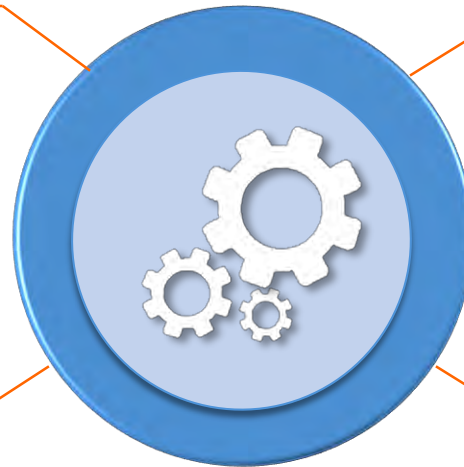
DISCO keeps your data safe
through its N-way replication &
self-healing mechanisms.

HA support

Data integrity is always
preserved no matter
what disaster occurs.

Fast volume cloning

No copy of metadata nor
data while cloning a
volume.



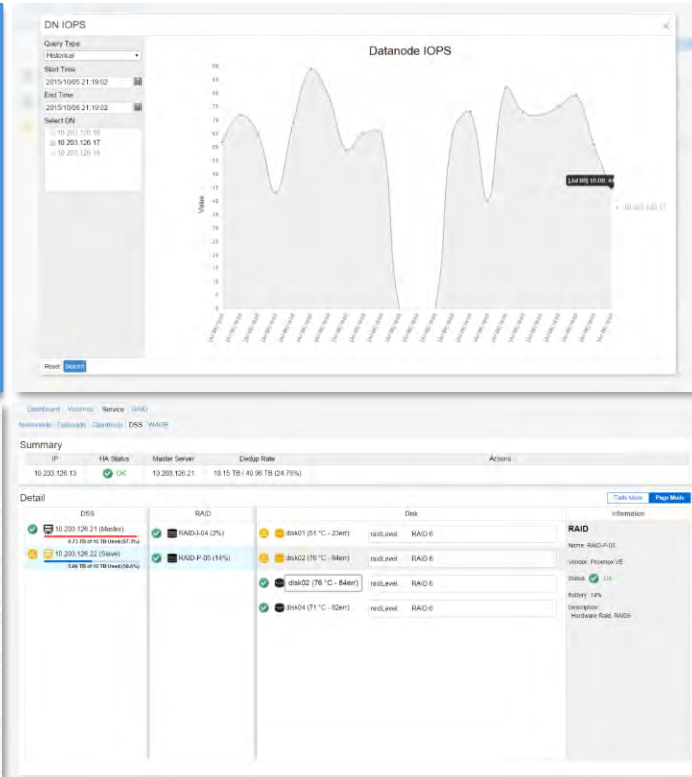
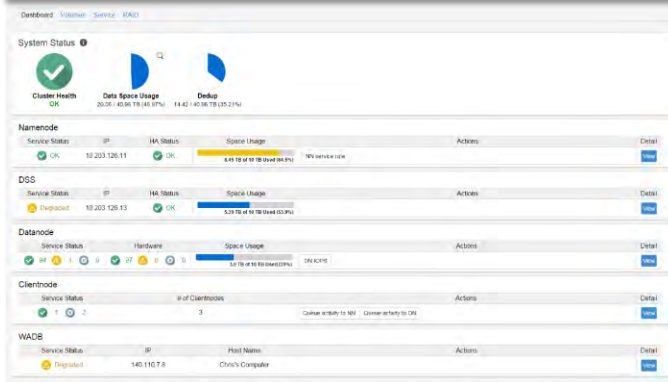
De-duplication

- Process the dirty blocks when taking the snapshot
- Data deduplication is a specialized data compression technique for eliminating duplicate copies of repeating data
- Background process without performance impact



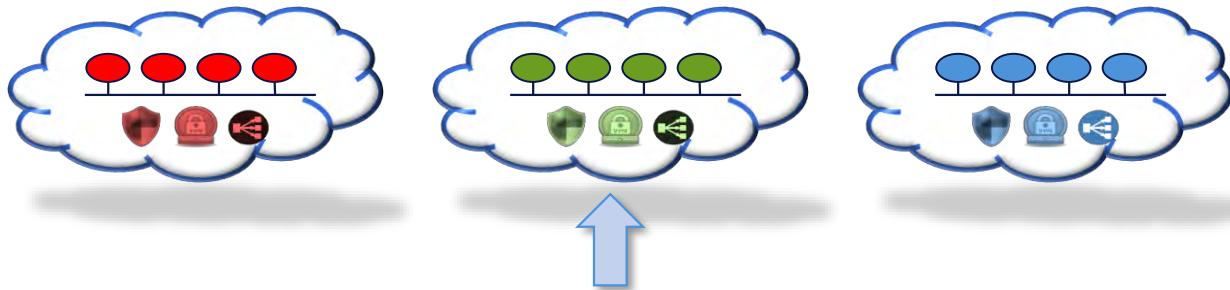
Diagnostic UI

Monitor service & hardware
Volume to component mapping
Component performance
OpenStack integration



Storage team - Division for Data Center System - ICL - ITRI Taiwan

SDN(Peregrine)



Peregrine hybrid SDN solution

ITRI contributes SNMP4SDN plugin to OpenDaylight, the plugin use SNMP and CLI to control Ethernet switches

Commodity Ethernet Switch

No vendor lock-in and no need to spend money in expensive hardware

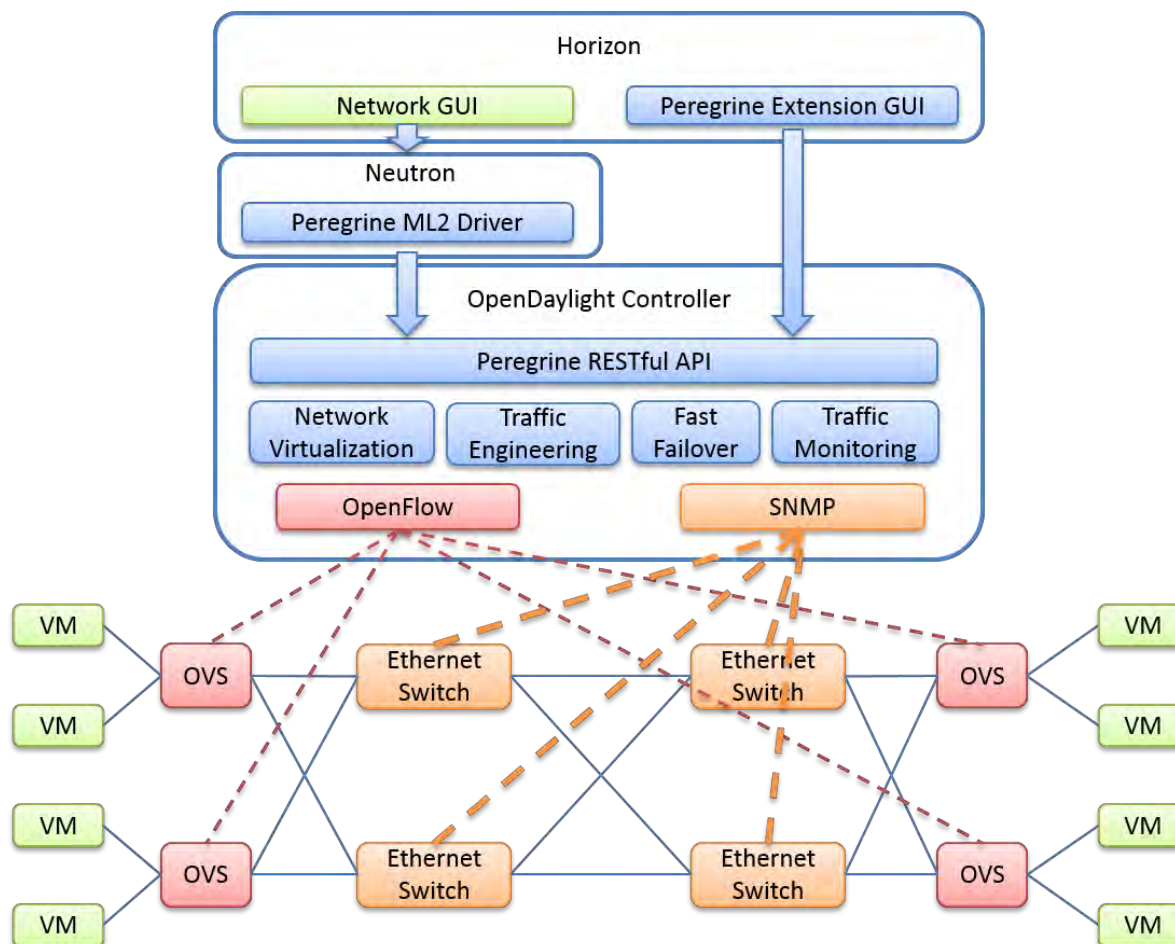


Virtual OpenFlow Switch (OVS)

Provide powerful edge intelligence

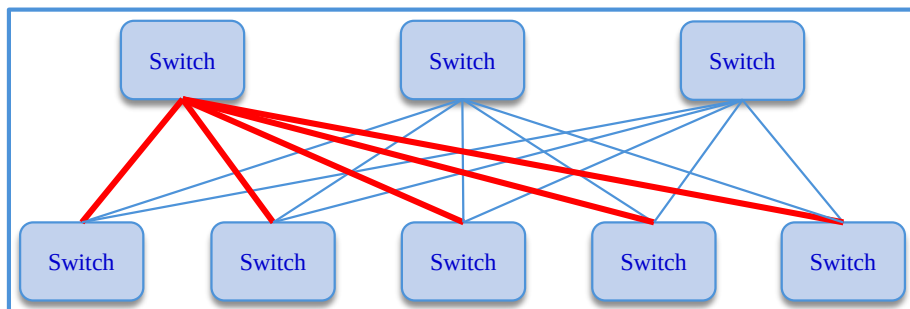


Architecture

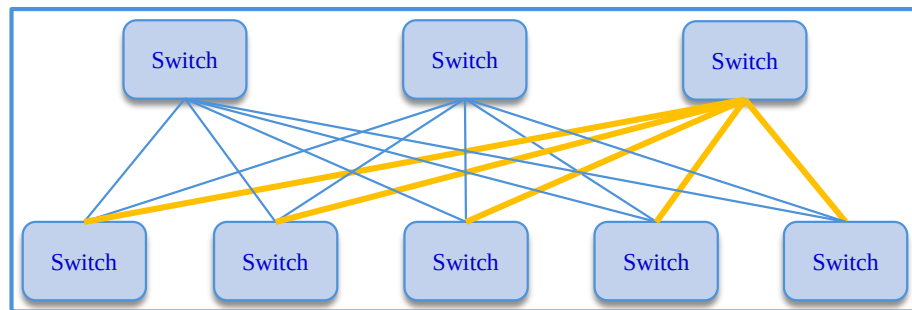
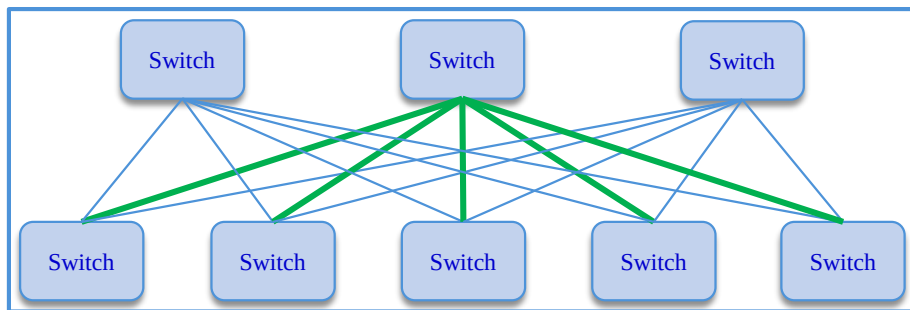


Features

Peregrine is L2 fabric architecture and able to achieve optimal load-balanced of all the physical networks by dynamically calculates the packet transmission path.

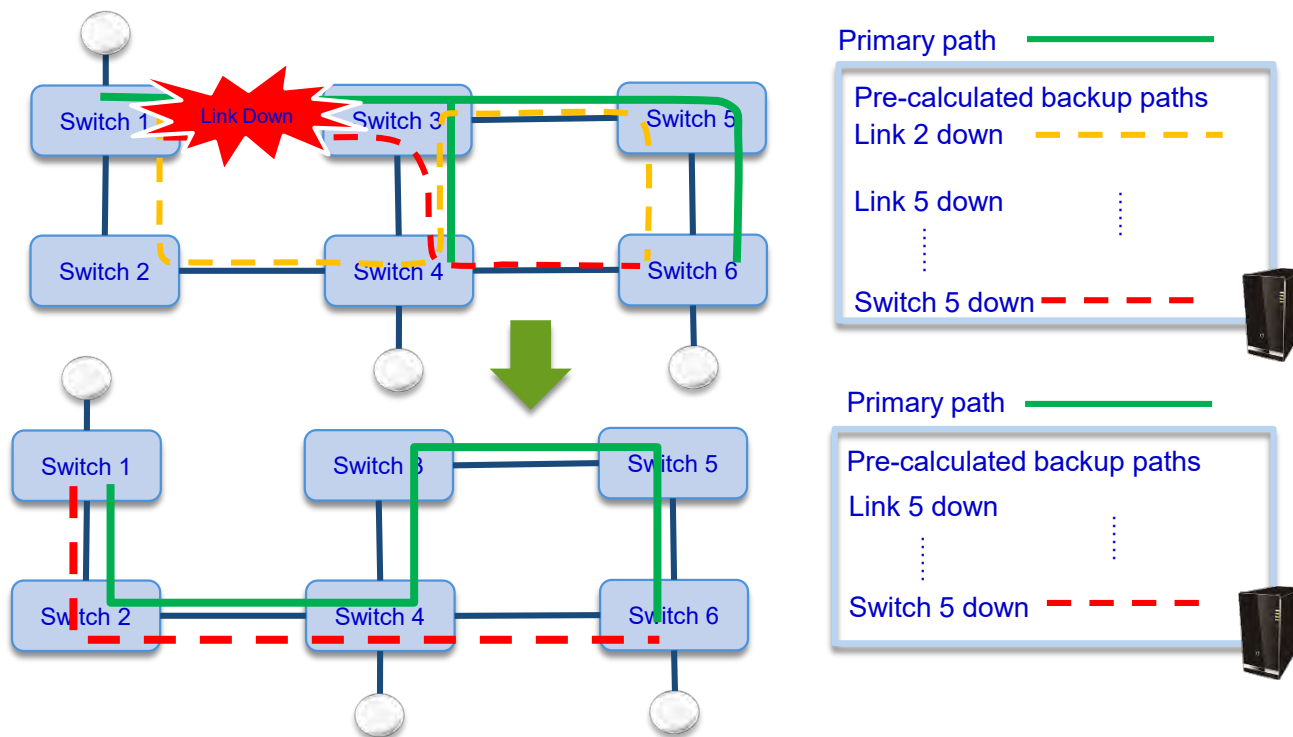


— VLAN: 10
— VLAN: 20
— VLAN: 30



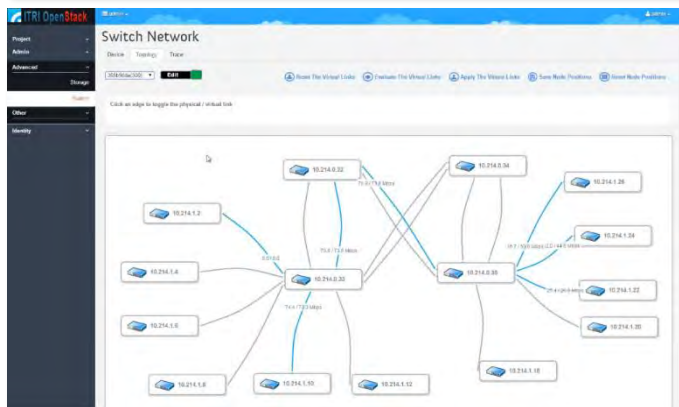
Features

Peregrine is able to re-deploy packet transmission path when any of link or device is failed by applying centralization control architecture in Fast Failover.



Features

Physical & virtual topology
Physical & virtual traffic load
VM traffic analysis
User defined data path
OpenStack integration



Time	Source	Destination	Protocol	ID	Flags	Seq	Ack	Win	Length	Other
05:34:28.624652	10.10.10.5.57009	10.10.10.5.6001							1470	UDP
05:34:28.624801	10.10.10.5.57009	10.10.10.5.6001							1470	UDP
05:34:28.624844	10.10.10.5.57009	10.10.10.5.6001							1470	UDP
05:34:28.624917	10.10.10.5.57009	10.10.10.5.6001				140200000	140200000	1	228	65540 [seq=140200000, win=65540, len=65540, flags=0]
05:34:28.624959	10.10.10.5.57009	10.10.10.5.6001							1470	UDP
05:34:28.625001	10.10.10.5.57009	10.10.10.5.6001							1470	UDP
05:34:28.625043	10.10.10.5.57009	10.10.10.5.6001							1470	UDP
05:34:28.625085	10.10.10.5.57009	10.10.10.5.6001							1470	UDP
05:34:28.625127	10.10.10.5.57009	10.10.10.5.6001							1470	UDP
05:34:28.625169	10.10.10.5.57009	10.10.10.5.6001							1470	UDP
05:34:28.625211	10.10.10.5.57009	10.10.10.5.6001							1470	UDP
05:34:28.625253	10.10.10.5.57009	10.10.10.5.6001							1470	UDP
05:34:28.625295	10.10.10.5.57009	10.10.10.5.6001							1470	UDP

Links	Virtual Networks	VM Pairs
10.214.0.33 P15 - 10.214.0.32 P16	VLAN 304	10.10.10.5 - 10.10.10.5
10.214.0.32 P16 - 10.214.0.33 P15	VLAN 304	10.10.10.5 - 10.10.10.5
	VLAN 303	10.10.10.5 - 10.10.10.5

What is PDCM?

- PDCM stands for Physical Data Center Management.
- It is a hardware monitor system and a service management system.
- Features:
 - ✓ Health monitoring of physical devices
 - ✓ Health monitoring of OpenStack system components
 - ✓ Traffic load and resource usage reporting
 - ✓ Event and alerting system



PDCM provides a comprehensive solution for monitoring OpenStack cloud, including hardware devices and OpenStack services.

What Can PDCM Do?

VM State

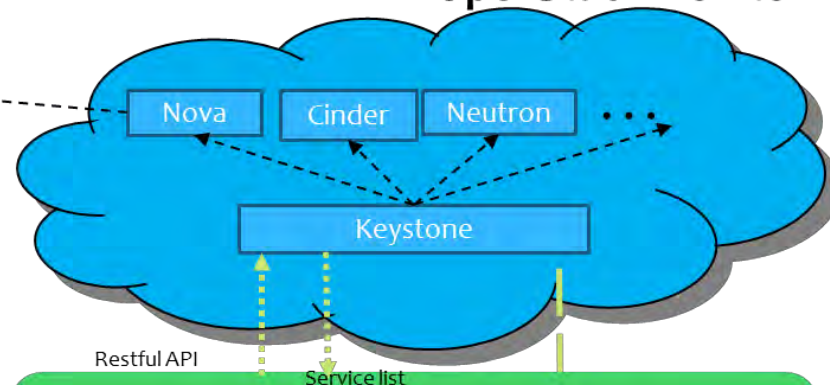
Events	Name	Flavor	Image	Tenant	Host	Floating IPs	Fixed IPs	Status
✓	celometer-test	m1.tiny	cirros	admin	WSR7-4106		10.5.0.7	ACTIVE
✓	cirros001	m1.tiny	cirros	admin	WSR7-3606	10.207.155.2	10.5.0.3	ACTIVE
✓	cirros02	m1.tiny	cirros	admin	WSR7-3606	10.207.155.5	10.5.0.6	ACTIVE
✓	new_instance	m1.tiny	cirros	admin	WSR7-3606		10.5.0.8	ACTIVE
✓	ubuntu001	m1.xsmall	Ubuntu	admin	WSR7-3406	10.207.155.3	10.5.0.4	SHUTOFF
✓	ubuntu002	m1.xsmall	Ubuntu	admin	WSR7-3906	10.207.155.4	10.5.0.5	ACTIVE

Authentication information
+
Keystone endpoint URL

Device List

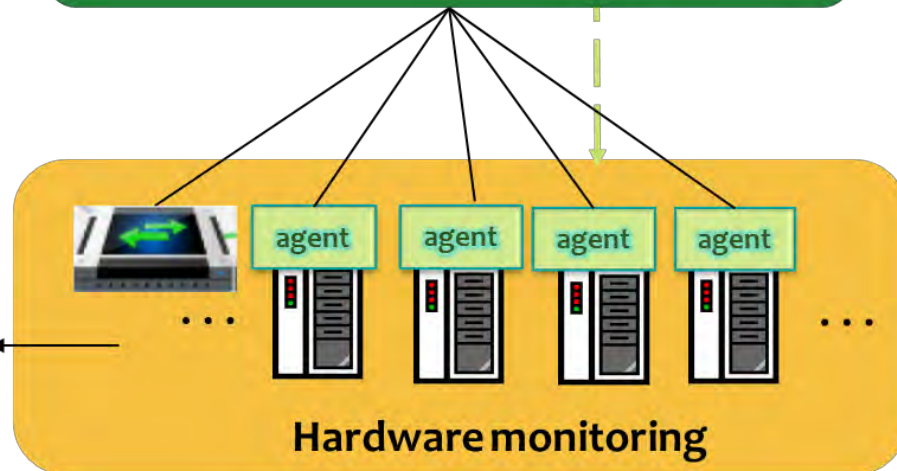
Device	IP Address	Device Class	Production State	Events
OpenStack		OpenStack/Infra	Production	1
40-controller-01	10.214.168.152	Server/SSH/Linux	Production	12
42-controller-02	10.214.168.153	Server/SSH/Linux	Production	4
44-controller-03	10.214.168.154	Server/SSH/Linux	Production	4
48-compute-01	10.214.168.156	Server/SSH/Linux	Production	8
50-compute-02	10.214.168.157	Server/SSH/Linux	Production	12
DISCO	10.203.126.7	OpenStack/DISCO	Production	

OpenStack monitoring



PDCM

Hardware monitoring



議程簡介



林建男
中華電信 工程師



Session Part 1(10分鐘)
專案計畫簡介



黃俊傑
工業技術研究院 資深工程師



Session Part 2(15分鐘)
軟體定義資料中心(SDDC)



簡士哲
中華電信 副理



Session Part 3(15分鐘)
雲端整合管理平台介紹

企業私雲與管理解決方案 ECoreCloud

簡士哲
中華電信 副理
2016/7/12

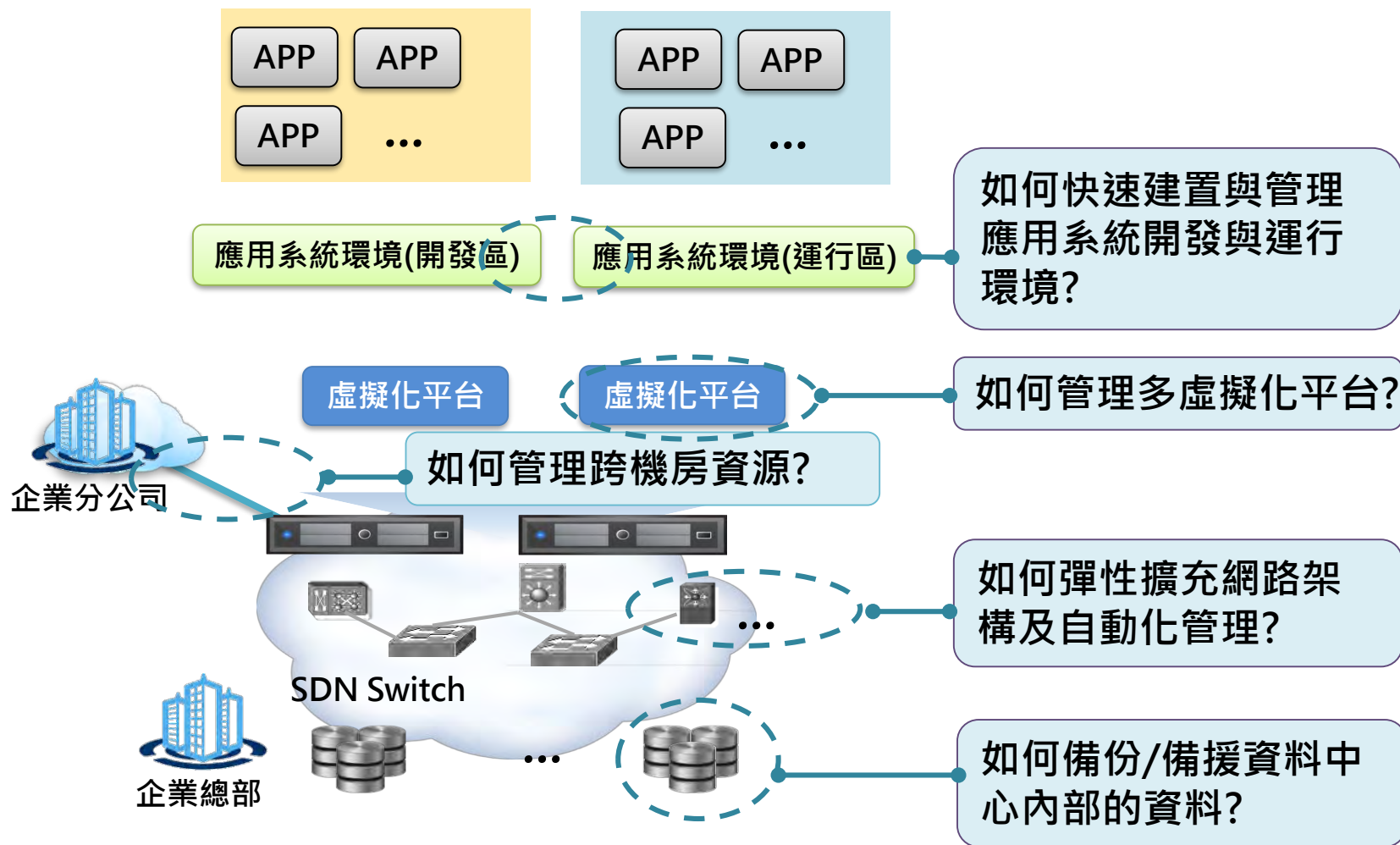


Outline

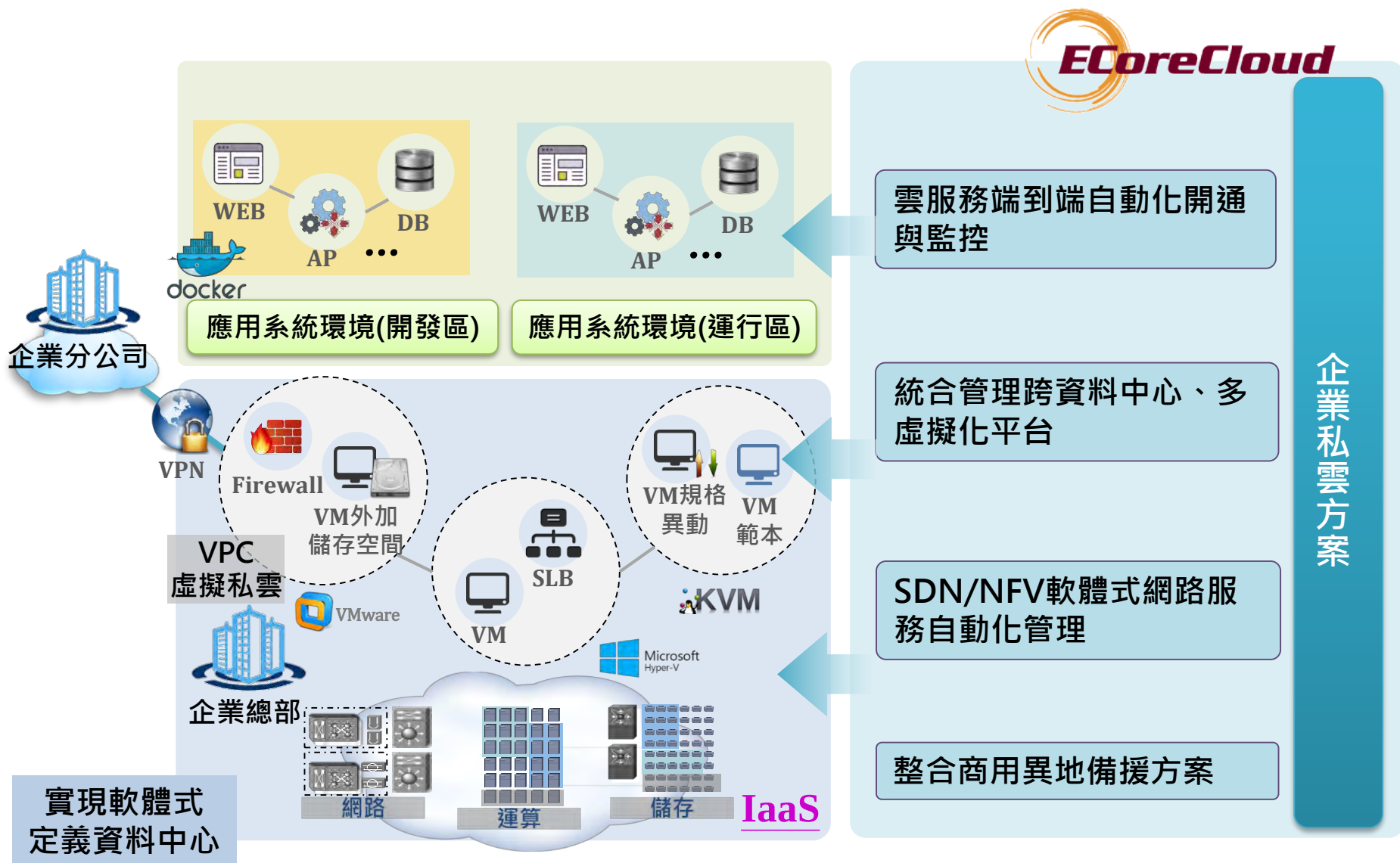
- ❖ 企業私雲管理方案ECoreCloud
- ❖ OpenStack支援Multi-Hypervisor
 - VMware vCenter



企業成功上私雲的關鍵議題



企業私雲方案 - ECoreCloud



IaaS: Infrastructure as a Service
VPC: Virtual Private Cloud

功能特色總覽



企業資訊部門

Web Portal

API

虛實資源管理

多虛擬化平台

私雲服務開通

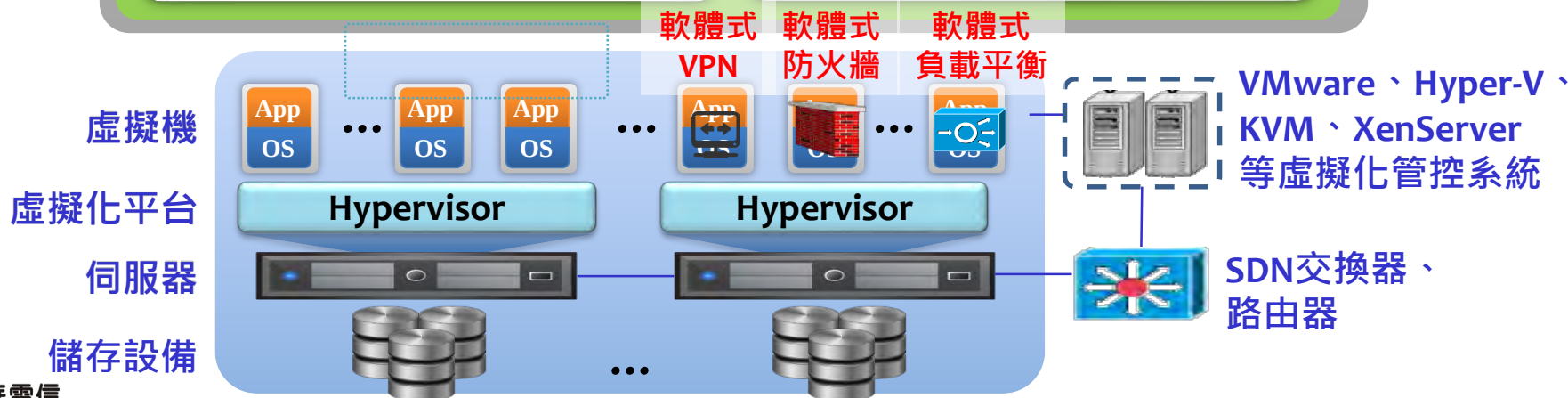
資安防護機制

SDN軟體式網路

異地備份備援

NFV網路功能虛擬化

資源監控告警



完善的虛實資源統整管理



- 統整管理多機房、多虛擬化平台 (如KVM、VMware、Hyper-V、XenServer)，彈性管理運算/儲存/網路等虛實資源



多元的私雲服務自動開通

Web Portal	API
虛算資源管理	多虛擬化平台
私雲服務開通	資安防護機制
SDN軟體式網路	異地備份備援
NFV網路功能虛擬化	資源監控告警



- 支援多類私雲服務，提供通用網路服務及範本，依需自主快速建置專屬虛擬私雲及應用系統開發環境



虛擬私雲



服務型錄

應用系統



範本



映像檔



自動擴展

運算服務



虛擬機



範本



複製



規格擴充



備份



監控



磁碟外掛



自動擴展

網路服務



防火牆



負載平衡



VPN



範本



流量監控



中華電信
Chungwa Telecom

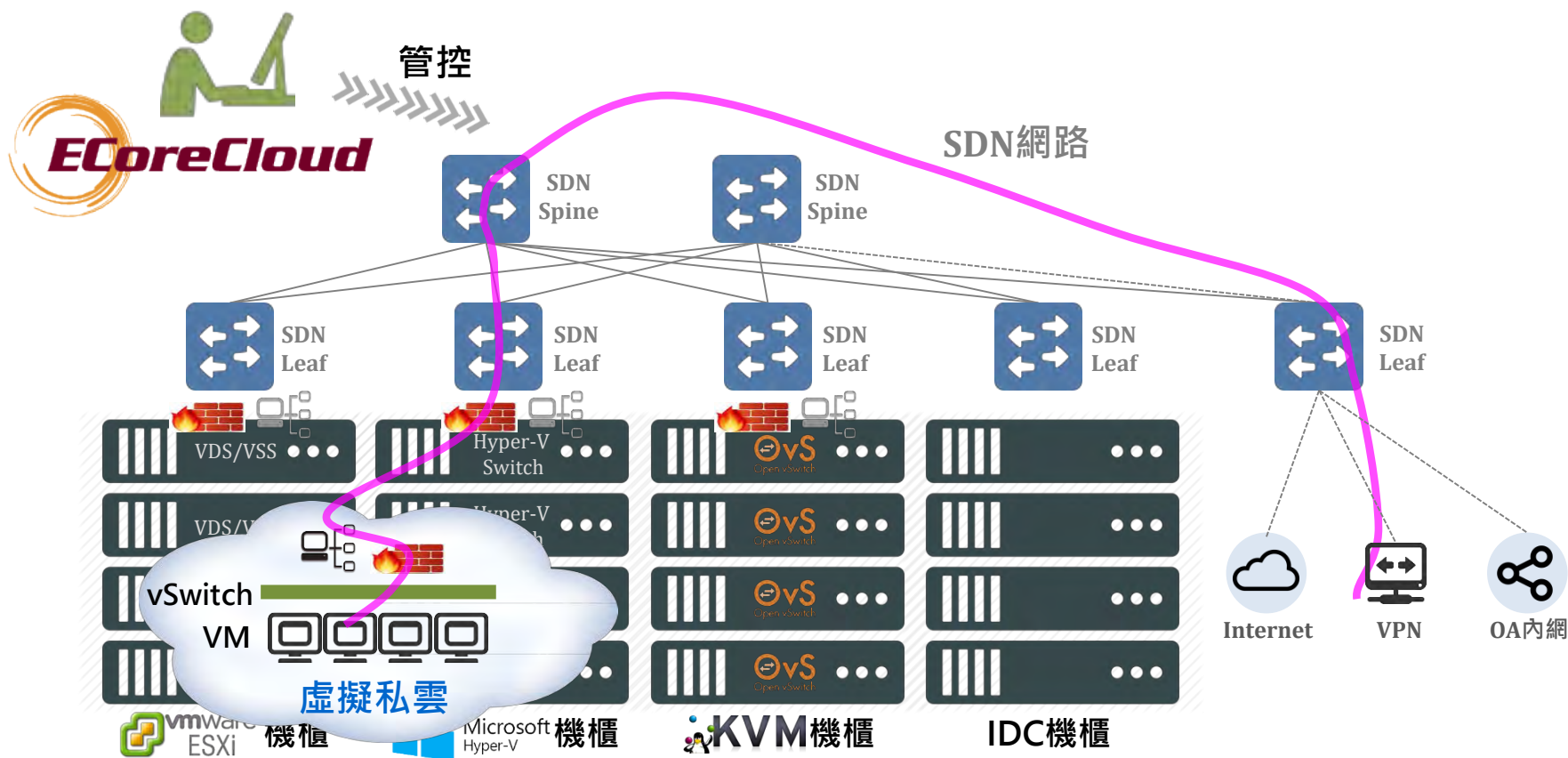
為了你 一直走在最前面 Always Ahead

彈性的虛擬私雲網路架構

Web Portal	API
虛實資源管理	多虛實化平台
私雲服務開通	資安防護機制
SDN軟體式網路	異地備份機制
NFV網路功能虛實化	資源監控告警



- 以SDN技術設計標準化網路架構，具備彈性擴充的特性，能動態開通網路服務
- 具備跨虛實化平台網路連通機制，提升虛實資源應用的彈性及效率



無縫的軟體網路功能整合

Web Portal	API
虛實資源管理	多虛擬化平台
私雲服務開通	資安防護機制
SDN軟體式網路	異地備份備援
NFV網路功能虛擬化	資源監控告警



- 支援軟體式網路功能，透過動態網路服務串接(Network Service Chain)技術，彈性組裝及快速建置企業網路環境
- 整合網路加速技術如SR-IOV、Intel DPDK，有效提升軟體式網路功能的處理效能

功能選單

快速建置範本



DMZ網路



Internet連線



Intranet連線

Drag & Drop

軟體式網路服務模組



Firewall



SLB



VPN



網路服務



Internet



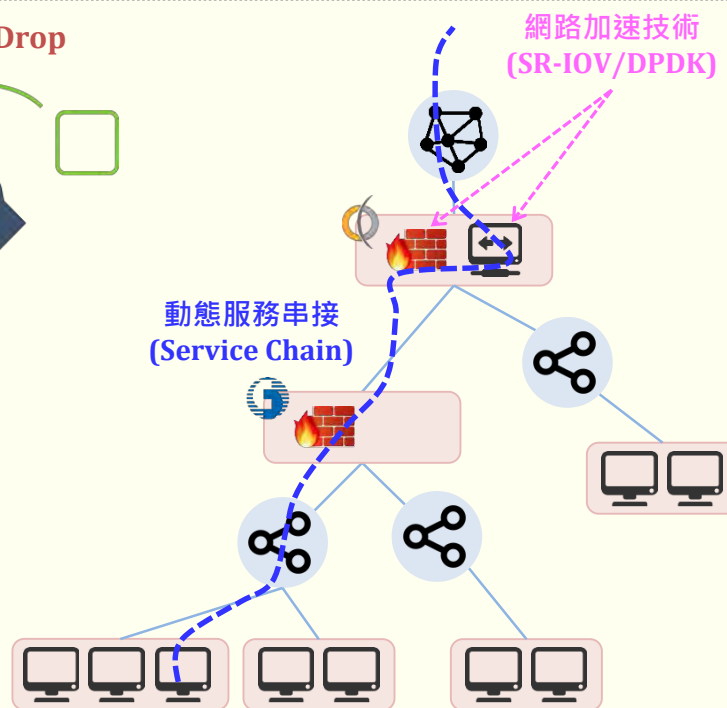
Subnet



DMZ



VM



網路拓樸



ECoreCloud

SR-IOV : Single Root I/O Virtualization

DPDK : Data Plane Development Kit (Intel® DPDK)

為了你 一直走在最前面 Always Ahead

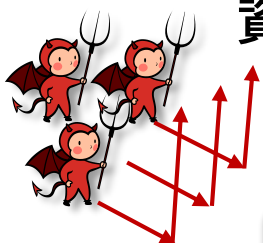
可靠的網路資安防護方案

Web Portal	API
虛實資源管理	多虛擬化平台
私雲服務鏈通	資安防護機制
SDN軟體式網路	異地備份備援
NEF網路功能虛擬化	資源監控告警



- 虛擬私雲網路彼此隔離，搭配軟體式防火牆增強資安保護
- 整合OpenFlow通訊技術，管控虛擬/實體交換器，強化虛擬化平台資安防護

資安威脅

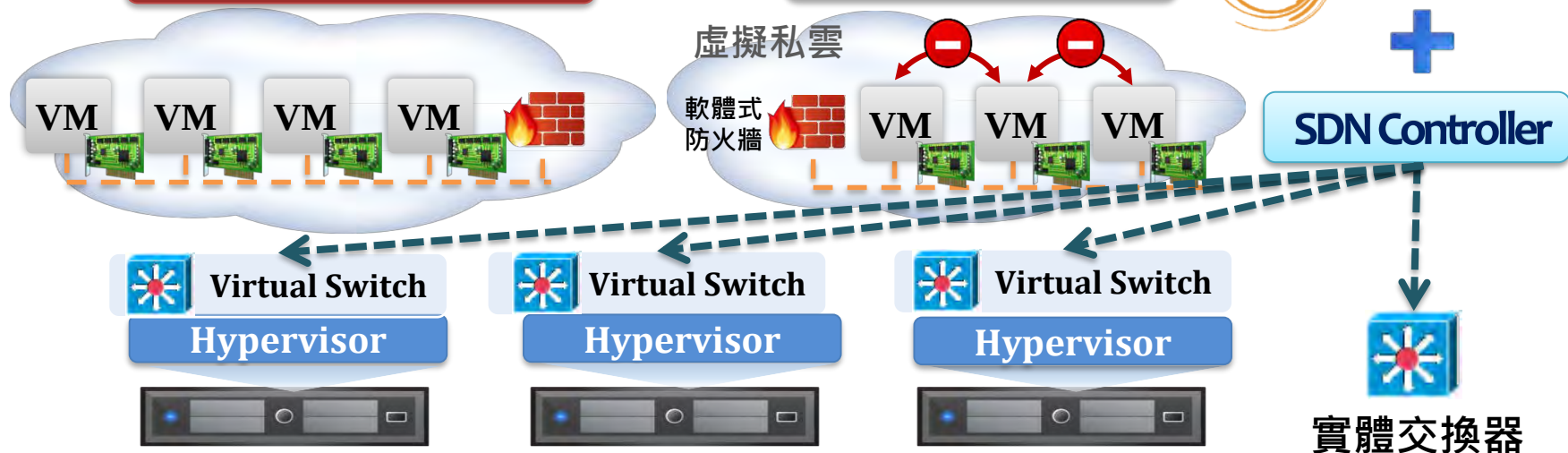


虛擬機存取管控

虛擬機IP/MAC防竄改

虛擬機動態隔離

ECoreCloud

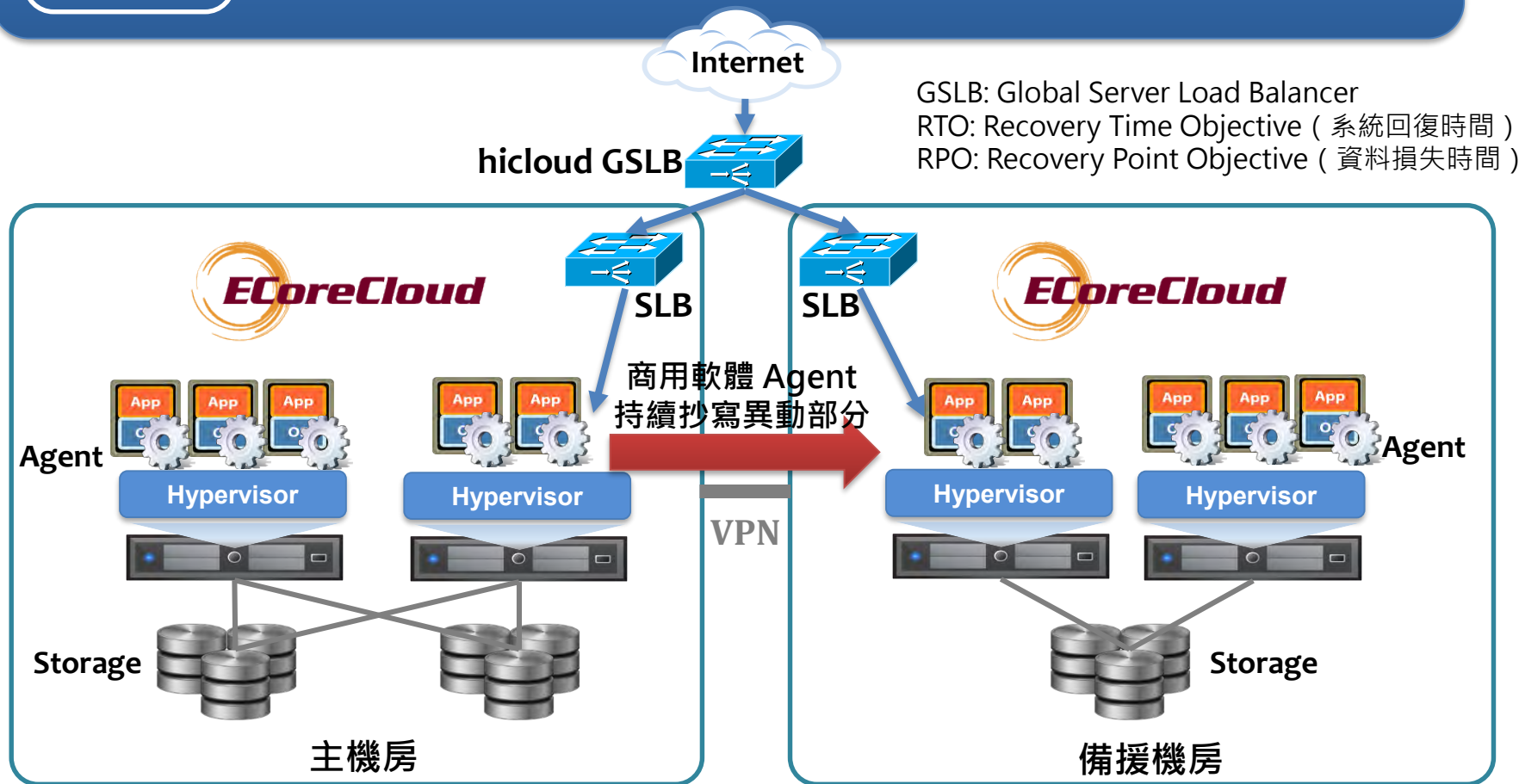


穩定的異地備份備援機制

Web Portal	API
虛實資源管理	多虛擬化平台
私密服務開通	資安防護機制
SDN軟體式網路	異地備份備援
NFV網路功能虛擬化	資源監控告警



- 整合商用備援方案，提供檔案/應用軟體層級備份備援，滿足關鍵應用系統高等級備援需求，將企業營運中斷風險降至最低

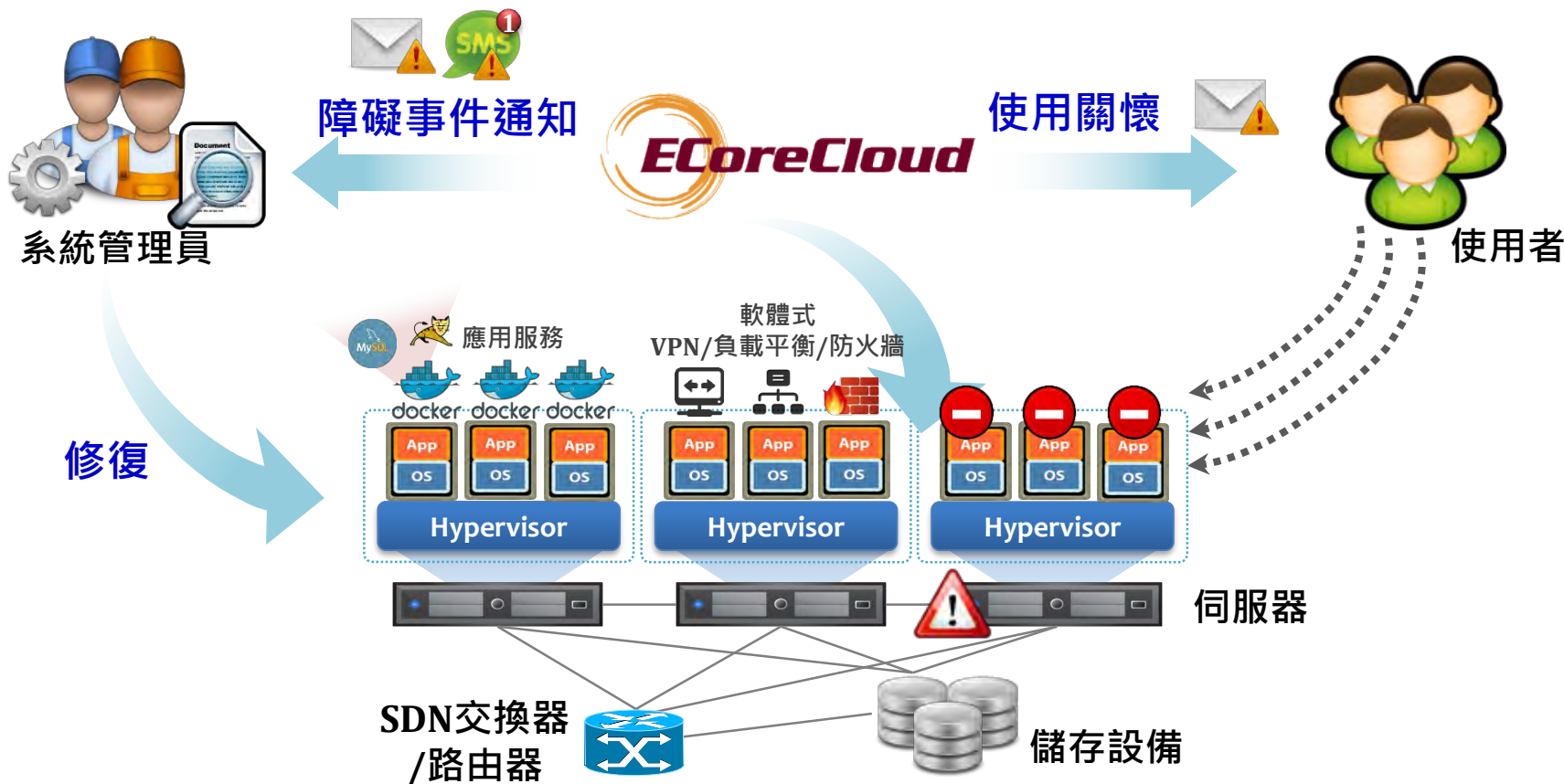


主動的虛實資源整合監控

Web Portal	API
虛實資源管理	多虛擬化平台
私雲服務開通	資安防護機制
SDN軟體式網路	異地備份備援
NEV網路功能虛擬化	資源監控告警



- 完整事件關聯分析，掌握資源異常潛在影響服務範圍
- 完善資安稽核機制，存錄各式資源/服務等異動事件，有效預防不當的操作行為



完善的障礙處理回覆流程

Web Portal	API
虛實資源管理	多虛擬化平台
私雲服務開通	資安防護機制
SDN軟體式網路	異地備份備援
NEV網路功能虛擬化	資源監控告警



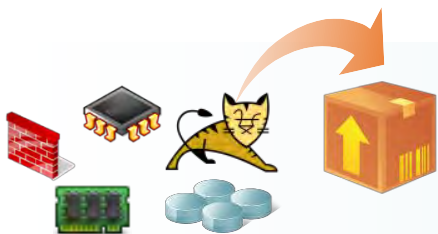
- 線上問題受理，結合企業人事組織進行障礙處理作業
- 事件告警規則設定、稽催、升級通報功能，有效分工指派異常事件配對處理人員

線上反應



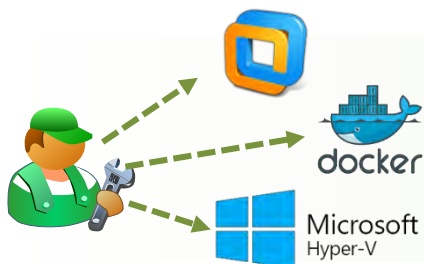
應用效益(1/2)

導入前



雲端資源取得與環境建置效率不彰

傳統雲服務管理系統取得運算/儲存/網路等基礎服務，以及建構應用系統環境，需花費較多時間

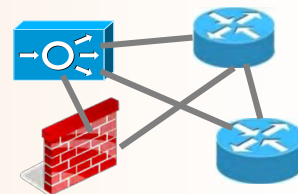


多機房、多虛擬化平台管理不易

多機房、多設備管理議題複雜，若採用多類型的虛擬化平台，在資源統合管理上更加困難

機房網路架構複雜，人工設定費時

隨著機房資源擴充，網路架構逐漸複雜且不具彈性，人工設定耗時費力且易出錯

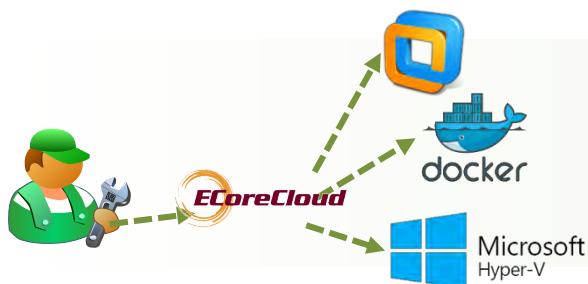


應用效益(2/2)

導入後



快速建構虛擬私雲及應用服務研發/運作環境
視覺化建構雲端環境，**10分鐘**快速建置虛擬私雲

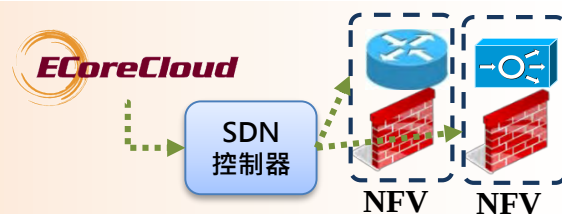


多機房、多虛擬化平台統整管理

統整管理跨機房資源池及多類型虛擬化平台，除了**減輕維運負擔**，更能**提高資源利用率**

結合SDN/NFV技術，網路架構更具彈性

結合SDN與NFV技術，彈性管理、動態設定軟體網路，使雲端機房網路架構更具彈性及高可用性，同時也**降低建置成本**



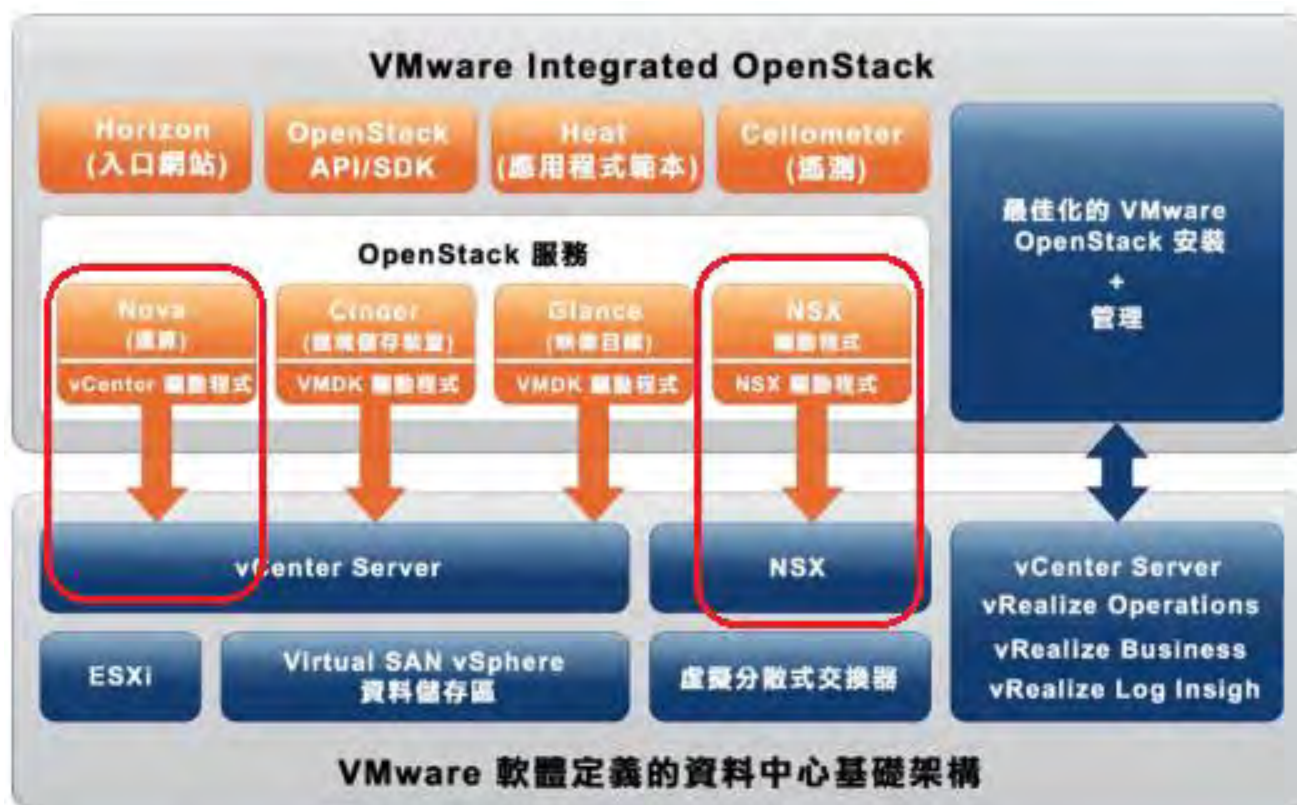
ECoreCloud Support Multi-Hypervisor

- ❖ How does OpenStack Support VMware vCenter?
- ❖ How does OpenStack integrate VMware Network?
- ❖ Where is the VM?

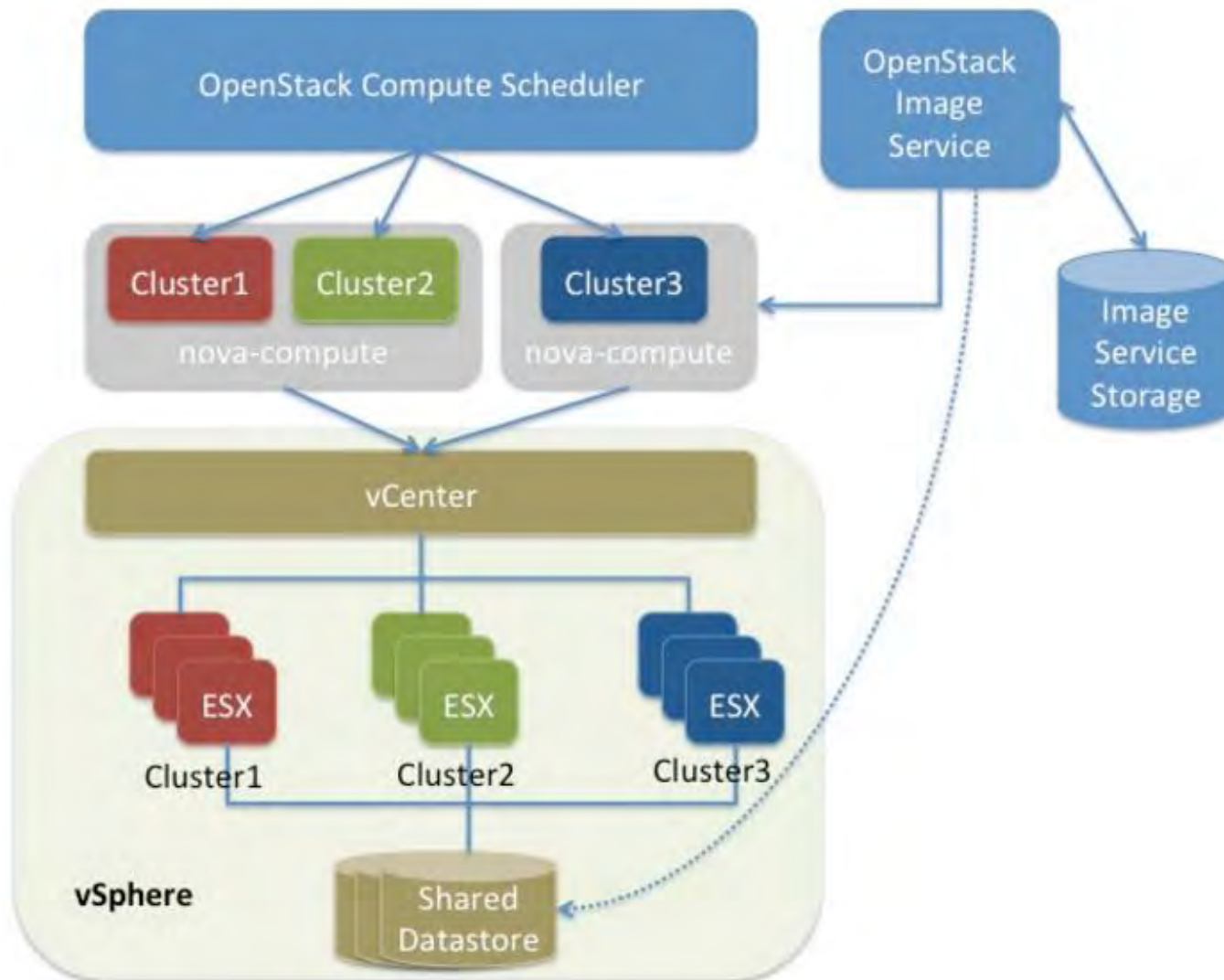


VMware Integrated OpenStack

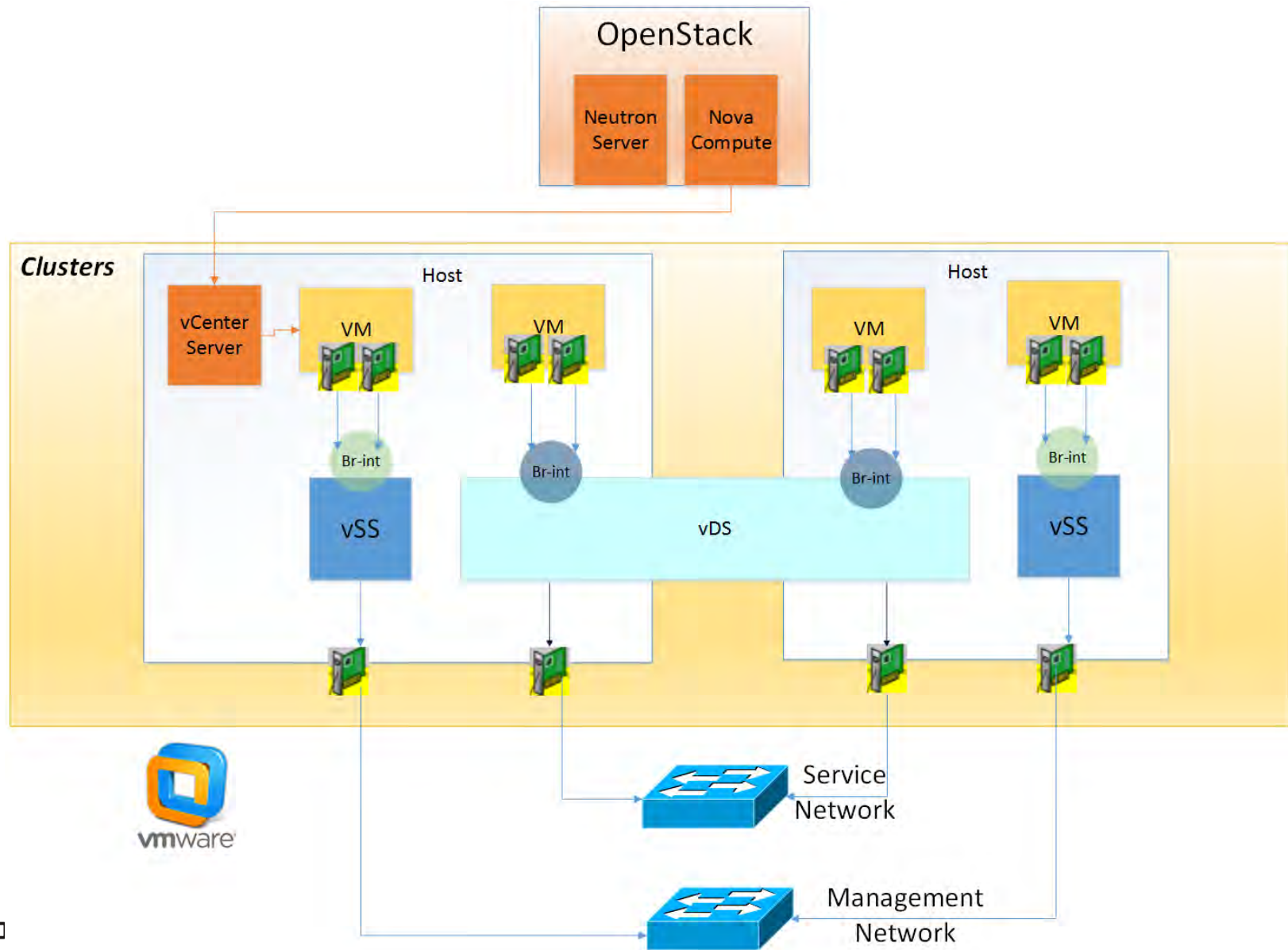
- ❖ VMware Integrated OpenStack(VIO) 2.0
 - Network component uses VMware NSX Plugin



VMware vCenter and Nova Compute



OpenStack VPC Network integrated with VMware



OpenStack VPC Network integrated with VMware Driver

❖ NSX Solution

- Need **NSX License**

❖ vCenter Solution

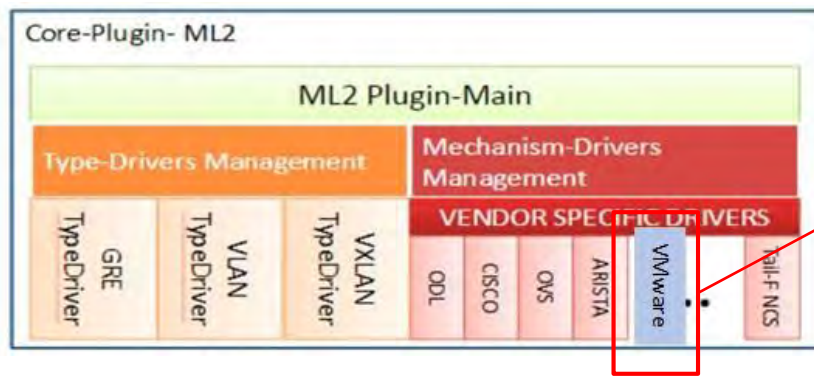
- **Nova Compute** : **contained the VMware driver**, but integrated with OpenStack still has the following problems currently:
 - **VM could only bind on the unique bridge(br-int), therefore, VM could not be isolated by different networks**
- **Neutron network** : **Need to create bridge in VMware manually**
 - Could not use Neutron API to create various networks in VMware, E.g. vSS/vDS, Flat/VLAN, and Port Groups



ECoreCloud VPC Network(with VMware)

❖ ECoreCloud Solution

- **Enhance VMware Driver in Nova**
 - Use Neutron to find the ESXi host which VM located
 - VM could be isolated by different Networks(Different VM Port Groups)
- **Implement VMware ML2 Mechanism Driver in Neutron**
 - Support vDS and vSS
 - Use Neutron APIs to create various networks in VMware



Implement VMware Mechanism Driver to add the functionalities of Create/Delete/Update Network/Subnet/Port in VMware.



*Value Creator for
Investors, Customers, Employees, and Society*

敬請指教

