Journey to the Private Cloud: Delivering IT-as-a-Service

Scott Manson
DC Leader for KSA, ME, Turkey
What to do with the Cloud? And Why?

Package hosting, networking, security, and connectivity together as a service. Available to all Ministries, Partners and Supply Chain. Users can acquire server capacity rapidly, for short or long-term use, using Pay as you grow OPEX funding, without the need for capital acquisitions.
Cloud Services typical evolution path

- Application Services
- Infrastructure Services

- Software as a Service
- Content Distribution Services
- Hosted UC/collaboration services
- Business Continuity Services
- Backup/restore Services
- Email Services
- HRIS Payroll Services
- IT Infrastructure Management
- Corporate Website

- Management
- Technology
- Customer Experience
- Data Centre Connectivity
Private Cloud Lifecycle Reference Model

**Tier 1:**
- Self-Service Portal
- Define Service:
  - Customer Catalogue

**Tier 2:**
- Service Management
- Resource Management (Automated Provisioning)
- TIER 2: Physical Servers
- TIER 2: Virtual Servers
- TIER 2: Network
- TIER 2: Storage
- TIER 2: Burst Capacity

**Tier 3:**
- TIER 3: Resource Management (Automated Provisioning)
- Performance Management
- Compliance Management
- Metering & Chargeback

**Tier 4:**
- Private Cloud Lifecycle Reference Model
IT-as-a-Service:
On demand allocation of Services

COMPANY X

Internal Ministries
Supply chain

Dynamic allocation of shared resources across the Data Center based on priority

Service Catalogue

Email-as-a-service
Storage-as-a-service
Infrastructure-as-a-service
Voice/Video-as-a-Service
DR/Backup-as-a-Services
Virtual Desktop-as-a-Service
Typical Services Engagement Model for UCS

**Phase 1**
Public / Private Cloud Infrastructure
- Base Nexus + UCS foundation
- Multitenant virtualization
- Integration with 3rd party Cloud Orchestration SW
- Secure Data Center Interconnect over VPN
- Scale up / down DC infrastructure
- Additional security capabilities

**Phase 2**
Private and Virtual Private Cloud
- Federation and automation of workload moves across DCs
- Infrastructure available for SaaS offerings
- Secure Data Center Interconnect over VPN
- Infrastructure available for SaaS offerings
- Automation of DC to network connectivity

**Phase 3/4**
Deeper Unified Fabric, Automation and APIs
- Federation and automation of workload moves across DCs
- Infrastructure available for SaaS offerings
- Unified Fabric throughout the data center
- Automation of DC to network connectivity

**Problem Definition**
- Analysis of current IT infrastructure and business requirements

**Solution Design**
- Designing cloud solutions to meet business needs
- Determining cost-effective cloud architectures

**Best Practices**
- Optimization of cloud resources
- Security considerations

**Trusted Advisor**
- guidance and support throughout the implementation process
Tier 1

Self Service Portal

- Email-as-a-service
- Storage-as-a-service
- Infrastructure-as-a-service
- Voice/Video-as-a-Service
- DR/Backup-as-a-Services
- Virtual Desktop-as-a-Service

Service Catalogue

Request Service → Customer
Service Catalogue

- Email-as-a-service
- Storage-as-a-service
- Infrastructure-as-a-service
- Voice/Video-as-a-Service
- DR/Backup-as-a-Services
- Virtual Desktop-as-a-Service

Service Management

Resource Management

Cisco Virtual Multi-Tenant Data Center

Tier 4

Cisco Server Provisioner
Cloud Automation Packs

CCP (Cisco Cloud Process Orchestrator)

Cloud Service Assurance
Virtualization Charging Solution
Chargeback Solution
A Platform to facilitate the Critical Capabilities for Cloud

- Predictable Deployment
- Rapid Tenant Provisioning
- Efficient workload deployment
- Use of Shared resource pools & service Catalogues
I would like a new SharePoint application server running Windows in a virtual machine and I would like it be added to my current SharePoint environment.

1. Orchestrator receives request to initiate provisioning of virtual infrastructure.

2. Orchestrator calls Automation to provision the new virtual machine.

3. Automation controls vCenter Provisioning the new virtual machine.


5. Automation adds the virtual machine details in the load balancer configuration.

6. Orchestrator updates the CMDB with the provisioned server details.

7. User gets notified that virtual infrastructure is provisioned.
Private/Public Cloud Critical Capabilities

Networking for Cloud

- Network architecture needs to be flexible, instead of being a static stumbling block.
- Network services need to be location independent: delivered wherever data, applications, and users are and whenever the services are needed.
- Network resources need to be abstracted so that provisioning can be automated and actions orchestrated through common interfaces.
OTV: allowing Ethernet traffic from a local area network (LAN) to be tunnelled over an IP network to create a “logical data center” spanning several data centers in different locations.

VMware VMotion can now leverage Cisco OTV to easily and cost-effectively move data center workloads across long distances, providing customers with resource flexibility and workload portability that span across geographically dispersed data centers.
Private/Public Cloud Critical Capabilities

Multi-Tenant Architecture

Flexible design to enable different classes of service for different tenants

Traffic isolation via dynamic provisioning of VLANs, VRFs, ACLs, and Virtual Data Centers

Multi-tenant partitioning provided by network container provisioning, executed with a level of rigor and auditability that may not be required if the data is not sensitive
Validated Design for Multi-Tenancy: **Path Isolation**

- Each tenant is logically isolated from the others using VRF as a container
- Dedicated logical instances of vrf, vlan, fw, Service Load Balancing etc .. for each tenant to provide security, privacy, policy compliance

**Customer = Virtual Routing and Forwarding**

- **VRF Blue**
- **VRF Purple**
Leveraging Network Container Architecture

Pods = Physically assigned Resources

Network Containers
Virtually and securely isolated by tenant within a Pod

Unique Benefit: Logical Multi-tenancy - allows creation of one-to-many zones

Zones – Contain Customized policy-based workloads

Key Benefit: Policy driven “placement” makes decision on best resource placement.

Resource Management configures and places services within Network Containers and Zones
Pre-packaged NW Services as Containers

- **Bronze**
  - LB, 1 VLAN
  - Virtual FW + pVLANs
  - Shared VMFS, No Data Protection

- **Silver**
  - Multiple VLANs
  - System Configs
  - Virtual FW + pVLANs
  - Dedication VMFS, DP via Snapshots

- **Gold**
  - Multiple VLANs
  - System Configs
  - Virtual FW + pVLANs
  - Dedicated VMFS, 100% DP, Cloning

- **VPN Offload**
  - SLB & SSL offload
  - Dedicated VMFS
  - Cloning
Out of the box flexible Service Classes

“Gold”
- One VRF and multiple VLANs per customer
- VPN Off load
- Firewall
- SLB & SSL offload

“Silver”
- One VRF and multiple VLANs per customer
- SLB & SSL offload

“Bronze”
- One VLAN and VRF per customer

Out of the box flexible Service Classes

Dedicated VMFS Data store and 100% Data protection and recovery with cloning

Dedicated VMFS data store and Data protection and recovery with Snapshoting

Shared VMFS data store and no Data protection
“Pre-validated Cloud computing platform for service providers that combines Cisco’s CRS-1 core Internet router, Nexus 7000 data center switches and its Unified Computing System (UCS), which integrates blade servers with switching, storage access, virtualization and management”
Typical Services Engagement Model for UCS

**Business Value**

**Phase 1**
Public / Private Cloud Infrastructure
- Base Nexus + UCS foundation
- Multitenant virtualization
- Additional security capabilities
- Integration with 3rd party Cloud Orchestration SW
- Secure Data Center Interconnect over VPN
- Scale up / down DC infrastructure
- Additional security capabilities

**Phase 2**
Private and Virtual Private Cloud
- Private Cloud
- Integration with 3rd party Cloud Orchestration SW
- Secure Data Center Interconnect over VPN
- Scale up / down DC infrastructure
- Additional security capabilities

**Phase 3/4**
Deeper Unified Fabric, Automation and APIs
- Federation and automation of workload moves across DCs
- Automation of DC to network connectivity
- Infrastructure available for SaaS offerings
- Unified Fabric throughout the data center

**Deployment**
- IaaS Optimization
- IaaS Implementation

**Architecture**
- Unified Fabric
- Roadmap

**Solution**
- Problem Definition
- Solution Design
- Best Practices
- Trusted Advisor