Build VMware Powered Hybrid Clouds: See How vCloud Director and NSX Work Together to Build True Hybrid Clouds

Boskey Savla

#VMworld #LHC2626BE
Disclaimer

• This presentation may contain product features that are currently under development.
• This overview of new technology represents no commitment from VMware to deliver these features in any generally available product.
• Features are subject to change, and must not be included in contracts, purchase orders, or sales agreements of any kind.
• Technical feasibility and market demand will affect final delivery.
• Pricing and packaging for any new technologies or features discussed or presented have not been determined.
Agenda

1. VMware Cloud Service Provider Program
2. Hybridity – What/Why?
3. Problems getting from point A → Point B
4. vCloud Director and NSX – Our Heros!
5. Architecture and various Hybrid Paths
6. Demo
7. Q & A
VMware Cloud Service Provider Program
VMware Cloud Provider Name Change

vCloud Air™ Network

Is Now

CLOUD PROVIDER™ PROGRAM
VMware Cloud Provider Program

- VMware owned and operated
- Seamless integration from private cloud
- Single support call

>4,000 partners
Established program
Global reach
The world’s largest network of validated cloud services based on VMware technology, providing our customers with unprecedented flexibility and choice of cloud providers on a local basis.

The VMware Cloud Provider Program covers >99% of the cloud TAM*

*Gartner Forecast: Public Cloud Services, Worldwide, 2012-2018, 1Q14 Update
Hybridity

Why? What? Paths?
# Connecting Sites – Data Center Extension

## Layer 2 Network Extension:
- Seamless VM migration (incl. Long distance vMotion) w/o IP address change
- May require Egress Optimization
- Reduced Interoperability

## Layer 3 Network Extension:
- Better Interoperability (standard protocols, i.e. IPSEC)
- Simple routing: no Egress Optimization required
- IP addresses must change when VMs migrate

## Remote User Access VPNs:
- Easy to use
- Simple network requirements (usually L3)
- Reduced Interoperability
Connecting Sites – Cross Sites

Multi Site Management:
• Single pane of Management for multiple sites
• Manage cross site vCenter Servers
• Higher Operational Efficiency

Disaster Recovery:
• Manage Multi site Disaster Recovery Solution
• Preserve IP Addressing during Failover
Connecting Sites – Application

SSL VPN:
• Access to servers running in private, DMZ environment over VPN (Client based mode)
• Access web based servers over a browser based portal (Web Access Mode)
• Remote Authentication via Active Directory, RSA Secure ID, LDAP, Radius

Application Load Balancing
• Use edge Gateway and Load balancers to define traffic distribution
• Connect clients on prem or in branch offices to central workloads
Hybrid Cloud Journey – For an End Consumer

- Define Cloud Endpoint
- Identify and Request Capacity
- Determine Hybrid Path to Cloud
- Establish and Connect
Hybrid Cloud Journey – For an End Consumer

- Identify what cloud endpoint to talk to
- Identify what are the Hybridity needs
  - Applications that need DR?
  - Migrate Apps to cloud
  - Extend Datacenter networks
- Identify access/users that will have access to cloud resources

Define Cloud Endpoint
Hybrid Cloud Journey – For an End Consumer

- Capacity Planning
  - # CPU?
  - Networks
  - Public IP’s
  - Storage requirements
- Access Information
- Direct Connect requirements?
- Service delivery type?
- SLA’s

Define Cloud Endpoint

Identify and Request Capacity

Determine Hybrid Path to Cloud
Hybrid Cloud Journey – For an End Consumer

- What kind of connectivity will I need?
  - Do I have to Re-IP my workloads
  - How do we transfer workloads
- Management of remote environment
- Security
  - What kind of policies will be in place
- Load balancing needs
- How do I bridge my on prem network to cloud networks?
Hybrid Cloud Journey – For an End Consumer

- Identity management
- User portals
Hybrid Cloud Journey – For a Service Provider

Identify and abstract resource for Tenant

Allocate Resources

Publish Hybrid paths to Tenant

Authenticate and Connect
Hybrid Cloud Journey – For a Service Provider

- Estimate Customer resource needs
- Find a place that fits customer needs
  - Which vCenter can I use?
  - Do I have enough storage in it?
  - What vLAN’s can I use for this customer?
Hybrid Cloud Journey – For a Service Provider

- Configure vCenter server/Resource Pool
- Carve out Storage and make it available to vCenter server
- Carve out vLAN’s
  - Make the network Routable across the backend
- Create Firewall policies identified by customer
- Secure and separate the environment against other customers

Allocate Resources

Publish Hybrid paths to Tenant
Hybrid Cloud Journey – For a Service Provider

- Create users and groups to tenant environments
  - Consider admin/user roles
- Assign Public IP’s to access remote environments
- Manage user request for various services

Publish Hybrid paths to Tenant
### Lets Recap....

<table>
<thead>
<tr>
<th>Current State</th>
<th>Ideal State</th>
<th>Solution</th>
<th>vCD</th>
<th>NSX</th>
</tr>
</thead>
<tbody>
<tr>
<td>Estimate Customer resource needs</td>
<td>Automatically identify resource and placement</td>
<td>Software defined Allocation Models</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Find a place that fits customer needs</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Which vCenter can I use?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do I have enough storage in it?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>What vLAN’s can I use for this customer?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Configure vCenter server/Resource Pool</td>
<td>Automatically Identify</td>
<td>Software Defined allocation Model</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>• Carve out Storage and make it available to vCenter server</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Carve out vLAN’s</td>
<td>Automatically Networking with Software</td>
<td>Overlay Virtual Networks</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>• Make the network Routable across the backend</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create Firewall policies identified by customer</td>
<td>Give Customer control to define</td>
<td>Self service Firewall, Overlay Virtual Networks, Software Edge Firewalls</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Secure and separate the environment against other customers</td>
<td>Automatic</td>
<td>Overlay Virtual Networks, Software Edge Firewalls</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Introducing! Our Hero's!

- vCloud Director (vCD)
- NSX
What Is vCloud Director?

VMware vCloud Director orchestrates the provisioning of hybrid clouds that are ready for consumption in a matter of minutes.
vCloud Director: Datacenter Resource Consolidation

- Automate Policy Based Compute Pools
- Automate Creation of Tenant Networks
- Update Network Policies

Data Center Resource Consolidation
vCloud Director: Software Defined Allocation (Automation)

Infrastructure Automation
- Automate Policy Based Compute Pools
- Automate Creation of Tenant Networks
- Update Network Policies

Service Provider Infrastructure Automation

Resource Request
- x Ghz CPU
- x GB memory
- xIOPS

Resource Allocation Policy?

vCloud® Air Network Cloud

Resource Pool A
Resource Pool B

vCenter Resource Pools

Customer A

Service Provider

Customer B
vCloud Director: Multi Tenant

Multi Tenancy
- Isolation of Compute, Storage and Network Resources
- Identity Management

Tenant Virtual Data Center Isolation

Provider VDC

Org VDC 1 (Customer X)
- VM
- Virtual Machine

Org VDC 1 (Customer Y)
- VM
- Virtual Machine

NSX Edge/vCNS Edge
- Org vDC Networks (X)
- Org vDC Networks (Y)

vSphere
- Resource Pool X
- Resource Pool Y
- Storage Profile (Gold)
- Storage Profile (Silver)
What Does NSX Do?

Provide Logical Networking services to Virtual Networks

Decouples Network from Hardware

Provides inside Perimeter Security

Presents Physical Networking Services logically to Virtual Networks

Builds Network segments and isolation for Multi-tiered applications

Physical Gateway + Router

Firewall, VPN

Post-Hypervisor

Hypervisor + NSX

Hypervisor

vSwitch

x86

Storage

Network Interface

Distributed Routing and Firewall Services

Logical Networking Services

vSwitch1

VM

VM

VM

VM

vSwitch2

VM

VM

VM

VM

vSwitch3

VM

VM

VM

VM

Hypervisor

NSX

x86

Storage

Network Interface

VMworld 2017 Content: Not for publication or distribution
vCD + NSX
**Multi-Tenant Self-Service Service Networking**

**Features**
- Tenants self-manage NSX Advanced edge features
- Tenant self-manage and configure NSX Distributed Firewall for micro-segmentation
- North-bound multi-tenant NSX API for service providers and tenants

**Benefits**
- Drive revenue—Service Providers can offer and monetize self-service consumption of NSX services by tenants
- Improve customer experience—NSX services on SP cloud compatible with on-premises environments
Dynamic Routing

External SP Network

SP-Edge Router

On-Prem Networks

On-prem DC

EDGE GATEWAY

EDGE GATEWAY

EDGE GATEWAY

vDC @vCD

vDC @vCD

vDC @vCD

Multi Tenant Networking + Path to Build Hybrid Cloud

VMworld 2017 Content: Not for publication or distribution
vCD + NSX = Multi Tenant Self Service Networking

vCD Works with NSX and vCenter Switches to:

- Build Virtual overlay (VxLAN) Customer Networks
- These Overlay Networks or Organization vDC networks are Routed to underlying vCenter based virtual Switches (DvSwitch) via NSX Edge Services Gateway
- The NSX Edge service Gateway provides networking services to the Organization Networks
- vCD works with NSX Manager to Automatically deploy NSX Edge gateways and Org Networks

vCD + NSX = Multi Tenant Self Service Networking

Customer Overlay Networks

External Network (vSphere Networks)

Org vDC Network

vSwitches

VM

Org vDC

Security Groups

DFW

NSX Edge Services Gateway

- Distributed Firewall
- Network Routing
- Perimeter Firewall
- DHCP
- NAT
- IPSec/SSL VPN/L2
- Dynamic Routing (OSPF, BGP)
- Load Balancer (L4-L7)
Automated and On-Demand Hybrid Connections

HOW

- vCD works with NSX to identify Org vDC Networks that will be stretched across sites
- vCD enables L2 VPN server/client on the Edge Gateway
- vCD will identify the OrgNetwork being stretched as a trunk interface via NSX Manager
- The Client side can have NSX installed or can use the NSX Standalone Edge installed and trunked to the vLAN being trunked
- Supports both VxLAN to vLAN stretching

ADVANTAGES

- Workloads across the stretched network do not need to be re-IP’ed
- Implement Hybrid Cloud
- Create on-demand Hybrid Networks
- SP’s: Monetize L2 VPN as a Service
Automated and On-Demand Hybrid Connections
…via Layer2 VPN

NSX L2VPN Solution

Enterprise

L2VPN Client

Existing Router

Site A

Standalone Edge

VLAN 50
172.16.10.0/24
Tunnel ID 5

VM1

VLAN 51
172.16.20.0/24
Tunnel ID 6

VM1

SSL

Site A

Uplink Network

VLAN Trunk Interface

Tenant vCD

Edge GW

Provider vDC

Provider Uplink NW
Tenant External Network

Uplink Interface

SSL

Tenant Org vDC

L2 VPN Server

Trunk Interface

VM4

VXLAN 5000
172.16.10.0/24
Tunnel ID 5

VM4

VXLAN 5001
172.16.20.0/24
Tunnel ID 6

 ✓ Simple VM form factor
 ✓ VLANs/VXLANs Trunk support

Stretched Network

VMware Cloud Provider Program Service Provider
Automated and On-Demand Hybrid Connections

...via SSL VPN

ADVANTAGES
• Enables **Hybrid connectivity** between clients and workloads in cloud
• Can connect laptops/mobile devices to workloads in Cloud
• Opportunity for SP’s to **Monetize**

THINGS TO CONSIDER
• Supports client configuration for Windows, Mac and Linux
• Assigns Private IP to incoming client connections
• Local users need to be defined
Automated and On-Demand Hybrid Connections

...via Layer2 VPN

THINGS TO CONSIDER

- Both sites connected via L2 VPN need to have Network that’s trunked to an NSX Edge Gateway
- In vCD, while defining a Org-Network to be stretched,
  - An Existing Network will have to be converted to ‘Enable Sub-interface type’ by right clicking Org Network
  - A new Network will have to have the checkbox on ‘Create as Subinterface’
- Only Routed-Org-Networks can be used for L2 stretching
Tenants Manage Their Own Routing/NAT Tables

...via Dynamic Routing

**HOW**

- Tenants can define Routing protocols by right clicking Edge Gateway -> Configure Services
- **OSPF, BGP** protocols are supported
Tenants Configure Their Own Firewall for In-cloud Workloads

...Distributed Firewall as a Service

HOW

• Tenant can define DFW rules by right clicking Org vDC, manage firewall
• Define Source and destination, Service type and direction

THINGS TO CONSIDER

• DFW rules are applied per Org-vDC
• SP need to add rights in Organization for a Tenant to enable DFW
• Service type can be defined from an OOB service categories
Tenants Configure Their Own Firewall for In-cloud Workloads

...Distributed Firewall as a Service

VCD WORKS WITH NSX TO PROVIDE MULTI-TENANT DISTRIBUTED FIREWALL SERVICE

- Ability to define security policies per Virtual machine
- Secures traffic flowing within the same Organization network
- Manages East-west traffic
- Define Firewall policies on various Objects
  - VM’s, IP sets, Org vDC, Org vDC Networks etc.

ADVANTAGES

- Provides segmented security to workloads
- Helps execute Industry standard compliance
- Offloads Security management from Service Provider to Tenant
- Gives tenants a self-service portal to manage Security
- Lower service request volume for SP’s
- Opportunity to Monetize service for SP’s
L2 VPN – Walk through
Automated and On-Demand Hybrid Connections
...via Layer2 VPN

NSX L2VPN Solution
L2 VPN vCD Setup (Server)

<table>
<thead>
<tr>
<th>Edge Gateway Settings</th>
<th>Enable Distributed Routing</th>
<th>External IP Allocation</th>
<th>Re-Deploy</th>
<th>Synchronize Syslog Server Settings</th>
<th>Modify Form Factor</th>
<th>Delete</th>
<th>Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Edge Gateway - EdgeB

#### Distributed Firewall

<table>
<thead>
<tr>
<th>No.</th>
<th>Name</th>
<th>Type</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>dns</td>
<td>Internal High</td>
<td>Internal</td>
<td>192.168.1.1</td>
<td>udp:53:any</td>
<td>Accept</td>
</tr>
<tr>
<td>2</td>
<td>default rule for ingress traffic</td>
<td>Default Policy</td>
<td>Any</td>
<td>Any</td>
<td>tcp:53:any</td>
<td>Accept</td>
</tr>
</tbody>
</table>

**Note:**
- The firewall rules are enabled.
- Show only user-defined rules is disabled.

---

**VMworld 2017 Content: Not for publication or distribution**
### Edge Gateway - EdgeB

**IPsec VPN**

<table>
<thead>
<tr>
<th>Distribution Firewall</th>
<th>DHCP</th>
<th>NAT</th>
<th>Routing</th>
<th>Load Balancer</th>
<th><strong>VPN</strong></th>
<th>SSL VPN Plus</th>
<th>Certificates</th>
<th>Grouping Objects</th>
<th>Statistics</th>
<th>Edge Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPsec VPN</td>
<td>L2 VPN</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**IPsec VPN Configuration**

<table>
<thead>
<tr>
<th>Activation Status</th>
<th>Global Configuration</th>
<th>Logging Settings</th>
<th>IPsec VPN Sites</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**IPsec VPN Service Status**

- [ ]
Edge Gateway - EdgeB

L2 VPN

You have unsaved changes.

Enabled

L2VPN Mode

Server
Client

Server Global  Server Sites

Site Configuration Details

Stretched Interfaces

Deleted

DELETE CONFIGURATION
L2 VPN vCenter Setup (Client)
vCloud Director Extender

PREVIEW
Tasks you can perform next:

- **CONNECT vCD ORG**
  You can connect to vCD Org as a vCD Org to which you can migrate a VM or extend a network. Please also refer to the vCD Orgs tab.

- **NEW MIGRATION**
  After you connect to vCD Org, you can start your migration flow. Please also refer to the Migrations tab.

- **NEW EXTENSION**
  After you connect to vCD Org, you can start to extend your local network to the cloud. Please also refer to the DC Extensions tab.

Recent Notifications (3/38)
VMware Cloud Provider Sponsors
Visit their booths at Solution Exchange!

IBM

OVH

Skytap

CenturyLink

Fujitsu

Virtustream

Spectrum Enterprise

Rackspace

Iland
# Recommended Sessions – VMware Cloud Partners

Accelerate your digital business transformation with VMware Cloud Provider Partners. Learn more: [cloudproviders.vmware.com](http://cloudproviders.vmware.com)

<table>
<thead>
<tr>
<th>SESSION ID</th>
<th>NAME</th>
<th>TIME</th>
</tr>
</thead>
<tbody>
<tr>
<td>LHC3139SU</td>
<td>Spotlight Session: Achieving Success in a Multi-Cloud World</td>
<td>Wednesday, 11:00</td>
</tr>
<tr>
<td>LHC1661BU</td>
<td>Getting Started with the VMware Cloud Provider Program (Technical Tips and Tricks)</td>
<td>Tuesday, 11:00</td>
</tr>
<tr>
<td>LHC1539BU</td>
<td>Paving the Way to the Hybrid Cloud with VMware Cloud Service Providers and vCloud Availability</td>
<td>Tuesday, 12:30</td>
</tr>
<tr>
<td>LHC1716BU</td>
<td>On-Ramp to the Cloud: Migration Tools and Strategies</td>
<td>Tuesday, 14:00</td>
</tr>
<tr>
<td>LHC2573BU</td>
<td>Achieving Hybrid Cloud Data Agility Securely with VMware NSX</td>
<td>Tuesday, 17:00</td>
</tr>
<tr>
<td>LHC1746BU</td>
<td>Automating Disaster Recovery with vCloud Availability for vCloud Director and vRealize Orchestrator</td>
<td>Wednesday, 8:00</td>
</tr>
<tr>
<td>LHC2424BU</td>
<td>200 to 40,000 VMs in 24 Months: Building Highly Scalable SDDC on Hybrid Cloud: Real-World Example</td>
<td>Wednesday, 8:00</td>
</tr>
<tr>
<td>LHC2626BU</td>
<td>Build VMware Powered Hybrid Clouds: See How vCloud Director and NSX work together to build true Hybrid Clouds</td>
<td>Wednesday, 11:00</td>
</tr>
<tr>
<td>LHC1753BU</td>
<td>Case Study: How VMware NSX Is Empowering a Service Provider to Help Customers Achieve and Maintain Industry Compliance</td>
<td>Wednesday, 12:30</td>
</tr>
<tr>
<td>LHC1809BU</td>
<td>Use NSX to Deploy a Secure Virtual Network Bridging Multiple Locations for a True Hybrid Cloud</td>
<td>Thursday, 13:30</td>
</tr>
</tbody>
</table>
Please fill out your survey.
Take a survey and enter a draw for a VMware company store gift card.
Thank You