Table of Contents

Lab Overview - HOL-1987-01-HBD - VMware Cloud on AWS - Getting Started.............2
  Lab Guidance ..................................................................................................................3
  Student Check-In ..........................................................................................................8
  Lab Scenario ....................................................................................................................14
  Introduction to Amazon Web Services (AWS) .................................................................15
  Introduction to VMware Cloud on AWS .......................................................................16
  VMware Cloud on AWS Architecture and Service Overview .........................................19
  Conclusion ......................................................................................................................28

Module 1 - Introducing VMware Cloud on AWS (30 Minutes) .....................................30
  Introduction to Deploying a SDDC Through The User Interface ....................................31
  VMware Cloud on AWS Network Configuration ..........................................................41
  Getting Information About Your vCenter ......................................................................51
  Getting Support with VMware Cloud on AWS is Easy! ...............................................53
  Conclusion ......................................................................................................................55

Module 2 - Deploying an SDDC with the Native RESTful API (30 Minutes) ............58
  Student Check-In ..........................................................................................................59
  Introduction to Developer Center and RESTful APIs .....................................................65
  Deploying SDDC with Native RESTful APIs ................................................................75
  Conclusion ......................................................................................................................82

Module 3 - Using the vCenter in VMware Cloud on AWS (iSIM) (30 Minutes) ....86
  Introduction ....................................................................................................................87
  Hands-on Labs Interactive Simulation: Using the vCenter in VMware Cloud on AWS ..................................................................................................................88
  Conclusion ......................................................................................................................89

Module 4 - Introduction to VMware Site Recovery Add-On (iSIM) (30 Minutes) ....97
  Introduction ....................................................................................................................98
  Hands-on Labs Interactive Simulation: Introduction to VMware Site Recovery Add-On ..................................................................................................................100
  Conclusion ......................................................................................................................101
Lab Overview - HOL-1987-01-HBD - VMware Cloud on AWS - Getting Started
Lab Guidance

Note: It will take more than 120 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.

Be among the first to see the new VMware Cloud on AWS solution. You will interact with the VMware Cloud on AWS interface to perform basic tasks and manage your public cloud capacity.

Note: A My VMware user account is required to access this lab.

The Student Check-In chapter will cover the My VMware requirements and how to access Cloud Services.

Lab Module List:

- **Module 1 - Deploying an SDDC through the User Interface** (30 minutes) (Beginner) With the HTML5 user interface, deploy and configure SDDCs on VMware Cloud on AWS.
- **Module 2 - Deploying an SDDC with the Native RESTful API** (30 Minutes) (Beginner) In this module we will introduce you to the API Explorer, and will utilize the native REST API and PowerCLI to deploy and configure an SDDC.
- **Module 3 - Using the vCenter in VMware Cloud on AWS (iSIM)** (30 Minutes) (Beginner) - Using iSIM, you will walk through vCenter and how to use it in VMware Cloud on AWS.
- **Module 4 - Introduction to VMware Site Recovery Add-On (iSIM)** (30 Minutes) (Beginner) - Using iSIM, you will walk through enabling of VMware Site Recovery.

Lab Captains:

- Andrea Siviero, Principal Architect, Global
- Jennifer Schmidt, Consulting Architect, USA

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

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:
Location of the Main Console

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 can not 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 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**

![On-Screen Keyboard](image)

1. Click on the "@ key".

Notice the @ sign entered in the active console window.

**Activation Prompt or Watermark**

![Activation Prompt](image)

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**

![Lab Status Screen](image)

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", please ask for assistance.
Student Check-In

This article will provide guidance on how to gain access to VMware Cloud Services. You will locate the Student Check-In page, search for your email address and then use a provided My VMware account for the VMware Cloud Services login.

Open Student Check-In Web Page

Open Chrome Browser

1. On top of browser click Student Check-In
2. This will navigate to https://checkin.hol.vmware.com

Search and Validate

1. Enter your email address used to login and start the lab
2. Click Search
3. Click the My VMware account provided e.g myvmware127@vmware-hol.com

When prompted, VMware1! will be the password

**Capacity Limits**

If you searched for your email address and this response is returned please END your lab and try again later. Each student is assigned a cloud services organization (org). When your lab started, all these orgs were in use.
The VMware Cloud Services portal can translate between English and Japanese languages.
1. Look for the dropdown and select your preferred language. In most cases, this should already be ENGLISH
2. Then click **NEXT**

1. Enter password: **VMware1!**
2. Click **SIGN IN**

After logging in:
1. Click the drop down in the right hand corner where your login name is
2. Make sure you have selected Organization name HOL-SDDC-XXX, where XXX can be any number.
Select VMware Cloud on AWS

This is the Console landing page which provides navigation to any cloud services you have subscribed to.

In this lab, only VMware Cloud on AWS will be available to open.

Click on VMware Cloud on AWS to open

You now have access to VMware Cloud on AWS until this lab expires or ends. Enjoy!
Lab Scenario

Rainpole Systems is a large multi-national manufacturer with operations concentrated in North America and Europe. They operate datacenters in both geographies but datacenter capacity is limited so they need to find a solution that will allow them to expand their IT infrastructure without the large capital expenditure of an on-premises datacenter expansion. They are also looking to expand operations into Asia and will need net new capacity in the region.

The CIO of Rainpole Systems has tasked the VP of Infrastructure to come up with a cost-effective plan to address their expansion and capacity needs while minimizing capital expenditure.

The Solution

The VP of Infrastructure contacts VMware to discuss their capacity concerns and desire to expand into Asia. Through the course of these discussions and an overview of the VMware Cloud on AWS™ solution, it looks like this could solve both issues for Rainpole Systems. They could easily extend their existing datacenters to the cloud allowing capacity additions on demand while maintaining the same operational model. Also, when the decision is made to expand in Asia, VMware Cloud on AWS™ can provide datacenter capacity without the need to build a physical presence in the geography.

The remainder of this lab will walk through a technology overview of VMware Cloud on AWS and how it can be used to satisfy both use cases for Rainpole Systems.

Please continue to the overview of Amazon Web Services and VMware Cloud on AWS.
Introduction to Amazon Web Services (AWS)

In 2006, Amazon Web Services (AWS) began offering IT infrastructure services to businesses in the form of web services now commonly known as cloud computing. One of the key benefits of cloud computing is the opportunity to replace up-front capital infrastructure expenses with low variable costs that scale with your business. With the cloud, businesses no longer need to plan for and procure servers and other IT infrastructure weeks or months in advance. Instead, they can instantly spin up hundreds or thousands of servers in minutes and deliver results faster. Today, AWS provides a highly reliable, scalable, low-cost infrastructure platform in the cloud that powers hundreds of thousands of businesses in 190 countries around the world.

What is Cloud Computing?

Cloud computing is the on-demand delivery of compute power, database storage, applications, and other IT resources through a cloud services platform via the Internet with pay-as-you-go pricing. Whether you are running applications that share photos to millions of mobile users or you’re supporting the critical operations of your business, a cloud services platform provides rapid access to flexible and low-cost IT resources. With cloud computing, you don’t need to make large upfront investments in hardware and spend a lot of time on the heavy lifting of managing that hardware. Instead, you can provision exactly the right type and size of computing resources you need to power your newest bright idea or operate your IT department. You can access as many resources as you need, almost instantly, and only pay for what you use.

Cloud computing provides a simple way to access servers, storage, databases and a broad set of application services over the Internet. A cloud services platform such as Amazon Web Services owns and maintains the network-connected hardware required for these application services, while you provision and use what you need via a web application.
Introduction to VMware Cloud on AWS

A Truly Compelling and Differentiated Solution

We are bringing together the best technologies from the leader in private cloud and the leader in the public cloud to deliver a jointly engineered solution that will bring significant value to customers.

VMware:

- The leader in enterprise compute, storage, and network virtualization
- Support a broad range of workloads
- The de-facto standard for the enterprise datacenter

Amazon Web Services (AWS):

- Flexible consumption economics
- Broadest set of native cloud services
- Global scale and reach
VMware Cloud on AWS is newly available in the AWS Europe (Frankfurt) Region, in addition to AWS Europe (London), AWS US East (N. Virginia) and AWS US West (Oregon) Regions. VMware Cloud on AWS is GDPR ready with a host of key industry certifications. We have also introduced rich capabilities that allow customers to enhance enterprise readiness, accelerate cloud migration and simplify hybrid cloud deployments. Extend on-premises data centers to the cloud with a consistent operational model, retaining your familiar VMware tools, policies, and management as well as investments in third-party tools. Leverage AWS services to extend the value of enterprise applications over their lifecycle.

VMware is working on bringing VMware Cloud on AWS to new AWS regions and enable more use cases over time.

- **Cloud Migrations** - Rapidly and easily migrate vSphere-based workloads to the cloud with VMware Cloud on AWS. Reduce the risk and cost of cloud migrations compared to alternatives that require conversions or re-architecture. Leverage familiar VMware tools and skill sets to accelerate cloud migrations. Once in the cloud, leverage VMware and AWS services to modernize your applications at your pace.
- **Application Migration** - Extend on-premises data centers and easily migrate targeted application workloads to VMware Cloud on AWS without conversions. Obtain bi-directional workload portability between on-premises and VMware Cloud on AWS. Modernize your applications through optimized access to native AWS services.
- **Footprint Expansion** - Got new projects? Want to expand into a new geography? Easily extend your footprint into the cloud and get VMware-consistent, enterprise-
grade environments in the AWS cloud in a fast and cost-effective way with VMware Cloud on AWS.

- **On-demand Capacity** - Get VMware SDDC capacity in the AWS Cloud in minutes whenever your business needs to meet temporary, seasonal, or unplanned demand. Take advantage of elastic capacity and usage-based economics of VMware Cloud on AWS by seamlessly moving your live applications into an environment that is operationally consistent with your VMware data center.
- **New Application Development and Test** - Deliver VMware SDDC-consistent dev/test environments that can integrate with modern CI/CD automation tools. Access native AWS services seamlessly for new app development.
- **Disaster Recovery as a Service with VMware Site Recovery** - Easily deliver business continuity with VMware Site Recovery: on-demand disaster recovery as a service, optimized for VMware Cloud on AWS. Accelerate time-to-protection, simplify disaster recovery operations, and reduce secondary site costs with cloud economics, while providing a secondary site that is operationally consistent with your VMware data center.

### Provide and Maintain Operational Consistency

Leveraging existing skill-sets and tools

VMware Cloud on AWS™ enables operational consistency for customers of all sizes whether their workloads operate on-premises or in the public cloud.

This jointly engineered solution between VMware and Amazon Web Services provides global scale and allows customers to leverage their existing skills and tools while maintaining compatibility with their existing applications with no re-platforming required. Through the power of NSX customers can architect networking and security to suit the needs of their applications. VMware Cloud on AWS™ is a software defined enterprise solution that enables customers to maintain consistent SLA’s across private, public and hybrid cloud infrastructures.

Please proceed to learn more about the scalable and robust VMware Cloud on AWS™ architecture.
VMware Cloud on AWS Architecture and Service Overview

VMware Cloud on AWS is powered by VMware Cloud Foundation, a unified Software Defined Datacenter (SDDC) platform that integrates VMware vSphere, VMware Virtual SAN and VMware NSX virtualization technologies. VMware Cloud on AWS will provide access to the broad range of native AWS services, together with the functionality, elasticity, and security customers have come to expect from the AWS Cloud.

VMware Cloud on AWS integrates VMware’s flagship compute, storage and network virtualization products (vSphere, vSAN and NSX) along with vCenter management, and optimizes it to run on next-generation, elastic, bare-metal AWS infrastructure. vSphere allows customers to operate their virtual machines and containers in a similar fashion to their on-premises architecture.

- All-Flash vSAN acts as the storage platform and consumes host-local NVMe flash devices.
- NSX is used for all network functionality and it connects the ESXi hosts to the AWS network and exposes logical networks for virtual machine networking.
An in-cloud SDDC can be used on its own, but most customers have a hybrid cloud strategy. With vCenter Hybrid Linked Mode (a new feature for VMware Cloud on AWS), customers can connect the two vCenters to create a single pane of glass for hybrid cloud management.

Most customers run a vRealize product on-premises such as vRealize Operations, or vRealize Automation. The in-cloud vCenter is just another end-point so customers can continue using their existing on-premises vRealize products. This way, customers can manage both their on-premises SDDC and the VMware Cloud on AWS SDDC in a single pane of glass for operations and provisioning.

VMware Cloud on AWS provides access to a broad range of native AWS services. This helps with data gravity because customers are now able to place the application closer to the AWS services acting as a data source. Instead of network traffic flow from the DC firewalls to AWS and vice versa, they are now connected to the same network as the underlying AWS services. This enables you to build and operate new application architectures with minimal latency, network overhead and reduced AWS network outbound costs.

**Flexible Consumption Models**

VMware Cloud on AWS leverages cloud economics aligned for capacity and demand with one point of contact:

- Single bill for VMware software + AWS infrastructure
- Consume elastically scalable SDDC clusters
- On-demand or reserved instance model
- Leverage global AWS footprint
VMware Cloud on AWS is a Cloud Service

VMware Cloud on AWS is delivered, operated and directly supported by VMware.

All software components of the cloud service are fully certified and supported by VMware.

- Jointly engineered, VMware Cloud on AWS provides customers a one-stop shop for native AWS services from within their SDDC
- All components of the solution are delivered, operated and supported by VMware Global Support Services (GSS)
- VMware fully certifies and supports all software components of the service
- VMware removes the burden of managing software patches, updates or upgrades for users. When operating as a cloud service VMware takes the responsibility of ensuring the service is always up to date
Making the Hybrid Cloud a Reality

Extend Cloud Foundation into the public cloud and consume as a service

PRIVATE CLOUD
Privately Managed and Operated

PUBLIC CLOUD
Delivered as-a-service

vSphere
vSAN
NSX

VMware Cloud on AWS can help customers achieve a true hybrid cloud and operate their application estate across private and public clouds seamlessly!

Features of VMware Cloud on AWS

- vCenter Hybrid Linked Mode
- Automate Cluster Remediation
- Stretched Clusters for VMware Cloud on AWS
- VMware Hybrid Cloud Extension
- VMware Site Recovery
- Horizon 7 on VMware Cloud on AWS

Read on for more detailed information about these features.
vCenter Hybrid Linked Mode

Simplifies hybrid resource management with a single inventory view between on-premises and VMware Cloud on AWS using vCenter Hybrid Linked Mode. Enhanced single logical view and hybrid management of resources by extending Hybrid Linked Mode to connect a VMware Cloud on AWS environment with multiple linked on-premises vCenter Server instances (external PSC topology).
Automate Cluster Remediation

Automated Cluster Remediation

HOST FAILS, OR PROBLEM IDENTIFIED

NEW HOST ADDED TO CLUSTER, DATA FROM PROBLEM HOST REBUILT, AND/OR MIGRATED

PREVIOUS HOST EVACUATED FROM CLUSTER, FULLY REPLACED BY NEW HOST

Failed hosts in a VMware SDDC are automatically detected by VMware and replaced with healthy hosts.

Stretched Clusters for VMware Cloud on AWS
Zero RPO high availability for enterprise applications virtualized on vSphere across AWS Availability Zones (AZ), leveraging multi-AZ stretched clustering. Stretched clusters enable developers to focus on core application requirements and capabilities, instead of infrastructure availability.

- Significantly improve your application's availability without needing to architect it into your application - the VMware Cloud on AWS infrastructure delivers protection against failures of AWS AZs at an infrastructure level.

- Stretching an SDDC cluster across two AWS AZs within a region means if an AZ goes down, it is simply treated as a vSphere HA event and the virtual machine is restarted in the other AZ.

**VMware Hybrid Cloud Extension**

- Enables large-scale, flexible, bi-directional workload portability between on-premises and VMware Cloud on AWS with VMware Hybrid Cloud Extension.
- Migrations can be done live and in bulk (warm and cold) between various vSphere versions on-premises and VMware Cloud on AWS.
- Enables multisite interconnect between various vSphere versions on-premises and VMware Cloud on AWS.
- Create high-performance, secure, WAN-optimized interconnects that stretches networks, without having to change IP addresses.
- Includes policy-based traffic engineering, intelligent routing and automated VPN set up.

VMware Hybrid Cloud Extension (HCX) is a SaaS service that provides application migration and infrastructure hybridity without application downtime or infrastructure retrofit.

The VMware HCX service offers bi-directional application landscape mobility and datacenter extension capabilities between any vSphere version.
HCX includes patent-pending capabilities to support VMware vSphere vMotion, Bulk Migration, High Throughput Network Extension, WAN optimization, traffic engineering, automated VPN with Strong Encryption (Suite B) and secured datacenter interconnectivity with built-in vSphere protocol proxies.

VMware HCX enables cloud on-boarding without retrofitting source infrastructure supporting migration from vSphere 5.0+ to VMware Cloud on AWS without introducing application risk and complex migration assessments.

**VMware Site Recovery**

**VMware Site Recovery**

*Disaster Recovery to VMware Cloud on AWS*

- Delivered as an add-on service with granular, on-demand pricing
- Built on VMware’s proven disaster recovery solutions
- Automated DR runbook with application-centric runbooks
- Bidirectional protection between cloud and on-premises as well as between AWS availability zones
- Integrated deeply with the VMware Cloud on AWS services

The VMware Site Recovery™ service expands and simplifies traditional disaster recovery operations by delivering on-demand site protection across a common, vSphere-based operating environment from on-premises to the cloud. The service protects workloads between on-premises datacenters and VMware Cloud on AWS, as well as between different instances of VMware Cloud on AWS. Based on industry leading, enterprise-grade recovery plan automation (VMware Site Recovery Manager™) and native hypervisor-based replication capabilities (VMware vSphere® Replication™) trusted by thousands of customers, the service provides an end-to-end disaster recovery solution that reduces the requirements for a secondary DR site, accelerates time-to-protection, and simplifies DR operations.

**Key Features:**

- Natively integrated into VMware Cloud on AWS
- Proven Site Recovery Manager orchestration and automation capabilities
- Recovery plan orchestration delivers aggressive RTO capabilities
- Non-disruptive testing of disaster recovery plans
• VM-centric replication for fine-grained control
• Support for bulk migration of workloads to VMware Cloud on AWS
• Streamlined HTML 5 user interface
• Support for multiple vSphere versions on-premises

**Horizon 7 on VMware Cloud on AWS**

- Flexible deployment - Horizon 7 can be deployed either on-premises, on VMware Cloud on AWS, or both
- Build your hybrid cloud by straddling Horizon 7 CPA (Cloud Pod Architecture) across on-premises and VMware Cloud on AWS
- As easy as deploying one of the pods on AWS for federated management
- Same admin management experience on-premises and in the cloud
- CPA pods can also be deployed in multiple AWS locations
- Simplified vSphere deployment with the flexibility and elasticity with VMware Cloud on AWS, and option of hourly billing
Conclusion

In this introduction, we covered a high level overview of the VMware Cloud on AWS service and the architecture. We explained how it can help Rainpole Systems solve the need for additional capacity and regional expansion.

**VMware Cloud on AWS is a Unified Hybrid Cloud Management Solution**

![Unified Hybrid Cloud Management with support for vRealize Cloud Management Platform technologies](image)

This solution integrates VMware's flagship compute, storage and network virtualization products, along with vCenter management and optimizes it to run on next generation, elastic bare metal AWS infrastructure.
See how the leader in private cloud and the leader in public cloud brought their powerful capabilities together to deliver a truly compelling and differentiated solution.

**Onboarding to VMware Cloud on AWS - 6:35**

Dig a little deeper to see how the VMware SDDC stack runs on AWS to provide a consistent operational hybrid model that delivers capacity and services on demand. Includes a look into networking configuration options and the power of elastic DRS (eDRS) and auto remediation.
Module 1 - Introducing VMware Cloud on AWS (30 Minutes)
Introduction to Deploying a SDDC Through The User Interface

Deploying a Software Defined Data Center (SDDC) is the first step in making use of the VMware Cloud on AWS service.

In this module, we will discuss one of the most common scenarios for deploying new applications onto a Software Defined Data Center on VMware Cloud on AWS.

It is peak manufacturing season at Rainpole Systems and additional capacity is needed based on the increased load on the systems. Because their North American datacenters are at capacity, they decided to utilize VMware Cloud on AWS for additional capacity. Mary is an administrator on their information technology team and is tasked with deploying an SDDC to meet these needs.

Let's walk through how Mary can quickly deploy a Software Defined Data Center and meet the needs of Rainpole Systems.

We will provide an overview of the VMware Cloud on AWS user interface and become familiar with the options available with the solution.

Before Beginning this Module

Please verify your login credentials by following the instructions in the Student Check-in module here; It is very important that the email address you logged into Hands-On-Labs matches your My VMware credentials.
Once you receive your login information and have completed your VMware Cloud on AWS activation process, you may log into the VMware Cloud on AWS portal.

If not already signed in follow the steps below:

1. Open a Google Chrome browser and login to [http://vmc.vmware.com](http://vmc.vmware.com) with your My VMware Portal credentials or use the bookmark at the top of the browser

2. Either enter in your login credentials, or if you were previously logged in you can select your user name and then enter your password when prompted

**Deploy a Software Defined Data Center (SDDC) through the VMC Console**

After logging in:
1. Click the drop down in the right hand corner where your login name is.
2. Make sure you have selected Organization name HOL-SDDC-XXX, where XXX can be any number.
Please select the service **VMware Cloud on AWS** to start creating your first SDDC.

![VMware Cloud Services](image)

**Create SDDC**

![VMware Cloud on AWS](image)

Welcome to VMware Cloud on AWS!

VMware Cloud on AWS makes it easy to run your familiar vSphere-based clouds on AWS.

Create your first Software-Defined Data Center (SDDC) in the cloud now.

1. Click the **Create SDDC** button

Creating your first SDDC is simple.
Configure SDDC Parameters

Deploying an SDDC to host your workloads in the cloud provides a simple Control Plane for IT. You can manage, govern and secure applications running in private and public clouds. VMware Cloud on AWS centralizes management, provides comprehensive visibility to your SDDC, and enterprise-class security.

When you deploy an SDDC on VMware Cloud on AWS, it is created within an AWS VPC dedicated to your organization. VMware creates and manages this VPC, and you have no direct access to it.

**Note:** For demonstration purposes and to meet the time constraints of the Hands-on-Labs environment, we will be deploying SDDC instances which are datacenters that do not include any physical hardware. This allows us to demonstrate how an SDDC is created while not waiting for the actual installation.

Execute the following steps to deploy your SDDC on VMware Cloud on AWS.

1. For the AWS Region leave the default **US West (Oregon)** selected
2. Select **Multi-Host** for the deployment
3. Enter a **Name** for your SDDC.
4. **Select 4** for the **Number of Hosts**
5. Click **Next**
Connect to AWS

1. As this is a lab/demo environment, we will not be connecting an AWS account. Click **Next**

Configure Management Network

The final step before deploying your SDDC is to define the CIDR range for the management network.
1. Enter an **IP address range** for the management network as a CIDR block (i.e. 10.2.0.0/16) or leave the text box blank to use the default. Consider the following when choosing the management subnet:
   - Specify a private subnet range (RFC 1918) to be used for vCenter Server, NSX Manager, and ESXi hosts.
   - Choose a range that will not conflict with other networks you will connect to this SDDC.
   - Minimum CIDR sizes: /23 for up to 27 hosts, /20 for up to 251 hosts, /16 for up to 4091 hosts

2. Click **Deploy SDDC**. The SDDC will take a few moments to deploy

**Note:** CIDR notation is a compact representation of an IP address and its associated routing prefix. The notation is constructed from an IP address, a slash('/') character, and a decimal number. The number is the count of leading bits in the routing mask, traditionally called the network mask. The IP address is expressed according to the standards of IPv4 or IPv6.

The address may denote a single, distinct interface address or the beginning address of an entire network. The maximum size of the network is given by the number of addresses that are possible with the remaining, least-significant bits below the prefix. The aggregation of these bits is often called the host identifier.

For example:

- 192.168.100.14/24 represents the IPV4 address 192.168.100.14 and its associated routing prefix 192.168.100.0, or equivalently, its subnet mask 255.255.255.0, which has 24 leading 1-bits.
- the IPV4 block 192.168.100.0/22 represents the 1024 IPV4 addresses from 192.168.100.0 to 192.168.103.255.
Explore the VMware Cloud on AWS Console

Once you have deployed the SDDC, we can take a tour of the VMware Cloud on AWS console. The SDDC overview is available right away with the Summary, Network, Add Ons, Troubleshooting, Settings and Support tabs. Customers can get a quick Data Center Snapshot of their SDDC infrastructure and manage it all from this console. To access the information specific to the SDDC that was just created:

1. Click View Details on the SDDC
Explore Details about the Software Defined Datacenter

Key areas to understand about your VMware Cloud on AWS Console:

1. **Summary** - this is the default management page for your SDDC. View CPU, Memory and Storage metrics, Network configuration, Connection Info and Support as well as Actions that control your SDDC. You can also directly open your vCenters from your VMware Cloud on AWS console for ease of management, VM Migrations, Content migration and much more!

2. **Network** - Provides a full diagram of the Management and Compute Gateways. This is where you can view which VPNs are configured and Firewall Rules. We will cover this in more detail later.

3. **Add Ons** - Here you will find Add On services for your VMware Cloud on AWS environment, like Hybrid Cloud Extension and Site Recovery.

4. **Troubleshooting** - Allows you to run network connectivity tests to ensure all necessary access is available to perform select use cases.

5. **Settings** - gives you access to your vSphere Client (HTML5), vCenter Server API, PowerCLI Connect, vCenter Server and reviews your Authentication information.

6. **Support** - you can contact Support with your SDDC ID, Org ID, vCenter Private and Public IPs and the date of your SDDC Deployment.

7. **Actions Menu** - This will contain any actions available for your SDDC including deletion of the environment.
8. **Open vCenter** - you can directly access your Private SDDC through this option. Before you can login to your vCenter, you must open network access to vCenter through the management gateway. Choose an option for opening network access by creating a Firewall Rule and setting up your VPN access.

**Note:** Because this is a demonstration environment, you will not have access to a vCenter server.

There are a few areas to cover regarding configuring the VMware Cloud on AWS Management Gateway.

To connect to vCenter Server and manage your new SDDC, you must either configure a VPN connection to the management gateway or configure a firewall rule to allow access to vCenter Server.

We will discuss the Management Gateway Firewall Rules, Management Gateway DNS and creating a Management VPN for vCenter connectivity in the next article [VMware Cloud on AWS Network Configuration](#).

Please proceed to the next article to learn more about VMware Cloud on AWS Network Configuration.
VMware Cloud on AWS Network Configuration

Network optimization is just one of the benefits of utilizing VMware Cloud on AWS. You gain operational visibility, control, and compliance across workloads running in VMware Cloud on AWS. You can also optimize performance, health, and availability of your network between the private and public cloud.

In the VMware Cloud on AWS Console, you can view the Networking diagram of your Hybrid cloud. You will configure your network configuration to complete your VMware Cloud AWS connection to your private cloud.

In the VMware Cloud on AWS Console, you can configure firewall rules, configure an IPsec VPN, and configure DNS for the management gateway. To connect your Private Cloud to VMware Cloud on AWS, you need to configure a Management Gateway.

We will review how to configure the following networking components to setup your Management Gateway.

- Configure Management Gateway Firewall Rules
• Configure Management Gateway DNS
• Create a Management VPN

Once your Management Gateway is configured, the Compute Gateway needs to be configured to complete the networking connectivity for your VMware Cloud on AWS environment. The reason there are two gateways is to isolate the management network from the compute network through separate VPN connections.

The Compute Gateway handles network traffic for your workload VMs. You will review the following components to setup a Compute Gateway:

• Set Compute Gateway Firewall Rules
• Configure network address translation(NAT) rules to your workload virtual machines
• Create a Compute VPN back to the on-premises network
• Set Compute Gateway DNS
• Request Public IP Addresses

Note: This is a simulated lab and we will NOT be able to create any VPN to your private cloud with VMware Cloud on AWS during this lab. The steps that require connectivity to your private cloud will be noted. The steps are provided for demonstration purposes only.

Please continue to learn how to configure a VMware Cloud on AWS Management Gateway.

Create a Management VPN

Creating a management VPN allows you to securely access the vCenter Server system and Content Library deployed in your SDDC. Configure an IPsec VPN between your on-premises data center and cloud SDDC to allow easier and more secure communication. You don’t have to set up a VPN connection, but transferring virtual machine templates and disk images into your SDDC in the cloud is easier and more secure if the connectivity is complete.

Configuring a management VPN requires the following steps:

• An on-premises router or firewall capable of terminating an IPsec VPN, such as Cisco ISR, Cisco ASA, CheckPoint Firewall, Juniper SRX, NSX Edge, or any other device capable of IPsec tunneling.
• The router or firewall should be configured with cryptography settings as described in Recommended Cryptography Settings in the VMware Cloud on AWS documentation.

If your on-premises gateway is behind another firewall, allow IPsec VPN traffic to pass through the firewall to reach your device by doing the following:
• Open UDP port 500 to allow Internet Security Association and Key Management Protocol (ISAKMP) traffic to be forwarded through the firewall.
• Set UDP port 4500 for Internet Key Exchange (IKE) (required only if NAT is used) to the list of firewall ports
• Set IP protocol ID 50 to allow IPsec Encapsulating Security Protocol (ESP) traffic to be forwarded through the firewall.
• Set IP protocol ID 51 to allow Authentication Header (AH) traffic to be forwarded through the firewall.

Configure the Management Gateway side of the tunnel.

Add a VPN
1. Click the arrow next to IPsec VPNs under Management Gateway
2. Click ADD VPN

Configure IPsec VPN
1. Enter **Rainpole Management VPN** for the name of the VPN.
2. Click **Remote Gateway Public IP** and enter the IP address of your on-premises gateway - Enter **1.2.3.4** for this example.
3. Click **Remote Gateway Private IP** and enter the Private IP address of your on-premises gateway - Enter **1.2.3.5** for this example.
4. Click **Remote Networks** and enter **10.8.0.0/16** for the address of your on-premises management network.
5. There are 3 types of **Encryption** available in VMware Cloud on AWS (AES, AES 256, and AES GCM) - Select **AES-256**.
6. **Perfect Forward Secrecy** select **Enabled**.
7. **Diffie Hellman** select **DH14**.
8. Enter **VMware1!** for the **Pre-Shared Key** - the key is a string with a maximum length of 128 characters that is used by the two ends of the VPN tunnel to authenticate with each endpoint.
9. Click **Save**.

**Verifying the VPN Connection**

Note: Because this is a simulated environment, the connection will remain disconnected. Please ignore any errors and move on to the next step.

In a customer deployment, you would need to configure the on-premises side of the tunnel. Configuration of the gateway device in your on-premises data center might need to be performed by a member of your networking team.
• Consult the VMware Cloud on AWS documentation for your gateway or firewall device to learn how to configure it to match the on-prem VPN settings.

When the VPN tunnel is configured in the private cloud, you should be able to verify connectivity in both the VMware Cloud on AWS Console and by accessing the vCenter Server deployed in your environment with a Web browser.

After you have saved the configuration, the VPN should now show as connected in the console diagram and the VPN settings.

**VMware Cloud on AWS Management Gateway Firewall Rules**

![VMware Cloud on AWS Management Gateway Firewall Rules](image)

By default, the firewall for the management gateway is set to deny all inbound and outbound traffic. You may add additional firewall rules to allow traffic as needed.

In the browser session previously opened perform the following task:

1. Select the **Network** tab and scroll the page down to the Management Gateway
2. Click the **arrow** next to Management Gateway **Firewall Rules**
3. Click **Add Rule (May Not Look As Shown)**
4. For the **Rule Name**, enter **vCenter Access**
5. For the **Source**, enter **10.8.0.0/16** which is the CIDR block for the Rainpole internal management networks. Once the VPN connection is established, this network will be able to communicate with vCenter.
6. Click the drop down below **Destination** and select **vCenter** to identify the vCenter server for VMware Cloud on AWS
7. Click the drop down below **Service** and select **HTTPS (TCP 443)** to enable SSL access
8. Click **Save** to save the firewall rule

### Firewall Rule Accelerator

![Image of Firewall Rule Accelerator](image)

After creating the VPN the Firewall Rule Accelerator is enabled. The Firewall Rule Accelerator can be used to automatically create firewall rules for things like vCenter Access, Hybrid Linked Mode, and Site Recovery.

1. Click the **arrow** next to Management Gateway **Firewall Rule Accelerator**
2. Click **Create Firewall Rules**
3. The firewall rules in the table will be automatically created and once successful will have a green check box to the left of each rule. You will also see the rules in the table added to the **Firewall Rules** section. You will notice the green check mark next to the Firewall Rule we created manually earlier in this module.
Configure DNS

The steps required to connect to the customer private cloud would be as follows:

1. Click the arrow next to DNS
2. Click Edit on the far right-hand side under DNS

1. Enter 8.8.8.8 and 8.8.4.4 for DNS Server 1 and 2 (In a customer deployment these would be the private IP addresses for your internal DNS servers)
2. Click Save to save the configuration

This completes the configuration of the management gateway.

Viewing Compute Logical Networks

Since you are unable to create logical networks, you can utilize the default logical network created during the SDDC build for the remainder of this networking section of the manual.

To find the logical network information, follow these steps:

1. Click the Arrow next to Logical Networks under the Compute Gateway
2. You can see the default logical network has a CIDR block of 10.0.0.0/24 and has DHCP enabled

For the next few sections, we will assume a workload virtual machine has been deployed to this network and has an IP address of 10.0.0.10.
Setup Compute Gateway Firewall Rules

By default, the firewall for the compute gateway is set to deny all inbound and outbound traffic. You may add additional firewall rules to allow traffic as needed.

In the browser session previously opened perform the following task:

1. Scroll down the network page to the network settings for the compute gateway (not management)
2. Click the arrow next to Firewall Rules
3. Click Add Rule (Not Shown)
4. For the Rule Name, enter Rainpole Web Access
5. Under Action, select Allow in the drop down
6. For the Source, type Any which will allow any computer on the internet to connect to this web server
7. For Destination, type 10.0.0.10. This is the IP address of the virtual machine that was deployed
8. Click the drop down below Service and select HTTP (TCP 80) to enable HTTP access
9. Click Save to save the firewall rule

Proceed to request a public IP address

Request a Public IP Address
Before you can configure a Network Address Translation (NAT) rule, you must request a public IP address.

In the browser session previously opened perform the following task:

1. Scroll down the network page to the network settings for the compute gateway
2. Click the arrow next to Public IPs
3. Click Request Public IP (Not Shown)
4. Below Notes, type Rainpole Web Server Public IP
5. Click Request to get a public IP address

### Confirm Public IP Address

![Confirm Public IP Address](image)

After you click Request, you will see the new Public IP address associated with the SDDC now.

### Set Inbound NAT Settings

![Set Inbound NAT Settings](image)

Inbound Network Address Translation (NAT) allows you to map internet traffic to a public-facing IP address and port to a private IP address and port inside your SDDC's compute network.

1. Scroll down the Network page to the Network settings for the Compute Gateway
2. Under Compute Gateway, click the arrow next to NAT
3. Click Add NAT Rule (Not Shown)
4. Type Rainpole Web NAT under Description
5. Select the drop down under Public IP and select the IP Address you requested in the Request a Public IP lesson
6. For Service, select HTTP (TCP 80) to allow inbound web traffic
7. Under Public Ports leave the default of 80
8. For Internal IP specify our Web Server IP address of 10.0.0.10
9. Click **Save** to activate the rule.

After completing this configuration, the web server would be available via the internet through the public IP address on port 80.

**Remaining Tasks on the Compute Gateway**

You can now configure the [Compute VPN](#) and [Compute DNS](#) following the same steps that were completed on the Management Gateway explained in this article. You will need to replace the SDDC IP ranges on the VPN with the IP range for the logical switch on the Compute Gateway.

This concludes the configuration steps needed to connect your private cloud to VMware Cloud on AWS. You have completed setting up the VMware Cloud on AWS Management and Compute Gateways.

Please proceed to the next article for more information about VMware Cloud on AWS.
Getting Information About Your vCenter

The VMware Cloud on AWS portal provides connectivity information for the vCenter server associated with the environment. This information includes URLs to access the vCenter server, authentication credentials and PowerCLI connection information.

vCenter connectivity information is highlighted in the screenshot:

1. Click **Settings** in the details for the SDDC you provisioned in previous steps
2. Expand the section **Default vCenter User Account** to see the Authentication credentials in order to login to the vCenter Server. You can **Click** the boxes next to the credentials to copy them to the clipboard
3. Expand the section **vSphere Client HTML5** to view the URL for the vCenter HTML5 Client
4. Expand the section **vCenter Server API Explorer** to view the URL for the API Explorer
5. Expand the section **PowerCLI Connect** to view an example string to access the vCenter server using PowerCLI.

6. Expand the section **vCenter FQDN** to view additional details about the vCenter Server.

Note: vCenter WILL NOT WORK in this environment. In order to see this function complete [Module 3 - Using the vCenter in VMware Cloud on AWS (iSIM)](#).

Proceed to the next article to learn about getting support for VMware Cloud on AWS.
Getting Support with VMware Cloud on AWS is Easy!

VMware Cloud on AWS allows customers to have one point of contact for Support. You have a number of options for getting help for your VMware Cloud on AWS environment.

Before you contact VMware for support, have the support information for your SDDC ready. Click **Support** in the details view for the SDDC you provisioned earlier in this module.

Select a method for getting help or support:

1. **Chat** - Click the Chat icon and Click New Conversation. Type your message in the chat window. You can include images by dragging them into the chat window. **Note:** Please do not use chat support as part of this lab!
2. **File a support request on My VMware** - Click the help icon and click Support Center. You are taken directly to a form for filing a support request after you log into the My VMware portal. **(Function may not be available in this lab)**
3. When contacting support, please have your **Org ID and SDDC ID** available to expedite the support process

In summary, VMware Cloud on AWS offers new methods to get support for the product through live chat, support forums and context sensitive help.
It is also important to remember that traditional phone and web support are included as part of the product. You can utilize the method that comfortably aligns with your companies standard.

Please proceed to the next article to learn more about VMware Cloud on AWS.
Conclusion

In this module, we covered a first introduction to VMware Cloud on AWS and how to deploy your first SDDC.

Please continue to discover more on the next module.

VMware Cloud on AWS Overview - 2:13

See how the leader in private cloud and the leader in public cloud brought their powerful capabilities together to deliver a truly compelling and differentiated solution.
Onboarding to VMware Cloud on AWS - 6:35

Dig a little deeper to see how the VMware SDDC stack runs on AWS to provide a consistent operational hybrid model that delivers capacity and services on demand. Includes a look into networking configuration options and the power of elastic DRS (eDRS) and auto remediation.

You have completed Module 1

Congratulations on completing Module 1.

Lab Module List:

- **Module 1 - Deploying an SDDC through the User Interface** (30 minutes) (Beginner) With the HTML5 user interface, deploy and configure SDDCs on VMware Cloud on AWS.
- **Module 2 - Deploying an SDDC with the Native RESTful API** (30 Minutes) (Beginner) In this module we will introduce you to the API Explorer, and will utilize the native REST API to deploy and configure an SDDC.
- **Module 3 - Using the vCenter in VMware Cloud on AWS (iSIM)** (30 Minutes) (Beginner) - Using iSIM, you will walk through vCenter and how to use it in VMware Cloud on AWS.
- **Module 4 - Introduction to VMware Site Recovery Add-On (iSIM)** (30 Minutes) (Beginner) - Using iSIM, you will walk through enabling of VMware Site Recovery.

Lab Captains:

- Andrea Siviero, Principal Architect, Global
- Jennifer Schmidt, Consulting Architect, USA
How to end the Lab

To end your lab click on the **END** button.
Module 2 - Deploying an SDDC with the Native RESTful API (30 Minutes)
Student Check-In

Skip this article if Student Check-In has already been completed.

This article will provide guidance on how to gain access to VMware Cloud Services. You will locate the Student Check-In page, search for your email address and then use a provided My VMware account for the VMware Cloud Services login.

Open Student Check-In Web Page

Open Chrome Browser

1. On top of browser click Student Check-In
2. This will navigate to https://checkin.hol.vmware.com

Search and Validate
1. Enter your email address used to login and start the lab
2. Click **Search**
3. Click the My VMware account provided e.g **myvmware127@vmware-hol.com**

When prompted, VMware1! will be the password

**Capacity Limits**

If you searched for your email address and this response is returned please END your lab and try again later. Each student is assigned a cloud services organization (org). When your lab started, all these orgs were in use.
The VMware Cloud Services portal can translate between English and Japanese languages.
1. Look for the dropdown and select your preferred language. In most cases, this should already be ENGLISH.
2. Then click NEXT.

1. Enter password: **VMware1!**
2. Click **SIGN IN**

After logging in:
1. Click the drop down in the right hand corner where your login name is
2. Make sure you have selected Organization name HOL-SDDC-XXX, where XXX can be any number.
Select VMware Cloud on AWS

This is the Console landing page which provides navigation to any cloud services you have subscribed to.

In this lab, only VMware Cloud on AWS will be available to open.

Click on **VMware Cloud on AWS** to open

You now have access to VMware Cloud on AWS until this lab expires or ends. **Enjoy!**
Introduction to Developer Center and RESTful APIs

VMware Cloud on AWS includes a comprehensive RESTful API that can perform a number of functions that include adding, modifying and deleting SDDCs. Through the course of this module, you will learn about the RESTful APIs and how to leverage them to automate common operations.

Rainpole Systems has recently adopted a DevOps methodology for application development and would like to automatically create and delete SDDCs via their development pipeline. Mike who leads one of the DevOps teams has been tasked with automating the deployment of these environments and it is critical that the environments are deleted when a pipeline is completed to minimize costs.

VMware Cloud on AWS is an ideal solution for this use case and Mike begins the process of integrating VMware Cloud on AWS though the API.

We will provide an overview of the VMware Cloud on AWS user interface and become familiar with the options available.

Before Beginning this Module

Please verify your login credential by following the instructions in the Student Check-in. It is very important that the email address you logged into Hands-On-Labs matches your My VMware credentials.

Also, please make sure you are logged into VMware Cloud on AWS via the Chrome browser before continuing.

What is a RESTful API?

REST stands for REpresentational State Transfer. This essentially refers to a style of web architecture that has many underlying characteristics and governs the behavior of clients and servers. REST is defined by 6 constraints: client-server, stateless, Cacheable, Layered system, Uniform Interface, Code on Demand (optional).

This kind of API works pretty much as any website. You send your request to a server via HTTP and you will get a website in response.

A REST API defines a set of functions which developers can perform requests and receive responses via HTTP protocol such as GET, DELETE and POST.

If an API follows the REST “rules”, it can be called RESTful API. Thanks to this interface, resources can be called upon singularly.
What is Developer Center?

Developer Center is a great resource area allowing developers to get up and running quickly with VMware Cloud on AWS. Developers can gain access to this information using the "Developer Center" tab in the VMware Cloud on AWS console.

To get started, let's go to the VMware Cloud on AWS Environment.

Launch Google Chrome and If you are not already logged in, log into your VMware Cloud on AWS org with your credentials.

1. From within the VMware Cloud on AWS tab, click on the **Developer Center** tab in the top menu
In the Developer Center there are a lot of great resources for you to explore.

For example, let's check out a code sample that was uploaded by one of our API developers. If you scroll through this screen you will see there are code samples for Postman (a REST API Development Environment), Python, PowerCLI, and many others. Anyone can contribute code samples to the community, if that interests you go to http://code.vmware.com or click on the link "VMware{code} Sample Exchange".

1. Click on **Code Samples** in the menu
2. Scroll down until you see the **PowerCLI - VMC Example Scripts** box
3. Click on **Download**
4. Click on **Save** in the pop up box to save the file
PowerCLI - VMC Example Script

After the script downloads

1. Click on the dropdown arrow in the bottom left corner
2. Click on Show in Folder

PowerCLI - VMC Example Script

1. Navigate to \PowerCLI-Example-Scripts-master.zip\PowerCLI-Example-Scripts-master\Scripts\VMware_Cloud_on_AWS
2. Right click on VMC Example Script.ps1 and click Open
This will open a text document where you can see the PowerShell commands you can use with your SDDC.

3. Close the text document and file explorer windows

**Software Development Kits (SDKs)**

There is a wide variety of Software Development Kits (SDKs) available to interact with the VMware Cloud on AWS APIs and the deployed SDDC products. The SDK section provides easy access to each of these open-sourced SDKs that are available on GitHub. There are also links to the documentation, samples, and even the ‘Getting Started’ blog post for each SDK.

1. Click on the **SDKs** tab

Explore the SDKs available today, you may already find the one you are interested in!
1. Click on the Downloads tab

There are command line resources like Datacenter CLI (DCLI) and PowerCLI.
The API Explorer section brings easy access to interact directly with the RESTful APIs available from the Cloud Services API and the VMware Cloud on AWS API.

These APIs are presented as an interactive API browser with some useful integrations to make it easier to work with.

The API Explorer being internal to the Cloud console allows us to use the existing refresh token to authenticate. We can also automatically populate certain fields, such as the Organization ID, to help improve the experience of learning and using these APIs.

Learning the API and seeing the responses from within the API Explorer could not be easier with the ability to “Execute” these APIs and see the live responses.

Let’s now run some simple REST API commands built into the Developer Center

1. Click on the **API Explorer** tab
2. Select your **SDDC** (ex, HOL-SDDC-01)
3. Click on the **drop down arrow** next to **Organizations**
4. Click on the **drop down arrow** next to the **first "GET" API**
5. Click on **Execute**
API Explorer - Organization GET Response

Let's look through the response.

1. Click on the **Organization's alphanumerics name** to expand the response details
2. The organization **id**. NOTE: Copy the ID number, without the quotes, for possible use in the next step.
3. The organization **name**
4. The organization **version**
In this step, we will GET some information about the organization we selected in the previous step.

1. Click on the drop down arrow by SDDCs
2. Click on the first GET arrow to expand
3. The Org ID should already be filled in for you, another great feature the developers built in based on customer feedback. NOTE: If this Org ID did not automatically fill in, paste it in.
4. Click on Execute
API Explorer - SDDC GET Response

Now let's look at the response body

1. Click on **Sddc (HOL-SDDC-01)** to expand the response body
2. The **creation date of the SDDC**
3. The SDDC **ID**
4. The SDDC **state**
Deploying SDDC with Native RESTful APIs

Deploying a Software Defined Data Center (SDDC) is the first step in making use of the VMware Cloud on AWS service.

In this module, we will discuss how to programmatically create an SDDC leveraging Native APIs.

Requirements to Create an SDDC

The first time you're deploying an SDDC, one of the key requirements is that you will need to link an AWS account to the VMware Cloud on AWS service. This allows you to do many things but the main reason is that it will allow you to connect your SDDC to an existing AWS VPC which is mandatory for a real environment.

In this lab, you are not required to do that step but is important to remember it for any real deployment.

It is also worth noting that the Management Subnet parameter is optional but for a production environment it is important to define it properly, since it cannot be changed later and will require you to destroy the SDDC to do so.

These are the rules:

- Specify a private subnet range (RFC 1918) to be used for vCenter Server, NSX Manager, and ESXi hosts.
• Choose a range that will not conflict with other networks you will connect to this SDDC.
• Minimum CIDR sizes: /23 for up to 27 hosts, /20 for up to 251 hosts, /16 for up to 4091 hosts.
• Reserved CIDRs: 10.0.0.0/15, 172.31.0.0/16.

For the purpose of this lab there is no need to link any AWS account, nor to define a Management Subnet, together with VPC and subnets and a lot of other optional parameters (i.e. Stretched Cluster) since we are going to use the defaults for most of them and a special "cloud provider" called ZEROCLoud.

*If you wish to perform these steps they are depicted in Module 1 - Introduction to Deploying a SDDC Through The User Interface.

**API Explorer**
API Explorer is the quickest and easiest way to interact with Native RESTful API. It doesn't require any code skills and provides an intuitive UI using the browser.

The API Explorer can be found in the Developer Center Tab:

1. Select the Developer Center tab from the top menu
2. Click on the API Explorer sub-tab

**Browsing the API to Provision an SDDC**

Browsing APIs using the API Explorer is integrated into the UI and has been designed to be intuitive and quick to validate API executions.

In this section, we will navigate to the API specific for creating an SDDC, which is a POST call that submits a set of configuration parameters that need to be defined and set in the API Call.

Now that we’re in the API Explorer, we are going to:

1. Browse to the SDDCs section and click the drop down arrow to expand it
2. Expand the following top section labeled POST /orgs/{org}/sddcs
3. We’ll see the org parameter already has our Org Id filled in as well as a blank sddcConfig value
4. We can populate that value with an example JSON body containing empty values by clicking on the AwsSddcConfig link in the Data Type column.
Configure JSON Parameters and Execute

The **sddcConfig** text area is where we are going to define the configuration parameters that will be sent during the POST API call.

Most of the sddcConfig parameters have defaults and are optional, we are going to configure just the bare minimum mandatory one to execute that task.

1. Click on the **AwsSddcConfig**: the sddcConfig area will get populated with an empty template of the parameters
2. Edit the **sddcConfig** text area to look EXACTLY like the below JSON (avoid any blank line at the beginning and end, remove the last comma after "region");
3. Click **Execute**

Please note that for simplicity purpose, we omitted most of the parameters, especially the account_link_sddc_config since we are using ZEROCLOUD provider.

Make sure to fill in **ONLY** the information provided in the example below in the sddcConfig Value.

```
{
  "name": "APIExplorer-Example-SDDC",
  "num_hosts": 4,
  "provider": "ZEROCL OUD",
  "region": "EU_CENTRAL_1"
}
```
Confirm JSON Parameters

Are you sure?

Executing this API call will cause modifications to your resources. Are you sure you want to continue?

☐ Don't show this again

1. Click **Confirm**

**TIPS:**

In a real environment you can retrieve:

- the _connected_account_id_ from the API with the following:
  
  Method: GET /orgs/{org}/account-link/connected-accounts

  Property: ID

- _customer_subnet_ids_: (desired subnet ID for VPC traffic)
  
  Method: GET /orgs/{org}/account-link/compatible-subnets

  Property: subnet_id
Validating the API execution

If the POST is successfully executed you should get a Task ID in the Response, similar to the picture.

Once you see the successful Response with a Task ID, you can go to the main SDDC Menu and follow the progress of it.
View Progress of SDDC Creation

1. Click on **SDDCs** on the top menu
2. You should see a progress bar configuring the just created SDDC

**Congratulations!**

After a few minutes, you should see your brand new SDDC card with its parameters in the SDDCs main page.
Conclusion

In this module, we covered how to browse REST API and accessing all the resources needed for developers using Developer Center. We also deployed a full SDDC in VMware Cloud on AWS utilizing the native RESTful API preparing simple JSON configuration file.

You can also find a PowerShell version of the same API calls in the code samples.
# --- Deployment code ---
# Connect to VMware Cloud Service
Connect-Vmc -RefreshToken $oauthToken | Out-Null

# Get ORG ID
$orgSvc = Get-VmcService -Name com.vmware.vmc.orgs
$org = $orgSvc.List()
Write-Host "Org:"$org.display_name" ID:"$org.id

# Get Linked Account ID
$connAcctSvc = Get-VmcService -Name com.vmware.vmc.orgs.account_link.connected_accounts
$connAcctId = $connAcctSvc.get($org.id) | Select-Object -ExpandProperty id
Write-Host "Account ID: $connAcctId"

# Get Subnet ID
$connSubnetSvc = Get-VmcService -Name
com.vmware.vmc.orgs.account_link.compatible_subnets
$vpcMap = $connSubnetSvc.Get($org.id, $connAcctId, $region) | Select-Object
-ExpandProperty vpc_map
$connSubnets = $vpcMap | Select-Object -ExpandProperty Values | Select-Object
-ExpandProperty subnets
$connSubnet = $connSubnets | where {$_.name -ne $null} | Select-Object -first 1
Write-Host "Subnet CIDR":$connSubnet.subnet_cidr_block"ID:"$connSubnet.subnet_id

# Deploy the SDDC
$sddcSvc = Get-VmcService com.vmware.vmc.orgs.sddcs
$sddcCreateSpec = $sddcSvc.Help.create.sddc_config.Create()
$sddcCreateSpec.region = $awsRegion
$sddcCreateSpec.Name = $sddcName
$sddcCreateSpec.num_hosts = $hostCount
if ($org.properties.values.sddcTypes) {$sddcCreateSpec.sddc_type = "1NODE"}
$sddcCreateSpec.Provider = "AWS"
accountLinkSpec =
$sddcSvc.Help.create.sddc_config.account_link_sddc_config.Element.Create()
accountLinkSpec.connected_account_id = $connAcctId
$cri = $sddcCreateSpec.account_link_sddc_config.Element.Create()
$cri.customer_subnet_ids.Add($custSubId0) | Out-Null
$sddcCreateSpec.account_link_sddc_config.Add($cri) | Out-Null
$newSddc = $sddcSvc.create($org.Id, $sddcCreateSpec)
$newSddc
See how the leader in private cloud and the leader in public cloud brought their powerful capabilities together to deliver a truly compelling and differentiated solution.

**Onboarding to VMware Cloud on AWS - 6:35**

Dig a little deeper to see how the VMware SDDC stack runs on AWS to provide a consistent operational hybrid model that delivers capacity and services on demand. Includes a look into networking configuration options and the power of elastic DRS (eDRS) and auto remediation.
You have completed Module 2

Congratulations on completing Module 2.

Lab Module List:

- **Module 1 - Deploying an SDDC through the User Interface** (30 minutes) (Beginner) With the HTML5 user interface, deploy and configure SDDCs on VMware Cloud on AWS.
- **Module 2 - Deploying an SDDC with the Native RESTful API** (30 Minutes) (Beginner) In this module we will introduce you to the API Explorer, and will utilize the native REST API to deploy and configure an SDDC.
- **Module 3 - Using the vCenter in VMware Cloud on AWS (iSIM)** (30 Minutes) (Beginner) - Using iSIM, you will walk through vCenter and how to use it in VMware Cloud on AWS.
- **Module 4 - Introduction to VMware Site Recovery Add-On (iSIM)** (30 Minutes) (Beginner) - Using iSIM, you will walk through enabling of VMware Site Recovery.

Lab Captains:

- Andrea Siviero, Principal Architect, Global
- Jennifer Schmidt, Consulting Architect, USA

How to end the Lab

To end your lab click on the **END** button.
Module 3 - Using the vCenter in VMware Cloud on AWS (iSIM) (30 Minutes)
Introduction

In this simulation, the SDDC has already been deployed. You will log into the VMware Cloud on AWS to configure Firewall Rules and then accessing the vCenter you will configure Content Libraries, create a Logical Network, create a Linux customization spec, deploy a virtual machine, and then convert that virtual machine to a template.

By default, the firewall for the management gateway is set to deny all inbound and outbound traffic. In order to access vCenter in VMware Cloud on AWS, additional firewall rules are needed in order to allow access to reach vCenter Server and allow other traffic as needed.
Hands-on Labs Interactive Simulation: Using the vCenter in VMware Cloud on AWS

This part of the lab is presented as a Hands-on Labs Interactive Simulation. This will allow you to experience steps which are too time-consuming or resource intensive to do live in the lab environment. In this simulation, you can use the software interface as if you are interacting with a live environment.

1. Click here to open the interactive simulation. It will open in a new browser window or tab.
2. When finished, click the “Return to the lab” link to continue with this lab.

The lab continues to run in the background. If the lab goes into standby mode, you can resume it after completing the module.
Conclusion

In this module, you experienced common activities that can be performed in the VMware Cloud on AWS vCenter Server. As you can see, just like on-premises activities the majority of common administrative activities can be performed in the same manner. Below we point out the differences in the restrictive access model that exists in the vCenter Server in VMware Cloud on AWS.

Privileges Reference for CloudAdmin and CloudGlobalAdmin

In a cloud SDDC, VMware performs host administration and other tasks for you. Because of that, a Cloud Administrator requires fewer privileges than an Administrator user on an on-premises data center.

VMware assigns a different role on different objects to a cloud administrator: either the CloudAdmin role or the CloudGlobalAdmin role. As a result, you can either perform global tasks on that object, or you can perform specific tasks such as creating virtual machines or folders.

<table>
<thead>
<tr>
<th>Privilege Set</th>
<th>CloudAdmin</th>
<th>CloudGlobalAdmin</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarms</td>
<td>All Alarms privileges.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Auto Deploy</td>
<td>--</td>
<td>--</td>
<td>VMware performs host management.</td>
</tr>
<tr>
<td>Content Library</td>
<td>--</td>
<td>All Content Library privileges</td>
<td></td>
</tr>
<tr>
<td>Privilege Set</td>
<td>CloudAdmin</td>
<td>CloudGlobalAdmin</td>
<td>Comment</td>
</tr>
<tr>
<td>--------------------</td>
<td>------------</td>
<td>------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Cryptographer--</td>
<td>--</td>
<td>--</td>
<td>Not supported in this version of the product.</td>
</tr>
<tr>
<td>Datacenter</td>
<td>--</td>
<td>--</td>
<td>VMware performs data center creation, deletion, and other data center operations.</td>
</tr>
</tbody>
</table>

A CloudAdmin user has the following Datastore privileges:

- **Datastore > Allocate space**
- **Datastore > Browse datastore**
- **Datastore > Configure datastore**
- **Datastore > Low level file operations**
- **Datastore > Remove file**
- **Datastore > Update virtual machine metadata**

<p>| dvPort Group       | --         | --               | VMware performs data center network operations.                        |</p>
<table>
<thead>
<tr>
<th>Privilege Set</th>
<th>CloudAdmin</th>
<th>CloudGlobalAdmin</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distributed Switch</td>
<td>--</td>
<td>--</td>
<td>VMware performs data center network operations.</td>
</tr>
<tr>
<td>ESX Agent Manager</td>
<td>--</td>
<td>--</td>
<td>VMware performs host management.</td>
</tr>
<tr>
<td>Extension</td>
<td>--</td>
<td>--</td>
<td>Not supported in the cloud SDDC</td>
</tr>
<tr>
<td>Folder</td>
<td>All Folder privileges.</td>
<td>--</td>
<td></td>
</tr>
</tbody>
</table>

**Global**

A CloudAdmin user has the following Global privileges:
- Global > Cancel Task
- Global > Global Tag
- Global > Health
- Global > Log Event
- Global > Set custom attribute
- Global > System Tag

A CloudGlobalAdmin user has the following Global privileges:
- Global > Manage custom attributes
- Global > Service manager

**Host**

A CloudAdmin user has the following Host privilege: --

VMware performs all other host management.
<table>
<thead>
<tr>
<th>Privilege Set</th>
<th>CloudAdmin</th>
<th>CloudGlobalAdmin</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host &gt; vSphere</td>
<td>--</td>
<td></td>
<td>A CloudGlobalAdmin user has the following Hybrid Linked Mode privilege:</td>
</tr>
<tr>
<td>Replication &gt; Manage replication</td>
<td>--</td>
<td></td>
<td>Not currently documented for the on-premises version of vSphere.</td>
</tr>
<tr>
<td>Hybrid Linked Mode</td>
<td>--</td>
<td></td>
<td>Hybrid Linked Mode &gt; Manage</td>
</tr>
<tr>
<td>Inventory Service</td>
<td>--</td>
<td>All Inventory Service privileges.</td>
<td>Not currently documented for the on-premises version of vSphere.</td>
</tr>
<tr>
<td>Network</td>
<td>--</td>
<td></td>
<td>A CloudAdmin user has the following Network privilege:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Network &gt; Assign network</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>VMware performs other network management tasks.</td>
</tr>
<tr>
<td>Performance</td>
<td>--</td>
<td>--</td>
<td></td>
</tr>
<tr>
<td>Permissions</td>
<td>--</td>
<td>Permissions &gt; ModifyPermissions</td>
<td></td>
</tr>
<tr>
<td>Profile-driven Storage</td>
<td>--</td>
<td>All Profile-driven Storage privileges.</td>
<td></td>
</tr>
<tr>
<td>Privilege Set</td>
<td>CloudAdmin</td>
<td>CloudGlobalAdmin</td>
<td>Comment</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------------------------</td>
<td>-------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Resource</td>
<td>All Resource privileges.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Scheduled Task</td>
<td>A CloudAdmin user has the following Scheduled Task privilege:</td>
<td>A CloudGlobalAdmin user has the following Scheduled Task privilege:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Scheduled Task &gt; Create</td>
<td>• Scheduled Task &gt; Global Message</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Scheduled Task &gt; Delete</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Scheduled Task &gt; Edit</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Scheduled Task &gt; Run</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sessions</td>
<td>--</td>
<td>A CloudGlobalAdmin user has the following Session privileges:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Sessions &gt; Message</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Sessions &gt; Validate</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Sessions &gt; Validate</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Sessions &gt; Validate</td>
<td></td>
</tr>
<tr>
<td>Storage Views</td>
<td>A CloudAdmin user has the following Storage Views privilege:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Storage Views &gt; View</td>
<td></td>
<td></td>
</tr>
<tr>
<td>System</td>
<td>All System privileges.</td>
<td></td>
<td>Task privileges control the ability of extensions to manage tasks. VMware manages extensions for you.</td>
</tr>
<tr>
<td>Task</td>
<td>--</td>
<td>--</td>
<td></td>
</tr>
<tr>
<td>Privilege Set</td>
<td>CloudAdmin</td>
<td>CloudGlobalAdmin</td>
<td>Comment</td>
</tr>
<tr>
<td>---------------</td>
<td>------------</td>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td>vApp</td>
<td>All vApp privileges.</td>
<td></td>
<td>..</td>
</tr>
<tr>
<td></td>
<td>A CloudAdmin user has most Virtual Machine privileges. The following privileges are NOT available:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Virtual Machine &gt; Interaction &gt; Create Secondary</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Virtual Machine &gt; Interaction &gt; Disable Secondary</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Virtual Machine &gt; Interaction &gt; Enable Secondary</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Virtual Machine &gt; Interaction &gt; Make Primary</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Virtual Machine &gt; Interaction &gt; Record</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Virtual Machine &gt; Interaction &gt; Replay</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| vService      | All vService privileges. | | -- |
VMware Cloud on AWS Overview - 2:13

See how the leader in private cloud and the leader in public cloud brought their powerful capabilities together to deliver a truly compelling and differentiated solution.

Onboarding to VMware Cloud on AWS - 6:35

Dig a little deeper to see how the VMware SDDC stack runs on AWS to provide a consistent operational hybrid model that delivers capacity and services on demand. Includes a look into networking configuration options and the power of elastic DRS (eDRS) and auto remediation.
You have completed Module 3

Congratulations on completing Module 3!

Lab Module List:

- **Module 1 - Deploying an SDDC through the User Interface** (30 minutes) (Beginner) With the HTML5 user interface, deploy and configure SDDCs on VMware Cloud on AWS.
- **Module 2 - Deploying an SDDC with the Native RESTful API** (30 Minutes) (Beginner) In this module we will introduce you to the API Explorer, and will utilize the native REST API to deploy and configure an SDDC.
- **Module 3 - Using the vCenter in VMware Cloud on AWS (iSIM)** (30 Minutes) (Beginner) - Using iSIM, you will walk through vCenter and how to use it in VMware Cloud on AWS.
- **Module 4 - Introduction to VMware Site Recovery Add-On (iSIM)** (30 Minutes) (Beginner) - Using iSIM, you will walk through enabling of VMware Site Recovery.

Lab Captains:

- Andrea Siviero, Principal Architect, Global
- Jennifer Schmidt, Consulting Architect, USA

How to end the Lab

To end your lab click on the **END** button.
Module 4 - Introduction to VMware Site Recovery Add-On (iSIM) (30 Minutes)
**Introduction**

VMware Site Recovery brings VMware enterprise-class Software-Defined Data Center (SDDC) Disaster Recovery as a Service to the AWS Cloud. It enables customers to protect and recover applications without the requirement for a dedicated secondary site. It is delivered, sold, supported, maintained and managed by VMware as an on-demand service. IT teams manage their cloud-based resources with familiar VMware tools without the difficulties of learning new skills or utilizing new tools.

VMware Site Recovery is an add-on feature to VMware Cloud on AWS, powered by VMware Cloud Foundation. VMware Cloud on AWS integrates VMware's flagship compute, storage, and network virtualization products: VMware vSphere, VMware vSAN, and VMware NSX along with VMware vCenter Server management. It optimizes them to run on elastic, bare-metal AWS infrastructure. With the same architecture and operational experience on-premises and in the cloud, IT teams can now get instant business value via the AWS and VMware hybrid cloud experience.

The VMware Cloud on AWS solution enables customers to have the flexibility to treat their private cloud and public cloud as equal partners and to easily transfer workloads between them, for example, to move applications from DevTest to production or burst capacity. Users can leverage the global AWS footprint while getting the benefits of elastically scalable SDDC clusters, a single bill from VMware for its tightly integrated software plus AWS infrastructure, and on-demand or subscription services like VMware Site Recovery Service.

VMware Site Recovery extends VMware Cloud on AWS to provide a managed disaster recovery, disaster avoidance and non-disruptive testing capabilities to VMware customers without the need for a secondary site, or complex configuration.

VMware Site Recovery works in conjunction with VMware Site Recovery Manager 8.x and VMware vSphere Replication 8.x to automate the process of recovering, testing, re-protecting, and failing-back virtual machine workloads.

VMware Site Recovery utilizes VMware Site Recovery Manager servers to coordinate the operations of the VMware SDDC. This is so that as virtual machines at the protected site are shut down, copies of these virtual machines at the recovery site startup. By using the data replicated from the protected site these virtual machines assume responsibility for providing the same services.

VMware Site Recovery can be used between a customers datacenter and an SDDC deployed on VMware Cloud on AWS or it can be used between two SDDCs deployed to different AWS availability zones or regions. The second option allows VMware Site Recovery to provide a fully VMware managed and maintained Disaster Recovery solution.
Migration of protected inventory and services from one site to the other is controlled by a recovery plan that specifies the order in which virtual machines are shut down and started up, the resource pools to which they are allocated, and the networks they can access. VMware Site Recovery enables the testing of recovery plans, using a temporary copy of the replicated data, and isolated networks in a way that does not disrupt ongoing operations at either site. Multiple recovery plans can be configured to migrate individual applications or entire sites providing finer control over what virtual machines are failed over and failed back. This also enables flexible testing schedules.

VMware Site Recovery extends the feature set of the virtual infrastructure platform to provide for rapid business continuity through partial or complete site failures.
Hands-on Labs Interactive Simulation: Introduction to VMware Site Recovery Add-On

In this simulation you will be guided through the steps needed to activate DRaaS capability with "VMware Site Recovery" Add-on, enabling firewall rules needed and mapping resources between the protected and recovery site. You will also been able to configure a recovery plan and run a test and reports.

This part of the lab is presented as a Hands-on Labs Interactive Simulation. This will allow you to experience steps which are too time-consuming or resource intensive to do live in the lab environment. In this simulation, you can use the software interface as if you are interacting with a live environment.

1. Click here to open the interactive simulation. It will open in a new browser window or tab.
2. When finished, click the “Return to the lab” link to continue with this lab.

The lab continues to run in the background. If the lab goes into standby mode, you can resume it after completing the module.

Conclusion

In this module, we covered how to utilize the "VMware Site Recovery" Add-on to enable the Disaster recovery as a service capability available in VMware Cloud on AWS. This knowledge should allow Rainpole Systems to quickly protect primary site infrastructure to meet the RPO/RTO in case of a Disaster.

VMware Cloud on AWS Overview - 2:13

See how the leader in private cloud and the leader in public cloud brought their powerful capabilities together to deliver a truly compelling and differentiated solution.
Onboarding to VMware Cloud on AWS - 6:35

Dig a little deeper to see how the VMware SDDC stack runs on AWS to provide a consistent operational hybrid model that delivers capacity and services on demand. Includes a look into networking configuration options and the power of elastic DRS (eDRS) and auto remediation.
Single Host SDDC

if you like the Lab and really want to continue experiment and test the VMware Cloud on AWS capabilities, please scan the QR Code below to start your 1-Host experience.

You have completed the lab!

Congratulations on completing the VMware Cloud on AWS Hands On Lab. If you would like to review any of the introductory information, you can return here.

Lab Captains:

• Andrea Siviero, Principal Architect, Global
• Jennifer Schmidt, Consulting Architect, USA
How to end the lab

To end your lab click on the END button.
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-1987-01-HBD

Version: 20190825-065916