

Virtual Networks for Multi Cloud (개요)

2020. 6.
(2020년 12월까지 사용 권장)

On/Offline Pilot 강의용 교재입니다.

안 종 석
james@jslab.kr
JS Lab

1

I. 개요
II. 멀티클라우드 아키텍처
III. 멀티클라우드 기술
IV. 멀티클라우드 네트워킹
V. 보안/관리

❖ 부록: 가상 네트워크 기술
❖ 실습교재 (별도)

JS Lab

2

james@jslab.kr

I. 개요

II. 멀티클라우드 아키텍처

III. 멀티클라우드 기술

IV. 멀티클라우드 네트워킹

V. 보안/관리

❖ 부록: 가상 네트워크 기술

❖ 실습교재 (별도)

JS Lab

3

james@jslab.kr

I. 개요

❖ Multi-Cloud는 Hybrid-Cloud와 Traditional IT를 연결하는 환경

- Multi Cloud: Public 클라우드간 연결
- Hybrid Cloud: Public 클라우드와 Private 클라우드의 연결
- Hybrid IT: 온프레미스(On-premise)와 Public 클라우드의 연결

```

graph TD
    subgraph Multi_Cloud [Multi Cloud]
        P1((Public)) <--> P2((Public))
    end
    subgraph Hybrid_Cloud [Hybrid Cloud]
        P3((Private))
    end
    subgraph Hybrid_IT [Hybrid IT]
        TIT[Traditional IT]
    end
    P3 <--> TIT
    
    P1 <--> P3
    P2 <--> TIT
    
```

JS Lab

온프레미스: 기업이 자체 시설에서 보유하고 직접 유지 관리하는 프라이빗 데이터 센터

4

I. 개요

❖ 계층화 인프라 고려

- 인프라의 계층별 추상화 (서비스에 집중)
- 계층간 격리와 정책 기반 서비스 노출
- 성능 개선 (계층 Offload 필요)
- 계층간 연결 호환성

- 제품화를 위한 영역과 계층 고려
- (Managed) Service 제품화 vs. Product 제품화

James@jlab.kr

JS Lab

5

I. 개요

❖ Multi Cloud Managed Service Platform (MCMSP)

❖ 하이브리드/멀티 클라우드 관리 (Hybrid/Multi Cloud Management)

클라우드 관리 플랫폼

James@jlab.kr

JS Lab

6

I. 개요

❖ Multi-Cloud 환경 이동 이유

**벤더 락인 우려
최고 솔루션 선택**

"Most organizations adopt a multicloud strategy out of a desire to avoid vendor lock-in or to take advantage of best-of-breed solutions" - Gartner analyst

**데이터 유실과
다운타임 최소화**

Minimize the threat of extensive data loss or downtime due to component failure in cloud.

JS Lab

7

I. 개요

❖ 동일 서비스 고려하는 Multi-Cloud Architecture

The diagram illustrates a Multi-Cloud Architecture with two main sections: AWS and Azure. Each section contains several service icons: Amazon API Gateway, Instances, Auto Scaling, AWS Lambda, Elastic Load Balancing, and DB in the AWS section; VMs, Autoscale, Azure Functions, Azure Load Balancer, and DB in the Azure section. Bidirectional arrows connect corresponding services between the two clouds, indicating interoperability and data flow. For example, AWS Instances connect to Azure VMs, AWS Auto Scaling connects to Azure Autoscale, AWS Lambda connects to Azure Functions, AWS Elastic Load Balancing connects to Azure Load Balancer, and both AWS and Azure have their own DB instances.

JS Lab

8

I. 개요

❖ 클라우드 서비스 가격과 멀티 클라우드 구성

Instance type	AWS Instances	AWS RAM (GiB)	Azure VMs	Azure RAM (GiB)	Google VMs	Google RAM (GiB)
General purpose	m5.xlarge	16	B4MS	16	n1-standard-4	15
Compute optimized	c5.xlarge	8	F4s v2	8	n1-highcpu-4	3.6
Memory optimized	r5.xlarge	32	E4 v3	32	n1-highmem-4	26
GPU instances	g3s.4xlarge	30.5	NC 6	56	NVIDIA@Tesla@P4	64

Instance type	AWS	Azure	Google	AWS Pricing (per hour)	Azure Pricing (per hour)	Google Pricing (per hour)
General purpose	m5.xlarge	B4MS	n1-standard-4	\$0.192	\$0.166	\$0.214
Compute optimized	c5.xlarge	F4s v2	n1-highcpu-4	\$0.170	\$0.169-\$0.17	\$0.1626
Memory optimized	r5.xlarge	E4 v3	n1-highmem-4	\$0.252	\$0.252	\$0.2696
GPU instances	g3s.4xlarge	NC 6	NVIDIA@Tesla@P4	\$0.75	\$0.899	\$2.4

JS Lab

<https://www.simform.com/compute-pricing-comparison-aws-azure-googlecloud/>

9

I. 개요

❖ 클라우드 서비스 가격의 유동성과 이를 고려한 아키텍처

❖ 빌링(Billing) 예

- Customer
- Managed Service
- Public Cloud

Discounted Pricing for 1-year Commitment with on upfront cost

Instance type	AWS	Azure	Google	AWS Pricing (per hour)	Azure Pricing (per hour)	Google Pricing (per hour)
General purpose	m5.xlarge	B4MS	n1-standard-4	\$0.123	\$0.097	\$0.128
Compute optimized	c5.xlarge	F4s v2	n1-highcpu-4	\$0.107	\$0.099	\$0.095
Memory optimized	r5.xlarge	E4 v3	n1-highmem-4	\$0.159	\$0.156	\$0.159
GPU instances	g3s.4xlarge	NC 6	NVIDIA@Tesla@P4	\$0.551	\$0.572	\$0.864

JS Lab

<https://www.simform.com/compute-pricing-comparison-aws-azure-googlecloud/>

10

I. 개요

- ❖ 현재 엔터프라이즈 인터넷 접속 환경과 Multi-Cloud
- ❖ 기존 WAN 네트워크 이슈
 - 엔터프라이즈 서비스의 클라우드 이동
 - 서비스를 위한 종단간 연결 경로

JS Lab

Versa Networks, SDxCentral.

11

I. 개요

- ❖ SD-WAN의 발전
- ❖ Multi-Cloud 를 위한 엔터프라이즈 인터넷 접속 (or Cloud Security as-a-Service)

JS Lab

Versa Networks, SDxCentral.

12

james@jslab.kr


I. 개요

- ❖ 멀티 클라우드 애플리케이션 제공
 - 혼합된 워크로드 구성
 - 고성능 컴퓨팅
 - 멀티 데이터 워크로드 오케스트레이션


클라우드 네이티브 애플리케이션

Tools Chain
 CI/CD, Provisioning, Automation, Registry, Telemetry, Policy, IAM, Security


서비스 메시 (Service Mesh)



kubernetes



kubernetes



kubernetes

JS Lab

13

james@jslab.kr

I. 개요

- II. 멀티클라우드 아키텍처
- III. 멀티클라우드 기술
- IV. 멀티클라우드 네트워킹
- V. 보안/관리

- ❖ 부록: 가상 네트워크 기술
- ❖ 실습교재 (별도)

JS Lab

14

II. 멀티클라우드 아키텍처

❖ Basic Cloud Architecture

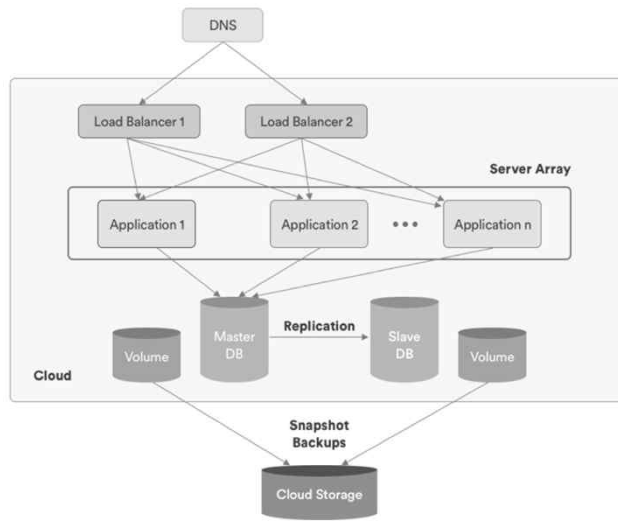


Image: Rightscale

15

II. 멀티클라우드 아키텍처

❖ Basic Cloud Architecture (2 Datacenters)

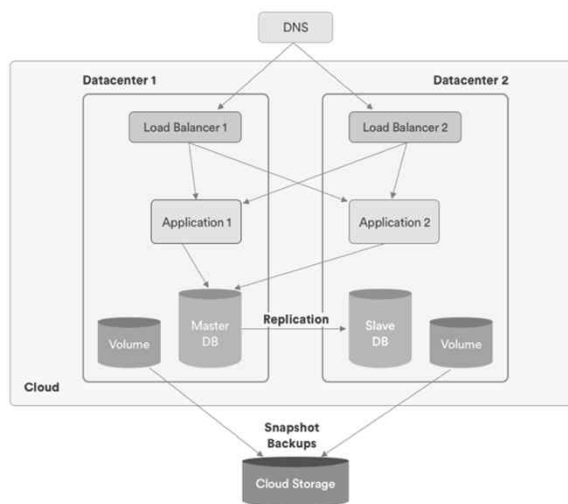
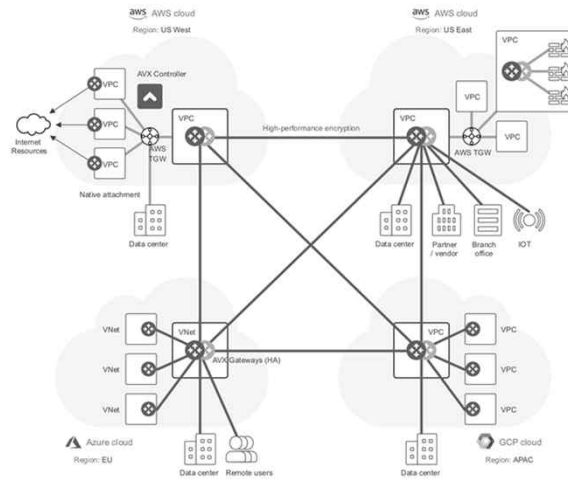


Image: Rightscale

16

II. 멀티클라우드 아키텍처

❖ Building the Enterprise Multi-Cloud Backbone (Aviatrix)



<https://www.simform.com/compute-pricing-comparison-aws-azure-googlecloud/>

JS Lab

17

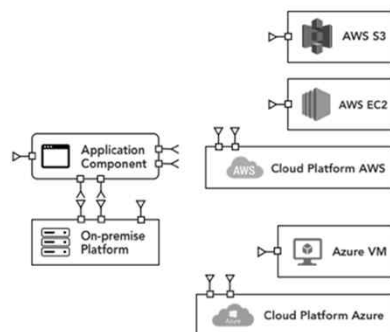
II. 멀티클라우드 아키텍처

❖ Multi-Cloud Architecture

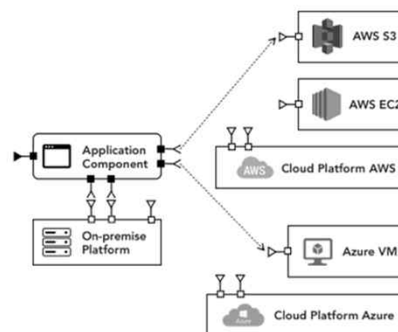
■ Cloudification

Cloudification

Before Migration



After Migration



Jignesh Solanki, leads Simform's Product Engineering team

JS Lab

18

II. 멀티클라우드 아키텍처

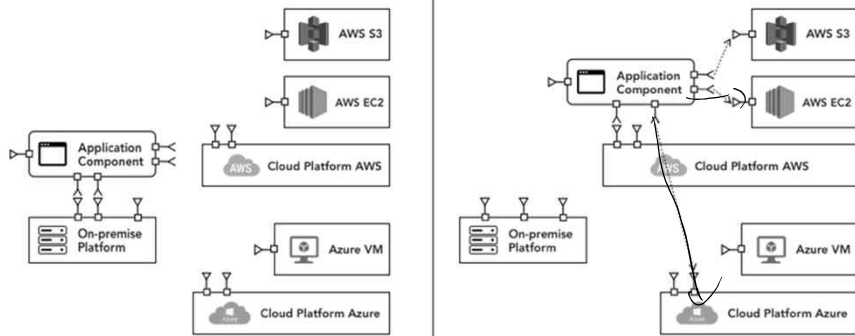
❖ Multi-Cloud Architecture

■ Multi-Cloud Relocation

Multi-Cloud Relocation

Before Migration

After Migration



Jignesh Solanki, leads Simform's Product Engineering team

JS Lab

19

II. 멀티클라우드 아키텍처

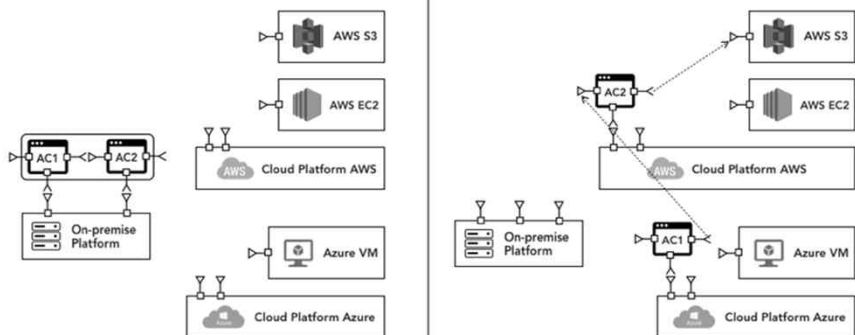
❖ Multi-Cloud Architecture

■ Multi-Cloud Refactor

Multi-Cloud Refactor

Before Migration

After Migration



Jignesh Solanki, leads Simform's Product Engineering team

JS Lab

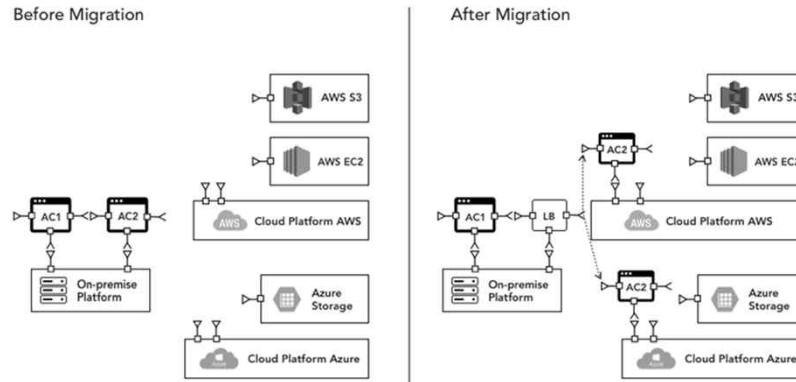
20

II. 멀티클라우드 아키텍처

❖ Multi-Cloud Architecture

■ Multi-Cloud Rebinding

Multi-Cloud Rebinding



Jignesh Solanki, leads Simform's Product Engineering team

JS Lab

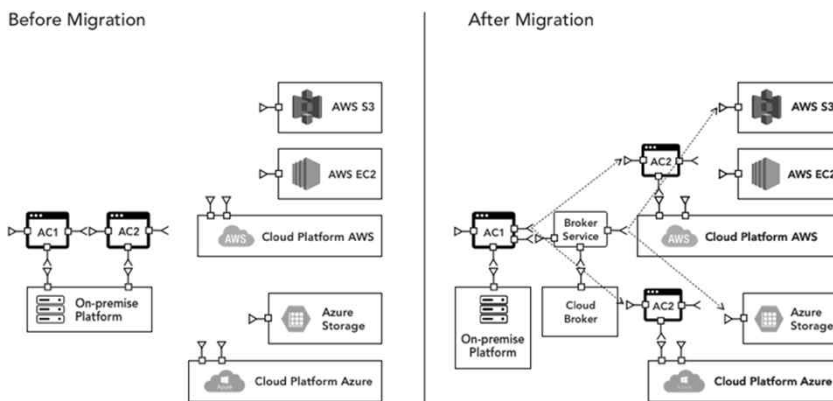
21

II. 멀티클라우드 아키텍처

❖ Multi-Cloud Architecture

■ Multi-Cloud Rebinding with Cloud Brokerage

Multi-Cloud Rebinding with Cloud Brokerage



Jignesh Solanki, leads Simform's Product Engineering team

JS Lab

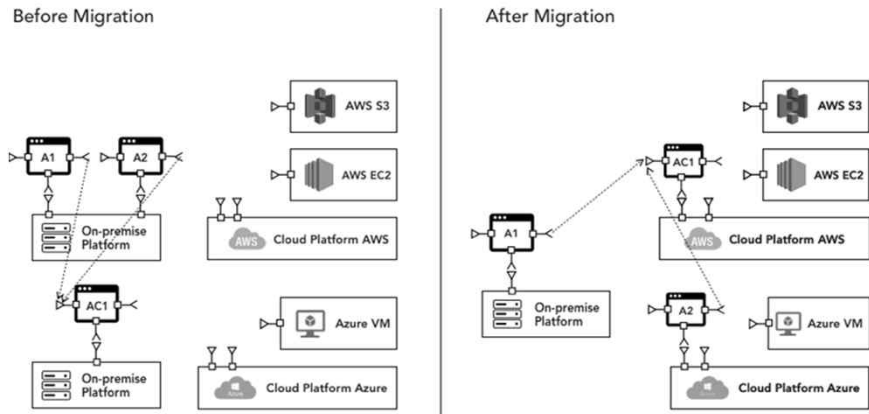
22

II. 멀티클라우드 아키텍처

❖ Multi-Cloud Architecture

■ Multi-Application Modernization

Multi-application Modernization



Jignesh Solanki, leads Simform's Product Engineering team

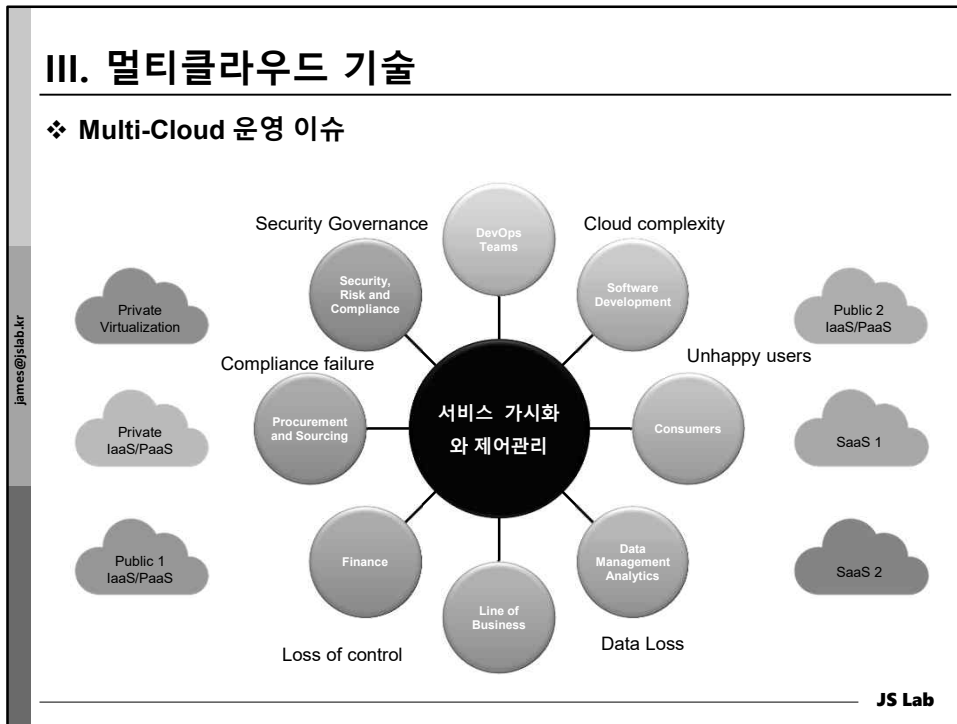
JS Lab

23

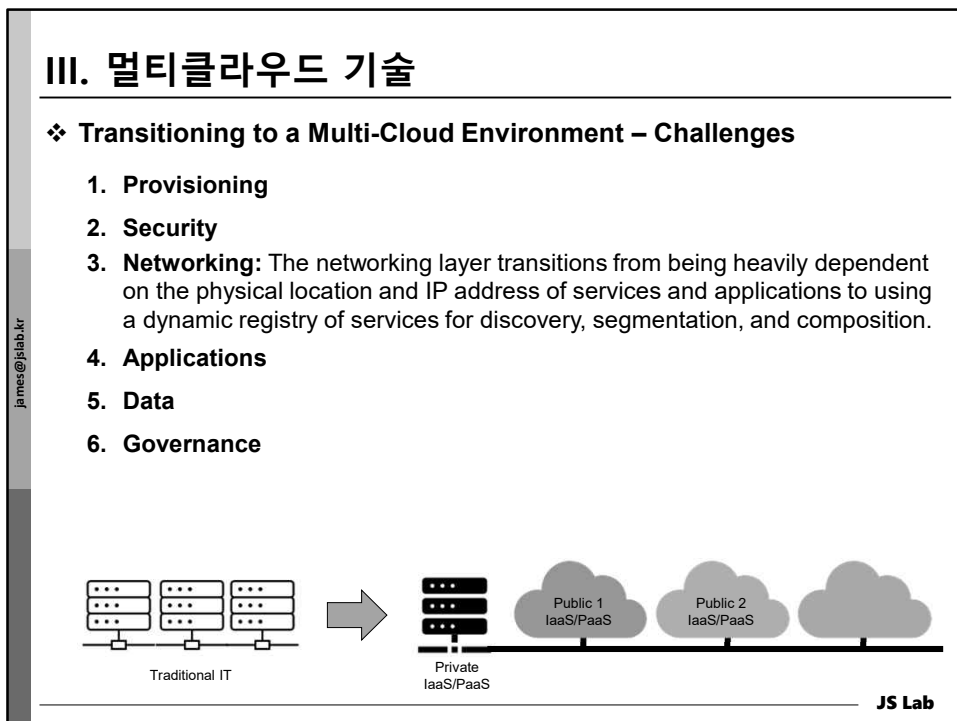
- I. 개요
 - II. 멀티클라우드 아키텍처
 - III. 멀티클라우드 기술
 - IV. 멀티클라우드 네트워킹
 - V. 보안/관리
- ❖ 부록: 가상 네트워크 기술
 - ❖ 실습교재 (별도)

JS Lab

24



25



26

III. 멀티클라우드 기술

❖ Simplifying Complexity

- While a multi-cloud strategy will help to avoid vendor lock-in, increase reliability and protect mission-critical data, it has inherent complexity. Before leaping into multi-cloud, consider these few potential methods to simplify the complexity.
- Potential Methods:
 - ✓ SD-WAN or Software-defined networking
 - ✓ Cloud On Ramp Service Providers
 - ✓ Carrier-Neutral Colocation Services
 - ✓ AWS Direct Connect
 - ✓ Azure Express Route
 - ✓ Products and Services from Local Vendors

JS Lab

27

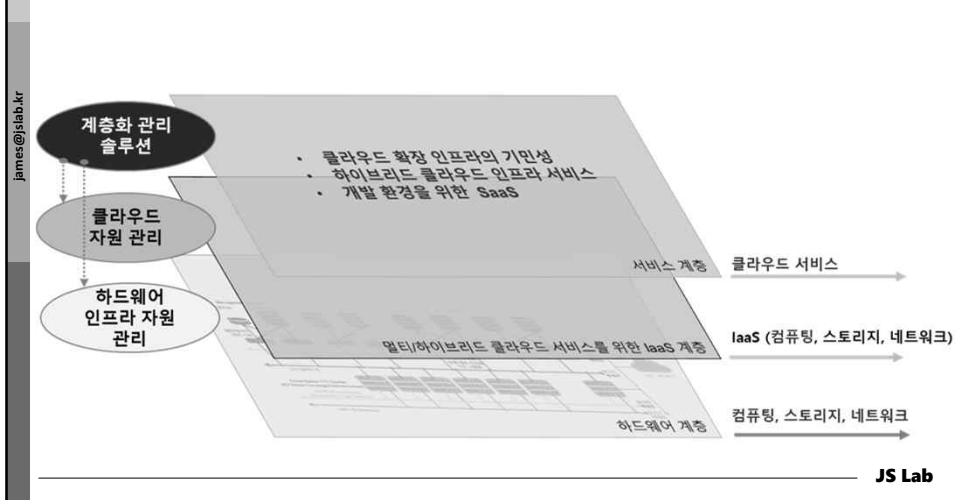
- I. 개요
 - II. 멀티클라우드 아키텍처
 - III. 멀티클라우드 기술
 - IV. 멀티클라우드 네트워킹
 - V. 보안/관리
- ❖ 부록: 가상 네트워크 기술
 - ❖ 실습교재 (별도)

JS Lab

28

IV. 멀티클라우드 네트워킹

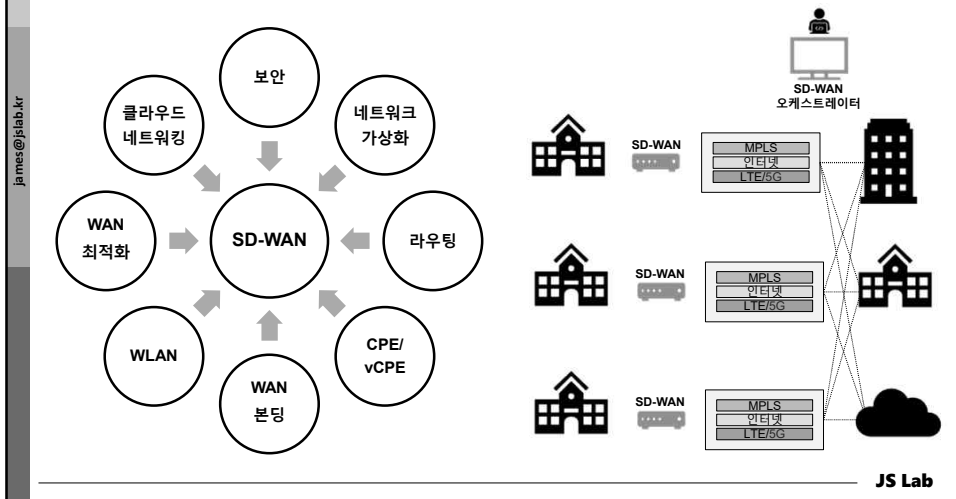
- ❖ 클라우드 네트워킹: 가상과 물리 네트워크와 독립적 추상화
- ❖ 가상 네트워크 환경 (Overlay SDN): VMware의 NSX 등
- ❖ 물리 네트워크 환경 (Underlay SDN): Cisco의 ACI 등



29

IV. 멀티클라우드 네트워킹

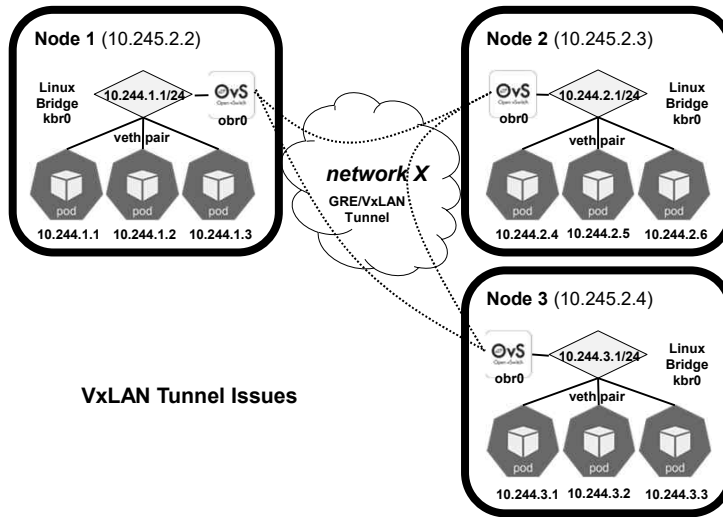
❖ SD-WAN is sometimes viewed as a catch-all marketing term for next-gen enterprise edge solutions (www.sdxcentral.com SDxCentral, 2019)



30

IV. 멀티클라우드 네트워킹

❖ Clustering for Multi-Cloud



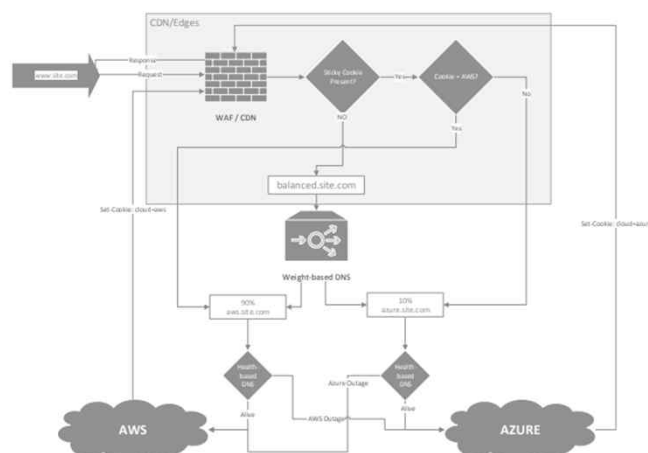
JS Lab

31

IV. 멀티클라우드 네트워킹

❖ Routing with cloud stickiness

- DNS – weight-based with health checks
- WAF/CDN + Rules Engine (on CDN Edges)
- Location stickiness



JS Lab

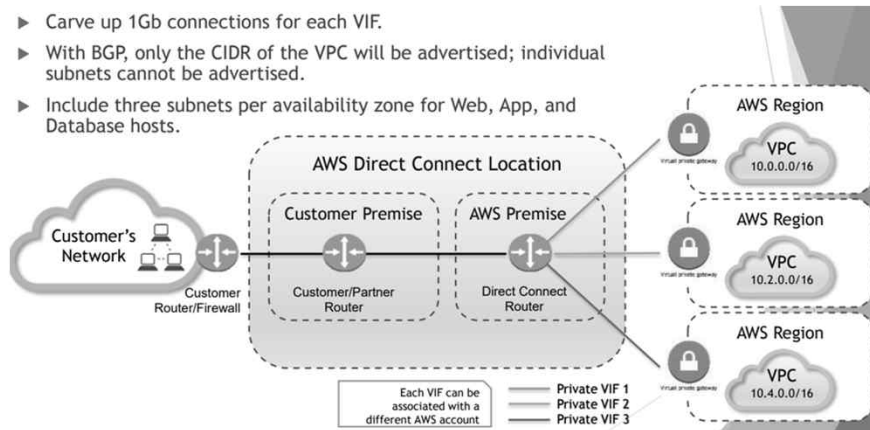
By Konstantin Tjuterev & Oleg Andreyev, Intechsystems SIA

32

IV. 멀티클라우드 네트워킹

- ❖ Direct Connect Architecture (AWS)
- ❖ Outpost for Hybrid Cloud

- ▶ Carve up 1Gb connections for each VIF.
- ▶ With BGP, only the CIDR of the VPC will be advertised; individual subnets cannot be advertised.
- ▶ Include three subnets per availability zone for Web, App, and Database hosts.



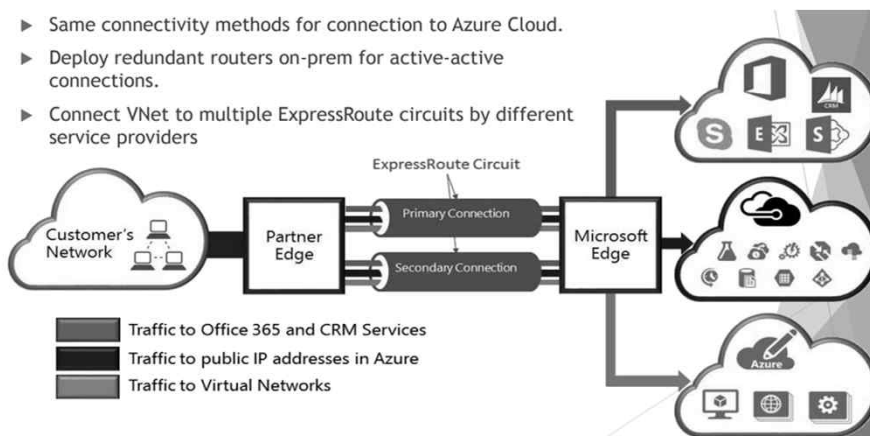
JS Lab

33

IV. 멀티클라우드 네트워킹

- ❖ ExpressRoute Architecture (Azure)
- ❖ Azure Stack (Edge) for Hybrid Cloud

- ▶ Same connectivity methods for connection to Azure Cloud.
- ▶ Deploy redundant routers on-prem for active-active connections.
- ▶ Connect VNet to multiple ExpressRoute circuits by different service providers

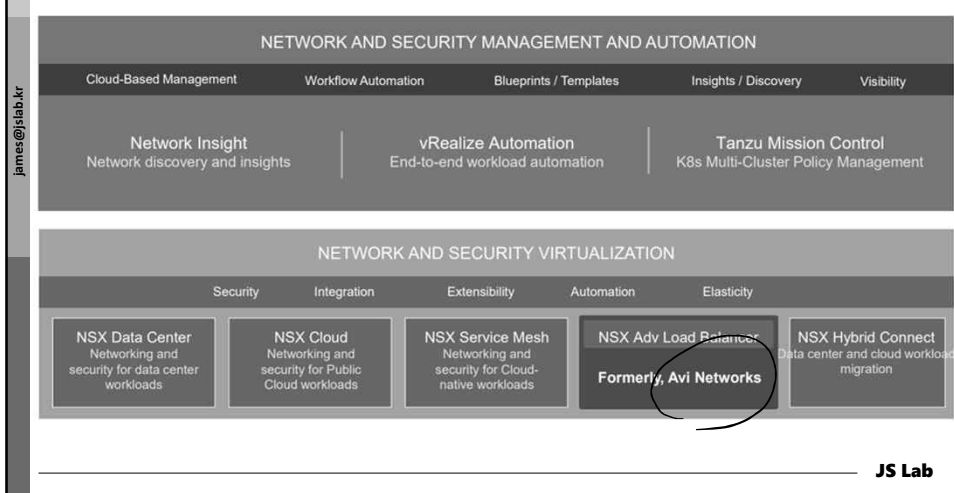


JS Lab

34

IV. 멀티클라우드 네트워킹

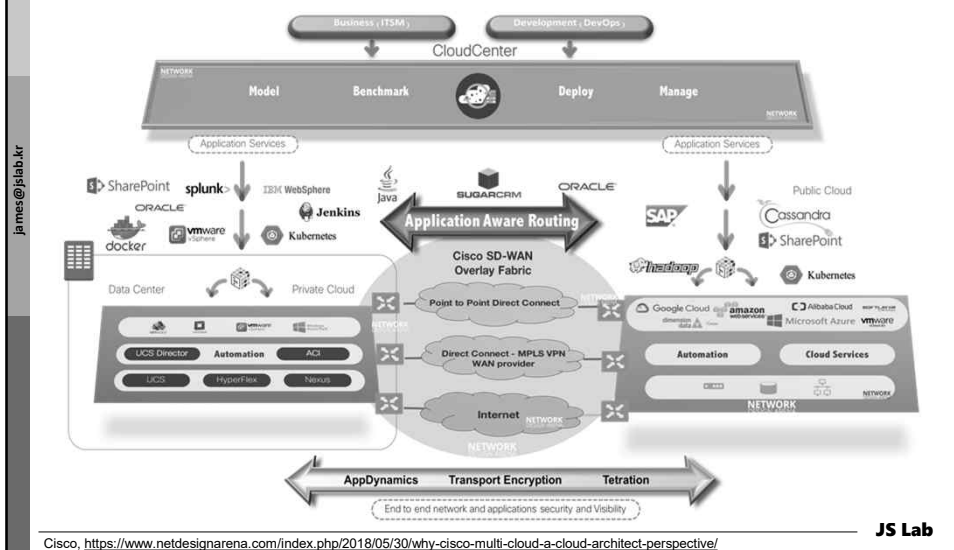
- ❖ VMware NSX
- ❖ VMware의 AVI 인수 (2019)



35

IV. 멀티클라우드 네트워킹

- ❖ Cisco Multi-Cloud – A Cloud Architect Perspective



Cisco, <https://www.netdesignarena.com/index.php/2018/05/30/why-cisco-multi-cloud-a-cloud-architect-perspective/>

36

IV. 멀티클라우드 네트워킹

❖ Cloud Networking Complexities

- Routing traffic rapidly and securely between disparate cloud platforms is complex; avoid complex Managed VPN solutions
- Automation needed for disparate CLI's, BGP ASN's, and routing tables
- Managing multiple cloud, SaaS, network, and colocation providers is a juggling act!
- Every provider will have their own proprietary method for management, monitoring, storage, and network solutions.
- Establishing standard security capabilities and policies
- Ability to enforce security for users, data, and applications everywhere is essential

10 Giga Internet Service for Enterprise in Korea

JS Lab

37



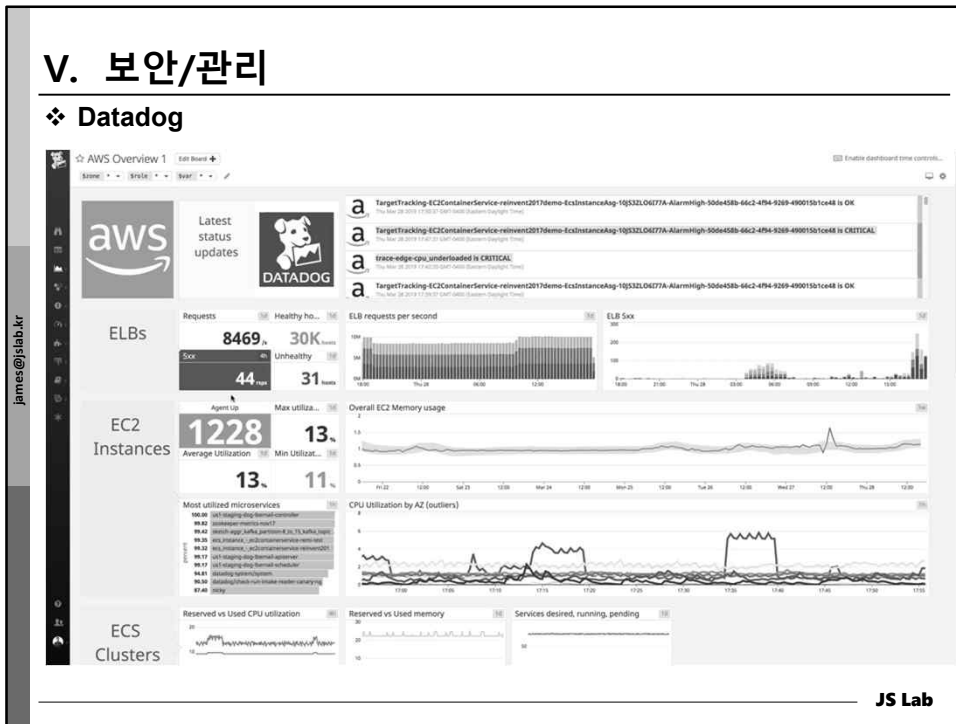
- I. 개요
 - II. 멀티클라우드 아키텍처
 - III. 멀티클라우드 기술
 - IV. 멀티클라우드 네트워킹
 - V. 보안/관리
- ❖ 부록: 가상 네트워크 기술
 - ❖ 실습교재 (별도)

JS Lab

38

V. 보안/관리

❖ Datadog



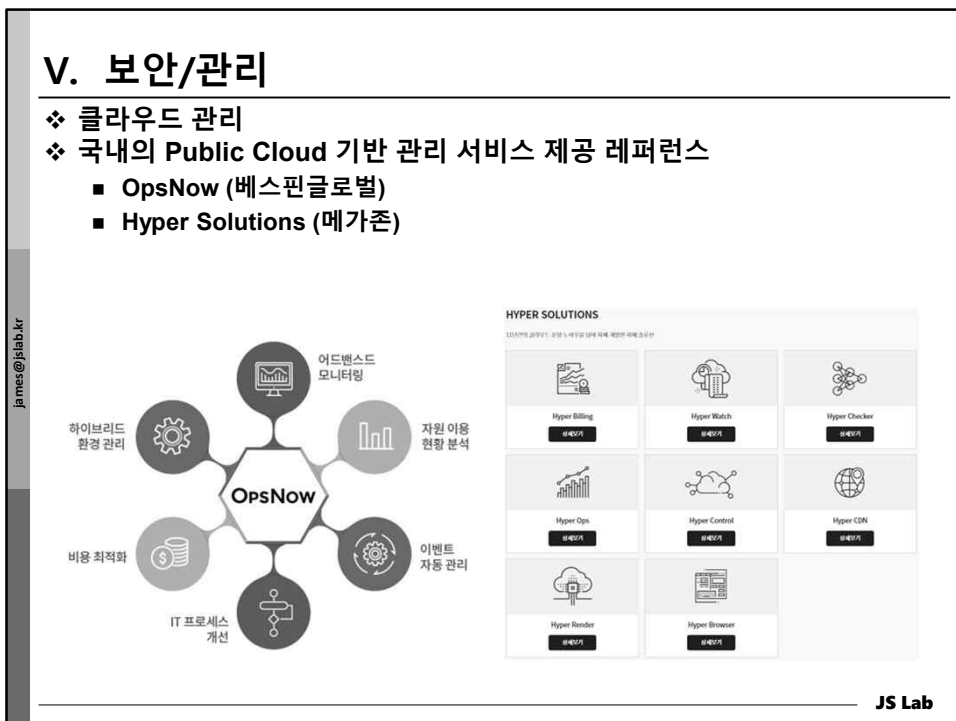
39

V. 보안/관리

❖ 클라우드 관리

❖ 국내의 Public Cloud 기반 관리 서비스 제공 레퍼런스

- OpsNow (베스핀글로벌)
- Hyper Solutions (메가존)



40

V. 보안/관리

❖ OpsNow

The screenshot displays the OpsNow interface with several key sections:

- CLOUD VENDOR:** Summary of cloud vendor usage with metrics like 1750ea, 300ea, and 2309ea.
- Service Groups:** Overview of different service environments (DEV, Staging, Production) with associated costs and counts.
- Performance & Alerts:** Graphs and lists showing system health, alerts, and performance trends.
- Resource Utilization:** Detailed views of CPU, memory, and storage usage across different services.

JS Lab

41

V. 보안/관리

❖ Multi-Cloud Security Tools (Gartner)

The diagram illustrates the Gartner Multi-Cloud Security Tools framework:

- Core Security Layers:** SaaS Security, IaaS Security, and PaaS Security.
- Central Pillars:** SaaS, IaaS, and PaaS.
- Supporting Pillars:** CASB (Cloud Access Security Broker), CWPP (Cloud Workload Protection Platform), and CSPM (Cloud Security Posture Management).
- Operational & Compliance Functions:** Data Loss Prevention, Compliance/Risk, Architecture, Adaptive Access Control, UEBA, Threat Protection, Cloud Risk Management, Operations and Monitoring, Governance, Exploit Protection, Application Whitelisting, System Integrity, Network Segmentation, System Monitoring, Workload Configuration, Compliance Assessment, Risk Identification, Operational Monitoring, DevSecOps Integration, Policy Enforcement, and Threat Protection.

CASB – Cloud Access Security Broker
CWPP – Cloud Workload Protection Platform
CSPM – Cloud Security Posture Management

Source: 2019 Gartner

JS Lab

42

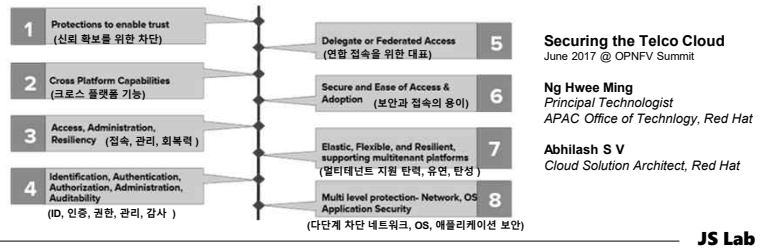
V. 보안/관리

❖ 보안 표준 적용 클라우드 구축 (해외 예)

1. ISO/IEC 27001:2013
2. ISO/IEC 27002:2013
3. ISO/IEC 27017:2015
4. SOC 1/SOC 2/SOC 3
5. NIST SP 800-53
6. PCI DSS



KEY SECURE CLOUD DESIGN PRINCIPLES

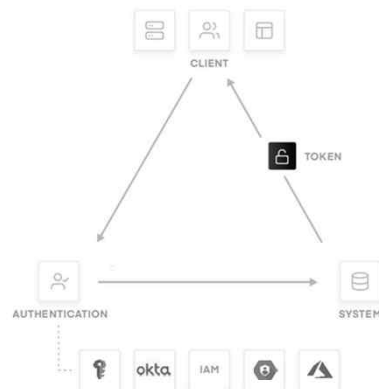


43

V. 보안/관리

❖ Multi-Cloud Security

- Secrets management
- Identity and Access Management [Identity as a Service (IDaaS)]
- Check Traditional IT Infrastructure for Enterprise



- Single Sign-On
- Universal Directory
- Multi Factor Authentication
- Life Cycle Management
- Mobility Management
- API Access Management
- Developer Platform

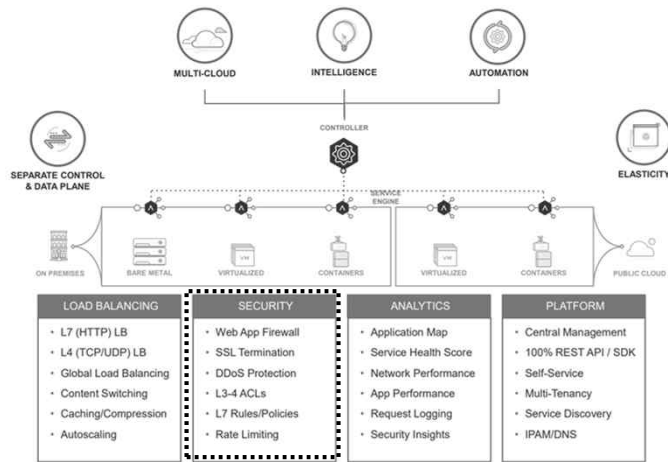
JS Lab

44

V. 보안/관리

❖ Multi-Cloud Application Services Challenges (VMware/AVI)

■ Multi-Cloud Architecture (Virtual Cloud Networking with NSX)

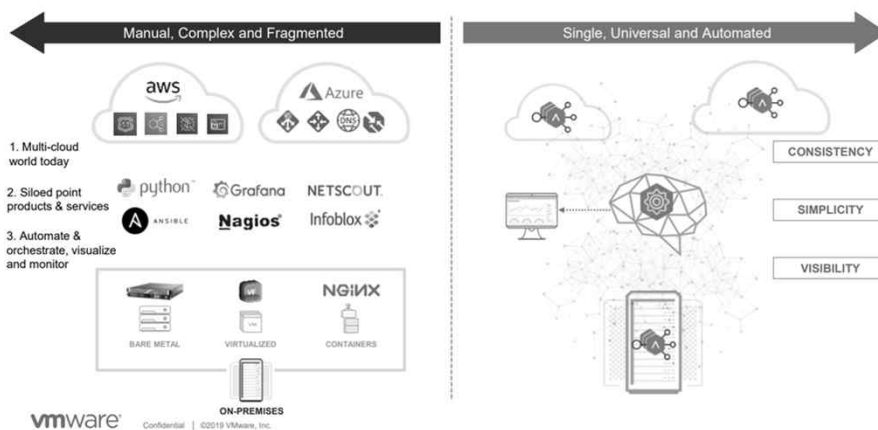


JS Lab

45

V. 보안/관리

❖ Infrastructure-centric Silos to Application-centric Multi-cloud Strategy (VMware/AVI)



JS Lab

46

V. 보안/관리

❖ Security Capability Software Stack

❖ 제조사(예): SD-Brance, SD-WAN, SD-Security (VERSA Networks)



Market Leading Security Functions					
Stateful Firewall	CGNAT	URL Feeds and Filtering	Lateral Movement Protection	Malware Protection	File Filtering
DOS Protection	NG-Firewall (NGFW)	IP Feeds and Filtering	Captive Portal	Network DLP (*)	NG-IPS
IPSec	User & Group Authentication	Device Fingerprinting	HTTP / SSL Proxy	DNS Feeds and Security (*)	Anti-Virus

- **Visibility & access control**
 - Application, domain & URL
 - User, device & location
- **Layer 7 & content security**
 - SSL decryption
 - App / URL / IP Feeds and filtering
 - File filtering
 - Anti-virus
 - IPS
 - DNS Security (*)
- **Layer 4**
 - Reconnaissance
 - DoS protection (ICMP, UDP, TCP flood)
 - Rate limiting
- **Layer 3**
 - ARP, IP ICMP protocol defence
 - IP spoofing
 - Strict source routing checks
 - Fragment overlaps



Versa Networks, SDxCentral.

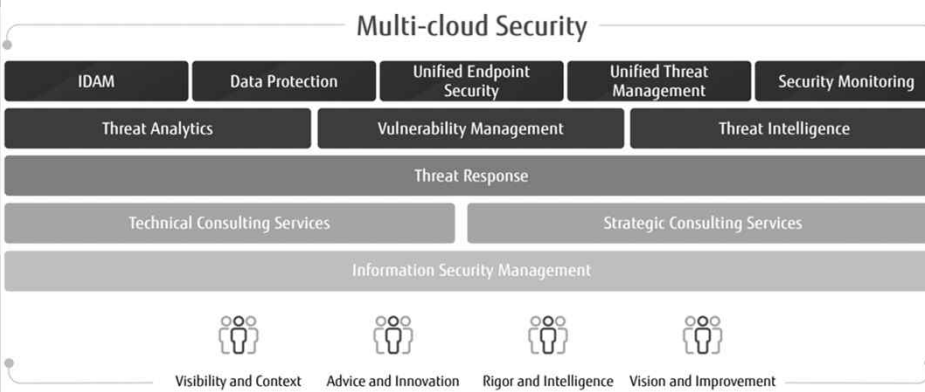
JS Lab

47

V. 보안/관리

❖ Multi-Layered Security

❖ 제조사(예): Multi-cloud Security for enterprise (Fujitsu)

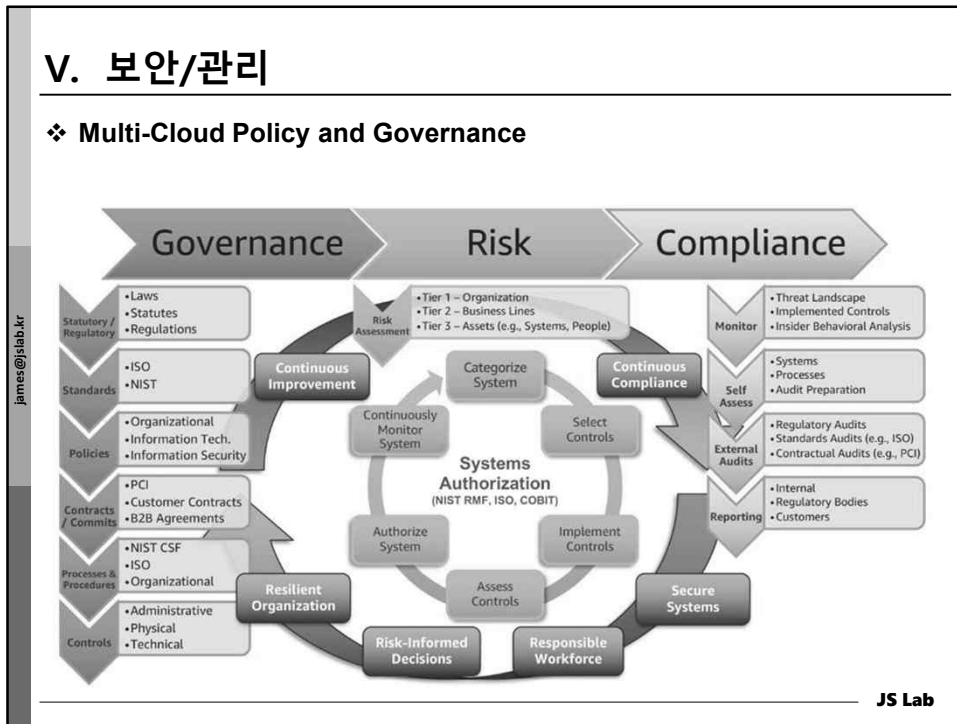


JS Lab

48

V. 보안/관리

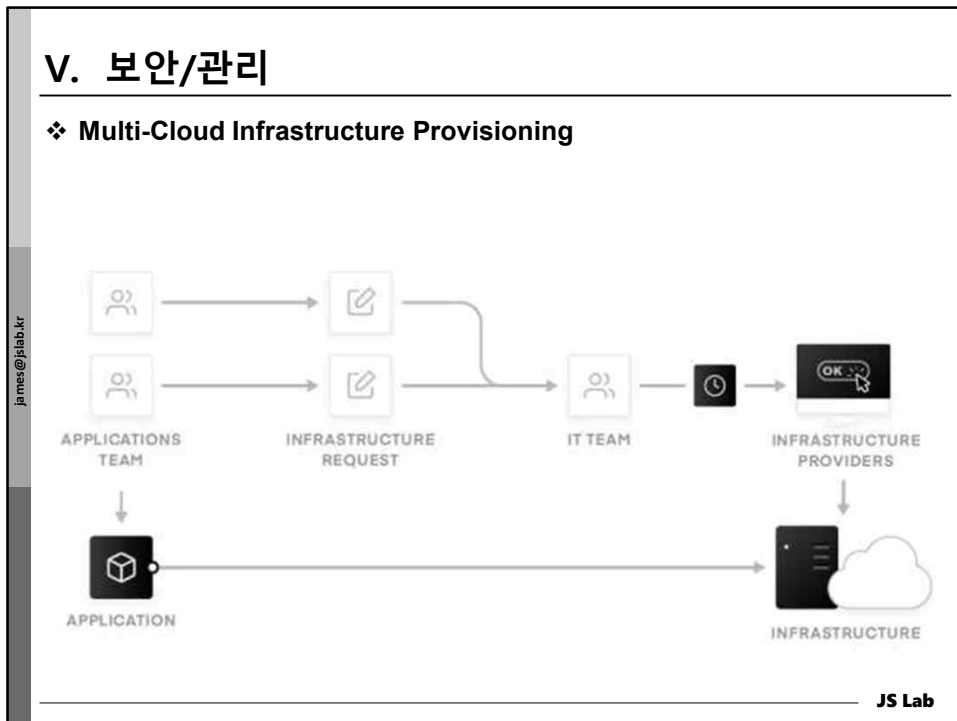
❖ Multi-Cloud Policy and Governance



49

V. 보안/관리

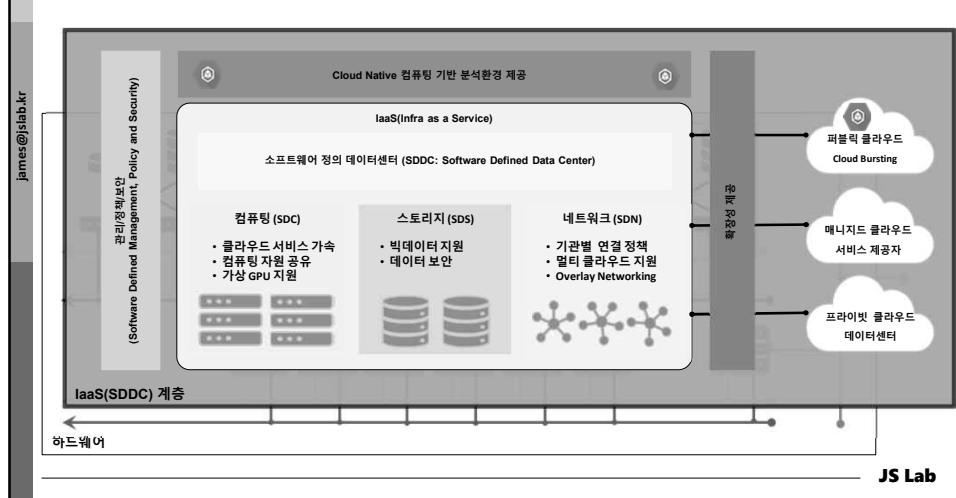
❖ Multi-Cloud Infrastructure Provisioning



50

V. 보안/관리

- ❖ 하드웨어의 추상화 기반 IaaS 인프라 운영 (SDDC)
- ❖ 가상화 자원 제공
- ❖ 하이브리드(Hybrid)/멀티(Multi) 클라우드 인프라 서비스



51


V. 보안/관리

❖ Other Complexities

- **Modernization:**
 - ✓ Hybrid clouds need modernized data center and processes to support both legacy and new applications.
 - ✓ New capabilities need to support rapid provisioning, higher performance, and data mobility between disparate clouds (public and private).
- **Monitoring and Security**
 - ✓ Multi-cloud networks need capability to monitor and secure traffic flows in/out of public cloud environments.
 - ✓ End-to-end encryption needed for every virtual circuit/path/connection.
- **Suppliers**
 - ✓ There are a plethora of options; need to carefully evaluate network requirements and migrate workloads accordingly to avoid vendor-lock.
- **Connectivity**
 - ✓ Network Abstraction: Purpose-built networking in the cloud is all software driven.
 - ✓ Automation needed for disparate CLI's, BGP ASN's, and routing tables.
 - ✓ End-to-end encryption needed for every virtual circuit/path/connection.

JS Lab

52



I. 개요

II. 멀티클라우드 아키텍처

III. 멀티클라우드 기술

IV. 멀티클라우드 네트워킹

V. 보안/관리

❖ 부록: 가상 네트워크 기술

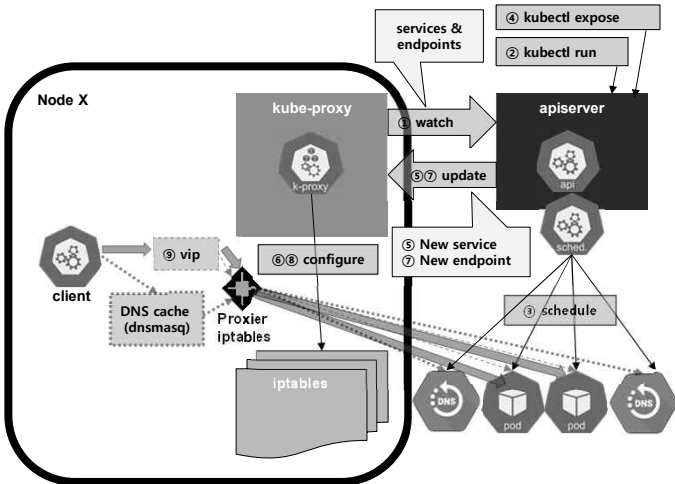
❖ 실습교재 (별도)

JS Lab

53

❖ 부록: 가상 네트워크 기술

❖ Access services from outside Kubernetes



The diagram illustrates the process of accessing services from outside Kubernetes. A client on Node X sends traffic to a virtual IP (VIP). This traffic is managed by kube-proxy, which interacts with the apiserver. The apiserver handles requests for services and endpoints, and schedules pods. The traffic path includes a DNS cache (dnsmasq) and iptables to reach the pods.

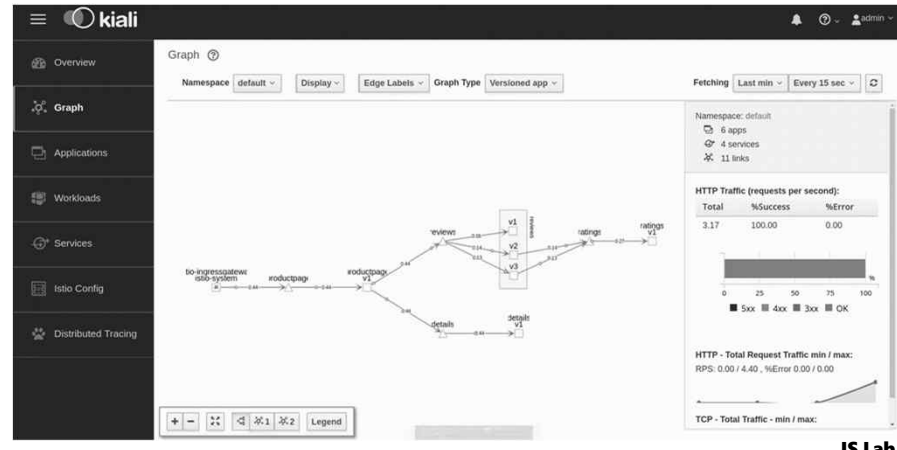
JS Lab

54

❖ 부록: 가상 네트워크 기술

❖ Multi-Cloud Service Networking

- Service Registry & Discovery
- Service Mesh

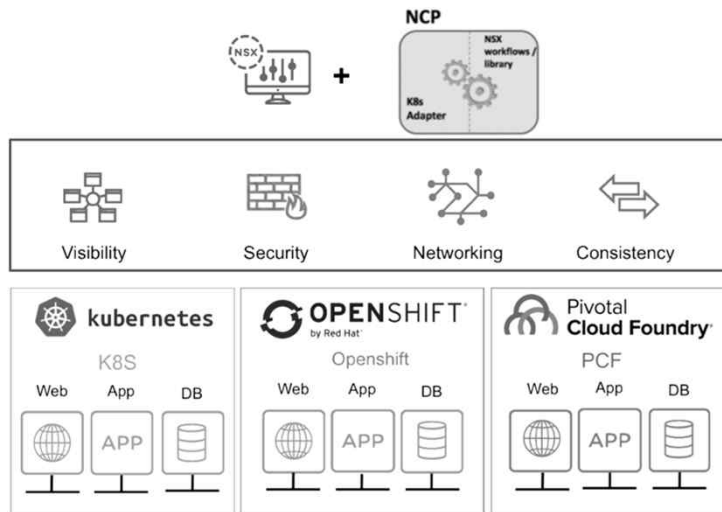


55

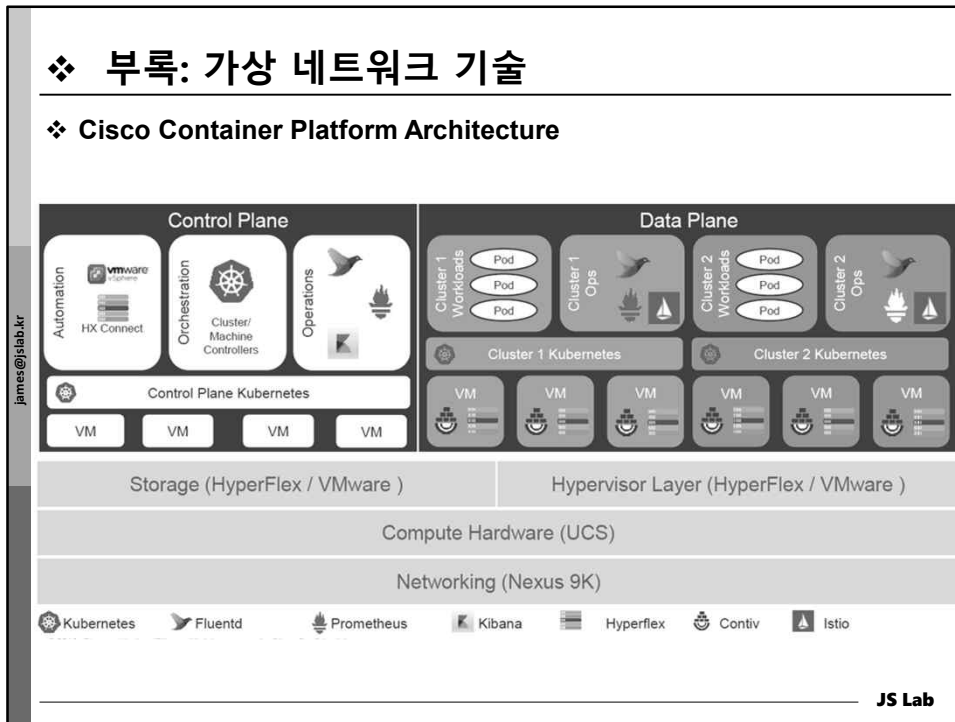
❖ 부록: 가상 네트워크 기술

❖ SDN 내재화 클라우드 솔루션

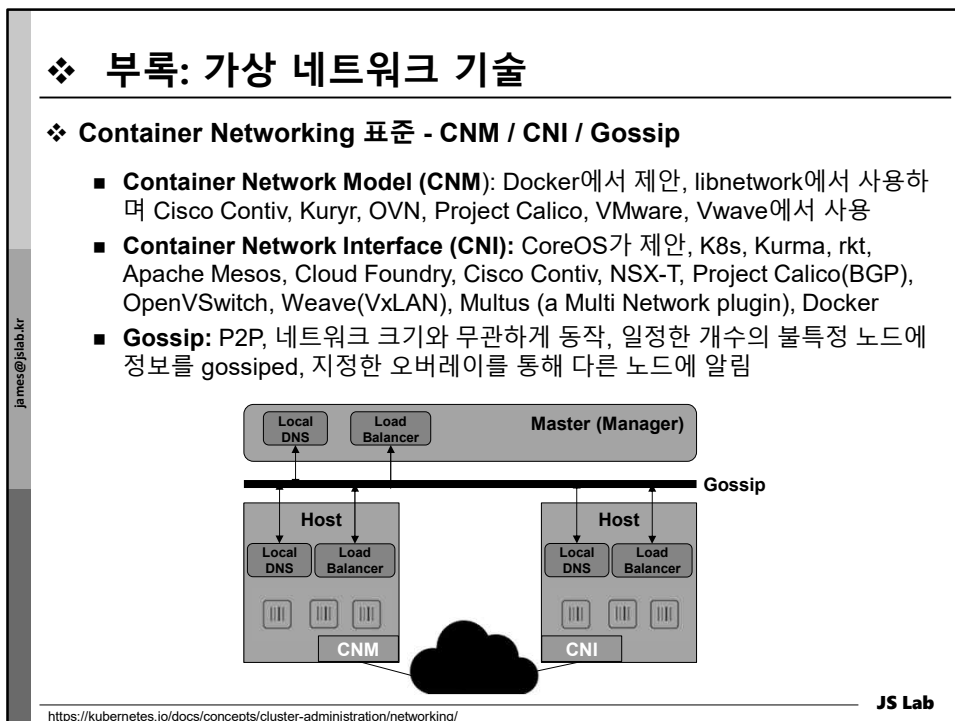
❖ VMware: Programmatic Integration with Various PaaS and CaaS



56



57



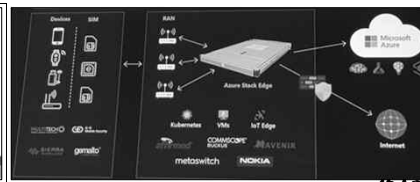
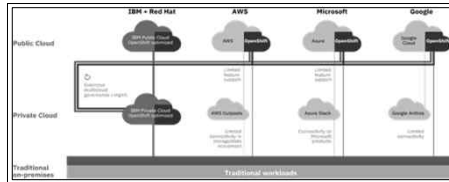
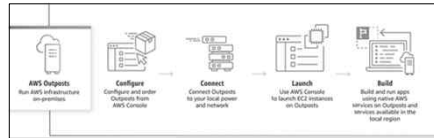
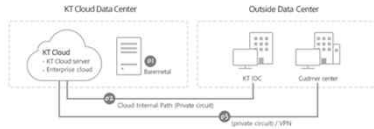
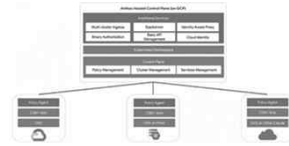
58

❖ 부록: 가상 네트워크 기술

❖ 하이브리드/멀티 클라우드 관리 수용

- KT Hybrid Cloud
- IBM Cloud Pak
- AWS Outpost
- MS Azure Stack (Edge)
- Google Anthos

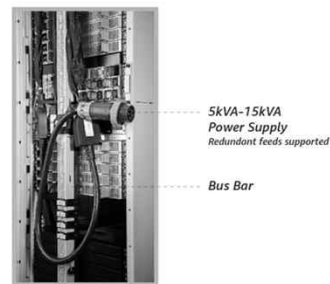
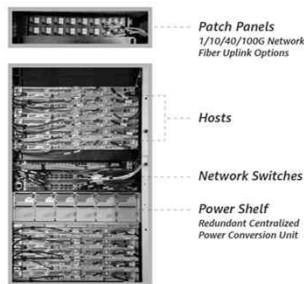
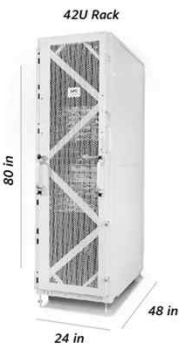
퍼블릭 클라우드 벤더들은 자사 위주의 하이브리드 서비스를 제공합니다.



59

❖ 부록: 가상 네트워크 기술

❖ AWS Outpost




<https://aws.amazon.com/outposts/>

JS Lab

60


❖ 부록: 가상 네트워크 기술

❖ Azure Stack HCI
❖ Azure Stack Edge
❖ Azure Stack Hub




Azure Stack HCI
Hyperconverged solution

Scalable virtualization and storage
Remote branch office
High-performance workloads



Azure Stack Edge
Cloud-managed appliance

Machine learning at the edge
Edge compute and IoT solutions
Network data transfer to cloud



Azure Stack Hub
Cloud-native integrated system

Disconnected scenarios
Data sovereignty
Application modernization

JS Lab

<http://www.darrylvanderpeijl.com/azure-stack-hci-edge-hub-azure-arc/>

61

❖ 부록: 가상 네트워크 기술

❖ IBM Cloud Pak

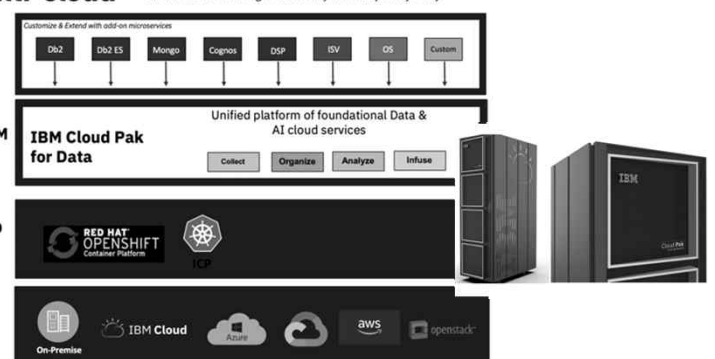
Built for Multi-cloud *Avoid vendor lock-in & get started on your cloud journey today*

PICK YOUR ADD-ON
Containerized Services

DATA & AI PLATFORM
#1 Ranked by Forrester

KUBERNETES BASED
Containerized, easy to manage

PICK YOUR CLOUD
Private or Public



Unified platform of foundational Data & AI cloud services

IBM Cloud Pak for Data

Red Hat OpenShift Container Platform ICP

On-Premise IBM Cloud Azure AWS OpenStack

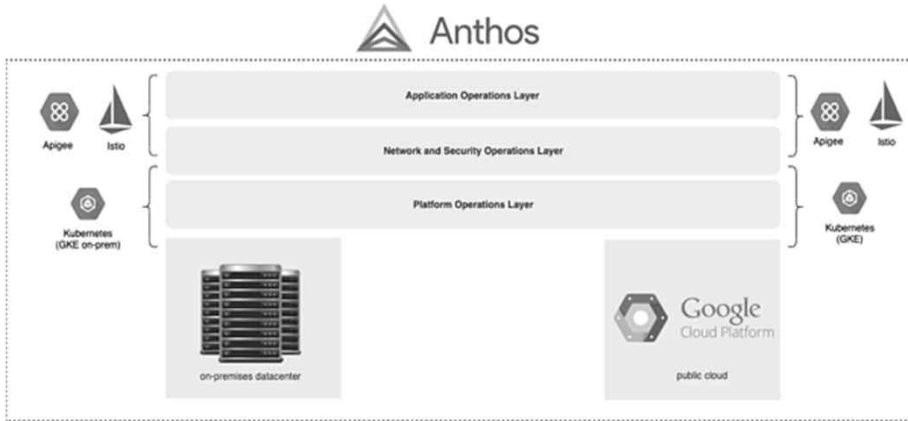
JS Lab

<https://www.ibmbigdatahub.com/blog/ibm-cloud-pak-data-v2dot1>

62

❖ 부록: 가상 네트워크 기술

❖ Google Anthos



<https://cloud.netapp.com/blog/hybrid-deployment-with-google-anthos-an-intro-gc-cvo-blq>

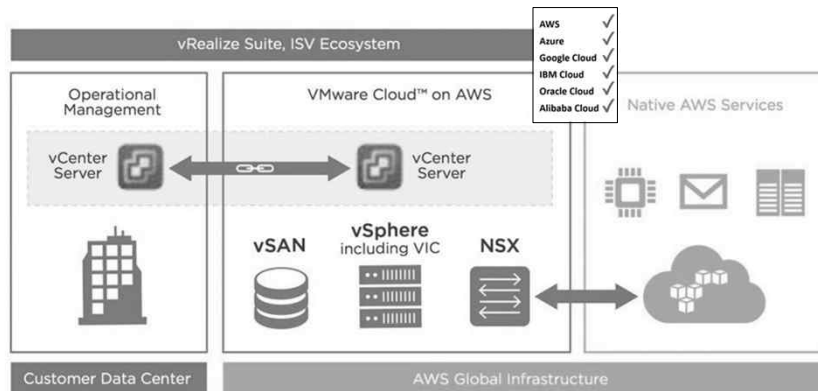
JS Lab

63

❖ 부록: 가상 네트워크 기술

❖ VMware Cloud

- KT Cloud 지원 (2019. 8.)
- VMware Cloud on AWS
- 지원 확장: Azure, Google, IBM, Oracle, Alibaba and KT Cloud



<https://www.actualtech.io/getting-hands-dirty-installing-vmware-cloud-aws/>

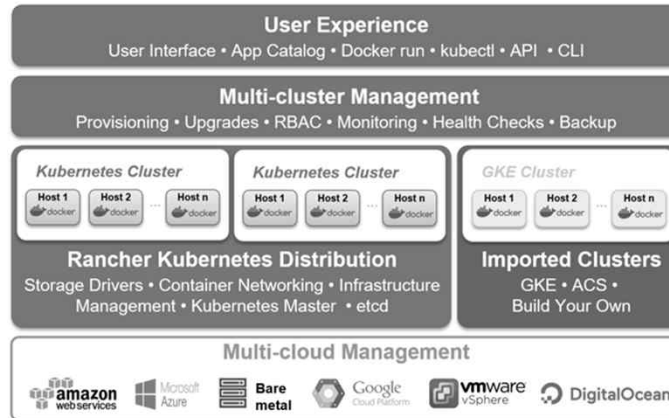
JS Lab

64

❖ 부록: 가상 네트워크 기술

❖ Rancher Labs

- 인프라와 독립적인 엔터프라이즈 급의 클라우드 네이티브 솔루션
- Rancher 2.x



<https://rancher.com/announcing-rancher-2-0/>

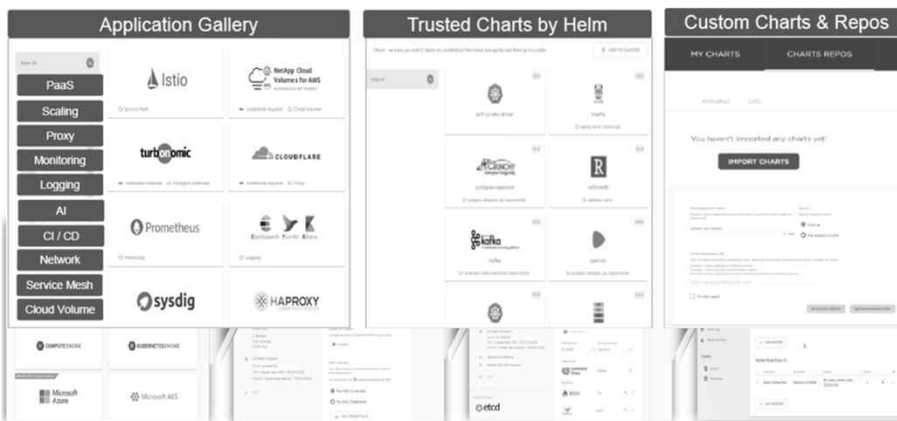
JS Lab

65

❖ 부록: 가상 네트워크 기술

❖ NKS (NetApp Kubernetes Service)

- 관리 및 배포를 위한 Cloud Native Solutions Marketplace
- 스토리지 자동화 기반의 배포 및 관리



JS Lab

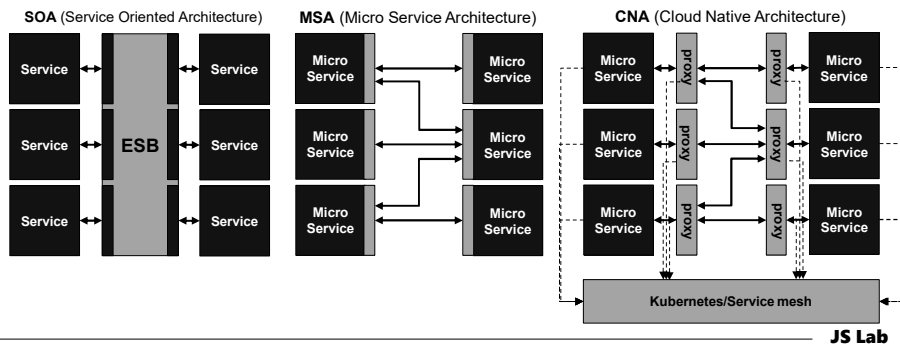
66

❖ 부록: 가상 네트워크 기술

❖ User Plane – Control Plane 분리 : SDN Architecture

❖ 컨테이너 기반 아키텍처

- **SOA** (Service Oriented Architecture): Smart pipes, dumb endpoints
- **MSA** (Micro Service Architecture): Smart endpoints, dumb pipes
- **CNA** (Cloud Native Architecture): Infrastructure focused smart platform, business logic focused smart services

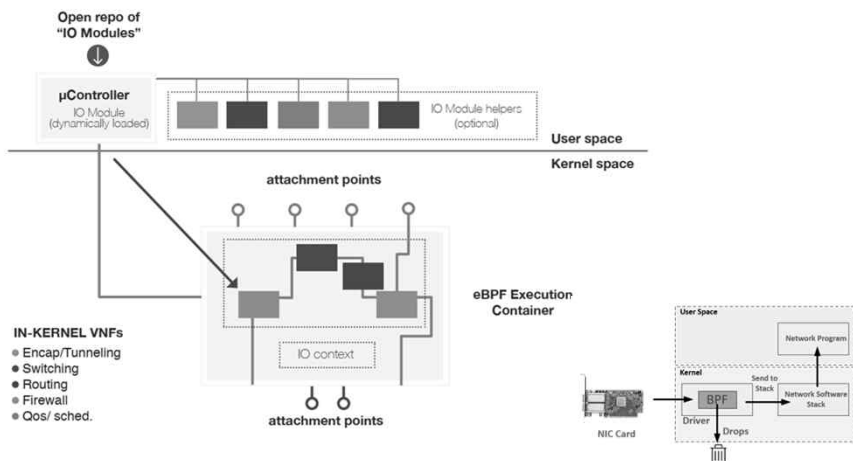


67

❖ 부록: 가상 네트워크 기술

❖ eBPF Framework for Networking

(by IO Visor, retrieved from iovisor.org)



68

