



# **VMware in the Hyperscalers Configuration**

## **NetApp Solutions**

NetApp  
August 02, 2023

This PDF was generated from <https://docs.netapp.com/us-en/netapp-solutions/ehc/aws/aws-setup.html> on August 02, 2023. Always check docs.netapp.com for the latest.

# Table of Contents

- Configuring the virtualization environment in the cloud provider . . . . . 1
  - Deploy and configure the Virtualization Environment on AWS. . . . . 2
  - Deploy and configure the Virtualization Environment on Azure . . . . . 18
  - Deploy and configure the Virtualization Environment on Google Cloud Platform (GCP). . . . . 26

# Configuring the virtualization environment in the cloud provider

Details for how to configure the virtualization environment in each of the supported hyperscalers are covered here.

## AWS / VMC

This section describes how to set up and manage VMware Cloud on AWS SDDC and use it in combination with the available options for connecting NetApp storage.



In-guest storage is the only supported method of connecting Cloud Volumes ONTAP to AWS VMC.

The setup process can be broken down into the following steps:

- Deploy and Configure VMware Cloud for AWS
- Connect VMware Cloud to FSx ONTAP

View the detailed [configuration steps for VMC](#).

## Azure / AVS

This section describes how to set up and manage Azure VMware Solution and use it in combination with the available options for connecting NetApp storage.



In-guest storage is the only supported method of connecting Cloud Volumes ONTAP to Azure VMware Solution.

The setup process can be broken down into the following steps:

- Register the resource provider and create a private cloud
- Connect to a new or existing ExpressRoute virtual network gateway
- Validate the network connectivity and access the private cloud

View the detailed [configuration steps for AVS](#).

## GCP / GCVE

This section describes how to set up and manage GCVE and use it in combination with the available options for connecting NetApp storage.



In-guest storage is the only supported method of connecting Cloud Volumes ONTAP and Cloud Volumes Services to GCVE.

The setup process can be broken down into the following steps:

- Deploy and Configure GCVE
- Enable Private Access to GCVE

View the detailed [configuration steps for GCVE](#).

# Deploy and configure the Virtualization Environment on AWS

As with on-premises, planning VMware Cloud on AWS is critical for a successful

production-ready environment for creating VMs and migration.

This section describes how to set up and manage VMware Cloud on AWS SDDC and use it in combination with the available options for connecting NetApp storage.



In-guest storage is currently the only supported method of connecting Cloud Volumes ONTAP (CVO) to AWS VMC.

The setup process can be broken down into the following steps:

## Deploy and configure VMware Cloud for AWS

[VMware Cloud on AWS](#) provides for a cloud native experience for VMware based workloads in the AWS ecosystem. Each VMware Software-Defined Data Center (SDDC) runs in an Amazon Virtual Private Cloud (VPC) and provides a full VMware stack (including vCenter Server), NSX-T software-defined networking, vSAN software-defined storage, and one or more ESXi hosts that provide compute and storage resources to your workloads.

This section describes how to set up and manage VMware Cloud on AWS and use it in combination with Amazon FSx for NetApp ONTAP and/or Cloud Volumes ONTAP on AWS with in-guest storage.



In-guest storage is currently the only supported method of connecting Cloud Volumes ONTAP (CVO) to AWS VMC.

The setup process can be broken down into three parts:

### Register for an AWS Account

Register for an [Amazon Web Services Account](#).

You need an AWS account to get started, assuming there isn't one created already. New or existing, you need administrative privileges in the account for many steps in this procedure. See this [link](#) for more information regarding AWS credentials.

### Register for a My VMware Account

Register for a [My VMware](#) account.

For access to VMware's cloud portfolio (including VMware Cloud on AWS), you need a VMware customer account or a My VMware account. If you have not already done so, create a VMware account [here](#).

## Provision SDDC in VMware Cloud

After the VMware account is configured and proper sizing is performed, deploying a Software-Defined Data Center is the obvious next step for using the VMware Cloud on AWS service. To create an SDDC, pick an AWS region to host it, give the SDDC a name, and specify how many ESXi hosts you want the SDDC to contain. If you don't already have an AWS account, you can still create a starter configuration SDDC that contains a single ESXi host.

1. Log into the VMware Cloud Console using your existing or newly created VMware credentials.



2. Configure the AWS region, deployment, and host type and the SDDC name:



3. Connect to the desired AWS account and execute the AWS Cloud Formation stack.

← → ↺ ⌂

https://us-west-2.console.aws.amazon.com/cloudformation/home?region=us-west-2#/stacks/quickcreate?stackName=vmware-sddc

Services 🔍 Search for services, features, marketplace products, and docs [Option+S] 550 Administrator/WILLStowe@metasp.com @cloudheroes Oregon Support

CloudFormation > Stacks > Create stack

Quick create stack

Template

Template URL  
https://vmware-sddc.s3.us-west-2.amazonaws.com/1eb9d184-a706-448b-abb8-692aadd0a25d0/mq5ijohktclieoh8l5b75ntega9kcc4bdd7iffq07m7v16fk36

Stack description  
This template is created by VMware Cloud on AWS for SDDC deployment and maintenance. Please do not remove.

Stack name

Stack name  
vmware-sddc-formation-a87f51c9-e5ac-4bb4-9d1e-9a3dabd197b7

Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).

Parameters

Parameters are defined in your template and allow you to input custom values when you create or update a stack.

Feedback English (US)

© 2008 - 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use Cookie preferences

← → ↺ ⌂

https://us-west-2.console.aws.amazon.com/cloudformation/home?region=us-west-2#/stacks/quickcreate?stackName=vmware-sddc

Services 🔍 Search for services, features, marketplace products, and docs [Option+S] 550 Administrator/WILLStowe@metasp.com @cloudheroes Oregon Support

Stack name

Stack name  
vmware-sddc-formation-a87f51c9-e5ac-4bb4-9d1e-9a3dabd197b7

Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).

Parameters

Parameters are defined in your template and allow you to input custom values when you create or update a stack.

No parameters  
There are no parameters defined in your template

Capabilities

The following resource(s) require capabilities: [AWS::IAM::Role]

This template contains Identity and Access Management (IAM) resources that might provide entities access to make changes to your AWS account. Check that you want to create each of these resources and that they have the minimum required permissions. [Learn more](#)

☐ I acknowledge that AWS CloudFormation might create IAM resources.

Cancel Create change set Create stack

Feedback English (US)

© 2008 - 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use Cookie preferences





Single-host configuration is used in this validation.

4. Select the desired AWS VPC to connect the VMC environment with.



5. Configure the VMC Management Subnet; this subnet contains VMC-managed services like vCenter, NSX, and so on. Do not choose an overlapping address space with any other networks that need connectivity to the SDDC environment. Finally, follow the recommendations for CIDR size notated below.



6. Review and acknowledge the SDDC configuration, and then click deploy the SDDC.



The deployment process typically takes approximately two hours to complete.



7. After completion, the SDDC is ready for use.



For a step-by-step guide on SDDC deployment, see [Deploy an SDDC from the VMC Console](#).

## Connect VMware Cloud to FSx ONTAP

To connect VMware Cloud to FSx ONTAP, complete the following steps:

1. With VMware Cloud deployment completed and connected to AWS VPC, you must deploy Amazon FSx for NetApp ONTAP into a new VPC rather than the original connected VPC (see the screenshot below). FSx (NFS and SMB floating IPs) is not accessible if it is deployed in the connected VPC. Keep in mind that iSCSI endpoints like Cloud Volumes ONTAP work just fine from the connected VPC.



2. Deploy an additional VPC in the same region, and then deploy Amazon FSx for NetApp ONTAP into the new VPC.

Configuration of an SDDC group in the VMware Cloud console enables the networking configuration options required to connect to the new VPC where FSx is deployed. In step 3, verify that “Configuring VMware Transit Connect for your group will incur charges per attachment and data transfers” is checked, and then choose Create Group. The process can take a few minutes to complete.

VMware Cloud

WBI Stowe  
NetApp

Launchpad

SDDCs

Subscriptions

Activity Log

Tools

Developer Center

<

Create SDDC Group

1. Name and Description

Create a name and description for your group

Name

sddcgroup01

Description

sddcgroup01

NEXT

2. Membership

Members: 1

3. Acknowledgement

Please confirm that you are aware of the following before creating this SDDC Group.

☒ Configuring VMware Transit Connect for your group will incur charges per attachment and data transfers.

Create firewall rules to establish connectivity between the SDDCs in the group

Learn More

CREATE GROUP

VMware Cloud

WBI Stowe  
NetApp

Launchpad

SDDCs

Subscriptions

Activity Log

Tools

Developer Center

<

Create SDDC Group

1. Name and Description

Name: sddcgroup01

2. Membership

Select SDDCs to be part of your group

| <input checked="" type="checkbox"/> | Name          | Sddc Id                              | Location         | Version   | Management OSB |
|-------------------------------------|---------------|--------------------------------------|------------------|-----------|----------------|
| <input checked="" type="checkbox"/> | ntap-5lx-demo | 829a6e22-92af-42db-ac03-9e4e07a908b5 | US West (Oregon) | 1.14.0.14 | 10.45.0.0/23   |

1

Items per page: 100

1 - 1 of 1 items

NEXT

3. Acknowledgement

Review and acknowledge requirements before creating the group.

Please confirm that you are aware of the following before creating this SDDC Group.

☒ Configuring VMware Transit Connect for your group will incur charges per attachment and data transfers.

Create firewall rules to establish connectivity between the SDDCs in the group

Learn More

CREATE GROUP



3. Attach the newly created VPC to the just created SDDC group. Select the External VPC tab and follow the [instructions for attaching an External VPC](#) to the group. This process can take 10 to 15 minutes to complete.





- As part of the external VPC process, you are prompted through the AWS console to a new shared resource via the Resource Access Manager. The shared resource is the [AWS Transit Gateway](#) managed by VMware Transit Connect.



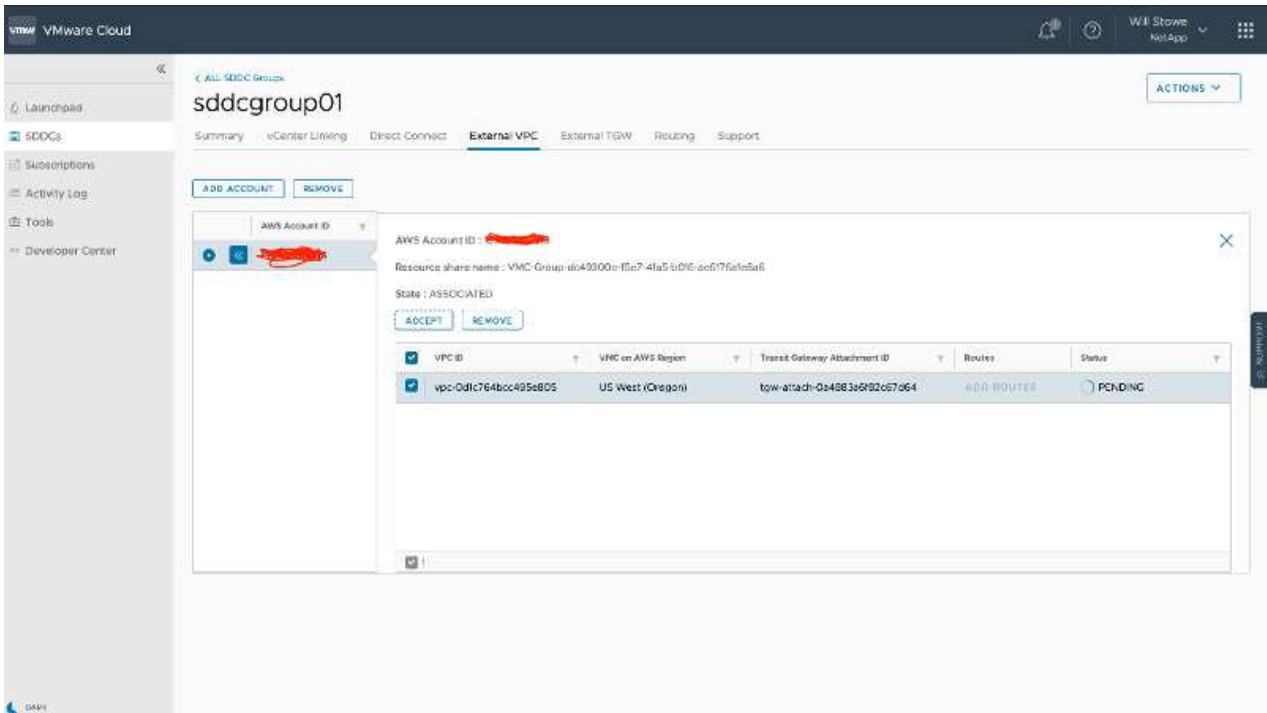




5. Create the Transit Gateway Attachment.

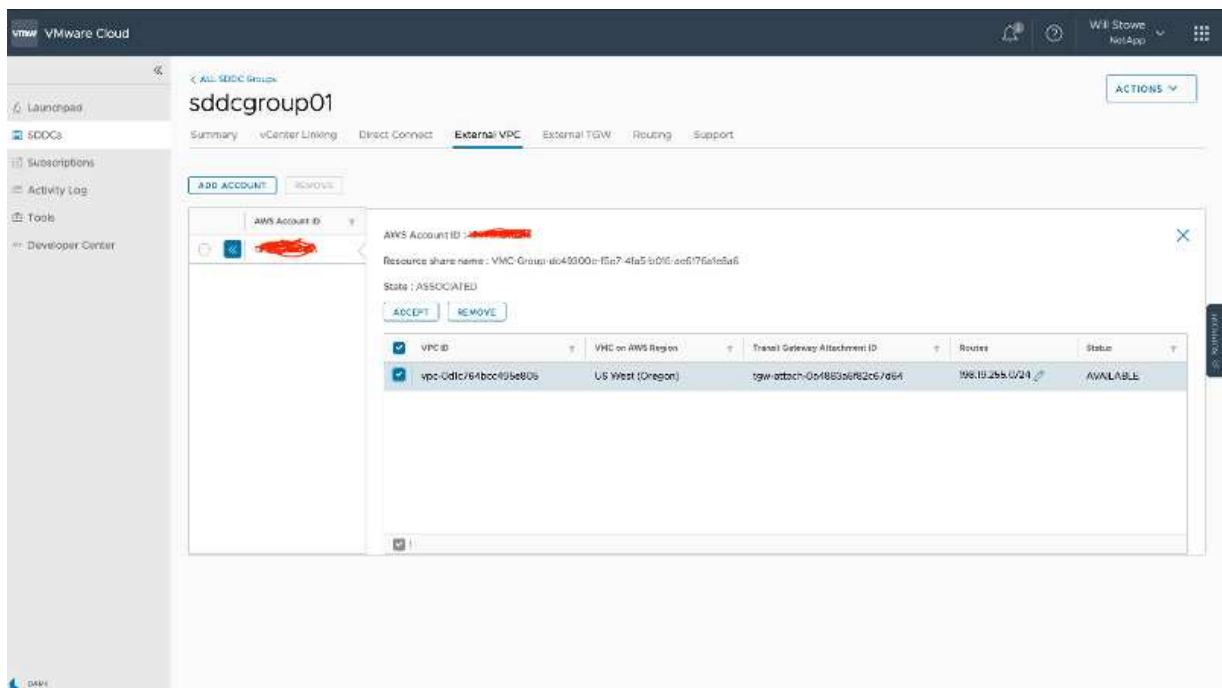


6. Back on the VMC Console, Accept the VPC attachment. This process can take approximately 10 minutes to complete.



7. While in the External VPC tab, click the edit icon in the Routes column and add in the following required routes:

- A route for the floating IP range for Amazon FSx for NetApp ONTAP [floating IPs](#).
- A route for the floating IP range for Cloud Volumes ONTAP (if applicable).
- A route for the newly created external VPC address space.



8. Finally, allow bidirectional traffic [firewall rules](#) for access to FSx/CVO. Follow these [detailed steps](#) for compute gateway firewall rules for SDDC workload connectivity.



- After the firewall groups are configured for both the Management and Compute gateway, the vCenter can be accessed as follows:



The next step is to verify that Amazon FSx ONTAP or Cloud Volumes ONTAP is configured depending on your requirements and that the volumes are provisioned to offload storage components from vSAN to optimize the deployment.

# Deploy and configure the Virtualization Environment on Azure

As with on-premises, planning Azure VMware Solution is critical for a successful production-ready environment for creating VMs and migration.

This section describes how to set up and manage Azure VMware Solution and use it in combination with the available options for connecting NetApp storage.

The setup process can be broken down into the following steps:

## Register the resource provider and create a private cloud

To use Azure VMware Solution, first register the resource provider within the identified subscription:

1. Sign in to the Azure portal.
2. On the Azure portal menu, select All Services.
3. In the All Services dialog box, enter the subscription and then select Subscriptions.
4. To view, select the subscription from the subscription list.
5. Select Resource Providers and enter Microsoft.AVS into the search.
6. If the resource provider is not registered, select Register.



| Provider                       | Status       |
|--------------------------------|--------------|
| Microsoft.OperationsManagement | ✓ Registered |
| Microsoft.Compute              | ✓ Registered |
| Microsoft.ContainerService     | ✓ Registered |
| Microsoft.ManagedIdentity      | ✓ Registered |
| Microsoft.AVS                  | ✓ Registered |
| Microsoft.Operationallnsights  | ✓ Registered |
| Microsoft.GuestConfiguration   | ✓ Registered |

7. After the resource provider is registered, create an Azure VMware Solution private cloud by using the Azure portal.
8. Sign in to the Azure portal.
9. Select Create a New Resource.
10. In the Search the Marketplace text box, enter Azure VMware Solution and select it from the results.
11. On the Azure VMware Solution page, select Create.
12. From the Basics tab, enter the values in the fields and select Review + Create.

#### Notes:

- For a quick start, gather the required information during the planning phase.
- Select an existing resource group or create a new resource group for the private cloud. A resource group is a logical container in which the Azure resources are deployed and managed.
- Make sure the CIDR address is unique and does not overlap with other Azure Virtual Networks or on-premises networks. The CIDR represents the private cloud management network and is used for the cluster management services, such as vCenter Server and NSX-T Manager. NetApp recommends using a /22 address space. In this example, 10.21.0.0/22 is used.

## Create a private cloud ...

Prerequisites \* Basics Tags Review and Create

**Project details**

Subscription \*

Resource group \*  [Create new](#)

**Private cloud details**

Resource name \*

Location \*

Size of host \*

Number of hosts \*  [Find out how many hosts you need](#)

**CIDR address block**

Provide IP address for private cloud for cluster management. Make sure these are unique and do not overlap with any other Azure vnets or on-premise networks.

Address block for private cloud \*

[Review and Create](#) [Previous](#) [Next : Tags >](#)

The provisioning process takes approximately 4–5 hours. After the process is complete, verify that the deployment was successful by accessing the private cloud from the Azure portal. A status of Succeeded is displayed when the deployment is complete.

An Azure VMware Solution private cloud requires an Azure Virtual Network. Because Azure VMware Solution doesn't support on-premises vCenter, additional steps are required to integrate with an existing on-premises environment. Setting up an ExpressRoute circuit and a virtual network gateway is also required. While waiting for the cluster provisioning to complete, create a new virtual network or use an existing one to connect to Azure VMware Solution.

[Home >](#)

 **nimoavspriv**    
AVS Private cloud

 Delete

 Overview

 Activity log

 Access control (IAM)

 Tags

 Diagnose and solve problems

**Settings**

 Locks

**Manage**

 Connectivity

 Identity

 Clusters

**Essentials**

Resource group [\(change\)](#)  
[NimoAVSDemo](#)

Status  
Succeeded

Location  
East US 2

Subscription [\(change\)](#)  
[SaaS Backup Production](#)

Subscription ID  
b58a041a-e464-4497-8be9-9048369ee8e1

Tags [\(change\)](#)  
[Click here to add tags](#)

Address block for private cloud  
10.21.0.0/22

Primary peering subnet  
10.21.0.232/30

Secondary peering subnet  
10.21.0.236/30

Private Cloud Management network  
10.21.0.0/26

vMotion network  
10.21.1.128/25

Number of hosts  
3

## Connect to a new or existing ExpressRoute virtual network gateway

To create a new Azure Virtual Network (VNet), select the Azure VNet Connect tab. Alternatively, you can create one manually from the Azure portal by using the Create Virtual Network wizard:

1. Go to Azure VMware Solution private cloud and access Connectivity under the Manage option.
2. Select Azure VNet Connect.
3. To create a new VNet, select the Create New option.

This feature allows a VNet to be connected to the Azure VMware Solution private cloud. The VNet enables communication between workloads in this virtual network by automatically creating required components (for example, jump box, shared services such as Azure NetApp Files, and Cloud Volume ONTAP) to the private cloud created in Azure VMware Solution over ExpressRoute.

**Note:** The VNet address space should not overlap with the private cloud CIDR.



4. Provide or update the information for the new VNet and select OK.



## Create virtual network



This virtual network enables the communication between workloads in this virtual network (e.g. a Jumpbox) to the private cloud created in Azure VMware Solution over an Express route. A default address range and a subnet is selected for this virtual network. For changing the default address range and subnet of this virtual network, follow these steps: Step 1: Change the "Address Range" to desired range (e.g. 172.16.0.0/16). Step 2: Add a subnet under "Subnets" with the name as "GatewaySubnet" and provide subnet's address range in CIDR notation (e.g. 172.16.1.0/24). [Learn more about virtual networks](#)

Name \*

**Address space**

The virtual network's address space specified as one or more address prefixes in CIDR notation (e.g. 10.0.0.0/16).

| <input type="checkbox"/> Address range | Addresses                                     | Overlap |  |
|--|---|---------|--|
| <input type="checkbox"/> 172.24.0.0/16 | 172.24.0.4 - 172.24.255.254 (65531 addresses) | None    |  |
| <input type="text"/>                   | (0 Addresses)                                 | None    |  |

**Subnets**

The subnet's address range in CIDR notation (e.g. 10.0.0.0/24). It must be contained by the address space of the virtual network.

| <input type="checkbox"/> Subnet name   | Address range        | Addresses                                 |  |
|--|----------------------|---|--|
| <input type="checkbox"/> GatewaySubnet | 172.24.0.0/24        | 172.24.0.4 - 172.24.0.254 (251 addresses) |  |
| <input type="text"/>                   | <input type="text"/> | (0 Addresses)                             |  |

The VNet with the provided address range and gateway subnet is created in the designated subscription and resource group.



If you create a VNet manually, create a virtual network gateway with the appropriate SKU and ExpressRoute as the gateway type. After the deployment is complete, connect the ExpressRoute connection to the virtual network gateway containing Azure VMware Solution private cloud using the authorization key. For more information, see [Configure networking for your VMware private cloud in Azure](#).

## Validate the network connect and access to Azure VMware Solution private cloud

Azure VMware Solution does not allow you to manage a private cloud with on-premises VMware vCenter. Instead, jump host is required to connect to the Azure VMware Solution vCenter instance. Create a jump host in the designated resource group and sign in to the Azure VMware Solution vCenter. This jump host should be a Windows VM on the same virtual network that was created for connectivity and should provide access to both vCenter and the NSX Manager.

### Create a virtual machine

Basics   Disks   Networking   Management   Advanced   Tags   Review + create


Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. [Learn more](#)

#### Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

|                  |  |
|------------------|--|
| Subscription *   | <div>SaaS Backup Production</div>            |
| Resource group * | <div>NimoAVSDemo</div> <div>Create new</div> |

#### Instance details

|                        |   |
|------------------------|---|
| Virtual machine name * | <div>nimAVS.R1</div>  |
| Region *               | <div>(US) East US 2</div>   |
| Availability options   | <div>No infrastructure redundancy required</div>  |
| Image *                | <div> Windows Server 2012 R2 Datacenter - Gen2</div> <div>See all images</div> |
| Azure Spot instance    | <div><input type="checkbox"/></div>   |
| Size *                 | <div>Standard_D2s_v3 - 2 vcpus, 8 GiB memory (\$130.67/month)</div> <div>See all sizes</div>  |

After the virtual machine is provisioned, use the Connect option to access RDP.

## nimAVSJH | Connect

Virtual machine

Search (Ctrl+/)

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Settings
  - Networking
  - Connect
  - Disks
  - Size

To improve security, enable just-in-time access on this VM. →

RDP SSH BASTION

### Connect with RDP

To connect to your virtual machine via RDP, select an IP address, optionally change the port number, and download the RDP file.

IP address \*

Public IP address (52.138.103.135)

Port number \*

3389

Download RDP File

Sign in to vCenter from this newly created jump host virtual machine by using the cloud admin user . To access the credentials, go to the Azure portal and navigate to Identity (under the Manage option within the private cloud). The URLs and user credentials for the private cloud vCenter and NSX-T Manager can be copied from here.

## nimoavspriv | Identity

AWS Private cloud

Search (Ctrl+/)

- Access control (IAM)
- Tags
- Diagnose and solve problems
- Settings
  - Locks
- Manage
  - Connectivity
  - Identity
  - Clusters
  - Placement policies (preview)
  - Add-ons

### Login credentials

#### vCenter credentials

Web client URL ⓘ

https://10.21.0.2/ ⓘ

Admin username ⓘ

cloudadmin@vsphere.local ⓘ

Admin password ⓘ



Certificate thumbprint ⓘ

AE26B15A5CE38DC069D35F045F088CA6343475EC ⓘ

#### NSX-T Manager credentials

Web client URL ⓘ

https://10.21.0.3/ ⓘ

Admin username ⓘ

admin ⓘ

Admin password ⓘ



Certificate thumbprint ⓘ

B2B722EA683958283EE159007246D5166D0509D3 ⓘ

In the Windows virtual machine, open a browser and navigate to the vCenter web client URL (<https://10.21.0.2/>) and use the admin user name as **cloudadmin@vsphere.local** and paste the copied password. Similarly, NSX-T manager can also be accessed using the web client URL (<https://10.21.0.3/>) and use the admin user name and paste the copied password to create new segments or modify the existing tier gateways.



The web client URLs are different for each SDDC provisioned.



The top screenshot shows the VMware vSphere login page. The URL bar indicates a connection to `vc.beeb9fd29eab4cbea81e62.eastus2.avs.azure.com/webssso/SAML2/SSO/vsphere.local?SAMLRequest=zVRdbSwfP0ryO9gMFFCrjCqa1atUrtmJZuniv...`. The login form includes the text "VMware® vSphere", a username field with `cloudadmin@vsphere.local`, a password field with masked characters, and a checkbox for "Use Windows session authentication". A blue "LOGIN" button is at the bottom.

The bottom screenshot shows the vSphere Client interface. The top navigation bar includes "vm vSphere Client", a search bar, and a user profile for `cloudadmin@VSPHERELOCAL`. The main content area displays the "SDDC-Datacenter" with a summary of resources: Virtual Machines: 0, Hosts: 3. On the right, resource usage is shown for CPU (Used: 18.92 GHz, Capacity: 247.75 GHz), Memory (Used: 246.61 GB, Capacity: 1.68 TB), and Storage (Used: 7.6 TB, Capacity: 41.92 TB). Below this are sections for "Custom Attributes" and "Tags". At the bottom, a "Recent Tasks" table shows a completed task:

| Task Name        | Target  | Status    | Details                     | Initiator       | Queued For | Start Time              | Completion Time         | Server             |
|------------------|---|-----------|-----------------------------|-----------------|------------|-------------------------|-------------------------|--------------------|
| Undeploy plug-in | vc.beeb9fd29eab4cbea81e62.eastus2.avs.azure.com | Completed | VMware vRops Client Plug-in | VSPHERELOCAL... | 8 ms       | 08/12/2021, 11:38:11 AM | 08/12/2021, 11:38:11 AM | vc.beeb9fd29eab... |

The Azure VMware Solution SDDC is now deployed and configured. Leverage ExpressRoute Global Reach to connect the on-premises environment to Azure VMware Solution private cloud. For more information, see [Peer on-premises environments to Azure VMware Solution](#).

## Deploy and configure the Virtualization Environment on Google Cloud Platform (GCP)

As with on-premises, planning Google Cloud VMware Engine (GCVE) is critical for a successful production-ready environment for creating VMs and migration.

This section describes how to set up and manage GCVE and use it in combination with the available options for connecting NetApp storage.

The setup process can be broken down into the following steps:

## Deploy and configure GCVE

To configure a GCVE environment on GCP, login to the GCP console and access the VMware Engine portal.

Click on the “New Private Cloud” button and enter the desired configuration for the GCVE Private Cloud. On “Location”, make sure to deploy the private cloud in the same Region/Zone where CVS/CVO is deployed, to ensure the best performance and lowest latency.

Pre-requisites:

- Setup VMware Engine Service Admin IAM role
- [Enable VMWare Engine API access and node quota](#)
- Make sure that the CIDR range doesn't overlap with any of your on-premises or cloud subnets. The CIDR range must be /27 or higher.



The screenshot shows the 'Create Private Cloud' form in the Google Cloud VMware Engine console. The form includes a sidebar with navigation icons for Home, Resources, Network, Activity, and Account. The main form fields are: 'Private Cloud name' (NIMoGCVE), 'Location' (us-east4 > v-zone-a > VE Placement Group 2, highlighted with a red box), 'Node type' (ve1-standard-72, 2x2.6 GHz, 36 Cores (72 HT), 768 GB RAM, 19.2 TB Raw, 3.2 TB Cache (All-Flash)), 'Node count' (3, with a range of 3 to 3), 'vSphere/vSAN subnets CIDR range' (192.168.100.0 / 22), and 'HCX Deployment Network CIDR range' (192.168.104.0 / 26). The form also displays the corresponding IP ranges for each CIDR range.

Note: Private cloud creation can take between 30 minutes to 2 hours.

## Enable Private Access to GCVE

Once the Private Cloud is provisioned, configure private access to the Private Cloud for high-throughput and low-latency data-path connection.

This will ensure that the VPC network where Cloud Volumes ONTAP instances are running is able to communicate with the GCVE Private Cloud. To do so, follow the [GCP documentation](#). For the Cloud Volume Service, establish a connection between VMware Engine and Cloud Volumes Service by performing a one-time peering between the tenant host projects. For detailed steps, follow this [link](#).

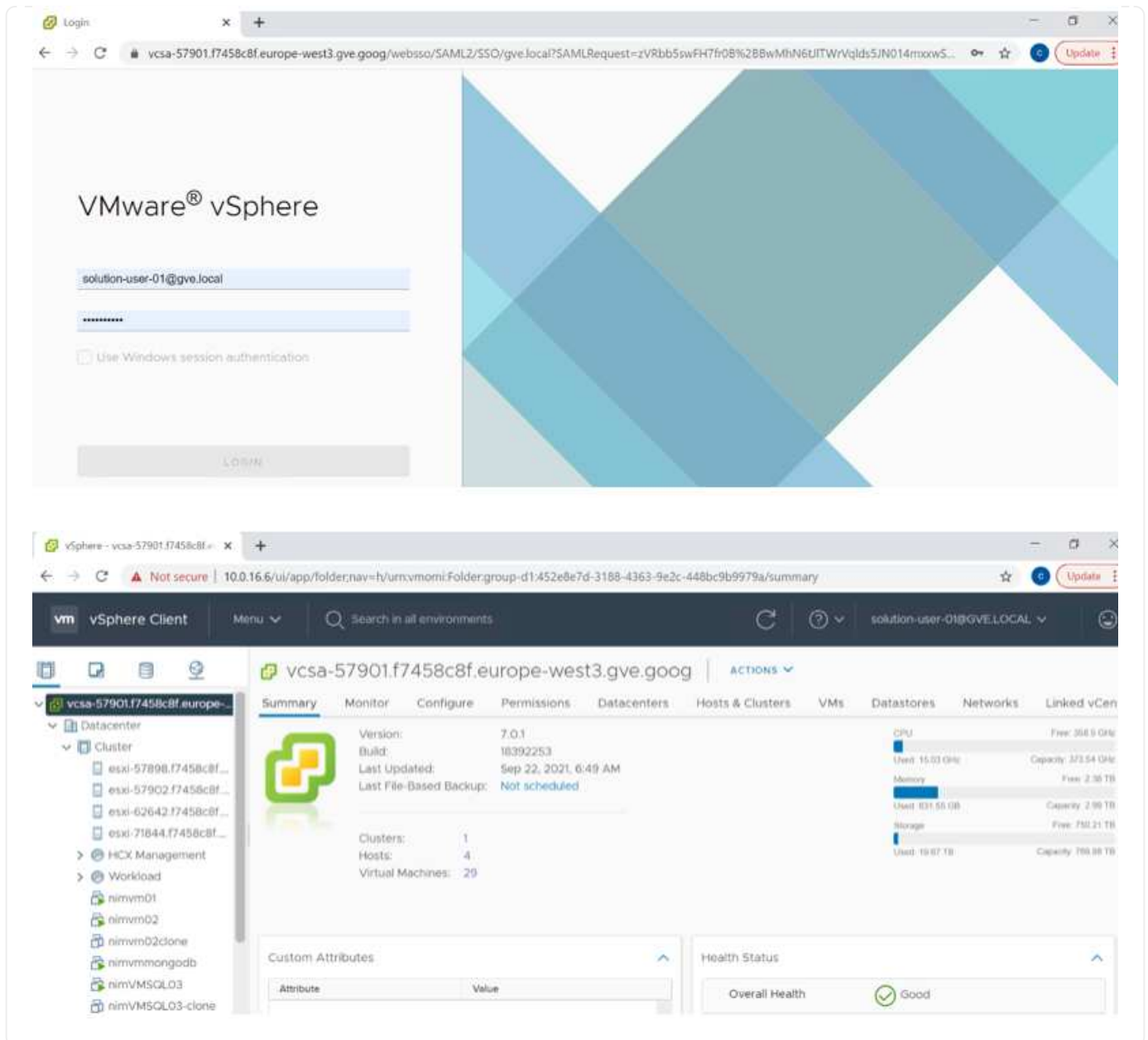
| Tenant P           | Service     | Region       | Routing Mode | Peered Project ID    | Peered VPC        | VPC Peering Sta... | Region Status |
|--------------------|-------------|--------------|--------------|----------------------|-------------------|--------------------|---------------|
| ke841388caa56b...  | VPC Network | europe-west3 | Global       | cy-performance-te... | cloud-volumes-vpc | Active             | Connected     |
| jbd729510b3ebbf... | NetApp CVS  | europe-west3 | Global       | y2b6c17202af6dc...   | netapp-tenant-vpc | Active             | Connected     |

Sign in to vcenter using the [CloudOwner@gve.local](#) user. To access the credentials, go to the VMware Engine portal, Go to Resources, and select the appropriate private cloud. In the Basic info section, click the View link for either vCenter login info (vCenter Server, HCX Manager) or NSX-T login info (NSX Manager).

The screenshot shows the Google Cloud VMware Engine (GCVE) console. The top navigation bar is blue with the 'Google Cloud VMware Engine' logo and several icons. The left sidebar contains a 'Resources' section with icons for Home, Resources, Network, Activity, and Account. The main content area is titled 'Resources' and shows a list of private clouds. The selected cloud is 'gcve-cvs-hw-eu-west3'. Below the cloud name, there are tabs for SUMMARY, CLUSTERS, SUBNETS, ACTIVITY, VSPHERE MANAGEMENT NETWORK, ADVANCED VCENTER SETTINGS, and DNS CONFIGURATION. The 'SUMMARY' tab is active, showing a table with columns for Name, Status, Location, Expandable, vCenter login info, NSX-T login info, Cloud Monitoring, Private Cloud DNS Servers, and Upgradeable. The table shows that the cloud is 'Operational' and provides links to view vCenter and NSX-T login info. Below the table, there is a 'Capacity' section showing 'Total nodes: 4', 'Total CPU capacity: 144 cores', and 'Total RAM: 3072 GB'.

In a Windows virtual machine, open a browser and navigate to the vCenter web client URL (<https://10.0.16.6/>) and use the admin user name as [CloudOwner@gve.local](#) and paste the copied password. Similarly, NSX-T manager can also be accessed using the web client URL (<https://10.0.16.11/>) and use the admin user name and paste the copied password to create new segments or modify the existing tier gateways.

For connecting from an on-premises network to VMware Engine private cloud, leverage cloud VPN or Cloud Interconnect for appropriate connectivity and make sure the required ports are open. For detailed steps, follow this [link](#).



## Deploy NetApp Cloud Volume Service supplemental datastore to GCVE

Refer [Procedure to deploy supplemental NFS datastore with NetApp CVS to GCVE](#)



## Copyright information

Copyright © 2023 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

## Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.