TECHNICAL WHITE PAPER - **FEBRUARY 2019**

PREPARING FOR VMWARE CLOUD™ ON AWS

Planning Guide

Table of Contents

Introduction

VMware Cloud on AWS is an on-demand service that enables you to run applications across vSphere-based cloud environments with access to a broad range of AWS services. Powered by VMware Cloud Foundation, this service integrates vSphere, vSAN and NSX along with VMware vCenter management, and is optimized to run on dedicated, elastic, bare-metal AWS infrastructure. With this service, IT teams can manage their cloud-based resources with familiar VMware tools.

VMware Cloud on AWS has introduced rich capabilities that allow customers to move, run and protect production applications at scale. 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 VMware Cloud on AWS to provide the following solutions for your business, among others:

- Seamless Cloud Migration
- Flexibility of On-Demand Capacity
- Disaster Recovery as a Service with VMware Site Recovery

The process of deploying your VMware Cloud Software Defined Data Center (SDDC) is quite simple and will only take you a matter of minutes. Prior to this, however, you ought to have properly prepared for the deployment: gathered the necessary data points, reviewed the documentation, discussed the options with your IT brethren, agreed upon the numerous decisions that need to be made, etc.

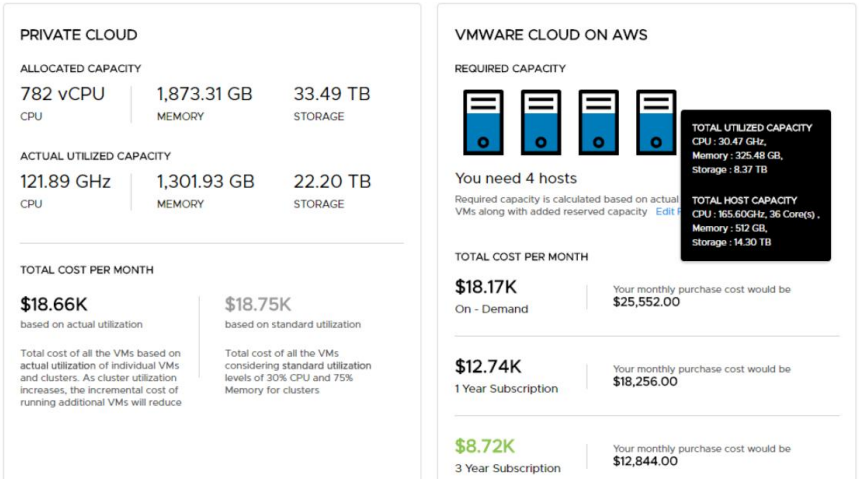
This document covers critical preparation steps and associated resources that will educate you on how to deploy your new SDDC environment quickly and correctly. If you use this document and follow its guidance you will be able to get the most out of your VMware Cloud on AWS on Day 1.

Cost Assessment

There are **several** things to think about before bringing a VMware Cloud on AWS SDDC into your business.

- How do I connect everything together?
- Which applications and workloads should I move first?
- How do I manage performance, cost and capacity?

But really, the first question you need to answered is “How much VMware Cloud on AWS do I need”. VMware provides an easy to use VMware Cloud for AWS Assessment tool which can quickly give you the number of hosts you will need, their estimated cost and a simple cost comparison to your private cloud environment. The assessment tool supports the two main ways customers like yourself want to move workloads into the cloud 1) Choosing specific apps or VMs to move and 2) Retiring old HW and moving over entire clusters at a time.



Technical Resources

- **How to run a VMware Cloud on AWS Assessment** – This blog provides detailed instructions on how to run a VMware Cloud on AWS cost assessment.
- Related Videos
  - VMware Cloud on AWS Cost Assessment

Task Checklist

- ☐ Contact your VMware sales associate to run a VMware Cloud on AWS assessment
- ☐ Deploy vRealize Business for Cloud 7.3.1 (or greater)
- ☐ Add applications, VMs, datacenters or clusters to the assessment tool to create a scenario

- Run the scenario to determine approximate costs and number of AWS hosts needed
- Export the assessment results to a CSV file as it will be used later

Planning for SDDC Administration

In this section of the preparation document we discuss the administration of your VMware Cloud on AWS SDDC. This includes the management options to be considered, the decisions you will need to make and the information that will need to be collected in order to hit the ground running with your new cloud environment the day you deploy it.

Organizational Users and Roles

VMware Cloud on AWS accounts are based on an Organization, which corresponds to a group or line of business subscribed to VMware Cloud on AWS services. Your MyVMware account, is used to create the Organization and will make you an Organization Owner. Organizational Owners are assigned the Organization Owner role which allows them to invite new users. New users can be assigned the Organization Owner role or the Organization Member role. Both types of users can manage the SDDC cloud, but only those with the Organizational Owner role can invite more users.

Both users will have access to all the resources and services of the Organization and can create, manage, and access SDDCs belonging to the Organization. The major tasks performed by organization users include, but are not limited to:

- Adding and removing hosts to the SDDC
- Configuring the management network for vCenter access/administration: VPN, DNS, Firewall rules
- Configuring and maintaining the compute network for workloads: logical networks, firewall rules, NAT, VPN, DNS, Public IPs

Technical Resources

- **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:
  - Account Creation and Management

Task Checklist

- ☐ Determine who will be your initial Organization Owner and will be responsible for the creation of your SDDC.
- ☐ Ensure this person has a valid My VMware account, if not you can create one here: https://my.vmware.com/web/vmware/registration
- ☐ Determine who else you will need to add to your SDDC organization as either another Organization Owner or as an Organization User.

Planning for vCenter Administration

In a cloud SDDC, VMware performs numerous administration tasks for you. This includes, but is not limited to, managing the lifecycle of the cloud SDDC software stack (deployment, configuration, patching, etc), configuring the AWS infrastructure, and adding/removing hosts and networks during failure scenarios or cluster-scaling operations. Because the service is doing all of this for you, a Cloud Administrator in the SDDC requires fewer privileges than an Administrator user on an on-premises data center.

vCenter Users, Roles and Administration

To better maintain the separation between the service and the customer, VMware Cloud on AWS introduce two new roles to the traditional vCenter user model: **CloudAdmin** and **CloudGlobalAdmin**. These new roles and associated privileges ensure that the Cloud SDDC infrastructure is configured in a prescriptive deployment architecture and the customer cloud administrators cannot adversely reconfigure the management component or appliances. With this model, the customer cloud administrator has full control over their workloads while having a read-only view of management workloads and infrastructure.

- **CloudAdmin Role**: The CloudAdmin role has the necessary privileges for you to create and manage workloads on your SDDC. However, you cannot access or configure certain management components that are supported and managed by VMware, such as hosts, clusters, and management virtual machines.

- **CloudGlobalAdmin Role**: The CloudGlobalAdmin role is associated with global privileges and allows you to perform only certain global tasks like create and manage Content Library objects.

A new vCenter user group called **CloudAdminGroup** will also be created and given the privileges associated with both roles.

For a detailed chart of all of the privileges mapped to these 2 roles you can review the Privileges Reference for CloudAdmin and CloudGlobalAdmin on VMware docs.

Discrete vCenter Administration

Discrete administration refers to separate management platforms and processes of on-premises and cloud SDDC workloads. One of the benefits of a hybrid cloud is the ability to connect your public and on-premise clouds together and to have unified management between the two environments. This, as you will see below, is easy to do with VMware Cloud on AWS. However, some customers may wish to manage their VMware Cloud on AWS separately from their on-premise environment and will not want to connect them together. Although you will be missing out many of the benefits of a true hybrid cloud, this is possible with VMware Cloud on AWS. You will need to manage vCenter users directly in the SDDC vCenter console and simply create new users you want to give cloud administrator rights to and add them to the CloudAdminGroup described above.

Unified Administration

Unified administration refers to a unified management platform that spans across your on-premise and cloud SDDC environments creating a cohesive management strategy. Hybrid Linked Mode (HLM) is a brand-new feature available only for VMware Cloud on AWS and provides the ability to extend an administrator's management view from on-premises to VMware Cloud on AWS. This may sound familiar if you are using Enhanced Linked Mode (ELM) in your on-premises environment. There are differences between ELM and HLM in their requirements, how they work, and what problem each is solving, which you can read more about in the blog article entitled Enhanced Linked Mode (ELM) vs Hybrid Linked Mode (HLM).

Before jumping into the configuration of HLM it's good to have an understanding of the feature and its requirements. When a Cloud SDDC is deployed and configured it is setup as its own stand-alone vSphere Single Sign-On domain. In order to manage both a Cloud SDDC and your on-premises vSphere SSO domain together, these two separate SSO domains need to establish a trust. They also need to continue to retain their autonomy since the SDDC has the flexibility to be created and destroyed as needed. For example, if we create HLM between a Cloud SDDC and an on-premises vSphere environment, we don't want the two environments to become fundamentally dependent on each other. This gives us the ability to tear down HLM without breaking permissions and creating a huge mess.

HLM is a flexible solution that allows us to jointly manage both the VMware Cloud on AWS and on-premises SSO domains. HLM provides a one-way trust from on-premises to VMware Cloud on AWS (i.e. VMware Cloud on AWS trusts the on-premises users) and gives us the option to link and unlink as needed. It also retains the separation between on-premises and VMware Cloud on AWS permissions if we need to break the two environments apart. Once HLM is established, on-premises workloads can be migrated to VMware Cloud on AWS. The bonus is that the migration works both ways and workloads can be migrated back from VMware Cloud on AWS to on-premises.

HLM Features

- Supports both embedded vCenter Server and external Platform Service Controller (PCS) deployment models for on-premises
- Easy to set up with an option to link and unlink as needed
- Configuration done in the VMware Cloud on AWS vSphere Client (HTML5)
- Management of both environments is done by logging in the VMware Cloud on AWS vSphere Client using an on-premises account
- One way trust from on-premises to Cloud SDDC

- Supports round-trip workload mobility via cold migration

Technical Resources

- **Enhanced Linked Mode (ELM) vs Hybrid Linked Mode (HLM)** – This blog will help you understand the differences between the two link mode options.
- **Configuring Hybrid Linked Mode (HLM) for VMware Cloud on AWS** – This blog which will provide an overview of HLM and a walk through of how it is deployed and configured.
- **Configuring Hybrid Linked Mode: What You Need to Know** – This blog covers troubleshooting issues with setting up and configuring HLM.
- Related Videos
  - Hybrid Linked Mode for 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:
  - Roles and Permissions in the SDDC
  - Hybrid Linked Mode

Task Checklist

Discrete Administration (Option 1)

- ☐ Determine which users you want to give cloud administrator rights to in your cloud SDDC. You will create new users and add these to the CloudAdminGroup in the SDDC vCenter once you have access to it.

Unified Administration (Option 2)

- ☐ Upgrade your on-premise vSphere to 6.0 U3 or higher in order to support HLM. This procedure is discussed in more detail on vSphere Central.
- ☐ Determine your identity source. Supported identity source types are Active Directory over LDAP(s) or Open LDAP.
- ☐ Create or use an existing cloud administrator's group from the on-premises identity source which will have access to login the VMware Cloud on AWS vCenter Server and manage both environments once HLM is configured.
- ☐ Identify users and add them to this newly created SSO group. Remember, members of this group will automatically be added to the CloudAdminGroup cloud and become administrators of the Cloud SDDC. They also will be able to login the VMware Cloud on AWS vSphere Client using their on-premises accounts and manage both environments in a single view.

- Determine your vSphere SSO on-premises environment account information to link to the on-premises environment to the Cloud SDDC.
    - Platform Services Controller FQDN
    - SSO Domain Name
    - SSO User Name & Password
- Determine the on-premises DNS server(s) that can resolve the on-premises identity source and Platform Services Controller which will be used when configuring HLM.

Planning Migration of Applications

One of the main use cases of VMware Cloud on AWS is the ability to extend on-premises data centers and easily migrate application workloads without conversions. In other preparation sections, we have described the underpinning technology and connectivity framework that drives this bi-directional workload portability between on-premises and VMware Cloud on AWS. We also discussed the requirements, configurations and preparations needed to be able to connect the new SDDC to your on-premises environment to leverage this application mobility. The VMware Cloud on AWS - Application Migration Use Case video provides a high-level understanding of migrating applications to the cloud.

Before your SDDC is deployed you should really start thinking about which application your planning to migrate. However, while deploying your SDDC and connecting it with your on-premises datacenter is a very structured process, deciding which applications to migrate is much more subjective and takes careful consideration to ensure things run smoothly.

- What applications or application components are the "best" to move to VMware Cloud on AWS?
- Are some applications better candidates than others and how do I rank them?
- Which VMs should not be moved and why?
- How do I ensure I am not splitting an application up, missing a VM that might be crucial to it functioning properly?

This white paper, Cloud Migration Planning – VMware Cloud on AWS, provides a structured migration planning process and outlines the steps that need to be undertaken when migrating applications to VMware Cloud on AWS. This document will walk you through:

- Collecting the migration data
- Tools that can be used to speed up the collection effort
- Analyzing the data for the purposes of application ranking
- Specific migration options available to help you move these applications
- VMware services that can help with the overall migration process

One thing you will want to investigate before moving over your applications is VMware's Hybrid Cloud Extension which can greatly simplify your migration. Hybrid Cloud Extension is an add-on feature to VMware cloud on AWS and abstracts on-premises and cloud resources and presents them to the apps as

one continuous hybrid cloud. Over this, Hybrid Cloud Extension provides high-performance, secure and optimized multisite interconnects. The abstraction and interconnects create infrastructure hybridity. Over this hybridity, Hybrid Cloud Extension facilitates secure and seamless app mobility across on-premises vSphere platforms and VMware Cloud on AWS.

Following the migration process outlined in the white paper and leveraging tools like Hybrid Cloud Extension will ensure you successfully migrate your applications to VMware Cloud on AWS.

Technical Resources

- **Cloud Migration Planning White Paper** - This white paper will go into the details of the process you can run to determine what applications and workloads are good candidates to move to VMware Cloud on AWS.
- **VMware Hybrid Cloud Extension** – This website provides detailed information on the power and use cases associated with this add-on feature for VMware Cloud on AWS.
- Related Video
  - VMware Cloud on AWS - Application Migration Use Case

Task Checklist

Build a Migration Plan

- ☐ Deploy collection and analysis tools used for data collection
- ☐ Gather technical and business criteria data about your applications and VMs
- ☐ Create migration weighting framework used for ranking migration candidates
- ☐ Analyze data and update weights for applications and VMs to rank
- ☐ Review migration options and determine your company's strategies (you will likely want to deploy more than one)

Enlist Professional Services

- ☐ Speak to your VMware sales associate to discuss the VMware Migration Services available to you. Some or all of these services may help you in your migration planning activities

Right-Size Workloads

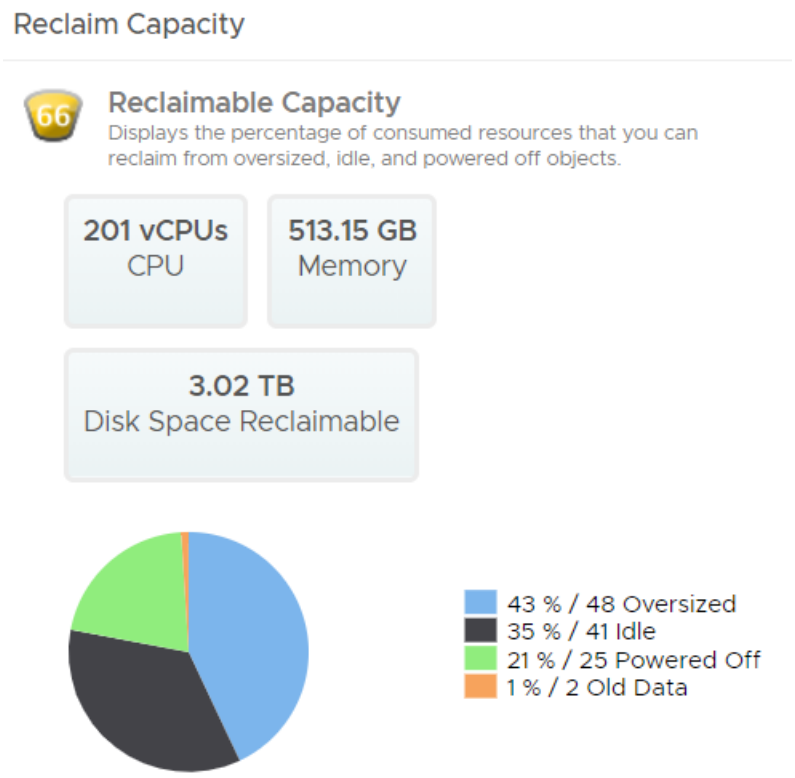
In your private datacenter, right sizing your workloads and reclaiming capacity ensures you have enough capacity to accommodate everything you need to run. After all, there is never an unlimited amount of funds available for hardware so you need to run your VMs and applications as efficiently as possible. The ability to quickly find and report on waste is paramount to running a cost-effective environment.

This same diligence towards efficiency needs to be undertaken in your VMware Cloud on AWS. The cloud offers new flexibility and agility; even though you can add a new host in about 10 minutes, you still have limits to how many hosts you can afford. This quick ability to expand your number of hosts and overall resource footprint means you will be able to run things "hotter" in the cloud. You should think about increasing your consolidation ratios and how much you over-allocate CPU and memory to get the most out of your new SDDC. This does not mean you should ignore your overall demand footprint or abandon your allocation/over-allocation strategy all together. Nevertheless, in the cloud, increasing the numbers compared to your private datacenter just makes sense.

Bottom line, you still want to have visibility and control over any waste in the cloud environment in order to meet these allocation targets. However, controlling that waste does not have to wait until you have migrated your workloads to VMware Cloud on AWS. In fact, it should start now. Once you have chosen your applications and know which workloads are associated with them you should look at trimming them down before migrating them to the cloud.

A solution like vRealize Operations can help you accomplish this task via its Capacity Reclaimable dashboard. This view helps you quickly find and automatically reclaim unused disk, CPU and memory from your virtual environment and right-size your workloads for the cloud.

Out-of-the-box vR Ops does this by datacenter or cluster which is perfect if you are migrating to the cloud due to retiring old hardware. By clicking the datacenter or cluster object you provided an overview of the reclaimable capacity therein.



The rest of the dashboard is also updated to highlight any VMs that have reclaimable disk, CPU or memory. Simply select the VM you want to right-size and use the action button to execute it. You can choose the recommended sizing or select your own.

The ***Reclaim Disk Space*** widget shows you VMs with large/old snapshot that you would not want to migrate to the cloud or filesystems that are over-provisioned and might need to be trimmed.

Reclaim Disk Space from these VMs

Name	Reclaimable Filesystem	Snapshots ↓
vrlivra01	35.09 GB	27.08 GB
mssql-svr-001	30.05 GB	4.4 GB
linux-base-02d	0.63 GB	0.63 GB
centos-base-01a	0.36 GB	0.36 GB
baselin-009	2.11 GB	0.34 GB
baselin-008	2.09 GB	0.32 GB
cmdev-009	1.92 GB	0.15 GB

The ***Reclaim Memory*** widget shows VMs with large memory allocation but with small actual memory utilization footprints. This is another area where you should look at right sizing before migration.

Reclaim Memory from these Large VMs

Name	Configured	Aggressive	Conservative
sap_app	15.62 GB	11.62 GB	7 GB
bca-e-ora12c	64 GB	59.57 GB	29 GB
vrlcm01	16 GB	14.09 GB	7 GB
vrli-master	32 GB	27.71 GB	13 GB

The Reclaiming Capacity with vRealize Operations video will walk you through the dashboard so you can better acquaint yourself with its usage.

While the out-of-the-box dashboard works great for the hardware retirement use case it may be a bit clunky if you are looking to move specific VMs and applications from across your entire datacenter. To assist you with this use case, VMware has provided a simple PowerShell script and a new vRealize Operation dashboard to meet this need.

The script takes the output from the VMware Cloud on AWS Assessment and loads the VMs into a custom group inside of vRealize Operations. The custom dashboard then provides you the ability to view only the VMs in this group and perform capacity reclamation tasks on them to right-size them and prepare them for migration to the cloud.

The Preparing for your VMware on AWS Cloud Connectivity video will walk you through the script and the steps needed to set all of this up. Its very simple and should only take a few minutes to do so. You can find the script and the dashboard here: https://code.vmware.com/samples/3178.

Right-sizing your workloads prior to moving them to the cloud will save you time and money and will allow you to have a cost-efficient cloud environment starting on day 1.

Technical Resources

- Related Videos
  - Reclaiming Capacity with vRealize Operations
  - Preparing for your VMware on AWS Cloud Connectivity

Task Checklist

- ☐ **Create a list of Migration Candidates** – Create a list of the VMs that are being proposed for migration to VMware Cloud for AWS.
- ☐ **Right-Size Workloads** – Using a capacity analytics tool like vRealize Operations, right-size the VM candidates to reclaim CPU, memory and disk space.
- ☐ **Optional Migration Specific Dashboard Flow** - Create a VMware for Cloud on AWS specific dashboard within vRealize Operations to assist with the right-sizing process.
  - Run the VMware Cloud on AWS Assessment
  - Export the migration candidates into a CSV file
  - Download the dashboard and migration group creation script from https://code.vmware.com/samples/3178
  - Run the script to create the migration group inside of vRealize Operations
  - Upload the dashboard into vRealize Operations
  - Use the new VMware Cloud on AWS Migration Dashboard to right-size your migration candidates

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
Copyright © 2019 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

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

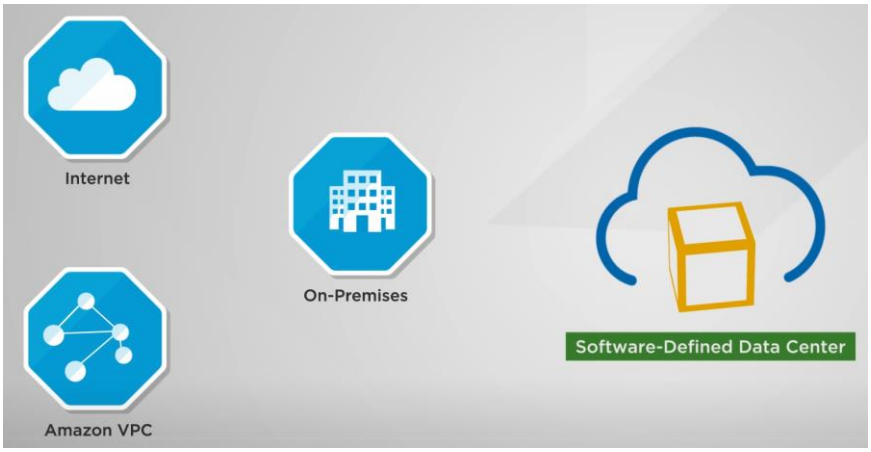
Task Checklist

- ☐ 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
Copyright © 2019 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

Preparing for Networking and Connectivity

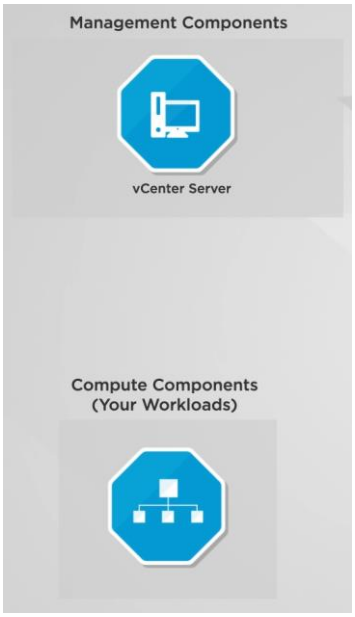
VMware Cloud on AWS helps customers rapidly provision Software Defined Data Centers (SDDC) with just a few clicks allowing them to have the power of their own public cloud together with their current on-premises private cloud. To leverage all the flexibility of your VMware Cloud on AWS we need to ensure 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
Copyright © 2019 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

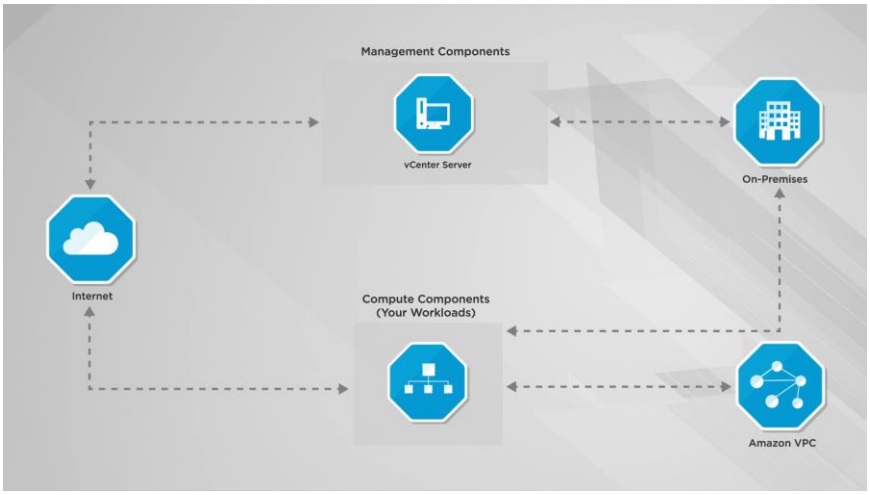


The management components of the SDDC such as vCenter, vSAN and NSX are accessed over a Management Gateway (MGW). This MGW is an NSX Edge Security gateway that provides network connectivity for the vCenter Server and NSX Manager running in the SDDC. The compute components, which are your actual workload 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
Copyright © 2019 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.



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
Copyright © 2019 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

- **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.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
Copyright © 2019 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

- **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
Copyright © 2019 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
Copyright © 2019 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

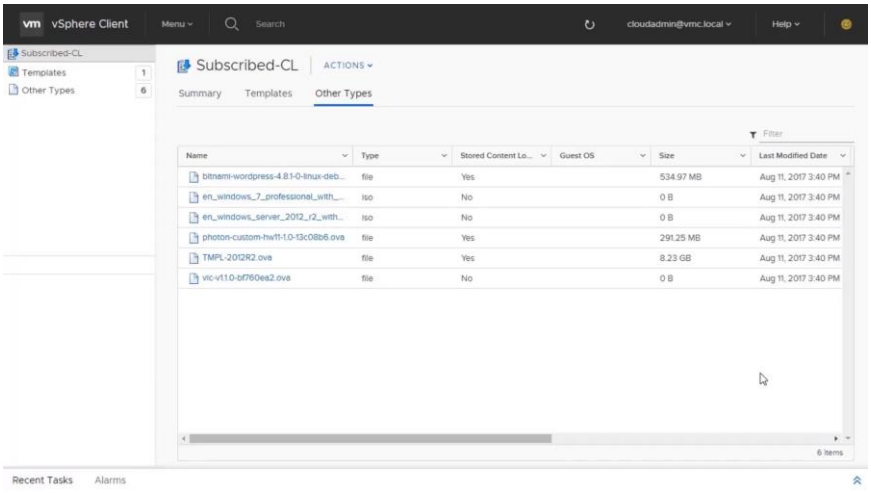
Hybrid Content Management

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.

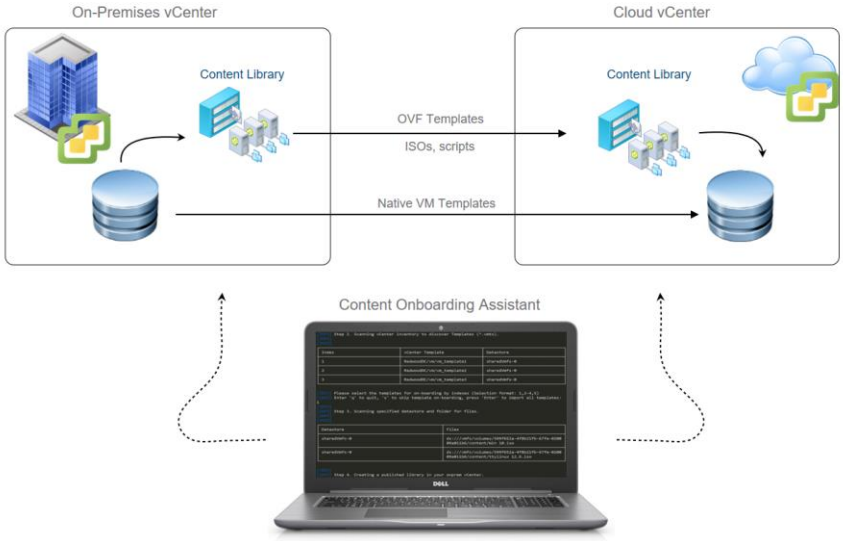
Content Onboarding Assistant (COA)

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

Copyright © 2019 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

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

Copyright © 2019 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

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:

Copyright © 2019 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

- 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
Copyright © 2019 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

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
Copyright © 2019 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

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.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
Copyright © 2019 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.