# Table of Contents

Lab Overview - HOL-1806-02-SLN - Automate IT: Making Private Cloud Easy ..............2  
   Lab Guidance ........................................................................................................................................3  
Module 1 - Better Together: vRealize Automation and NSX App Centric Networking &  
   Security (45 Minutes)................................................................................................................................9  
      Introduction........................................................................................................................................10  
      Converged Blueprint .........................................................................................................................12  
      On Demand Security Groups(ODSG) .............................................................................................18  
      On Demand Routed Networks ........................................................................................................28  
      On Demand Load Balancer .............................................................................................................40  
   Conclusion.........................................................................................................................................51  
Module 2 - vRealize Automation Day 2 Actions for NSX (30 Minutes) ......................52  
   Introduction........................................................................................................................................53  
   NSX-Day 2 Security Groups ..............................................................................................................54  
   NSX-Day 2 Reconfigure Of a Deployed Load Balancer .................................................................64  
   Conclusion.........................................................................................................................................71
Lab Overview -
HOL-1806-02-SLN -
Automate IT: Making Private Cloud Easy
Lab Guidance

Note: It will take more than 90 minutes to complete this lab. You should expect to only finish 2-3 of the modules during your time. The modules are independent of each other so you can start at the beginning of any module and proceed from there. You can use the Table of Contents to access any module of your choosing.

The Table of Contents can be accessed in the upper right-hand corner of the Lab Manual.

Lab Module List:

- **Module 1 - Better Together: vRealize Automation and NSX App Centric Networking & Security** (45 Minutes) (Advanced) In this module users will see how we can build out network services on a vRealize Automation blueprint to deliver a holistic multi-tier application architecture. We will cover building multiple networks and security groups on the same blueprint.

- **Module 2 - vRealize Automation Day 2 Actions for NSX** (30 minutes) (Basic) In this module we will show how to add and remove an existing security group to a deployed blueprint. We will also show how to scale out an existing deployment to add another node to a load balancer. This will show how we can network services from a day two perspective.

Lab Captains:

- **Module 1 - Chris Saunders, Staff Systems Engineer, USA**
- **Module 2 - Chris Saunders, Staff Systems Engineer, USA**

This lab manual can be downloaded from the Hands-on Labs Document site found here:

[http://docs.hol.vmware.com](http://docs.hol.vmware.com)

This lab may be available in other languages. To set your language preference and have a localized manual deployed with your lab, you may utilize this document to help guide you through the process:

1. The area in the RED box contains the Main Console. The Lab Manual is on the tab to the Right of the Main Console.
2. A particular lab may have additional consoles found on separate tabs in the upper left. You will be directed to open another specific console if needed.
3. Your lab starts with 90 minutes on the timer. The lab cannot be saved. All your work must be done during the lab session. But you can click the EXTEND to increase your time. If you are at a VMware event, you can extend your lab time twice, for up to 30 minutes. Each click gives you an additional 15 minutes. Outside of VMware events, you can extend your lab time up to 9 hours and 30 minutes. Each click gives you an additional hour.

Alternate Methods of Keyboard Data Entry

During this module, you will input text into the Main Console. Besides directly typing it in, there are two very helpful methods of entering data which make it easier to enter complex data.
Click and Drag Lab Manual Content Into Console Active Window

You can also click and drag text and Command Line Interface (CLI) commands directly from the Lab Manual into the active window in the Main Console.

Accessing the Online International Keyboard

You can also use the Online International Keyboard found in the Main Console.

1. Click on the Keyboard Icon found on the Windows Quick Launch Task Bar.
Click Once in the Active Console Window

In this example, you will use the Online Keyboard to enter the "@" sign used in email addresses. The "@" sign is Shift-2 on US keyboard layouts.

1. Click once in the active console window.
2. Click on the Shift key.

Click on the @ Key

1. Click on the "@" key.

Notice the @ sign entered in the active console window.
Activation Prompt or Watermark

When you first start your lab, you may notice a watermark on the desktop indicating that Windows is not activated.

One of the major benefits of virtualization is that virtual machines can be moved and run on any platform. The Hands-on Labs utilizes this benefit and we are able to run the labs out of multiple datacenters. However, these datacenters may not have identical processors, which triggers a Microsoft activation check through the Internet.

Rest assured, VMware and the Hands-on Labs are in full compliance with Microsoft licensing requirements. The lab that you are using is a self-contained pod and does not have full access to the Internet, which is required for Windows to verify the activation. Without full access to the Internet, this automated process fails and you see this watermark.

This cosmetic issue has no effect on your lab.

Look at the Lower Right Portion of the Screen

Wait for “Lab Status” to change to green “Ready”
Please check to see that your lab is finished all the startup routines and is ready for you to start. If you see anything other than "Ready", please wait a few minutes. If after 5 minutes your lab has not changed to "Ready", consider restarting the lab.
Module 1 - Better Together: vRealize Automation and NSX App Centric Networking & Security (45 Minutes)
Introduction

In this module users will see how we can build out network services on a vRealize Automation blueprint to deliver a holistic multi-tier application architecture. We will cover building multiple networks and security groups on the same blueprint.

Delivering Application-Centric Network and Security Services vRealize Automation provisions, updates and decommissions network and security services in lockstep with your virtualized applications. Network and security services are deployed as part of the automated delivery of the application, consistent with its connectivity, security, and performance requirements. Automation creates a standardized repeatable process that helps accelerate delivery, reducing the time needed to perform the task. At the same time automation also improves the consistency and reliability of the final configuration by elimination of manual errors. Finally automation reduces operational costs by eliminating many manual tasks, and improves development productivity by delivering application environments to engineers faster. vRealize Automation, used in conjunction with NSX, automates an application’s network connectivity, security, performance, and availability.
Connectivity: Proper network connectivity is fundamental to any business service. Various groups and different applications can have unique requirements. vRealize Automation’s resource reservations, service blueprints and network profiles assure that each application receives the right level of network connectivity, with the appropriate service level. For example, each business group can be provided with reserved network connectivity between the virtual and physical world, or specific mission critical applications can be configured with dedicated virtual switches and routers depending on their performance and reliability needs. In addition, virtual machines can be moved with a tool like VMware vSphere® vMotion® live migration without changes to the virtual machine networking configuration. This allows for the optimal placement of workloads on the compute infrastructure, ultimately leading to reduced capital expenditure.

Security: Ensuring appropriate security policies are applied is one of the most critical steps to delivering and managing your applications and data. Now with vRealize Automation and NSX, applications can be deployed on demand with network security applied at the application level or between application tiers to ensure that firewall rules are placed as close to the virtual machine as possible. This leads to a true defense-in-depth solution that cannot be achieved by other solutions. The IT administrator can define vRealize Automation application blueprints that specify NSX security policies which contain firewall rules, intrusion detection integration, and agentless anti-virus scanning at each application tier to allow application and per-tier security. When the application is provisioned, dynamic security groups are configured with the defined policies to safeguard the service from day one. These services can also be tagged with a security label, for example DB servers, PCI, HIPPA that enforces policies dynamically based on the tags (e.g. type of application) throughout their lifecycle. Finally, application isolation for these business services can also be defined to fence the service from the rest of the network entirely or to deny all traffic to the service except for what is defined in the applied security policies. This granular level of isolation keeps traffic to specific group environments (e.g., development, test, production) or even isolated at the individual application or application tier level.

Performance: vRealize Automation’s governance policies and automated delivery can be used to meet the specific network performance needs of each application being deployed. vRealize Automation can also configure NSX to minimize traffic through the oversubscribed core. Traffic between virtual machines on the same host will remain within the host while still receiving the distributed routing, switching, load-balancing, firewalling, and security services that are required by modern applications.

Availability: vRealize Automation improves application availability through the dynamic configuration of network load balancers in the context of deploying or updating application configurations. NSX load balancer can be used in all phases of the application lifecycle (development, staging, production) without requiring expensive physical hardware or manual configuration of legacy load-balancing components. Depending on vRealize Automation’s application blueprints and network profiles, applications can be added to an existing load balancer pool or configured with their own dedicated load balancers. This integration provides organizations with application centric availability management.
Converged Blueprint

Overview

The Converged Blueprint Designer (CBP) redefines how applications and services are authored, incorporating the full IT services stack using a unified drag-and-drop canvas. NSX has become a first-class citizen of vRealize Automation to provide application-centric networking and security through deep integration between the two products.

Open Browser

1. Click on the Google Chrome taskbar icon
Open vRealize Automation

1. Click on the **vRealize Automation** bookmark
2. Enter in **cloudadmin** in the username field
3. Enter in **VMware1!** in the password field
4. Click **Sign In**
Navigate to the Blueprint Designer

1. Click Design
Open an Existing Blueprint

1. Click on Multi Tier Application on CentOS
View the Blueprint in the Blueprint Editor

There you have it, a fully automated multi-tier application which includes network, application and availability services. This is the converged blueprint designer in all of its glory. As you can see, we have a web tier consisting of 3 nodes with an on-demand load balancer providing application availability and application services are provided by a database tier. Security policies for both web and database services are applied with each deployment ensuring enforcement of desired network policies. In the backend we have a database tier supporting the application. For security we have security groups configured so that every time this blueprint is requested, we enforce our network security policies.

vRealize Automation 7 features a new Blueprint format. A converged blueprint can have one to many components including:

- **Machines**: vCenter, OVH, vCloud Director, Amazon, KVM, Openstack, Citrix Xen, HyperV, SCVMM
- **Network & Security**: Security Group, Load balancer, NAT, Routed networks
- **Software (Install, configure, start, uninstall)**: Scripts to setup the OS or to install and configure applications
- **XaaS**: Workflows (I.E virtual machine customization, guest operations)

Combining these allow for the designing of complex applications

For example using the vRealize Automation design canvas you can put together a multiple instance machine to deploy cluster nodes with XaaS components to create shared disks and software components to install and configure the Operating System...
and application layers. In the following lessons, we will explore various key components NSX which can be used in the vRA Design canvas while building out a converged blueprint.
On Demand Security Groups (ODSG)

Overview

Network security, for a long time, has worked off of the old Russian maxim, "trust but verify". Trust a user, but verify it's them. However, today's network landscape -- where the internet of things, the cloud, and more are introducing new vulnerabilities -- makes the "verify" part of "trust but verify" difficult and inefficient. We need a simpler security model. That model: Zero Trust.

Forrester Research coined the term "Zero Trust" to describe a model that prevents common and advanced persistent threats from traversing laterally inside a network. This can be done through a strict, micro-granular security model that ties security to individual workloads and automatically provisions policies. It's a network that doesn't trust any data packets. Everything is untrusted. Hence: Zero Trust.

In this module, we will show you how to automate a zero trust network with vRealize Automation. In a blueprint we can drag and drop an on demand security group. This creates a new Security Group and binds one or more existing Security Policies. The desired security policies are added to the ODSG during blueprint configuration. This will ensure your deployed virtual machines, get the policies they require.

Open a Browser

1. Click on the Google Chrome taskbar shortcut
Log In to vRealize Automation

1. Type cloudadmin into the username field
2. Type VMware1! into the password field
3. Click Sign In
Navigate to the Blue Print Designer

1. Click on the **Design** tab

Copy an Existing Blue Print and Create New One
1. Click on the **CentOS** blueprint row to highlight it
2. Click on **Copy**

This is one of the value adds of the blueprint designer. We can copy existing blue prints and use them. We can even apply existing blueprints on to a new blueprints with additional components added. One of the clear themes of software development over the last ten years has been "re-use". This should be no different when you are managing and developing private cloud automation,

### Name the New Blueprint

![Image of blueprint creation process](image)

1. Type **CentOSDemo** into the Name field
2. Click on the **NSX Settings** tab
Set the NSX Networking Transport Zone

1. Select RegionAO-Global-TZ(vCenter) from the dropdown list next to Transport zone
2. Click OK

A transport zone controls which hosts a logical switch can reach and can span one or more vSphere clusters. Transport zones dictate which clusters VMs can participate in the use of a particular network.

Channel Your Inner Picasso
1. Click on **Network & Security** under the **Categories** list
2. Drag and drop **On-Demand Security Group** on to the **Design Canvas**

### Add a Security Policy to the Blueprint

1. On the **General** tab that appears at the bottom of the Design Canvas, click **Add** under **Security policies** (you may need to scroll down to see the Add button)

A security policy is a set of Guest Introspection, firewall, and network introspection services that can be applied to a security group. A Security Group is a way to manage multiple policies in one context. Security Groups are very powerful as they allow you to group a collection of objects in your vSphere Inventory. Sounds simple, however, this collection can be statically defined as an object in inventory, for example a Virtual Machine, Cluster, or Datacenter, or Dynamically defined for example a security tag on a virtual machine, Guest OS Type, or VM name. The groups can also be defined as a combination of static or dynamic; and you can start to see just how powerful a security group is.
Select an Existing Security Policy

1. Select the **Application Tier** security policy from the list
2. Click **OK**
Name the On-Demand Security Group

1. Change the ID to **On_Demand_App_Security**
2. Click on the **down arrow** to collapse the configuration information

Select the CentOS VM

1. Click on the **CentOS VM**
Assign the On-Demand Security Group to the VM

1. Click on the **Security** tab
2. Click the **check box** next to the **On_Demand_App_Security** security group we just created
3. Click on the **down arrow** to collapse the configuration information
4. Click On Save
Exit the Blueprint Designer

You have created a blueprint with an on demand security group, and when this VM gets provisioned, it will consume the security policy we assigned to it.

1. Click **Finish**
On Demand Routed Networks

Overview

On-Demand Routed Network (ODRTD) - Adds a dedicated interface on the upstream distributed logical router. This also creates a new logical switch for the router interface and the machine vnic. This also applies IP policy as defined in the corresponding network profile. In this module we will build on the last task, by adding an application tier to the existing blueprint.

Any corporate network that is larger than a very small business is likely going to have a routed network already. Segmenting networks improves performance and more importantly is used for security purposes. Many compliance regulations such as PCI-DSS state that machines need to be segmented from each other unless there is a specific reason for them to be on the same network. For instance your corporate file server doesn’t need to communicate directly with your CRM database full of credit card numbers. The quickest way to fix this is to put these systems on different networks but this can be difficult to manage in a highly automated environment. Developers might need to spin up new applications, which may need to be on different network segments from the rest of the environment. Its not very feasible to assume we can now spin up test and delete hundred of machines each day, but need the network team to manually create new network segments and tear them down each day. That wouldn’t be a nice thing to do to your network team.

Luckily NSX has the ability to create routed networks and vRealize Automation can leverage this, to automatically setup a new network when we deploy blueprints. The initial setup requires setting up an NSX edge and a transit network. This is done manually to get the environment prepared for the automation piece. In the module below, we will add an on-demand routed network to the blueprint designer.
Open a Browser

1. Click on the **Google Chrome** taskbar shortcut

Log In To vRealize Automation
1. Type **cloudadmin** into the username field
2. Type **VMware1!** in to the password field
3. Click **Sign In**

**Navigate to the Blue Print Designer**

1. Click on the **Design** tab
1. Click on the CentOSDemo blueprint

This is the blueprint we configured in the previous module.
Channel Your Inner Picasso

1. Click on **Network & Security**
2. Drag and drop **On-Demand Routed Network** onto the **Design Canvas**
Configure the On-Demand Routed Network

1. Click on the **General** tab that shows up at the bottom of the Design Canvas
2. Click on the **ellipsis** next to the Parent network profile field
Select the Network Profile

1. Select **Routed NSX Network**
2. Click **OK**

What is a routed network profile? A routed network profile is used when end-to-end routable access with unique IP addresses is needed.

1. e.g. I need to provide end-user access to my Production workloads

How long does this take in the physical world? For most organizations, there is a massive length of time it takes to get to this point. With NSX and vRealize Automation we can offer this in minutes to hours.
1. Type **App_Tier** into the ID field
2. **Click Save** (not shown)
Configure the Network for the vSphere Machine

1. Back on the Design Canvas, click on CentOS vSphere (vCenter) Machine

Configure the CentOS VM to use the On-Demand Routed Network
1. Click on the **Network** that shows up at the bottom of the Design Canvas
2. Click **New**

**Select the App-Tier On-Demand Routed Network**

1. Select **App_Tier** from the dropdown list box
2. Click **OK**

**Minimize the Configuration Information**

1. Click **down arrow** to collapse the configuration information
View the App_Tier On-Demand Routed Network

1. You can now see our virtual machine is connected to the on demand routed network **App_Tier** that we created

As you can see we have implemented a routed network so end users can access the web application that runs on this CentOS server. This has taken us minutes to create and provision, leading to lower opex and faster time to market for your lines of business.
Exit the Blueprint Editor

1. Click **Finish**
On Demand Load Balancer

Overview

Load Balancing is another network service available within NSX that can be natively enabled on the NSX Edge device. The two main drivers for deploying a load balancer are, scaling out an application (through distribution of workload across multiple servers), as well as improving its high-availability characteristics.

The NSX load balancing service is specially designed for cloud with the following characteristics:

- Fully programmable via API
- Same single central point of management/monitoring as other NSX network services

The load balancing services natively offered by the NSX Edge satisfies the needs of the majority of the application deployments. This is because the NSX Edge provides a large set of functionalities:

- Support any TCP applications, including, but not limited to, LDAP, FTP, HTTP, HTTPS
- Support UDP application starting from NSX SW release 6.1.
- Multiple load balancing distribution algorithms available: round-robin, least connections, source IP hash, URI
- Multiple health checks: TCP, HTTP, HTTPS including content inspection
- Persistence: Source IP, MSRDP, cookie, ssl session-id
- Connection throttling: max connections and connections/sec
- L7 manipulation, including, but not limited to, URL block, URL rewrite, content rewrite
- Optimization through support of SSL offload
We can use the blueprint designer to drag and drop an on demand load balancer (ODLB). This deploys a dedicated NSX Edge Services Gateway (ESG) and logical switch. It then automatically configures the appropriate load balancing policy (one-arm and inline load balancing policies are supported). This will shorten the time to deploy HA based network services, ensuring your web servers or other services are highly available at all times. In the following module we will add an on-demand load balancer to the blueprint designer.
Open a Browser

1. Click on the Google Chrome taskbar shortcut
Log In to vRealize Automation

1. Type **cloudadmin** into the username field
2. Type **VMware1!** into the password field
3. Click **Sign In**
Navigate to the Blueprint Designer

1. Click on the **Design** tab
1. Click on the **CentOSDemo** blueprint

Remove Existing Load Balancer

1. Click On **ON-Demand_Load Balancer**

2. Click on X
Delete Loadbalancer

1. Click Yes

**Add an On-Demand Load Balancer to the Blueprint**

1. Click on **Network & Security** under the Categories list
2. Drag and drop **On-Demand Load Balancer** on to the Design Canvas

How long does it take your operations teams to get an application added to a physical load balancer? Weeks? Months? With the power of NSX and vRA, you can see here we are able to do this in minutes. From design to consumption, we are driving down the overall operating expense of managing and using load balancers.
Configure the On-Demand Load Balancer

On the General tab for the On-Demand Load Balancer configuration

1. Select **CentOS** from the **Member** dropdown list box
2. Select **DefaultExternalNetworkProfile (NIC 0)** from the **Member network** dropdown list box
3. Select **DefaultExternalNetworkProfile** from the **VIP network** dropdown list box
4. Click on **New**, accept the defaults, and click **OK**
5. Click **Save**
6. Click on the **down arrow** to collapse the configuration information
Select the CentOS VM

1. Click on the CentOS vSphere (vCenter) Machine
Configure the Number of Instances for the VM

On the General tab for the CentOS VM

1. Change Minimum to 2
2. Change Maximum to 3
3. Click Save
Exit the Blueprint Designer

1. Click **Finish**

Now we have designed a complete software defined application stack using the converged blueprint designer. We started with automating our security policies with the on-demand security groups. We then moved on to adding a segmented vxlan for the application tier traffic. And finally we added an on-demand load balancer to ensure our application continues to function in the event of an issue.
Conclusion

In these modules we covered how to deploy a fully automated network stack with our application stack. In IT today, it's not just how fast you can deploy a virtual machine, but also how fast you can provide the network, security and availability services.

In the next module we are going to cover day two actions with NSX.

- **Module 2 - Day Two vRA Actions for NSX**, (30 minutes) (Basic) In this module we will show how to add and remove an existing security group to a deployed blueprint. We will also show how to scale out an existing deployment to add another node to a load balancer. This will show how we can network services from a day two perspective.
Module 2 - vRealize Automation Day 2 Actions for NSX (30 Minutes)
Introduction

In this module we will show how to add and remove an existing security group to a deployed blueprint. We will also show how to scale out an existing deployment to add another node to a load balancer. This will show how we can manage network services from a day two perspective.

A day two operation is simply an action that you can take on an existing resource, such as a running virtual machine. For a VM, they typically include power on, power off, reconfigure, destroy, etc. All of the basic and essential day two operations for standard objects, such as VMs and multi-machine deployments come out of the box with vRealize Automation. As VMware continues to invest in vRealize automation we will continuously add more day two operations. In the following lessons we will show the student how to perform day two operations on the security and availability of your virtual machines.
NSX-Day 2 Security Groups

Overview

It is no longer acceptable to utilize the traditional approach to data-center network security built around a very strong perimeter defense but virtually no protection inside the perimeter. This model offers very little protection against the most common and costly attacks occurring against organizations today, which include attack vectors originating within the perimeter. These attacks infiltrate your perimeter, learn your internal infrastructure, and laterally spread through your data center. In order to address these concerns customers are adopting micro-segmentation.

Micro-segmentation decreases the level of risk and increases the security posture of the modern data center. So what exactly defines micro-segmentation? For a solution to provide micro-segmentation requires a combination of the following capabilities, enabling the ability to achieve the below-noted outcomes.

**Distributed stateful firewalling for topology agnostic segmentation** – Reducing the attack surface within the data center perimeter through distributed stateful firewalling and ALGs (*Application Level Gateway*) on a per-workload granularity regardless of the underlying L2 network topology (i.e. possible on either logical network overlays or underlying VLANs).

**Centralized ubiquitous policy control of distributed services** – Enabling the ability to programmatically create and provision security policy through a RESTful API or integrated cloud management platform (CMP). In this module we will cover how cloud consumers can change NSX security groups on an active vRA deployment. If security creates some new policies, this will allow cloud consumers to add or remove a security policy from a running virtual machine from within the vRA portal. This allows end users to apply micro-segmentation to their existing deployments. Perhaps for testing as well. If you can turn these off and on via day two actions, this will help accelerate testing of these said rules.
Open a Browser

1. Click on the Google Chrome taskbar shortcut
1. Type **devuser** into the username field
2. Type **VMware1!** into the password field
3. Click **Sign In**
Navigate to the Deployment Items

1. Click on the **Items** tab

Change Security for the Deployed CentOS Virtual Machine

1. Select the CentOS Virtual Machine
2. Click the **Actions** dropdown
3. Select **Change Security**
1. Click on the **CentOS** deployment row to highlight it
2. Click the **Actions** dropdown
3. Click **Change Security**

### Add a Security Object for the Virtual Machine

![Image of adding security object]

1. Click on the **CentOS** virtual machine
2. Click **Add**
Apply and Existing Security Group to the Virtual Machine

1. Click **Existing Security Group**
Choose the Security Group to Apply

1. Turn on the check box next to WebTier
2. Click OK
Submit the Request to Add the Security Group to the Virtual Machine

1. Click **Submit**
Acknowledge the Request has been Submitted

1. Click **OK**
2. Wait for the request to finish (you can view the status of the request by going to the Requests tab)

Verify Security Group Exists

1. Click on the **Items** tab
Verify the Security Group has been Applied to the Virtual Machine

1. Click on the arrow next to CentOS
2. Now you can see the WebTier security group added to the deployment!
NSX-Day 2 Reconfigure Of a Deployed Load Balancer

Overview

Load balancing is a critical component for most enterprise applications to provide both availability and scalability to the system. Over the last decade we have moved from bare metal servers to virtual servers and from manual deployment of operating systems to using tools like vRealize Automation or other custom workflows. In addition to the movement towards virtualization and the API being the new CL. We are also seeing a movement to Network Functions Virtualization (NFV) where Virtualized Network Functions (VNF) such as routing, VPN, firewalls, and load balancing are moving to software. The value of automation, SDN, and NFV has been proven in the largest networks today and this migration to software has proven to have tremendous ROI. Many companies also want to leverage the same cost effective models. From a day zero perspective we have been able to use vRA to automate on-demand load balancers for a few releases. What about for day two network actions? In vRA 7.3 we provide the ability to reconfigure which services the load balancer is providing high availability to.

In this module will you show you how to reconfigure a load Balancer in a deployment. The reconfigure action will allow a cloud consumer to add, edit, or delete a virtual server in a deployed NSX load balancer.

Open a Browser

1. Click on the Google Chrome task bar shortcut
Log In to vRealize Automation

1. Type `devuser` into the username field
2. Type `VMware1!` into the password field
3. Click `Sign In`
Navigate to the CentOS Deployment

Click on the Items tab

Click the arrow to the left of Centos

Select the Action to Take on the On-Demand Load Balancer

1. Select the On-Demand_Load_Balancer row to highlight it
2. Click Actions
Reconfigure the Load Balancer

1. Click on Reconfigure

Add a New Virtual Service

1. Click on New next to Virtual servers
Configure the New Virtual Service

1. Click on the dropdown next to Protocol and select HTTPS
2. Click on Customize
3. Click on the Advanced tab to check out the advanced actions NSX has added in recent releases, all of which are configurable from vRA
4. Click OK
Submit the Request

1. Click **Submit**

Acknowledge the Request
1. Click **OK**
Conclusion

Congrats! You have just completed Module 2 - NSX Day 2 Operations. We showed you how to reduce the overall security risk of your data center by implementing security groups on deployed machines. We also showed you how to provide day 2 operations for providing high availability for data center services.

- Module 1 - Better Together: vRealize Automation and NSX App Centric Networking & Security (45 Minutes) (Advanced) In this module users will see how we can build out network services on a vRealize Automation blueprint to deliver a holistic multi-tier application architecture. We will cover building multiple networks and security groups on the same blueprint.
Conclusion

Thank you for participating in the VMware Hands-on Labs. Be sure to visit http://hol.vmware.com/ to continue your lab experience online.

Lab SKU: HOL-1806-02-SLN

Version: 20180321-155344