VMware NSX and vCloud Automation Center Integration Technical Deep Dive

Ray Budavari, VMware, Inc
Zackary Kielich, VMware, Inc
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  Background
2  NSX and vCloud Automation Center
3  What’s new in NSX & vCAC 6.1
4  Deployment Topologies
5  Demonstration
6  Q&A
Business Wants Agility. IT Wants Control.
Need to align requirements from multiple stakeholders

I just want my app - FAST.
Don’t ask me about networking and security.

Fast is good but I know exactly what
I need to connect, secure and scale my app.

I need to ensure SLAs for connectivity,
security & availability when I don’t even own
the infrastructure.

Cloud Consumer

Cloud Admin

If the network goes down, I have to
answer for it. ‘Self-service’ could
mean ‘no service’ if I don’t control
how systems are connected.

Zero trust ensures only clean &
compliant systems in the data center– but doesn’t self-service
mean loss of this control?

Users want to scale their app tiers on-
demand but they have to wait for me to
install and configure their service. Am I the
bottleneck to self-service IT?

Network Admin

Security Admin

Load Balancer Admin
Traditional Infrastructure Provisioning

Days - Weeks

Wait → Wait → Wait → Work

Manual effort

Network

Switch
Connect Ethernet cables, configure switch port, VLANs, access control lists, assign IP addresses

Router
Configure router interface to connect to switch ports. Configure routing protocols.

Firewall
Connect networks to firewall appliances, configure firewall rules based on physical constructs e.g. IP address and VLANs

Load Balancer
Connect networks to load balancer appliances, create and populate load balancer pool, assign Virtual IP Address to external interface

NETWORK OPS
SECURITY OPS
LOAD BALANCING ADMIN
<table>
<thead>
<tr>
<th></th>
<th>Agenda</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Background</td>
</tr>
<tr>
<td>2</td>
<td><strong>NSX and vCloud Automation Center</strong></td>
</tr>
<tr>
<td>3</td>
<td>What’s new in NSX &amp; vCAC 6.1</td>
</tr>
<tr>
<td>4</td>
<td>Deployment Topologies</td>
</tr>
<tr>
<td>5</td>
<td>Demonstration</td>
</tr>
<tr>
<td>6</td>
<td>Q&amp;A</td>
</tr>
</tbody>
</table>
Why NSX?
Support for Detailed, Programmable Application Topologies

Logical Switching, Routing, Firewall, Load Balancing

Security Policies

- **“Default”**
  - Firewall – Access shared services (DNS, AD)
  - Anti-Virus – Scan Daily

- **“Standard Web”**
  - Firewall – allow inbound HTTP/S, allow outbound ANY
  - IPS – prevent DOS attacks, enforce acceptable use

- **“Standard App”**
  - Firewall – allow inbound TCP 8443, allow outbound SQL

- **“Standard Database”**
  - Firewall – allow inbound SQL
  - Vulnerability Management – Weekly Scan
vCAC integrated with NSX

Dynamic Configuration and Deployment of NSX Logical Services

**NSX**

- Logical Switch
- Logical Router
- Logical Firewall
- Logical Load Balancer

**vCloud Automation Center**

- Service Catalog
- Resource Reservation
- Cloud Management Platform
- Multi-Machine Blueprint
- Security Policies
- Security Groups
- Network Profiles

**On Demand Application Delivery**

- Web
- App
- Database
vCAC Application Deployment Topologies
Support for Multiple Network Topologies

Multi-Tier App, Multiple Networks

Multi-Tier App, Single Flat Network
vCAC Application Deployment Topologies
Support for Multiple Network Topologies

Multi-Tier App, Multiple Networks

Multi-Tier App, Single Flat Network
Cloud Consumer Profile

The Typical User Wants Easy

I just want my app. Don’t ask me about networking and security.

Pre-defined by Cloud Architect

Cloud Consumer

Cloud Admin

Leverage Templates

Policy=Default_TestDev

Web

App

DB
Cloud Consumer Profiles
Some Users Want to Customize

I know exactly what I need for connecting, securing and scaling my app. Let me deal with it.
Understanding vCAC Network Profiles

- Network Admins pre-define ‘network profiles’ for connectivity
- Cloud Admins define multi-machine blueprints using these pre-defined network profiles
- Certain network types can be combined in a multi-machine blueprint

**4 NETWORK PROFILES**
- External
- Routed
- NAT
- Private

*Any upstream Router - can also be NSX Distributed Logical Router or NSX Edge Services GW*
Understanding vCAC Network Profiles

- Network Admins pre-define ‘network profiles’ for connectivity
- Cloud Admins define multi-machine blueprints using these pre-defined network profiles
- Certain network types can be combined in a multi-machine blueprint

**Why use a NAT Network Profile?**
When you have overlapping IP addresses across networks that need external connectivity.

**Why use a PRIVATE Network Profile?**
When you don’t need external connectivity.

e.g. “I want to do performance testing on my app, but I don’t need to set up remote access for end users”
Agenda

1 Background
2 NSX and vCloud Automation Center
3 What’s new in NSX & vCAC 6.1
4 Deployment Topologies
5 Demonstration
6 Q&A
Feature Overview - vCloud Automation Center 6.1 & NSX

Range of features from pre-created to on-demand network and security services.

**Connectivity**

- **Network Profiles for On-Demand Network Creation**
  - Define routed, NAT, private, external profiles for variety of app topologies
  - Option to connect to pre-created networks (logical or physical)

- **NSX Distributed Logical Router (DLR)**
  - Optimize for east-west traffic by connecting to pre-created DLR

**Security**

- **On-Demand Micro-segmentation**
  - Automatic creation of security group per app w/ default deny firewall rules

- **Apply Firewall and Advanced Security Policies**
  - Select pre-defined NSX security policies to apply to app/tier
  - Antivirus, DLP, Intrusion Prevention, Vulnerability Mgmt

- **Connect Business Logic to Security Policy**
  - Select pre-defined NSX security tag which is applied to workload and interpreted by NSX to place in pre-defined security group

**Extensibility**

- **Business Logic moved to NSX vCO Plugin**
  - Allows vCO workflows to be leveraged by Advanced Service Designer

**Availability**

- **On-demand Load Balancer in One-Armed Mode or Inline Mode**
  - Plus option for using pre-created load balancing
vCNS Model \[\text{vCloud Automation Center}\] \[\text{NSX for vSphere}\] \[\text{vCenter Server}\] \[\text{ESXi}\]
vCARE Networking and Security Architecture – 6.1 release

vCloud Automation Center

NSX Model

Rest API

NSX vCO Plugin

Rest API

NSX

vCenter Server

vSphere API

AMQP

ESXi
NSX vCenter Orchestrator Plugin

Benefits of abstracting with vCO

Benefits

• Ability to support multiple product versions (vCNS, NSX) transparently to vCAC
• Network and security workflows are decoupled from policy engine, enabling more rapid release and update to workflows
• Ability to deliver fixes and updates more rapidly
• Easier to extend/customize workflows by adding your own logic or leveraging other systems
• Provide Self Service access to NSX vCO workflows through Advanced Service Designer

Note: Initial version of NSX vCO Plugin is limited to functionality required by vCAC and is only supported for these out of the box workflows
NSX Distributed Logical Router

- Optimized routing for East/West traffic directly at the source Hypervisor, distributed across all Hosts
- No virtual appliance required for Routing
- Dynamic Routing available (OSPF and BGP)
- Previously Distributed Logical Routing could only be leveraged on External Networks

The Network Admin will configure a pre-defined Distributed Logical Router that can then be shared by multiple networks provisioned on-demand by vCAC.

Scales up to 1000 logical interfaces!
vCAC Routed Gateways

- Blueprint with routed network profile must use a routed gateway to talk to external networks
- Routed gateway is defined at the Reservation level for routed and external profiles
  - One gateway only per External Network Profile
  - Determines whether Distributed Logical Router or NSX Edge Gateway will be used by a Routed Network Profile
NSX Security Groups & Security Policies

- End-Users and Cloud Admins are able to select pre-defined **security policies** already approved by the Security Admin in NSX.
- **Security policies** are applied to one or more **security groups** where workloads are members.
- These **security groups** are created on-demand by vCAC at deployment time.

**Members (VM, vNIC) and Context (user identity, security posture)**

**Services** (Firewall, antivirus, IPS etc.) and **Profiles** (labels representing specific policies)

- "Standard Web":
  - **Firewall** – allow inbound HTTP/S, allow outbound ANY
  - **IPS** – prevent DOS attacks, enforce acceptable use
NSX Security Tags

- NSX Security Tags can be used to define **IF/THEN** workflows for security services, e.g. **IF** user selects a “Finance” application, **THEN** place the VM in the “Finance” security group.

---

**Step 1:** Security Admin pre-defines a **Security Group** and a **Security Policy** with dynamic membership based on a **Security Tag**

**Step 2:** Cloud Admin creates a Multi-Machine Blueprint which sets a **Security Tag**. Cloud Admin needs no knowledge of Security Groups or Security Policies.
NSX Security Tags

- NSX Security Tags can be used to define **IF/THEN** workflows for security services, e.g. **IF** user selects a “Finance” application, **THEN** place the VM in the “Finance” security group.

**Step 3:** End-User requests Application via the *Service Catalog*

**Step 4:** VM is automatically deployed with its *Security Tag*

**Step 5:** VM is dynamically assigned to the relevant pre-defined *Security Group*
NSX Application Isolation

- Application Isolation provides an optional first level of security. When selected all inbound and outbound application access is blocked, while inter application traffic is permitted.
- Component level Security Policies are applied at a higher precedence to permit selected traffic.
NSX Load Balancing

- vCAC leverages NSX for both on-demand and pre-created Logical Load Balancing
- If an NSX Edge is the default gateway for component VMs, Inline Load Balancing is used
- If the component VMs are connected to a network using the Distributed Logical Router or an External Network then Load Balancing is configured for One-Arm mode
NSX Load Balancing

- vCAC leverages NSX for both on-demand and pre-created Logical Load Balancing
- If an NSX Edge is the default gateway for component VMs, Inline Load Balancing is used
- If the component VMs are connected to a network using the Distributed Logical Router or an External Network then Load Balancing is configured for One-Arm mode
On Demand Micro-Segmentation

Isolation

Dev

Test

Production

No Communication Path

Segmentation

Web

App

DB

Controlled Communication Path

Advanced Services

Web

App

DB

Advanced Services Communication Path
## Agenda

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Background</td>
</tr>
<tr>
<td>2</td>
<td>NSX and vCloud Automation Center</td>
</tr>
<tr>
<td>3</td>
<td>What’s new in NSX &amp; vCAC 6.1</td>
</tr>
<tr>
<td>4</td>
<td>Deployment Topologies</td>
</tr>
<tr>
<td>5</td>
<td>Demonstration</td>
</tr>
<tr>
<td>6</td>
<td>Q&amp;A</td>
</tr>
</tbody>
</table>
vCAC with NSX – On Demand Deployment Model

- 2 Tiers of Routing
  - Distributed Logical Router or NSX Edge for Application Router
  - NSX Edge for Provider Router

- Dynamic Routing externally

- Dynamic Routing (DLR), Static Routing or NAT internally (Edge)

On Demand Model is typically used for more dynamic Test/Dev style workloads, particularly when there is a requirement for overlapping IP addresses.
vCAC with NSX – Pre Created Deployment Model

- **2 Tiers of Routing**
  - Distributed Logical Router for Application Router
  - NSX Edge for Provider Router

- **Dynamic Routing**

- **Use existing LS as external network profiles**

- **One Arm Load Balancing on demand** (vCNS Edge in 6.0, NSX Edge in 6.1)

- **Pre-Created model is typically used with Production or more static workloads and the application topology is multi-tier on a single network**
vCAC with NSX – Pre Created Deployment Model

- **2 Tiers of Routing**
  - Distributed Logical Router for Application Router
  - NSX Edge for Provider Router

- **Dynamic Routing**

- **Use existing LS as external network profiles**

- **One Arm Load Balancing on demand** (vCNS Edge in 6.0, NSX Edge in 6.1)

- Pre-Created model is typically used with Production or more static workloads and the application topology is multi-tier on a single network
vCAC with NSX – Pre Created Deployment Model

- **2 Tiers of Routing**
  - Distributed Logical Router for Application Router
  - NSX Edge for Provider Router
- **Dynamic Routing**
- **Use existing LS as external network profiles**
- **One Arm Load Balancing on demand** (vCNS Edge in 6.0, NSX Edge in 6.1)

Pre-Created model is typically used with Production or more static workloads and the application topology is multi-tier on a single network
vCAC with NSX – Pre Created Deployment Model

- **2 Tiers of Routing**
  - Distributed Logical Router for Application Router
  - NSX Edge for Provider Router

- **Dynamic Routing**
  - Use existing LS as external network profiles

- **One Arm Load Balancing on demand** (vCNS Edge in 6.0, NSX Edge in 6.1)

- Pre-Created model is typically used with Production or more static workloads and the application topology is multi-tier on a single network
vCAC with NSX – Pre Created Deployment Model

- **2 Tiers of Routing**
  - Distributed Logical Router for Application Router
  - NSX Edge for Provider Router

- **Dynamic Routing**
  - Use existing LS as external network profiles

- **One Arm Load Balancing on demand** (vCNS Edge in 6.0, NSX Edge in 6.1)

- Pre-Created model is typically used with Production or more static workloads and the application topology is multi-tier on a single network

---

- **External Networks**
  - Transit Uplink
    - 192.168.10.0/24 (External Network Profile)
  - Distributed Logical Router
  - Dynamic Routing (OSPF, BGP) with ECMP

- **Scale Out Provider Logical Router (NSX 6.1)**
  - MMS 1 VMs
  - MMS 2 VMs

- **Prod-01 Logical Switch**
  - 172.16.50.0/24 (External Network)

- **Dev-01 Logical Switch**
  - 172.16.60.0/24 (External Network)
vCAC with NSX – Pre Created Deployment Model

- **2 Tiers of Routing**
  - Distributed Logical Router for Application Router
  - NSX Edge for Provider Router

- **Dynamic Routing**

- **Use existing LS as external network profiles**

- **One Arm Load Balancing on demand** (vCNS Edge in 6.0, NSX Edge in 6.1)

- **Pre-Created model is typically used with Production or more static workloads and the application topology is multi-tier on a single network**

---

- **Scale Out Provider Logical Router (NSX 6.1)**
  - MMS 1 VMs
  - MMS 2 VMs

---

- **Transit Uplink**
  - 192.168.10.0/24 (External Network Profile)

---

- **Dynamic Routing**
  - OSPF, BGP
  - with ECMP

---

- **Prod-01 Logical Switch**
  - 172.16.50.0/24 (External Network)

---

- **Dev-01 Logical Switch**
  - 172.16.60.0/24 (External Network)

---

- VMs
  - Prod Web SG A
  - Prod App SG A
  - Prod DB SG A
  - Prod Web SG B
  - Prod DB SG B
  - App SG B
vCAC with NSX – Pre Created Deployment Model

- **2 Tiers of Routing**
  - Distributed Logical Router for Application Router
  - NSX Edge for Provider Router

- **Dynamic Routing**

- **Use existing LS as external network profiles**

- **One Arm Load Balancing on demand** (vCNS Edge in 6.0, NSX Edge in 6.1)

- Pre-Created model is typically used with Production or more static workloads and the application topology is multi-tier on a single network

![Diagram showing network architecture with vCNS and NSX components]
**vCAC with NSX – Pre Created Deployment Model**

- **2 Tiers of Routing**
  - Distributed Logical Router for Application Router
  - NSX Edge for Provider Router

- **Dynamic Routing**
  - Use existing LS as **external network profiles**
  - **One Arm Load Balancing on demand** (vCNS Edge in 6.0, NSX Edge in 6.1)

- **Pre-Created model is typically used with Production or more static workloads and the application topology is multi-tier on a single network**

---

**Diagram Details**

- **External Networks**
  - **Prod-01 Logical Switch**: 172.16.50.0/24 (External Network)
  - **Dev-01 Logical Switch**: 172.16.60.0/24 (External Network)

- **Scale Out Provider Logical Router (NSX 6.1)**
  - MMS 1 VMs
  - MMS 2 VMs
  - MMS 3 VMs
  - MMS 4 VMs

- **Uplinks**
  - Transit Uplink
    - 192.168.10.0/24 (External Network Profile)
  - Dynamic Routing (OSPF, BGP) with ECMP
vCAC with NSX – Pre Created Deployment Model

- **2 Tiers of Routing**
  - Distributed Logical Router for Application Router
  - NSX Edge for Provider Router

- **Dynamic Routing**

- **Use existing LS as external network profiles**

- **One Arm Load Balancing on demand** (vCNS Edge in 6.0, NSX Edge in 6.1)

- **Pre-Created model is typically used with Production or more static workloads and the application topology is multi-tier on a single network**

Scale Out Provider Logical Router  (NSX 6.1)

- Prod-01 Logical Switch 172.16.50.0/24 (External Network)
- Dev-01 Logical Switch 172.16.60.0/24 (External Network)

- Dynamic Routing (OSPF, BGP) with ECMP
- Transit Uplink 192.168.10.0/24 (External Network Profile)

- MMS 1 VMs
- MMS 2 VMs
- MMS 3 VMs
- MMS 4 VMs
Agenda

1 Background
2 NSX and vCloud Automation Center
3 What’s new in NSX & vCAC 6.1
4 Deployment Topologies
5 Demonstration
6 Q&A
Live Demonstration
<table>
<thead>
<tr>
<th></th>
<th>Agenda</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Background</td>
</tr>
<tr>
<td>2</td>
<td>NSX and vCloud Automation Center</td>
</tr>
<tr>
<td>3</td>
<td>What’s new in NSX &amp; vCAC 6.1</td>
</tr>
<tr>
<td>4</td>
<td>Deployment Topologies</td>
</tr>
<tr>
<td>5</td>
<td>Demonstration</td>
</tr>
<tr>
<td>6</td>
<td>Q&amp;A</td>
</tr>
</tbody>
</table>
Questions

VMworld Hands on Labs

• HOL-SDC-1413 IT Outcomes - Faster Delivery of Infrastructure and Apps through Automation
• HOL-SDC-1424 VMware NSX in the SDDC
<table>
<thead>
<tr>
<th>Existing</th>
<th>New Name</th>
<th>New SaaS</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCenter Operations Management Suite</td>
<td>vRealize Operations</td>
<td>vRealize Air Operations</td>
</tr>
<tr>
<td>vCloud Automation Center</td>
<td>vRealize Automation</td>
<td>vRealize Air Automation</td>
</tr>
<tr>
<td>IT Business Management</td>
<td>vRealize Business</td>
<td>vRealize Air Business</td>
</tr>
</tbody>
</table>

Other examples:
- vRealize Log Insight – formerly known as Log Insight
- vRealize Orchestrator – formerly known as vCenter Orchestrator
vRealize™ Suite 6

A cloud management platform purpose-built for the hybrid cloud

Includes:
• vCenter Operations Management Suite
• vCloud Automation Center
• IT Business Management Suite Standard
• vCenter Log Insight

vCloud Suite value proposition extended to hybrid cloud

Available: Q3 2014
Thank You

Ray Budavari (@rbudavari)
Zack Kielich (@zackomatic)

http://www.vmware.com/products/nsx/
Fill out a survey

Every completed survey is entered into a drawing for a $25 VMware company store gift certificate
VMware NSX and vCloud Automation Center Integration Technical Deep Dive

Ray Budavari, VMware, Inc
Zackary Kielich, VMware, Inc