TECHNICAL WHITE PAPER - **FEBRUARY 2018**

PREPARING FOR VMWARE CLOUD ON AWS

Planning Guide

Update PowerCLI, vRO & Other Scripts

One of the most powerful advantages of VMware Cloud on AWS is how well it integrates with your ***current*** vSphere environment including your virtual machine content, management tools and any scripts you may have created to automate your numerous daily tasks. This discussion focuses on these scripts in order to help you to prepare them for use in your new VMware Cloud on AWS SDDC.

For the most part, your scripts (PowerCLI, vRO workflows, Java scripts, API calls, etc) will work the same in VMware Cloud on AWS as they do today, after-all the underpinning technologies of VMware Cloud on AWS are vSphere, NSX and vSAN just like in your on-premises environment. This certainly makes the transition easier, but there are some things you may need to review and update.

As a part of the VMware Cloud on AWS service, VMware manages many of the SDDC components. For instance, this means VMware owns the configuration and maintenance of the hosts, clusters and datacenter objects. To that end, certain actions are just not executable by the customer, like putting a host into maintenance mode, adding a new host or deleting a host. Look for any scripts that make changes to host, datastores, cluster, etc and note that they will not be necessary in your new VMware Cloud on AWS SDDC.

Another difference with VMware Cloud on AWS is the new limited permissions model for vCenter (see Privileges Reference for CloudAdmin and CloudGlobalAdmin). This was implemented to to ensure there are no conflicts between what VMware and the consumer can control and modify in the environment. For example, because the placement of resources are restricted at certain levels of the SDDC, this model will have impact any scripts that create resources like VMs, folders and resource pools. Examples of such placement actions that will need to be modified are as follows:

Action Type	On Premises vSphere	VMware Cloud on AWS SDDC
VM Creation	Deployed to a cluster	Deployed to the WorkloadRP Resource Pool
VM Migration	Destination involved either a folder or a compute resource	Both a compute resource and a folder are required to be specified
Folder Creation	Created at the Datacenter level	Created within the Workloads folder

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

You will need review the Privileges Reference for CloudAdmin and CloudGlobalAdmin permissions model for VMware Cloud on AWS and read the blog entitled Getting Started with PowerCLI for VMware Cloud on AWS. Together they will provide more specifics on how your scripts may need to be updated to run successfully with VMware Cloud on AWS permissions.

Technical Resources

- **Getting Started with PowerCLI for VMware Cloud on AWS** - This blog provides an overview of the script changes necessary to ensure they work on VMware Cloud on AWS.
- **VMware Cloud on AWS Getting Started Guide** - This VMware document is used as the main source of technical information. The following sections are relevant to this topic:
  - Privileges Reference for CloudAdmin and CloudGlobalAdmin

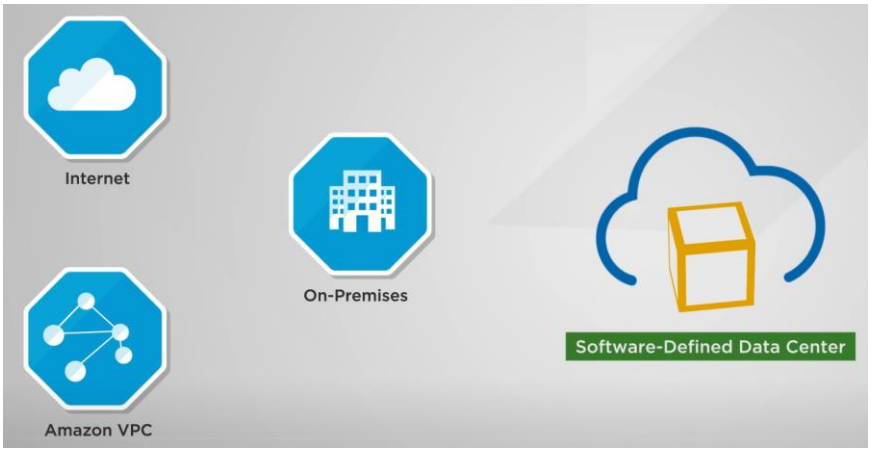
Task Checklist

- ☐ Review Getting Started with PowerCLI for VMware Cloud on AWS blog for more specifics on how your scripts may need to be updated.
- ☐ Review the Privileges Reference for CloudAdmin and CloudGlobalAdmin permissions model.
- ☐ Work with your operations team to locate the scripts that you use in your on-premise datacenter (PowerCLI, vRO workflows, Java scripts, API calls, etc).
- ☐ Updates scripts with additional parameters or other adjustments to ensure compliance with VMware Cloud on AWS permissions.
- ☐ If your scripts were created by VMware Professional Services please contact your VMware sales associate to discuss modifying these scripts.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

Preparing for Networking and Connectivity

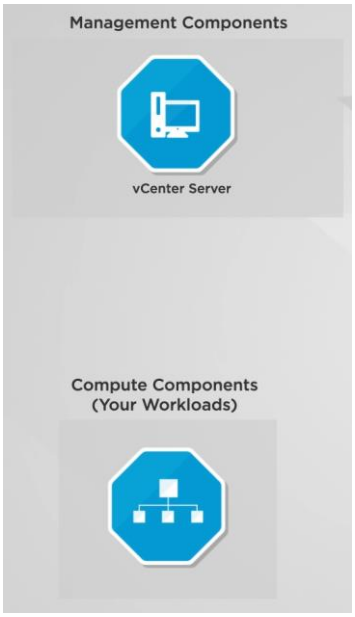
VMware Cloud on AWS helps customers rapidly provision Software Defined Data Centers (SDDC) with just a few clicks allowing them to have the power of their own public cloud together with their current on-premises private cloud. To leverage all the flexibility of your VMware Cloud on AWS we need to ensure connectivity exists between all the involved components including your on-premises datacenter, your Amazon VPC, the internet and your newly deployed SDDC.



In this preparation section, we will discuss the connectivity options available to connect everything together. We will provide a basic overview of the VPNs used by the SDDC, configuring the gateways and networks that will be used throughout the SDDC deployment, setting up your firewall rules, as well as other considerations you need to understand when managing and maintaining the VMware Cloud on AWS connectivity.

For control and security purposes, the SDDC is bifurcated into the management components and compute components (e.g. your workloads).

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

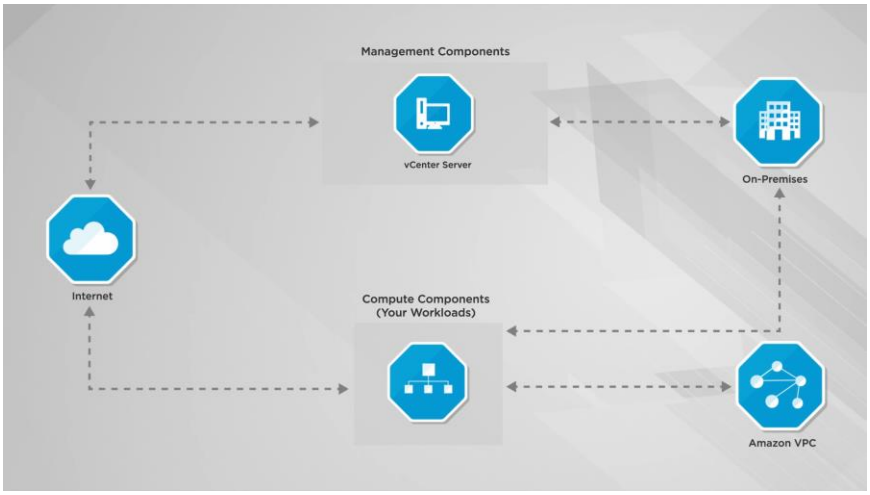


The management components of the SDDC such as vCenter, vSAN and NSX are accessed over a Management Gateway (MGW). This MGW is an NSX Edge Security gateway that provides network connectivity for the vCenter Server and NSX Manager running in the SDDC. The compute components, which are your actual workload virtual machines, connect over a Compute Gateway (CGW). The Compute Gateway (CGW) utilizes a separate NSX Edge instance and Distributed Logical Router (DLR) to enable ingress and egress of workload VM network traffic.

To provide access to both gateways in a secure manner connections must be established between your on-premises and the MGW and CGW in the SDDC. This takes the form of two (2) VPN connections. To further control the flow over these VPN connections you can configure firewall rules, inbound NAT, DNS, and the public IP addresses of your gateways.

You will also need to provide connectivity between your SDDC, the internet and your current Amazon VPC. This connectivity is provided in different forms in VMware Cloud on AWS and will utilize Elastic Network Interface, public IPs, logical networks, NAT and firewall rules to provide you complete control over the access.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com



The following video entitled Understanding Connectivity Options provides you a simple overview of the connectivity of your new SDDC and is a great way to understand the options available to you.

In the second related video, Preparing for your VMware on AWS Cloud Connectivity, we review the information you'll need to collect to get everything connected together and configured securely.

Together these 2 videos and the accompanying checklist below will walk you through the required prep-work and get the most out of VMware Cloud on AWS on day 1.

Technical Resources

- **Primer on IPSec VPN** - This blog provides an overview of IPSec with the intent of providing a simplified explanation of a very complex set of protocols. The discussion will be mostly limited to aspects of IPSec which are relevant to the VMware Cloud on AWS service and will focus on details which will help the administrator troubleshoot when issues arise.
- **VMware Cloud on AWS: Connecting with VPN** - This blog article provides details on setting up an IPSec VPN and considerations and configurations needed when preparing for its deployment.
- Related Videos
  - Understanding Connectivity Options
  - Preparing for your VMware on AWS Cloud Connectivity

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

- **VMware Cloud on AWS Getting Started Guide** - This VMware document is used as the main source of technical information. The following sections are relevant to this topic:
  - Configuring Management Gateway Networking
  - Configuring Compute Gateway Networking
  - Using AWS Direct Connect with VMware Cloud on AWS

Task Checklist

Management Considerations

- ☐ **Management Gateway Overview** - Review Configuring Management Gateway Networking.
- ☐ **Review IPSEC VPN Requirements** - Review the Recommended On-Premises VPN Settings with your networking staff to prepare for the VPN connectivity.
- ☐ **Internet vs Amazon Direct Connect** - VPN connectivity can traverse over the internet or AWS Cloud Direct Connect. AWS Direct Connect is a service provided by AWS that allows you to create a high-speed, low latency connection between your on-premises data center and AWS services. Review Using AWS Direct Connect with VMware Cloud on AWS to determine what transport would work best for your connectivity needs.
- ☐ **Management CIDR Block** – Review Deploy an SDDC from the VMC Console to determine the CIDR Block to be used for the Management Components (vCenter, ESXi hosts, etc).
- ☐ **DNS** – Review Set Management Gateway DNS to decide on a DNS server to allow the management gateway, ESXi hosts, and management VMs behind the DNS to resolve fully-qualified domain names (FQDNs) to IP addresses.
- ☐ **MGW Firewall Settings** - Review Set Management Gateway Firewall Rules and begin to note what firewall rules you will need to control management access to the SDDC.

Compute Considerations

- ☐ **Compute Gateway Overview** - Review Configuring Compute Gateway Networking.

- **IPSEC vs Layer 2 VPN** - The VPN for compute connectivity can be an IPSEC or a Layer 2 VPN. By configuring a layer 2 VPN for your compute gateway, you enable the VLAN to be stretched between your on-premises data center and your cloud SDDC. This allows you to migrate VMs to your cloud SDDC without having to change their IP addresses.
    - **Review IPSEC VPN Requirements** - Review the Recommended On-Premises VPN Settings with your networking staff to prepare for an IPSEC VPN connectivity.
    - **Review Layer 2 VPN Requirements** - Review the Configure a Layer 2 VPN with your networking staff to prepare for the Layer 2 VPN connectivity.
- **Internet vs Amazon Direct Connect** - VPN connectivity can traverse over the internet or AWS Cloud Direct Connect. AWS Direct Connect is a service provided by AWS that allows you to create a high-speed, low latency connection between your on-premises data center and AWS services. Review Using AWS Direct Connect with VMware Cloud on AWS to determine what transport would work best for your connectivity needs.
- **AWS VPC Subnet** – Review Deploy an SDDC from the VMC Console determine a dedicated subnet for the elastic network interfaces (ENI) connection between your workloads and your current Amazon VPC.
- **Logical Networks for Workloads** – Review Create a Logical Network to create a list of the logical networks (IP ranges) you will want to deploy in the SDDC that will be used to provide IP addresses to your workloads.
- **DNS** – Review Set Compute Gateway DNS to decide on a DNS server to allow the compute gateway and workload VMs to resolve fully-qualified domain names (FQDNs) to IP addresses.
- **Public IPs and NAT settings for Workloads** - Review Request Public IP Address and determine which workloads may need public internet access. These workloads will need to be assigned public IP addresses and NAT must be configured to allow access to these VMs from the internet. Details on configuring NAT can be viewed in Configure NAT Settings.
- **CGW Firewall Settings** - Review Set Compute Gateway Firewall Rules and begin to note what firewall rules you will need to control compute access for the workloads in the SDDC.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

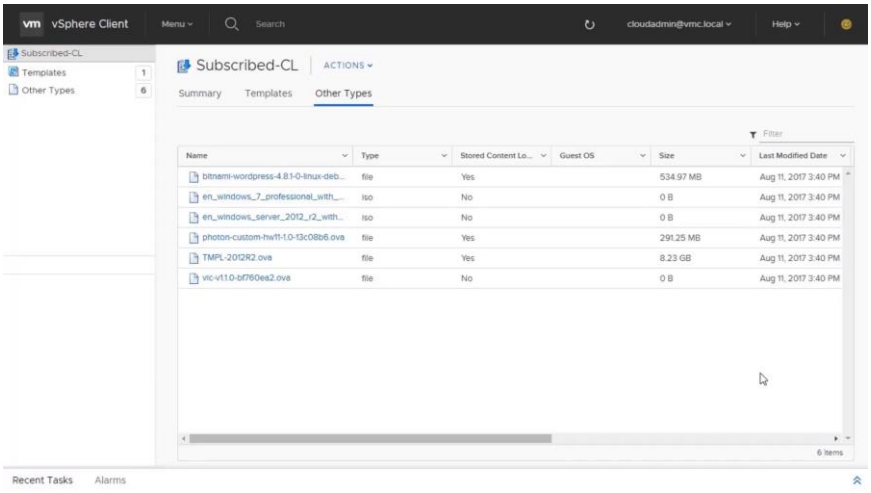
Hybrid Content Management

One of the first things you will want to do when you get access to your VMware Cloud on AWS SDDC is to spin up some new workloads. To do this simply, you will need to access your VM templates, ISOs, OVFs and scripts that you use today within your on-premises datacenter. There are several ways to onboard or share these objects to your new SDDC which will be discussed in this section.

Content Library

The fastest and easiest ways to onboard content into VMware Cloud on AWS is using a Content Library. If you are not familiar with the concept of a Content Library it organizes and automatically shares your corporate OVF templates, ISO images and scripts across vCenters, including your vCenter running within your new SDDC. To learn more about this feature of vSphere, view the series of walkthrough demos on Content Library.

The first step is to create a local Content Library in your on-premises vCenter and add the desired files to it. Then simply 'Publish' this content library to share this content with other vCenters. When you create your VMware Cloud on AWS you will simply create another content library as a 'Subscriber' library to the on-premises content library. This will allow you to either synchronize all files immediately, or choose to synchronize on-demand (files will be downloaded in the VMware Cloud on AWS content library only when needed).



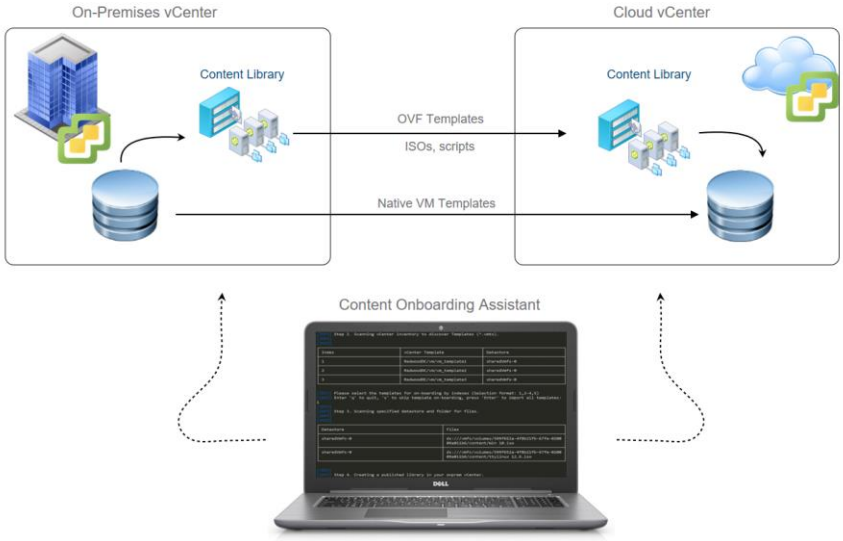
To see an example of this in action, watch this video which covers Uploading and Deploying a VM using Content Library.

Content Onboarding Assistant (COA)

If you are not already using content libraries on-premises, the idea of gathering all your numerous templates might be a daunting task. To speed

up your time to value of your new SDDC, VMware provides a simple tool to help you. The Content Onboarding Assistant (COA) is designed to simplify bulk onboarding of content by letting you specify which templates, ISO images, and scripts to publish and automates the transfer of these files.

When you run this standalone program, depending on the option you pick and which content you on-board, it first creates a publisher Content Library on-premises and a subscriber Content Library in your Cloud SDDC. It also populates the publisher library with ISO images and scripts that you specify, so they get copied to your cloud SDDC. It then automatically finds all the .vmtx templates registered to your on-premises vCenter Server and lets you select the templates that you want to on-board to your Cloud SDDC. All done for you automatically.



The list below outlines the four steps taken by the COA when you run it.

2. Checks connectivity to the cloud SDDC

3. Automatically created libraries on both ends (cloud and on-premises)), if necessary

4. Performs content selection

    - Scans Datastores to discover VM templates and allows you to select the ones you want to on-board

    - Scans a chosen datastore folder for ISO images and scripts

5. Transfers content

The COA can be used to transfer content to your SDDC more than once so if you find there are additional items you want to transfer, you can run it again with no adverse effect.

To see more details on the Content Onboarding Assistant watch this session from VMworld 2017 entitled Operating a Hybrid Environment with Hybrid Linked Mode.

By utilizing these content management methodologies, you should be ready to deploy new workloads in your VMware Cloud on AWS right after deployment.

Technical Resources

- **Operating a Hybrid Environment with Hybrid Linked Mode** - This VMworld 2017 session provides an overview of managing content in a hybrid environment, using content libraries and running the Content Onboarding Assistant.
- Content Library – This walk-through demo will explain the steps necessary to set up you first Content Library.
- Related Videos
  - Uploading and Deploying a VM using Content Library
- **VMware Cloud on AWS Getting Started Guide** - This VMware document is used as the main source of technical information. The following sections are relevant to this topic:
  - Use a Content Library to Import Content into Your SDDC
  - Getting Templates, ISOs, and Other Content into Your SDDC

Task Checklist

- ☐ **Upgrade vCenter** – In order to use content libraries or the Content Onboarding Assistant your on-premises vCenter must be running at least version 6.0 U3. For detailed on how to upgrade your vCenter to the latest version(s) please see vSphere Central.
- ☐ **Review the Different File Transfer Options** – Review Getting Templates, ISOs, and Other Content into Your SDDC.
- ☐ **Set up your Content Library** - Follow these simple steps to set up the two content libraries and share your files:

- If you don't already have one, create a Content Library in your on-premises data center.
- Add your OVF templates, ISO images, and scripts to the Content Library. Note that your .vmtx templates will be converted to OVF templates.
- Publish your Content Library.
- In your SDDC, create a Content Library
- Subscribe to the Content Library you published from your on-premises data center.
- Content is synchronized from your on-premises data center to your SDDC in VMware Cloud on AWS.

- **Run the Content Onboarding Assistant** Follow these simple steps to use the Content Onboarding Assistant and share your files:
  - Download the Content Onboarding Assistant
  - Run the COA in your on-premises datacenter
  - Point to an on-premises datastore folder with ISO, scripts, etc. and the COA will read all of the files and put them into the on-premises Content Library ready to share it across to the SDDC vCenter (publish→subscribe).

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

Preparing for Disaster Recovery Services

VMware has brought together their site recovery technologies and their VMware Cloud on AWS service to create a new enterprise-class Disaster Recovery as a Service (DRaaS) offering. This new add-on feature to VMware Cloud on AWS 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.

This DRaaS offering protects workloads between on-premises data centers and VMware Cloud on AWS, as well as between different instances of VMware Cloud on AWS. The new service also lets you take advantage of the consistent, vSphere-based infrastructure and operating environment that extends from on-premises to VMware Cloud on AWS.

The solution leverages our 10+ years of DR innovations by building on the proven technologies of VMware Site Recovery Manager for advanced orchestration automation and vSphere Replication for flexible, hypervisor-based replication. VMware Site Recovery allows customers to protect critical data and applications while taking advantage of cloud flexibility and economics—enabling admins to accelerate their time-to-protection by removing the need to build a secondary DR site and by dramatically simplifying disaster recovery (DR) operations and enabling ‘DR in a day’!

Disaster Recovery as a Service with VMware Site Recovery can solve can easily help you:

- Accelerate time-to-protection: Remove the need to build a secondary DR site and implement DR in a day with familiar tools and the same operating environment from on-premises to the public cloud
- Simplify DR operations: Streamline operations with automated failover and failback and simplify ongoing maintenance and non-disruptive testing
- Apply Cloud Economics: Reduce secondary site management costs with cloud-managed infrastructure and only pay for what you use with granular, on-demand cloud pricing

Getting your VMware Cloud deployed and configured correctly is a pre-requisite to use the DRaaS add-on service. That means many of the previous preparation steps are still valid and required. If you are ONLY going to use VMware Cloud on AWS for DRaaS use cases (meaning you will not be placing any running workloads into your SDDC outside of those needed for disaster recovery) then you might be able to skip running a cost assessment, updating your vSphere scripts and setting up your content library. Also, the migrating application section may be more than you need, although we still

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

recommend using vRealize Network Insight to map out your applications to ensure your protection groups are complete and all-encompassing.

Technical Resources

- Related Videos
    - VMware Cloud on AWS - VMware Site Recovery Use Case
- **VMware Site Recovery Delivers DRaaS for VMware Cloud on AWS** - This blog provides an overview of the service and details about how it can be used for disaster recovery purposes.
- **VMware Site Recovery Technical Overview** – This site provides a technical overview of the features and capabilities of VMware Site Recovery for VMC on AWS.
- **Getting Started with VMware Site Recovery** – This site provides a technical overview of the features and capabilities of VMware Site Recovery for VMC on AWS.
- **VMware Site Recovery Installation and Configuration Guide** - This VMware document is used as the main source of technical information for this service.
- **VMware Site Recovery Administration Guide** - This VMware document is used as the main source of technical administration information for this service.

Task Checklist

- ☐ Review and follow the steps laid out in the Getting Started with VMware Site Recovery document which outlines the pre-requisites necessary to use this service.