Cloud Service Orchestration and Management with Cisco VMDC

Ashley Woodbridge
Systems Engineer
Agenda

- Cloud Refresher
- Cisco Strategy
- What does the market want?
- Deploying Cloud using VMDC and CIAC
  - CIAC orchestration stack
  - Multi-tenant network architecture
- Recap
Cloud Computing

IT resources and services that are abstracted from the underlying infrastructure and are provided “On-Demand” and “At Scale”

Visual Model of NIST’s Working Definition of Cloud Computing

Essential Characteristics
- On-Demand Self Service
- Broad Network Access
- Resource Pooling
- Measured Service
- Rapid Elasticity

Service Models
- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

Deployment Models
- Public
- Private
- Hybrid
- Community

http://www.csrc.nist.gov/groups/SNS/cloud-computing/index.html
Cloud Traffic Increases 12x 2010 - 2015

Cloud Traffic Will Be Over One-Third of DC Traffic by 2015

Cloud Traffic Increases 12x 2010 - 2015

Cloud Traffic Will Be Over One-Third of DC Traffic by 2015
Cisco’s Cloud Strategy

Enabling Cloud Applications/Services by Uniquely Combining the Unified Data Center and Cloud Intelligent Network

Tailored Solutions for Building Clouds
Enable customers to build and operate private, public or hybrid clouds

Rich Ecosystem of Integrated Solutions
Enable customers to deploy tested, best of breed solutions

Innovative Cloud Services
Enable cloud services including people-centric collaboration and other applications
Cisco Validated Design Process
Innovation and Quality Through System Level Design and Validation

Key Customer Engagements
Consider end-to-end view

Product Development
Cross platform collaboration

System Development Fundamentals

System level innovations
Tested and validated designs

System Development Guidelines

Planning

Design

End-To-End Validation

Documentation
Cloud Deployment Models—
Private, Public, Hybrid

Stand-Alone Data Centers

Private Cloud

Public Cloud

PRESENT

Private Cloud

Public Cloud

Enterprise Extension Hybrid Cloud

Open Cloud

Inter-Cloud

Private Cloud

Private Cloud

Public Cloud #1

Public Cloud #2
Cloud Deployment Models

Ownership

Internal Resources
- All cloud resources owned by or dedicated to enterprise

External Resources
- All cloud resources owned by providers; used by many customers

Control

Private Cloud
- Cloud definition/governance controlled by enterprise

Public Cloud
- Cloud definition/governance controlled by provider
Cloud Deployment Models

Hybrid Cloud

Interoperability and Portability Between Public and Private Cloud Systems
The Journey to Cloud
Evolution of IT + Business Agility

Consolidation (Reduce Costs)
Virtualization (Improve Agility)
Automation (Transform IT)

IT Infrastructure
Business Applications
IT-as-a-Service
Cloud Adoption Curve

Cloud in Cautious Stages
- Mostly SMB adoption
- Sandbox Environments—Develop/Test
- Seasonal bursting scenarios
- Enterprises—Non Business Critical applications

Cloud Goes Mainstream
- Enterprise adoption will be driven by
  - Network performance
    - Application and Performance SLAs
  - Security
  - Reduce costs
  - Service assurance
- Hosting providers and Telcos are best poised to exploit this paradigm shift

Adoption of Cloud Services

 Mostly SMBs, Enterprises for Non Business Critical Applications

Today

Main Stream Enterprise Adoption of Cloud Services
Cloud Delivery
Using Cisco Stack
Cloud Building Blocks

Common Physical Infrastructure

- Network Services
- Data Centre Fabric
- Virtualized Resources
- Compute Resources
- Network Resources
- Storage Resources
- Pod

Orchestration and Management Software

- Network Manager
- Compute Manager
- Server Provisioner
- Virtualization Manager
- Orchestration Engine
- User Portal & Service Catalog
Orchestration and Management Software

**Orchestration:**
Cisco Intelligent Automation for Cloud (CIAC)

**Network Architecture:**
Virtual Multi-Tenant Data Center (VMDC)

**Domain Managers**
- **Network:** Cisco Network Services Manager
- **Compute:** Cisco UCS Manager
- **Virtualization:** vCenter
- **OS/Server:** Cisco Server Provisioner

**Orchestration:**
BMC Cloud Lifecycle Management (CLM)

**Network Architecture:**
Virtual Multi-Tenant Data Center (VMDC)

**Domain Managers**
- **Network:** Blade Logic for Networks (BBNA)
- **Compute:** Cisco UCS Manager
- **Virtualization:** vCenter
- **OS/Server:** Blade Logic for Servers (BBSA)
Cisco Intelligent Automation for Cloud
Orchestration and Management Software

- Service catalog and self-service portal – Cisco Cloud Portal
- Global orchestration and reporting – Cisco Process Orchestrator
- Multi-tenant network provisioning – Cisco Network Services Manager
- Adapter framework to communicate to compute, virtualization and storage domain managers
CIAC Components Explained

- Compute Manager
- Network Manager
- Orchestration Engine
- UCS Manager
- User Portal
- Service Catalog
- Virtualization Manager
- Server Provisioner
- vCenter
- Cisco Server Provisioner
- newScale
CIAC Orchestration Framework

- **Cisco Cloud Portal**
- **IT Service Catalog and Portal**
- **Cisco Process Or orchestrator**
- **Global Orchestration**
- **Adapter Framework**
  - **Compute Automation**
    - Cisco Server Provisioner
    - UCS Manager
    - VCenter
    - Win2008 R2 OS
    - UCS B-series
    - ESXi, VMs
  - **Network Automation**
    - Cisco Network Services Manager
    - DSN (Cat6500, ACE-SM, ACE30)
    - ASR, Nexus 1K, 5K, 7K
  - **Storage Automation**
    - EMC
    - NetApp

- **Orchestration**
  - Catalog, Order, Offer, Metering, Billing, Chargeback

- **Domain Managers**
  - AD (LDAP)
  - Chargeback
  - Governance
  - Monitoring
  - Ticketing
  - CMDB

- **NetApp**
- **EMC**
- **UCS B-series**
- **ESXi, VMs**
- **Win2008 R2 OS**
- **DSN (Cat6500, ACE-SM, ACE30)**
- **ASR, Nexus 1K, 5K, 7K**
- **Cisco Network Services Manager**
- **Cisco Process Orchestrator**
- **Global Orchestration**
- **Adapter Framework**
- **Compute Automation**
- **Network Automation**
- **Storage Automation**
- **Cisco Cloud Portal**
- **IT Service Catalog and Portal**

© 2012 Cisco and/or its affiliates. All rights reserved. Cisco Public
Hypervisor Support

Popular Hypervisors

- VMware
  - Supported in CIAC 3.0
  - Future

- Microsoft Hyper-V
  - Future

- KVM
  - Future

- Xen
  - Future
CIAC 3.0 - Intuitive User Interface
Service Catalog

Virtual or Physical?
Ordering a new server is as easy as plucking from one of the options below. Virtual machines provide a choice between a preconfigured template to configure your server, or starting from scratch and choosing the operating system of your choice. The physical server option always offers a choice of operating system.

- Order a Virtual Machine from a Template
- Order a Virtual Machine and Install an OS
- Order a Physical Server

About the Starter Edition
With the Cisco Intelligent Automation for Cloud Starter Edition, you can order a virtual machine or a physical server (if you have the right permissions) and get it ready in minutes.

- Select the VM template or OS image to install, and enter settings such as root password and VLAN. Once your order is complete, you’ll get an email with access details to your server.
- You can see your ordered servers in the My Servers page, view technical details, and manage them with actions such as power-up, power-down and extend lease.

Clearly laid out ordering choices
Easily accessible User and Admin options
# CIAC 3.0 – User Interface

## VM Ordering

### Order a Virtual Machine From Template

**Order a Virtual Machine From Template**
Order a new virtual machine from a template you select.

### Virtual Machine

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating system family</td>
<td>Select the operating system family (e.g., Windows, Linux) of the desired VM template from the list.</td>
</tr>
<tr>
<td>Operating system</td>
<td>Select the operating system of the desired VM template from the list.</td>
</tr>
<tr>
<td>VM template</td>
<td>Select the VM template you wish to use for deploying the virtual machine from the list.</td>
</tr>
<tr>
<td>Computer Name (Host)</td>
<td>Enter a host name for the new virtual machine. This name must be unique within the domain.</td>
</tr>
<tr>
<td>Virtual Machine Size</td>
<td>Select the hardware configuration (CPU, memory, storage) you’d like to have for your virtual machine from the list.</td>
</tr>
</tbody>
</table>

### Network Selection

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deploy to Network</td>
<td>Select the network on which to deploy the server. The server will be assigned and set up with a static IP address on this network.</td>
</tr>
</tbody>
</table>

### Lease Term

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Term</td>
<td>Select the duration of the lease term from the list. The server will be automatically decommissioned by the end of this term, unless you extend the lease.</td>
</tr>
</tbody>
</table>

### Administrator Password

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter Password</td>
<td>Enter the password for the new virtual machine.</td>
</tr>
<tr>
<td>Re-enter Password</td>
<td>Enter the password again to confirm.</td>
</tr>
</tbody>
</table>
CIAC 3.0 – User Interface

Template Management

Admin options to update, delete and add templates
Network Orchestration
Network Services Manager

Key Features

- Common network abstraction layer
- Standardized API
- Flexible and easily consumable interface
- Fast deployment of virtual data centers in cloud
- Device support in various roles
- Multi-Pod support
Network Services Manager Overview

- Instantiate Tenant Metamodel (Logical Topology, Tenant resources)
- Network Devices Configurations
- Service Directives
- Object Model (Physical Topology, Resources, Credentials etc)

POD
- Network
- Virtual Tenant N/W
- Compute
- SAN
Network Services Manager

- **Tenant**: An organization or individual subscribed to service offering
- **Tenant Network Container**: A layer 3 partition for a tenant. Can contain multiple Network Containers
- **Network Container**: A layer 2 or 3 network for tenant machines and services such as FW and LB
- **Metamodels**: Definition of and relationship between various entities and resources that exist in the network
Using Network Services Manager

Abstracting the Network

Provisioning System

REST Calls

API

Network Services Manager Engine

NSM

NSM Controller

Config Push
What does the market want?
Service Class Examples

<table>
<thead>
<tr>
<th>Bronze</th>
<th>Silver</th>
<th>Gold</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM ratio 4:1, Queue bandwidth–20% (dedicated vlan and VRF)</td>
<td>VM ratio 2:1, ACE, Queue bandwidth – 30% (dedicated vlan, VRF, and SLB. Local Data protection and recovery using Snap.). Remote replication to the DR site</td>
<td>VM ratio 1:1, ACE and FWSM, Queue bandwidth – 40% reserved, (Highly secure: dedicated vlan, VRF, firewall and SLB. 100% local data protection and recovery using clone (full copy). Remote replication to the DR site</td>
</tr>
</tbody>
</table>
Create offers with Service Profiles for the Application Lifecycle (Leveraging the DC & the Network)

**Mission Critical**
- Enterprise
- Premier
  - 99.995% SLA for HA
  - Stateful Firewalls
  - 3x Private VLANs
  - 1 Gbps Guarantee
  - 3-Tier ILM Storage

**Enterprise Web Hosting**
- Web Hosting, eCommerce
- Balanced
  - 99.99% SLA
  - Stateful Firewalls
  - 1x Private VLAN
  - 100 Mbps Guarantee
  - 2-Tier ILM Storage

**“Test/Dev”**
- Start using clouds for application development and testing environments
- Essential
  - 99.9% SLA
  - Lowest Cost
  - Easy On-boarding
Virtual Multi-Tenant Data Center (VMDC)
Cloud Infrastructure
Virtual Multi-tenant Data Center (VMDC)

- **Modular design** to enable easy expansion and incremental growth
- **Resilient and fault tolerant** infrastructure
- **Tiered security and end to end tenant traffic separation**
- **Layer 4-7 services** including Firewall and Load Balancing
- **Role based access control**
What Is VMDC?

- Virtualized, Multi-Tenant Data Center (VMDC) is a cloud blueprint that enables customer to readily deploy services or applications.
- A validated, full-system architecture for customers deploying virtualized services (application workloads) in a “cloud-style” environment, sharing common infrastructure for multiple cloud consumers or “tenants”.
- A flexible, modular design that can be used as a blueprint for cloud deployments.
- An architecture built to scale.
- An architecture that aggregates integrated compute stacks, unified data center, and data center interconnect into an end-to-end architecture.
VMDC – Concept and Design

Physical Setup

- Catalyst 6500 FWSM/ASA-SM
- Nexus 7000
- Nexus 5000
- UCS
- Storage

Virtual Setup

- WAN/Core
- Aggregation Public Zone VRF
- Services
- Aggregation Private Zone VRF
- Access
- Compute and Storage

Redundant connections are not shown for clarity
VMDC - customer view of network design

Customer A requests new resources from IT provider

Customer B requests new resources from IT Provider
VMDC Validated Infrastructure Containers

VMDC 2.0
- Bronze
  - L3
  - L2
  - vFW

- Silver
  - L3
  - LB
  - L2
  - vFW

- Gold
  - L3
  - FW
  - L2
  - vFW

VMDC 2.1
- Palladium
  - Protected Front-End
    - L3
    - FW
    - LB
  - Private Zone
    - L3
    - FW
    - LB
  - Protected Back-End
    - L2
    - vFW
    - LB

VMDC 2.2
- Expanded
  - L3
  - LB
  - vFW
  - Protected Back-End
    - L2
    - vFW
    - FW
  - Protected Front-End
    - L3
    - FW
    - LB
Cisco Virtualized Multi-Tenant Data Center

Comprehensive, Modular, and Flexible Approach
Cisco Virtualized Multi-Tenant Data Center

Comprehensive, Modular, and Flexible Approach
Cisco Virtualized Multi-Tenant Data Center

Modular for Each Step of the Journey

Enhanced Data Center Interconnect

Unified Data Center Networking

Integrated Compute Stacks

DCI and Hybrid

Network and Services Virtualization

Server and Application Virtualization

Enhanced DCI
- Cisco ASR 9000 and 1000
- Cisco Nexus 7000

Unified Data Center Networking
- Cisco Nexus 7000
- Cisco Nexus 5000
- Cisco Data Center Service Node
- Service Appliances

Integrated Compute Stacks
- NetApp FlexPod
- VCE Vblocks
- Cisco Unified Computing System
- Cisco MDS
- Cisco Nexus 1000v
- Hypervisors

© 2012 Cisco and/or its affiliates. All rights reserved.
Data Center Interconnect

- Interconnection Models:
  - Enterprise to Enterprise (E2E)
  - Enterprise to Service Provider (E2SP)
  - Service Provider to Service Provider (SP2SP)

- Overlay-Based Techniques
  - OTV, LISP, VXLAN

- Suitable for intra-Ent DC interconnect
  - NGN-Based DCI Solution:
    - Addresses E2SP for workload migration
    - Addresses SP2SP for regional or distributed data centres

- Standalone DCI Network
  - Provides interconnection between main SP DCs
  - Owned by SP DC team
  - Addresses SP2SP only
  - Very high bandwidth—packet/optical solution likely the most cost effective

<table>
<thead>
<tr>
<th>Overlay Solution</th>
<th>PE-Based Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet</td>
<td>(e)TRILL / 802.1ad</td>
</tr>
<tr>
<td>MPLS</td>
<td>VPLS, A-VPLS, EVPN, EoMPLS</td>
</tr>
<tr>
<td>IP</td>
<td>OTV, LISP, VXLAN</td>
</tr>
</tbody>
</table>
VMDC Security Framework

Security Management
- Visibility
- Event correlation, syslog, centralized authentication
- Forensics
- Anomaly detection
- Compliance

Services
- Initial filter for DC ingress and egress traffic; Virtual Context used to split policies for server-to-server filtering
- Additional firewall services for server farm specific protection

Infrastructure Security
- Infrastructure Security features are enabled to protect device, traffic plane, and control plane
- 802.1ae provides separation through encryption

Services
- IPS/IDS provide traffic analysis and forensics
- Network Analysis provide traffic monitoring and data analysis
- Server load balancing masks servers and applications

Core
Aggregation
Services
Access
Storage
Virtual Access
UCS

ACLs, Port Security, VN Tag, Netflow, ERSPAN, QoS, CoPP, DHCP snooping

Data security, authentication and access control
Virtual Firewall
Port security, authentication, QoS features

Real-Time Monitoring
Firewall Rules
VMDC Consumer Models
Addressing Application Requirements

- **Network Requirements**
  - Session persistence
  - High Availability
  - Scalability
  - Latency Mitigation
  - Reliable transport

- **Security Requirements**
  - Secure sessions with encryption may be required
  - Each layer of the application stack authenticates data transport
VMDC Consumer Model
Tiered Security in VMDC

Private (Tenant VRF)

Public/Shared

VRF

Protected VRF (control point)

Nexus 1000v

ASA Context (per tenant)

Public Zone (DMZ)

Protected FE

Front-End Zones

Zone 1

Zone 2

Back-End Zones

Sub-Zone W

Sub-Zone X

Sub-Zone Y

Sub-Zone Z

Less Trusted Zones

Front-End Tenant Perimeter

Back-End Tenant Perimeter

Back-End Management Perimeter

Public/Shared Zone

Protected FE Zone

Front-End Tenant

Perimeter

Back-End Tenant

Perimeter

Back-End Management

Perimeter

vPath

VSG
VMDC Building Blocks
Scaling the Data Center

The Data Center Core
Efficient replication of the PoD

Integrated Compute Stack
Data Center Services Node
Service Appliances

PoD

Integrated Compute Stack
Integrated Compute Stack
Integrated Compute Stack
Integrated Compute Stack

Storage	Network	Compute
Storage	Network	Compute
Storage	Network	Compute
Storage	Network	Compute

Cisco live!
Network Scale Considerations

POD Scalability

What Determines the Host Scale in a POD?

- Aggregation—Number of PoDs
- Work-load domain
- Number of MAC address and VLANs
- Failure Domain
- Features to facilitate L2/L3 Boundary

Compute/VMware

- VM Density
- MAC per VM
- Logical Ports
- Virtual Switch

Network

- Total number of MAC Addresses
- Total number of ARP entries
- STP logical ports

Storage

- Number of vFiler IP Space
- Number of VLANs supported
- Number of 10 Gig NICs
Compact POD Sizing—VMDC

64 Server POD Characteristics
- 2 UCS clusters, each of 32 blades
- 64 x B200 Blade server at 96GB RAM
- 512 Cores
- 512 Gold VMs 1vCore per VM (1:1) ov
- 1024 Silver VMs 0.50vCore per VM (2:1) ov
- 2048 Bronze VMs 0.25vCore per VM (4:1) ov
- 5–8 VMs/VLAN

Combination of All Three Service Tiers in a POD

<table>
<thead>
<tr>
<th>Service Tier</th>
<th>Number of Cores</th>
<th>Number of VMs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gold, 20%</td>
<td>102</td>
<td>102 (1:1 ov)</td>
</tr>
<tr>
<td>Silver, 30%</td>
<td>154</td>
<td>308 (2:1 ov)</td>
</tr>
<tr>
<td>Bronze, 50%</td>
<td>256</td>
<td>1024 (4:1 ov)</td>
</tr>
<tr>
<td><strong>Total VMs</strong></td>
<td><strong>1434</strong></td>
<td></td>
</tr>
</tbody>
</table>
Large POD Sizing—VMDC

512 Server POD Characteristics
- 8x8-chassis UCS systems (Vblock Type 2 Max)
- 8 blades/ESX cluster
- 512 x B200 Blade server at 96GB RAM
- 4096 Cores
- 816 Large VMs 1vCore per VM (1:1) ov
- 2464 Medium VMs 0.50vCore per VM (2:1) ov
- 8192 Small VMs 0.25vCore per VM (4:1) ov
- 5–9 VMs/VLAN
- 500–1000 tenants = 12–23 VMs/VLAN

Combination of All 3 Workload Types in a POD

<table>
<thead>
<tr>
<th></th>
<th>Number of Cores</th>
<th>Number of VMs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Large, 20%</td>
<td>802</td>
<td>816 (1:1 ov)</td>
</tr>
<tr>
<td>Medium, 30%</td>
<td>1232</td>
<td>2464 (2:1 ov)</td>
</tr>
<tr>
<td>Small, 50%</td>
<td>2048</td>
<td>8192 (4:1 ov)</td>
</tr>
<tr>
<td>Total VMs</td>
<td></td>
<td>11,472</td>
</tr>
</tbody>
</table>
Value Proposition Recap

Advantages of a Cisco Solution

- Standardized and automated IT infrastructure
- Validated, expandable and fault-tolerant architecture
- Support for standardized compute stacks: FlexPod and vBlock for Rapid Deployment
- User-friendly highly customizable service catalog
- Services led integration services with existing OSS systems
- Validated designs for assured system integration and risk reduction
Thank you.