



# ハイパースケーラ構成における **VMware** NetApp Solutions

NetApp  
April 10, 2024

# 目次

クラウドプロバイダでの仮想化環境の設定 .....	1
AWS に仮想化環境を導入して設定 .....	3
Azure に仮想化環境を導入して設定 .....	18
Google Cloud Platform （ GCP ） への仮想化環境の導入と構成 .....	26

# クラウドプロバイダでの仮想化環境の設定

サポートされている各ハイパースケーラで仮想化環境を設定する方法については、こちらで詳しく説明しています。

## AWS / VMC

このセクションでは、AWS SDDC で VMware Cloud をセットアップおよび管理する方法と、ネットアップストレージの接続に使用できるオプションについて説明します。



Cloud Volumes ONTAP をAWS VMCに接続する方法としてサポートされているのは、ゲスト内ストレージだけです。

セットアッププロセスは、次の手順に分けることができます。

- VMware Cloud for AWSを導入して設定
- VMware Cloud を FSX ONTAP に接続します

詳細を表示します ["VMCの設定手順"](#)。

## Azure / AVS

このセクションでは、Azure VMware 解決策をセットアップおよび管理する方法と、ネットアップストレージの接続に使用できるオプションについて説明します。



Cloud Volumes ONTAP をAzure VMware解決策 に接続する方法としてサポートされているのは、ゲスト内ストレージだけです。

セットアッププロセスは、次の手順に分けることができます。

- リソースプロバイダを登録し、プライベートクラウドを作成
- 新しい ExpressRoute 仮想ネットワークゲートウェイまたは既存の ExpressRoute 仮想ネットワークゲートウェイに接続します
- ネットワーク接続を検証し、プライベートクラウドにアクセス

詳細を表示します ["AVSの設定手順"](#)。

## GCP/GCVE

このセクションでは、GCVE のセットアップと管理方法、およびネットアップストレージの接続に使用できるオプションとの組み合わせについて説明します。



Cloud Volume と Cloud Volumes ONTAP サービスを GCVE に接続する方法としてサポートされているのは、ゲスト内ストレージだけです。

セットアッププロセスは、次の手順に分けることができます。

- GCVE を導入および設定します
- GCVE へのプライベートアクセスを有効にします

詳細を表示します ["GCVEの設定手順"](#)。

# AWS に仮想化環境を導入して設定

オンプレミスと同様に、VM と移行を作成する本番環境に適した VMware Cloud on AWS を計画することが重要です。

このセクションでは、AWS SDDC で VMware Cloud をセットアップおよび管理する方法と、ネットアップストレージの接続に使用できるオプションについて説明します。



現在、Cloud Volumes ONTAP (CVO) をAWS VMCに接続する方法としてサポートされているのは、ゲスト内ストレージだけです。

セットアッププロセスは、次の手順に分けることができます。

"[AWS 上の VMware Cloud](#)" AWS エコシステム内の VMware ベースのワークロードにクラウドネイティブのエクスペリエンスを提供します。各 VMware Software-Defined Data Center（SDDC）は Amazon Virtual Private Cloud（VPC）内で動作し、フル VMware スタック（vCenter Server を含む）、NSX ベースの Software-Defined Networking、VSAN ソフトウェア定義ストレージ、およびワークロードにコンピューティングリソースとストレージリソースを提供する 1 つ以上の ESXi ホストを提供します。

このセクションでは、AWS で VMware Cloud をセットアップおよび管理する方法について説明します。また、AWS で NetApp ONTAP を使用する場合は Amazon FSX、ゲスト内ストレージを使用する場合は Cloud Volumes ONTAP と組み合わせて使用する方法についても説明します。



現在、Cloud Volumes ONTAP（CVO）を AWS VMC に接続する方法としてサポートされているのは、ゲスト内ストレージだけです。

セットアッププロセスは、次の 3 つの部分に分けることができます。

### AWS アカウントを登録

に登録します "[Amazon Web Services アカウント](#)"。

まだ作成していない場合は、AWS アカウントが必要です。新規または既存の手順では、多くの手順を実行するためにアカウント内で管理者権限が必要です。を参照してください "[リンク](#)" をクリックしてください。

### My VMware アカウントに登録します

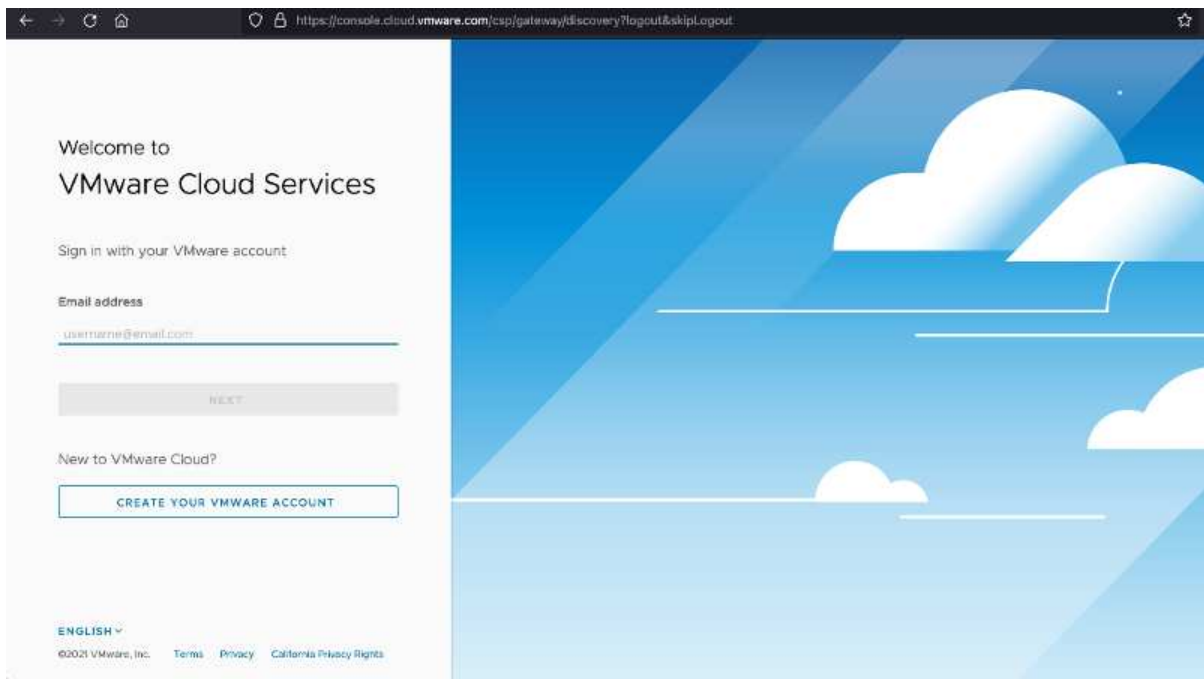
に登録します "[マイ VMware](#)" アカウント：

VMware のクラウドポートフォリオ（AWS 上の VMware Cloud を含む）にアクセスするには、VMware の顧客アカウントまたは My VMware アカウントが必要です。VMware アカウントをまだ作成していない場合は作成します "[こちらをご覧ください](#)"。

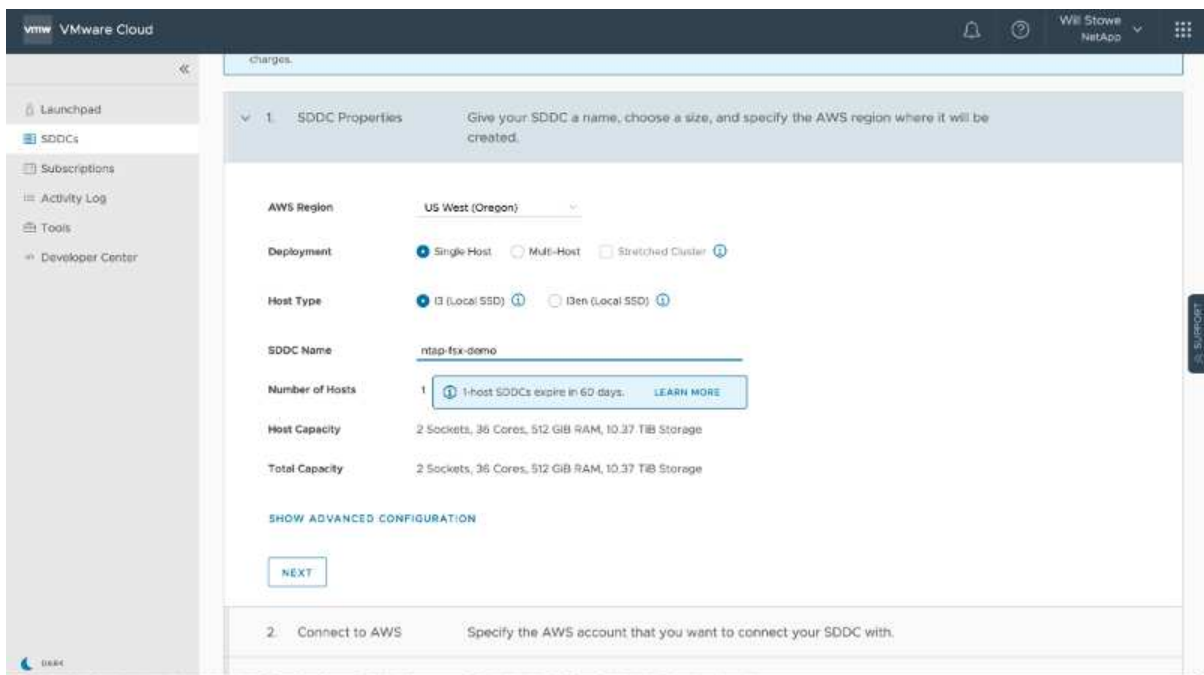
## VMware Cloud で SDDC をプロビジョニングします

VMware アカウントを設定して適切なサイジングを実行したら、AWS サービスで VMware Cloud を使用するための次の一歩として Software-Defined Data Center を導入します。SDDC を作成するには、そのホストとして AWS リージョンを選択し、SDDC に名前を付け、SDDC に含める ESXi ホストの数を指定します。AWS アカウントがない場合でも、単一の ESXi ホストを含むスターター構成の SDDC を作成できます。

1. 既存または新規に作成した VMware クレデンシャルを使用して、VMware Cloud Console にログインします。



2. AWS のリージョン、導入環境、およびホストタイプと SDDC 名を設定します。



3. 目的の AWS アカウントに接続し、AWS クラウド形成スタックを実行します。

The screenshot shows the AWS CloudFormation console in the 'us-west-2' region. The 'Quick create stack' page is displayed, showing the following details:

- Template:**
  - Template URL: `https://vmware-sddc.s3.us-west-2.amazonaws.com/1eb9d184-a706-4489-abb8-692aad0a25d0/mq5ijohctleoh8l5b75ntega9kcc4bdd7iffq07m7v16fk36`
  - 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.
  - No parameters are defined in the template.
- Capabilities:**
  - A warning box states: "The following resource(s) require capabilities: [AWS::IAM::Role]". It explains that the template contains IAM resources that might provide entities access to make changes to the AWS account. A link to "Learn more" is provided.
  - A checkbox labeled "I acknowledge that AWS CloudFormation might create IAM resources." is present.

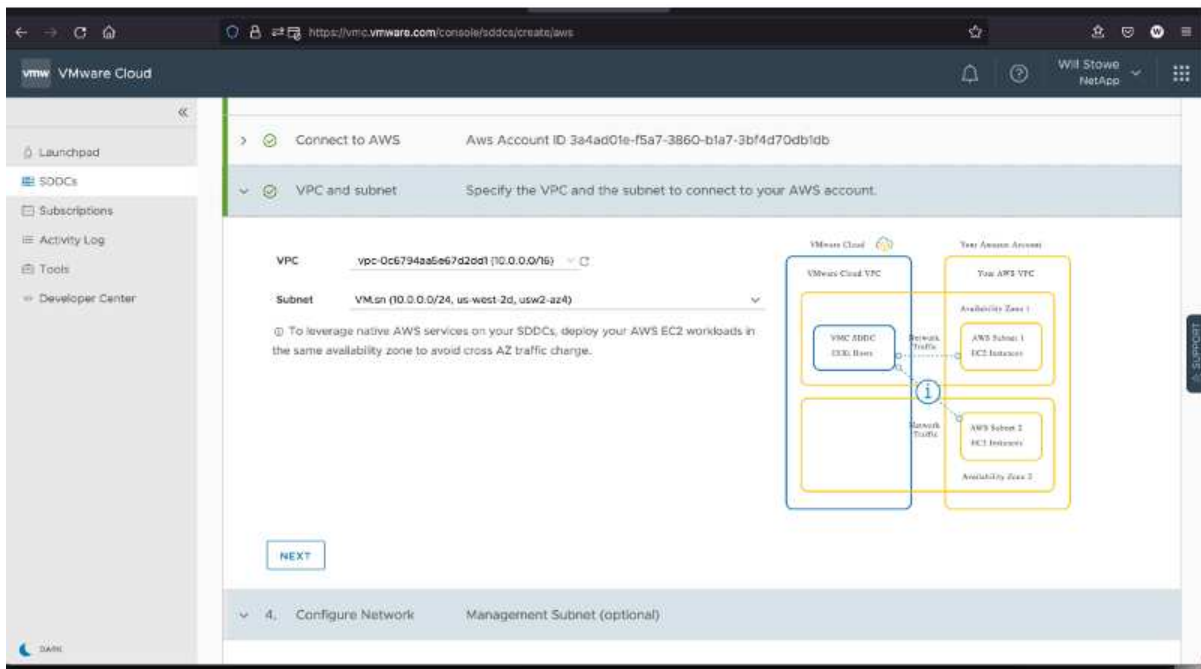
At the bottom of the page, there are three buttons: "Cancel", "Create change set", and "Create stack".



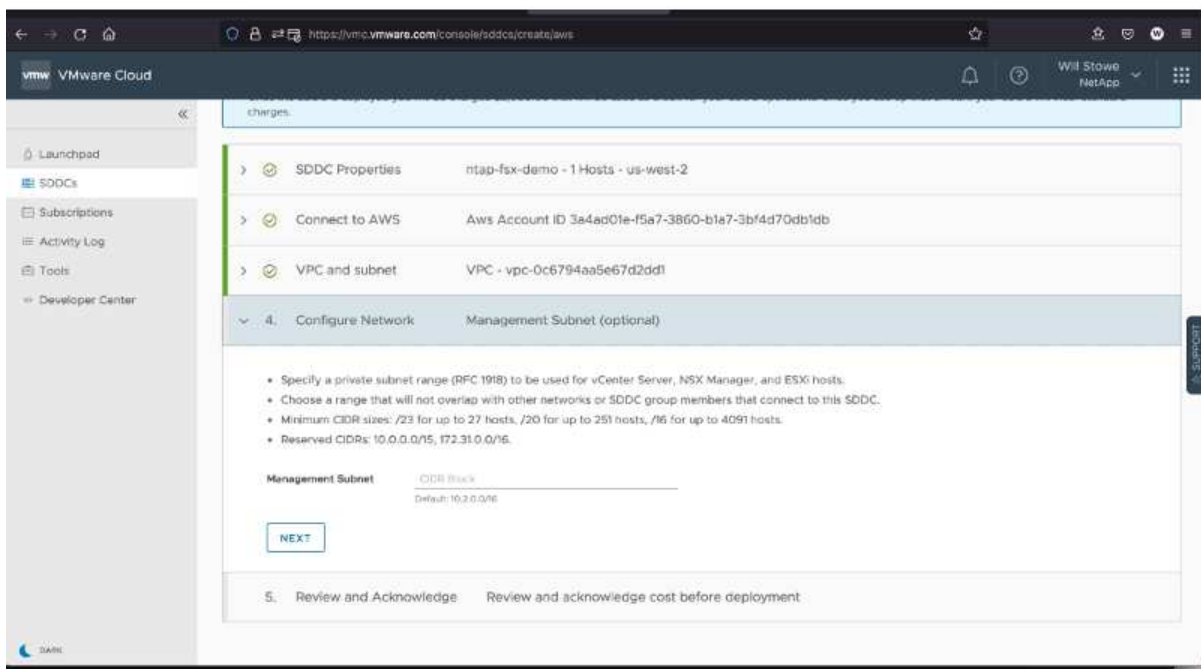


この検証ではシングルホスト構成を使用します。

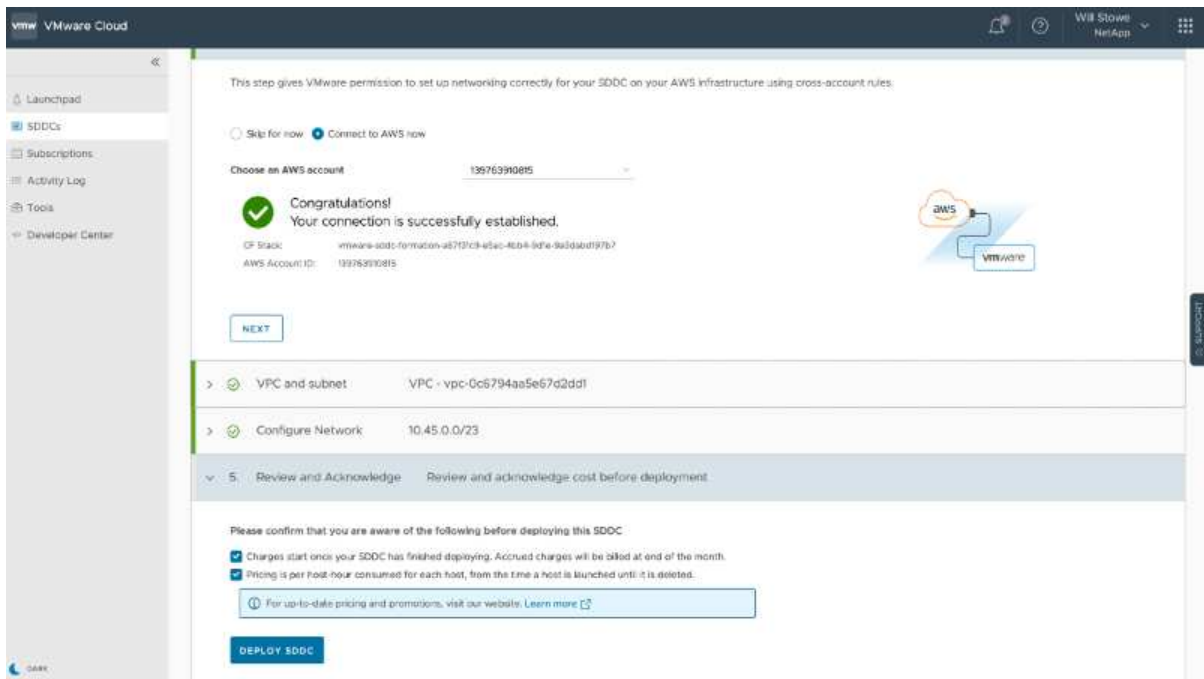
4. VMC 環境を接続する AWS VPC を選択します。



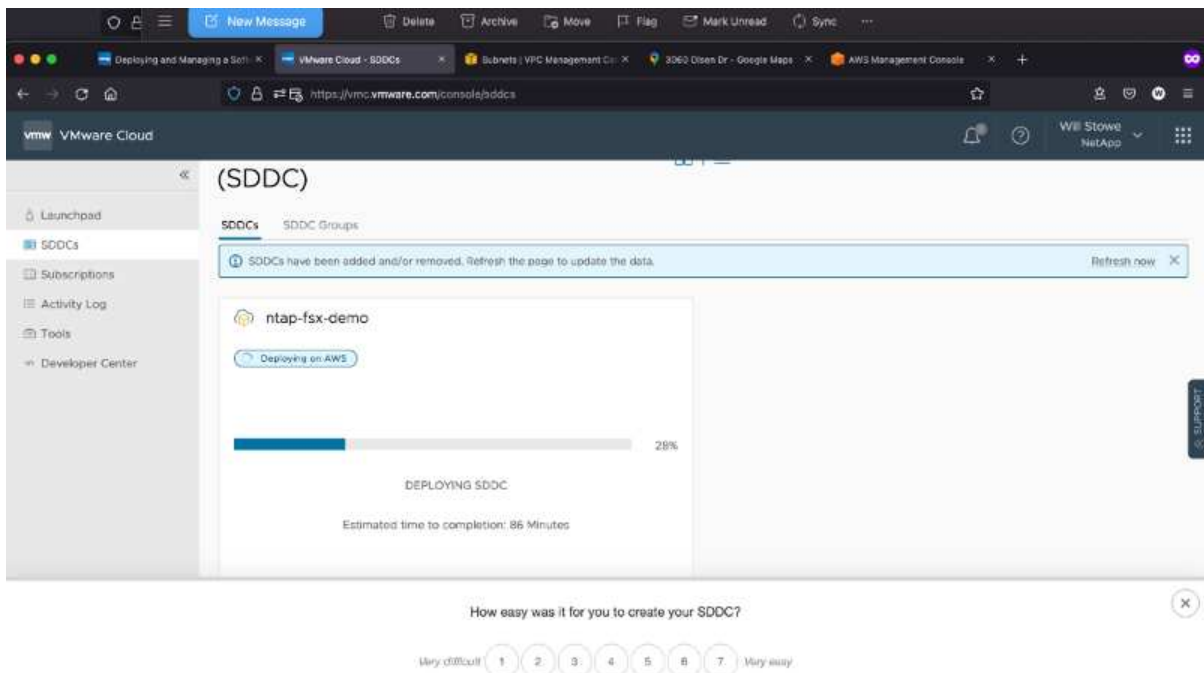
5. VMC 管理サブネットを構成します。このサブネットには、vCenter や NSX などの VMC 管理サービスが含まれます。SDDC 環境への接続が必要な他のネットワークと重複するアドレス空間を選択しないでください。最後に、以下に示す CIDR サイズの推奨事項に従います。



6. SDDC 構成を確認して承認し、[Deploy the SDDC] をクリックします。



導入プロセスの完了には、通常約 2 時間かかります。



7. 完了すると、SDDC を使用できるようになります。

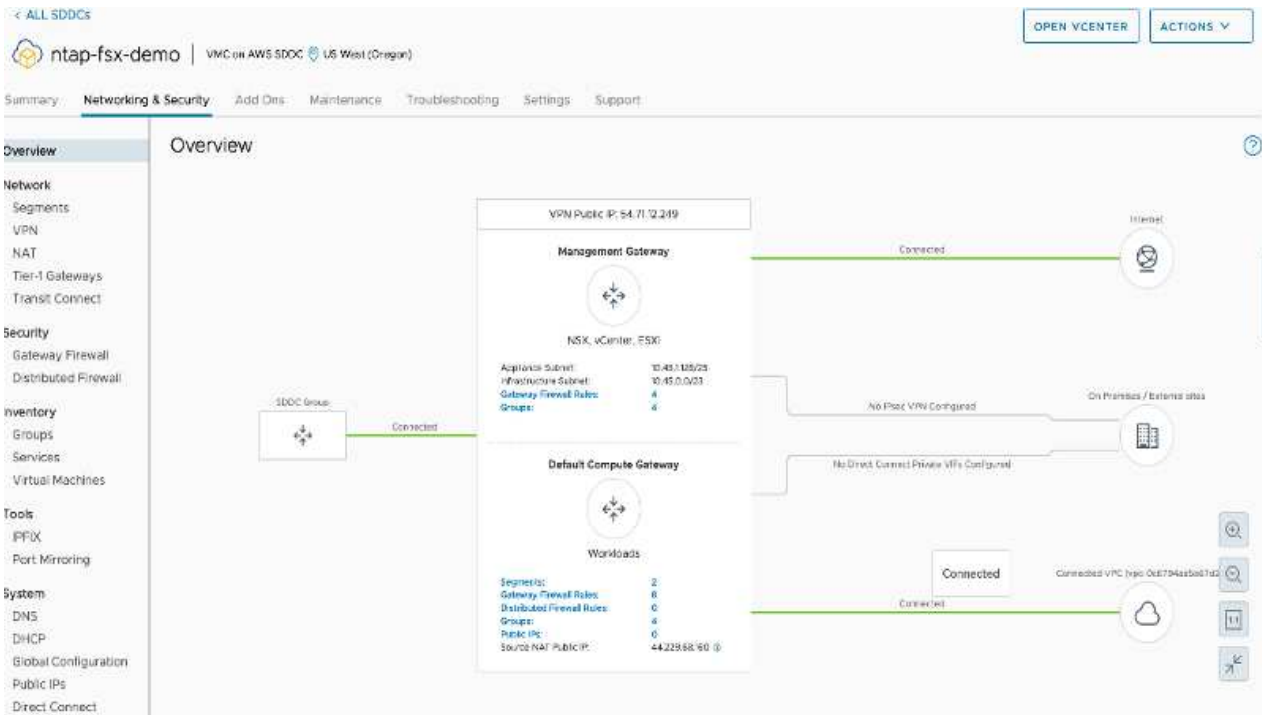


SDDC の導入の詳細な手順については、を参照してください "[VMC コンソールから SDDC を展開します](#)".

## VMware Cloud を FSX ONTAP に接続します

VMware Cloud を FSX ONTAP に接続するには、次の手順を実行します。

1. VMware Cloud の導入が完了して AWS VPC に接続されているため、Amazon FSX for NetApp ONTAP を、元の接続済み VPC ではなく新しい VPC に導入する必要があります（以下のスクリーンショットを参照）。接続された VPC に FSX（NFS および SMB のフローティング IP）が導入されている場合、これらの IP にはアクセスできません。Cloud Volumes ONTAP のような iSCSI エンドポイントは、接続された VPC からは正常に機能します。



2. 同じリージョンに別の VPC を導入し、その新しい VPC に Amazon FSX for NetApp ONTAP を導入します。

VMware Cloud コンソールで SDDC グループを構成すると、FSX が導入された新しい VPC に接続するために必要なネットワーク設定オプションが有効になります。手順 3 で、「グループ用の VMware トランジット接続の構成に添付ファイルおよびデータ転送ごとの料金が発生する」がチェックされていることを確認し、「グループの作成」を選択します。このプロセスが完了するまでに数分かかることがあります。

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	829b6e22-92af-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.

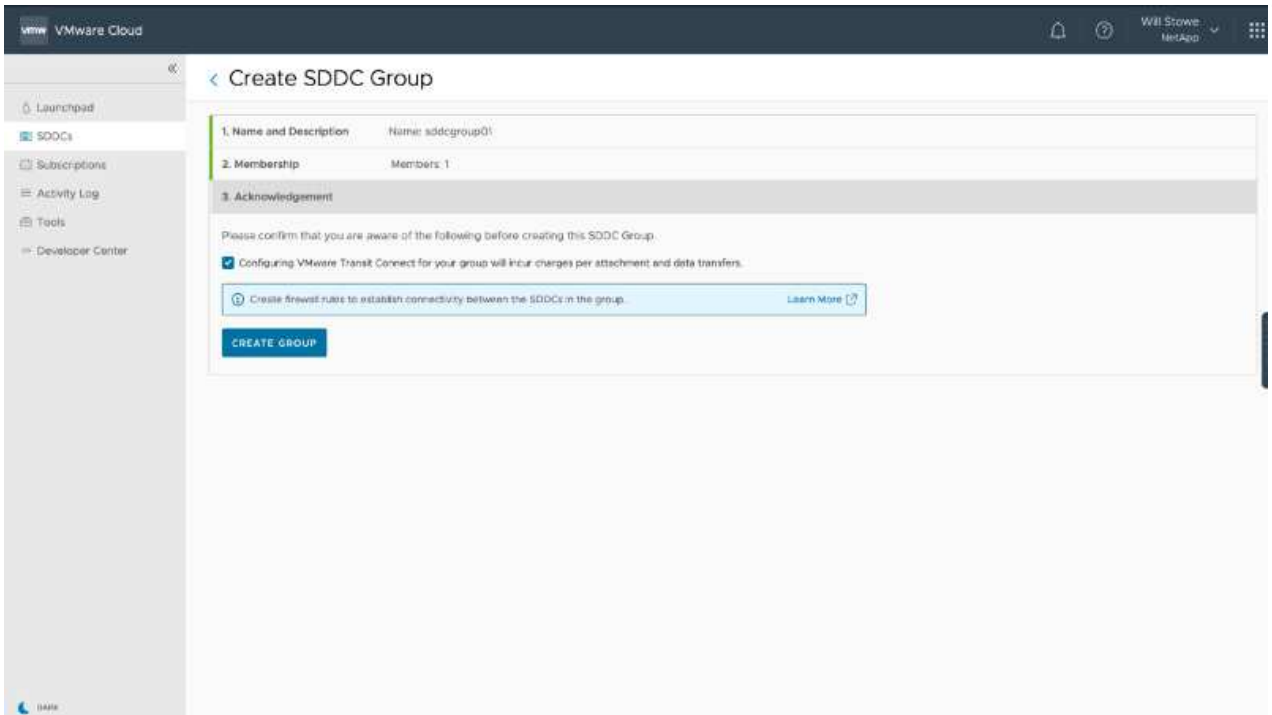
Please confirm that you are aware of the following before creating this SDDC Group.

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

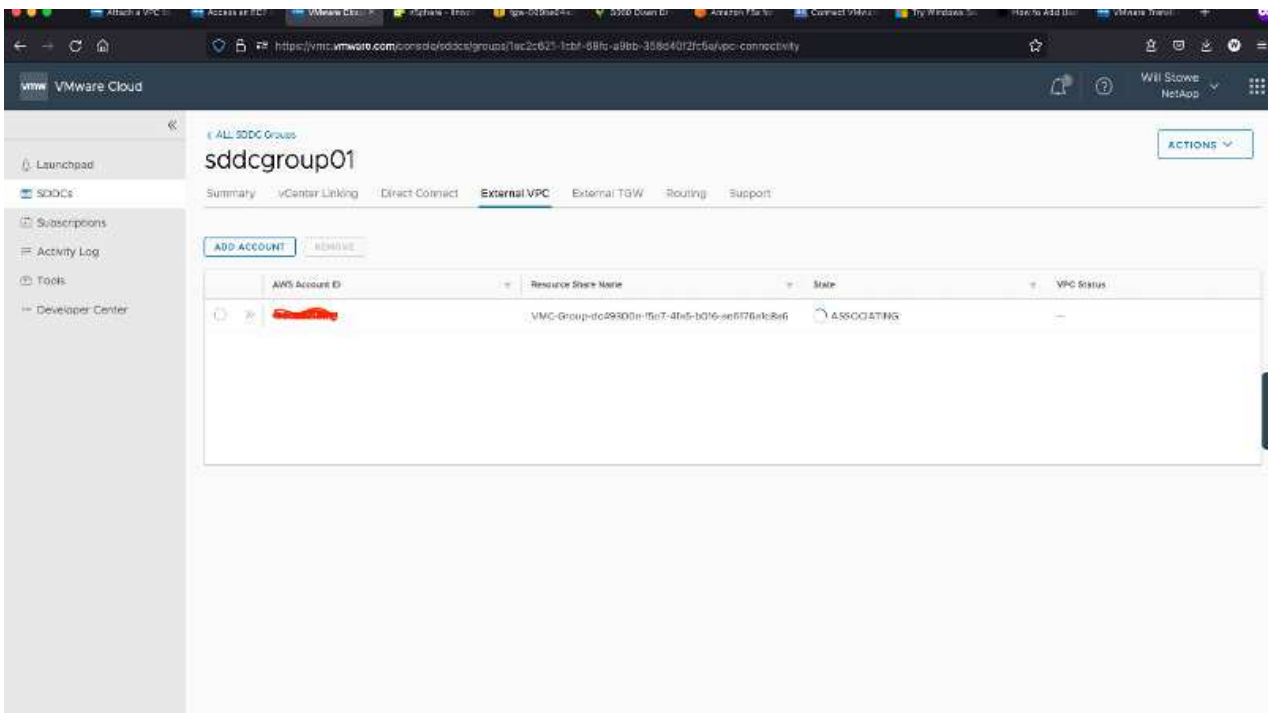
Create firewall rules to establish connectivity between the SDDCs in the group

Learn More

CREATE GROUP

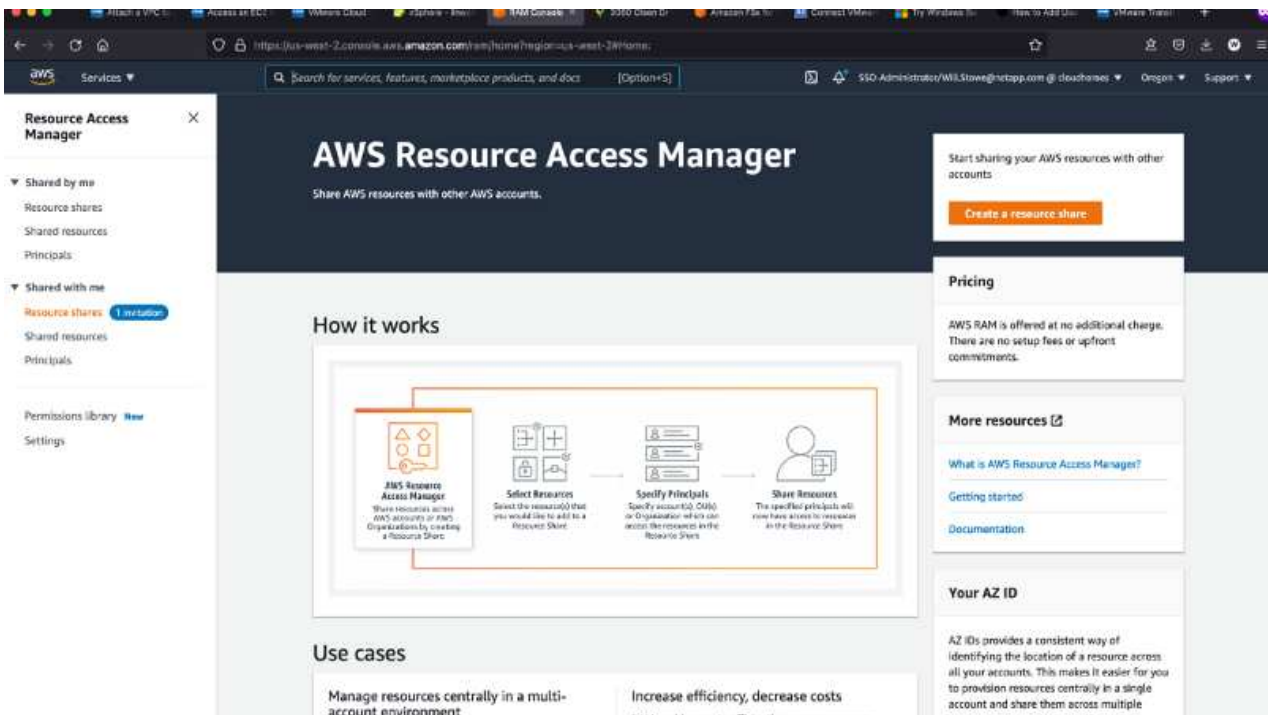


3. 新しく作成した VPC を作成した SDDC グループに接続します。[External VPC（外部 VPC）] タブを選択し、に従います "外部 VPC を接続する手順" をグループに追加します。このプロセスが完了するまでに 10~15 分かかることがあります。





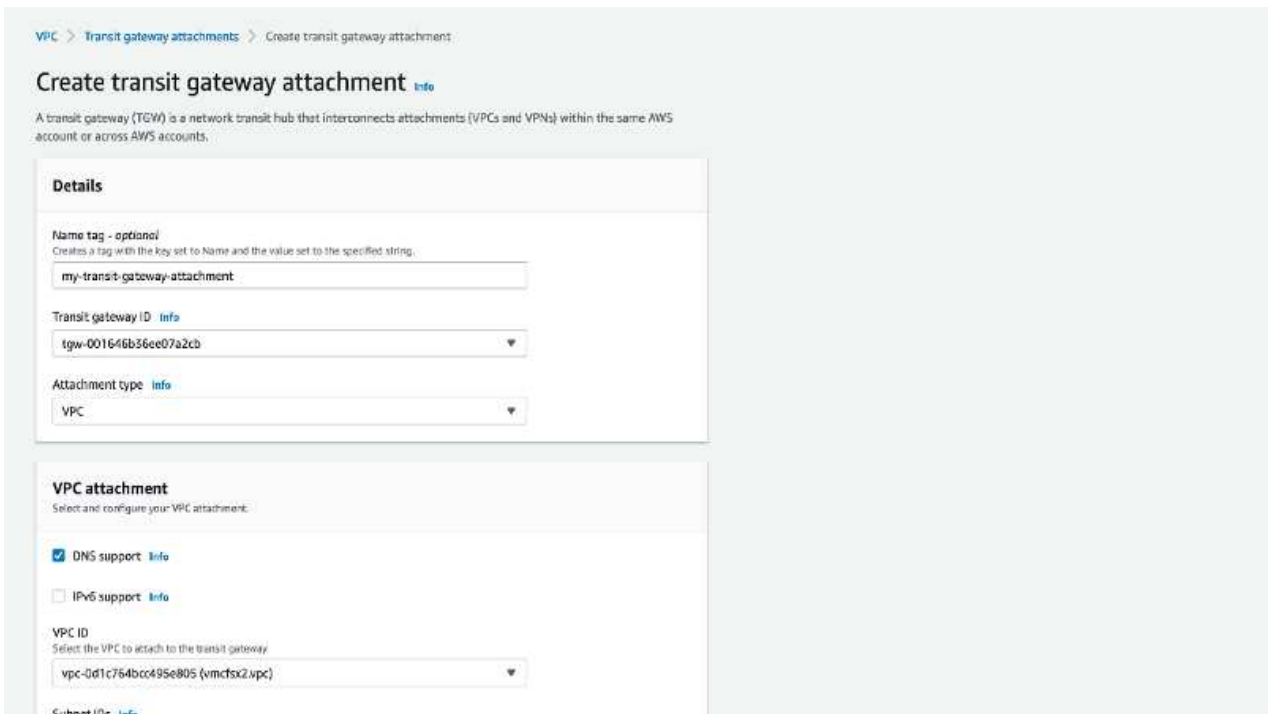
4. 外部 VPC プロセスの一環として、AWS コンソールから Resource Access Manager を使用して新しい共有リソースにアクセスするように求められます。共有リソースはです **"AWS 転送ゲートウェイ"** VMware Transit Connect によって管理されます。



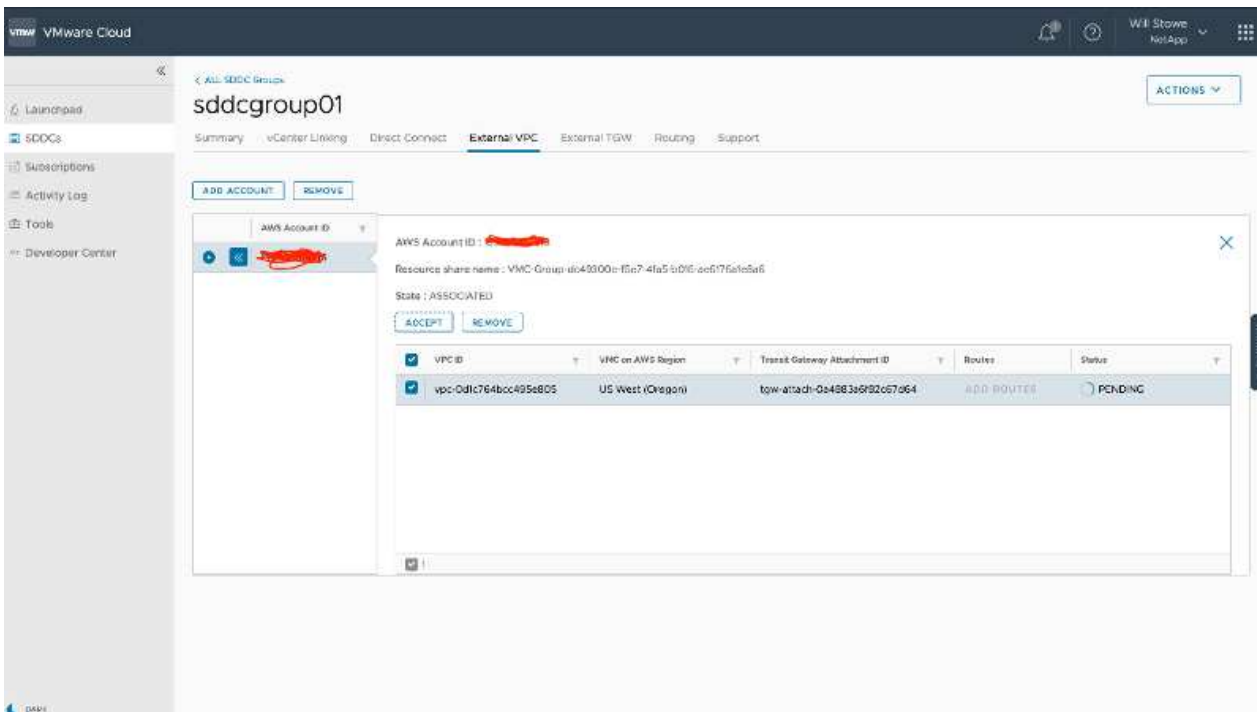




5. トランジットゲートウェイ添付ファイルを作成します。

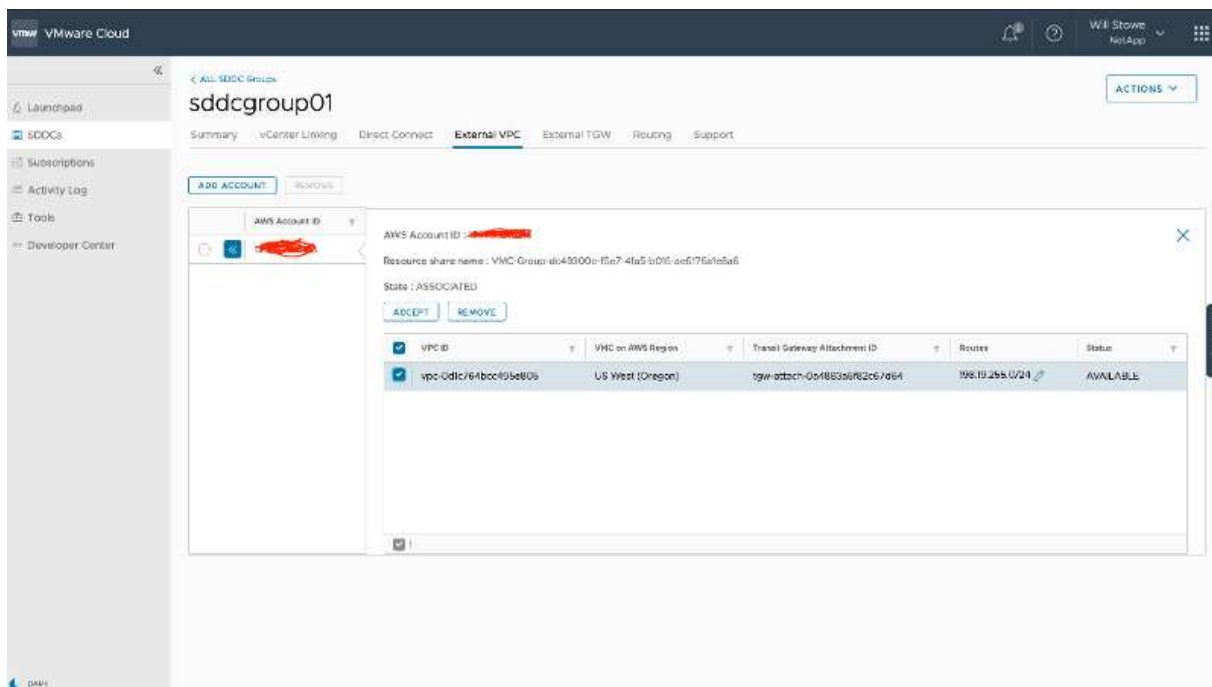


6. VMC コンソールに戻り、VPC 接続を受け入れます。この処理が完了するまでに約 10 分かかります。



7. [External VPC（外部 VPC）] タブで、[Routes] 列の編集アイコンをクリックし、次の必要なルートを追加します。

- NetApp ONTAP の Amazon FSX のフローティング IP 範囲のルート **"フローティング IP"**。
- Cloud Volumes ONTAP のフローティング IP 範囲のルート（該当する場合）。
- 新しく作成される外部 VPC アドレススペースのルート。



8. 最後に、双方向トラフィックを許可します **"ファイアウォールルール"** FSX/CVO へのアクセスに必要です。以下の手順に従ってください **"詳細な手順"** SDDC ワークロード接続用のコンピューティングゲートウェイファイアウォールルール用。



9. 管理ゲートウェイとコンピューティングゲートウェイの両方にファイアウォールグループを設定したら、次の手順で vCenter にアクセスできます。



次の手順では、Amazon FSX ONTAP または Cloud Volumes ONTAP が要件に応じて設定されていること、およびストレージコンポーネントを VSAN からオフロードして導入を最適化するようにボリュームがプロビジョニングされていることを確認します。

## Azure に仮想化環境を導入して設定

オンプレミスと同様に、Azure VMware 解決策を計画することは、VM と移行を作成する本番環境に欠かせません。

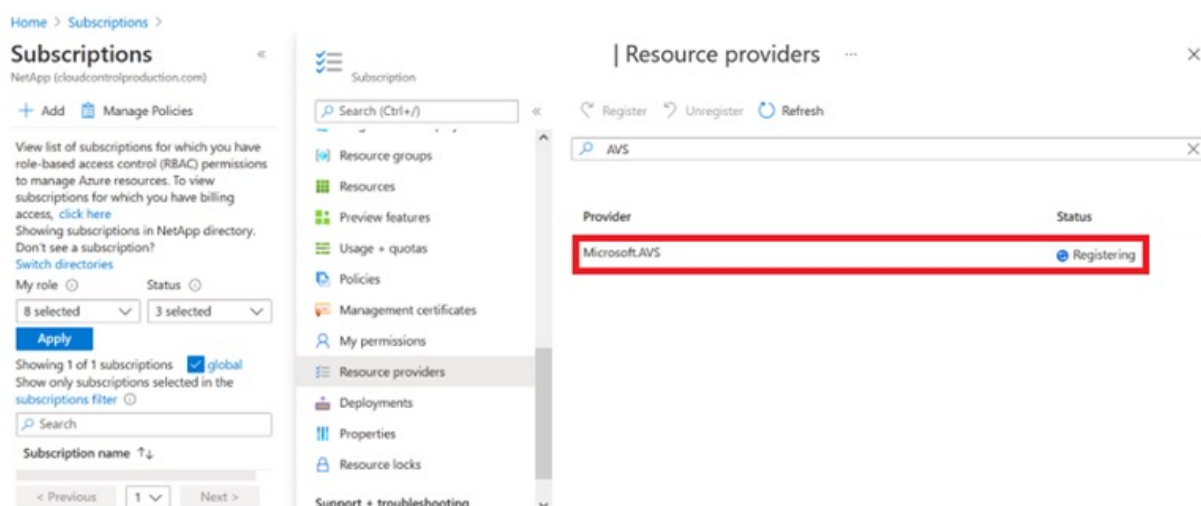
このセクションでは、Azure VMware 解決策をセットアップおよび管理する方法と、ネットアップストレージの接続に使用できるオプションについて説明します。

セットアッププロセスは、次の手順に分けることができます。

## リソースプロバイダを登録し、プライベートクラウドを作成

Azure VMware 解決策を使用するには、まず、特定されたサブスクリプションにリソースプロバイダを登録します。

1. Azure ポータルにサインインします。
2. Azure ポータルのメニューで、すべてのサービスを選択します。
3. [すべてのサービス] ダイアログボックスで、サブスクリプションを入力し、[サブスクリプション] を選択します。
4. 表示するには、サブスクリプションリストからサブスクリプションを選択します。
5. [リソースプロバイダ] を選択し、検索結果に「Microsoft.AVS」と入力します。
6. リソースプロバイダが登録されていない場合は、[登録] を選択します。



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

- リソースプロバイダの登録が完了したら、Azure ポータルを使用して Azure VMware 解決策プライベートクラウドを作成します。
- Azure ポータルにサインインします。
- 新規リソースを作成を選択する。
- [Search the Marketplace] テキストボックスに Azure VMware 解決策と入力し、検索結果から選択します。
- Azure VMware 解決策ページで、Create を選択します。
- [基本設定] タブのフィールドに値を入力し、[レビュー]、[作成] の順に選択します。

注：

- クイックスタートのために、計画フェーズで必要な情報を収集します。
- 既存のリソースグループを選択するか、プライベートクラウド用の新しいリソースグループを作成します。リソースグループは、Azure リソースを導入および管理する論理コンテナです。
- CIDR アドレスが一意で、他の Azure Virtual Network やオンプレミスネットワークと重複しないことを確認してください。CIDR はプライベートクラウド管理ネットワークであり、vCenter Server や NSX Manager などのクラスタ管理サービスに使用されます。ネットアップでは、/22 アドレススペースを使用することを推奨します。この例では、10.21.0.0/22 が使用されています。

## 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 VMs or on-premise networks.

Address block for private cloud \*

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

プロビジョニングプロセスには約 4~5 時間かかります。プロセスが完了したら、Azure ポータルからプライベートクラウドにアクセスして、導入が成功したことを確認します。導入が完了すると、「成功しました」のステータスが表示されます。

Azure VMware 解決策プライベートクラウドには Azure Virtual Network が必要です。Azure VMware 解決策はオンプレミスの vCenter をサポートしていないため、既存のオンプレミス環境と統合するには追加の手順が必要です。ExpressRoute 回線および仮想ネットワークゲートウェイのセットアップも行う必要があります。クラスタのプロビジョニングが完了するのを待っている間に、新しい仮想ネットワークを作成するか、既存の仮想ネットワークを使用して Azure VMware 解決策に接続します。

[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

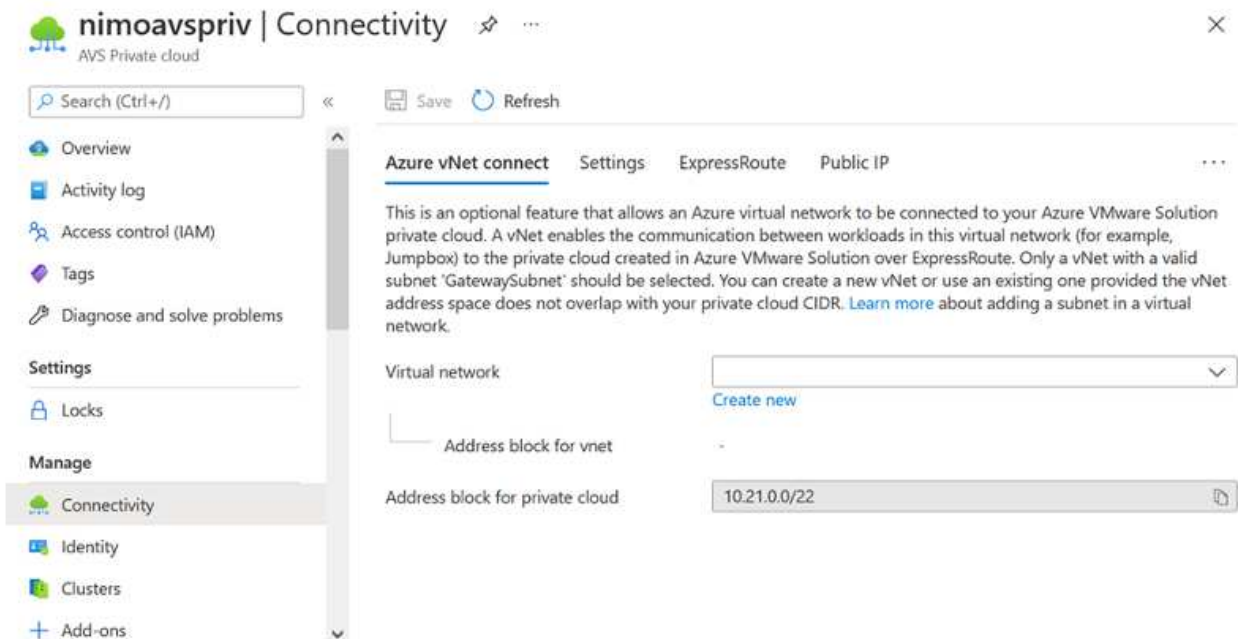
新しい **ExpressRoute** 仮想ネットワークゲートウェイまたは既存の **ExpressRoute** 仮想ネットワークゲートウェイに接続します

新しい Azure Virtual Network (VNet) を作成するには、Azure VNet Connect (Azure VNet 接続) タブを選択します。または、Create Virtual Network ウィザードを使用して、Azure ポータルから手動で作成することもできます。

1. Azure VMware 解決策プライベートクラウドに移動し、管理オプションで接続にアクセスします。
2. Azure VNet Connect を選択します。
3. 新しい VNet を作成するには、Create New オプションを選択します。

この機能により、VNet を Azure VMware 解決策プライベートクラウドに接続できます。VNet は、ExpressRoute 経由で Azure VMware 解決策で作成されたプライベートクラウドに必要なコンポーネント (ジャンプボックス、Azure NetApp Files などの共有サービス、クラウドボリューム ONTAP など) を自動的に作成することで、この仮想ネットワークのワークロード間の通信を有効にします。

。注：\* VNet アドレス空間はプライベートクラウド CIDR と重複しないようにしてください。



4. 新しい VNet の情報を入力または更新し、OK を選択します。



## Create virtual network

×

This virtual network enables the communication between workloads in this virtual network (e.g. a Jumpshot) 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)

指定したアドレス範囲とゲートウェイサブネットを使用した VNet は、指定したサブスクリプションとリソースグループに作成されます。



VNet を手動で作成する場合は、適切な SKU と ExpressRoute をゲートウェイタイプとして使用して仮想ネットワークゲートウェイを作成します。導入が完了したら、認証キーを使用して、ExpressRoute 接続を、Azure VMware 解決策プライベートクラウドを含む仮想ネットワークゲートウェイに接続します。詳細については、[を参照してください "Azure で VMware プライベートクラウド用のネットワークを設定します"](#)。

ネットワーク接続を検証し、**Azure VMware** 解決策プライベートクラウドにアクセスします

Azure VMware 解決策では、オンプレミスの VMware vCenter でプライベートクラウドを管理することはできません。代わりに、ジャンプホストが Azure VMware 解決策 vCenter インスタンスに接続する必要があります。指定したリソースグループにジャンプホストを作成し、Azure VMware 解決策 vCenter にサインインします。このジャンプホストは、接続用に作成された同じ仮想ネットワーク上の Windows VM であり、vCenter と NSX Manager の両方にアクセスする必要があります。



## 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 \*  SaaS Backup Production 

Resource group \*  NimoAVSDemo   
[Create new](#)

### Instance details

Virtual machine name \*  nimAVSJH1 

Region \*  (US) East US 2 









Availability options  No infrastructure redundancy required 

Image \*   Windows Server 2012 R2 Datacenter - Gen2   
[See all images](#)

Azure Spot instance  ☐

Size \*  Standard\_D2s\_v3 - 2 vcpus, 8 GiB memory (\$130.67/month)   
[See all sizes](#)

仮想マシンをプロビジョニングしたら、Connect オプションを使用して RDP にアクセスします。

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

新しく作成したジャンプホスト仮想マシンから、クラウド管理者ユーザを使用して vCenter にサインインします。クレデンシャルにアクセスするには、Azure ポータルにアクセスし、（プライベートクラウド内の管理オプションで）Identity に移動します。プライベートクラウド vCenter と NSX Manager の URL とユーザー資格情報は、ここからコピーできます。

nimoavspriv | Identity  
AVS 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 ⓘ



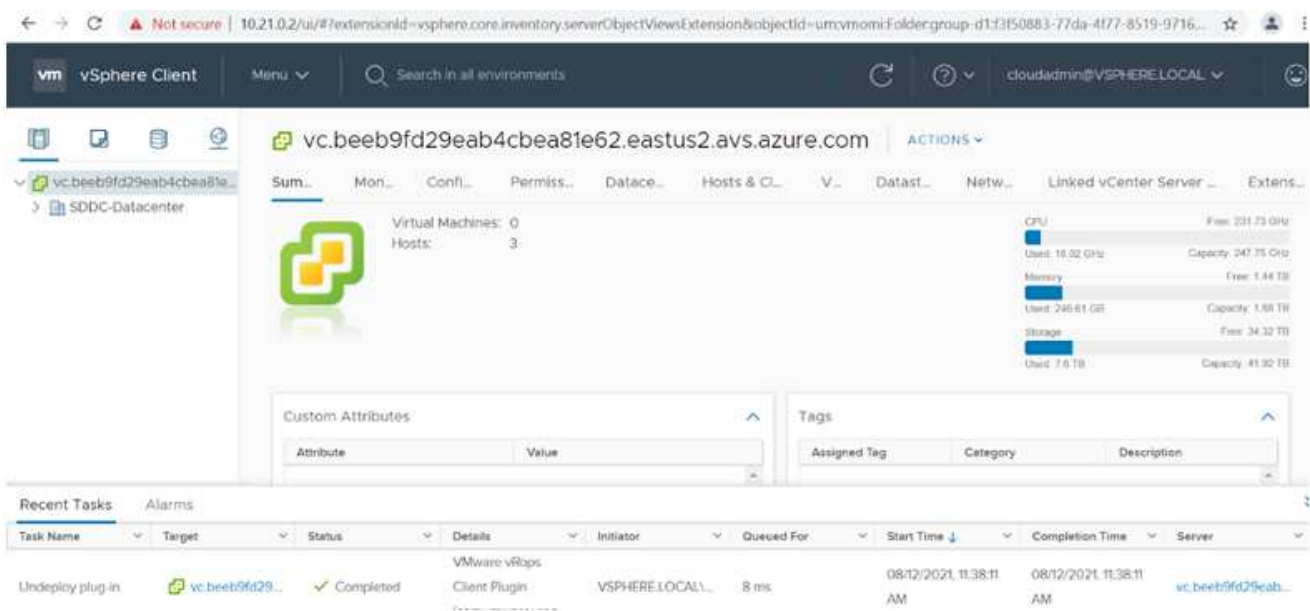
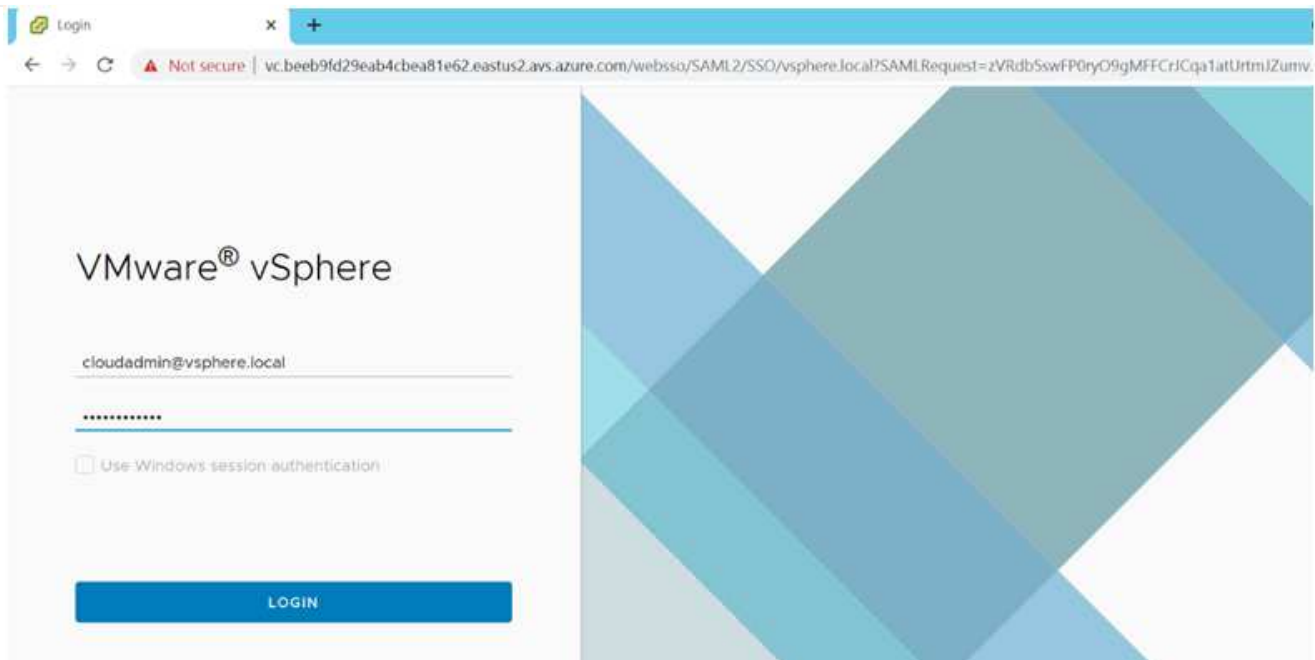
Certificate thumbprint ⓘ

B2B722EA683958283EE159007246D5166D0509D3 ⓘ

Windows 仮想マシンでブラウザを開き、vCenter Web Client の URL にアクセスします admin ユーザのユーザ名に「\* cloudadmin@vsphere.local \*」と入力し、コピーしたパスワードを貼り付けます。同様に、Web クライアントの URL を使用して NSX Manager にアクセスすることもできます admin ユーザ名を使用し、コピーしたパスワードを貼り付けて新しいセグメントを作成したり、既存の階層ゲートウェイを変更したりできます。



Web クライアントの URL は、プロビジョニングされる SDDC ごとに異なります。



これで、Azure VMware 解決策 SDDC の導入と設定が完了しました。ExpressRoute グローバルリーチを活用して、オンプレミス環境を Azure VMware 解決策プライベートクラウドに接続します。詳細については、を参照してください ["オンプレミス環境から Azure VMware 解決策へのピアリング"](#)。

## Google Cloud Platform （GCP）への仮想化環境の導入と構成

オンプレミスと同様に、VM と移行を作成する本番環境に成功するには、Google Cloud VMware Engine （GCVE）の計画が不可欠です。

このセクションでは、GCVE のセットアップと管理方法、およびネットアップストレージの接続に使用できるオプションとの組み合わせについて説明します。

セットアッププロセスは、次の手順に分けることができます。

## GCVE を導入して設定します

GCP で GCVE 環境を設定するには、GCP コンソールにログインし、VMware Engine ポータルにアクセスします。

[New Private Cloud] ボタンをクリックして、GCVE プライベートクラウドに必要な設定を入力します。「場所」で、CV/CVO を導入するリージョン / ゾーンにプライベートクラウドを導入して、最高のパフォーマンスと最小のレイテンシを確保してください。

### 前提条件

- VMware Engine Service Admin IAM ロールを設定します
- ["VMware Engine API アクセスおよびノードクォータを有効にします"](#)
- CIDR 範囲がオンプレミスサブネットやクラウドサブネットと重複しないようにしてください。CIDR 範囲は /27 以上である必要があります。

Google Cloud VMware Engine

← Create Private Cloud ⓘ

Private Cloud name \*

NIMoGCVE

Location \*

us-east4 > v-zone-a > VE Placement Group 2

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  
(3 to 3)

vSphere/vSAN subnets CIDR range \*

192.168.100.0 / 22

IP Range: 192.168.100.0 - 192.168.103.255

HCX Deployment Network CIDR range

192.168.104.0 / 26

IP Range: 192.168.104.0 - 192.168.104.63

注：プライベートクラウドの作成には、30 分から 2 時間かかります。

## GCVE へのプライベートアクセスを有効にします

プライベートクラウドのプロビジョニングが完了したら、プライベートクラウドへのプライベートアクセスを設定して、高スループットで低レイテンシのデータパス接続を実現します。

これにより、Cloud Volumes ONTAP インスタンスが実行されている VPC ネットワークが、GCVE プライベートクラウドと通信できるようになります。これを行うには、に従ってください "[GCP ドキュメント](#)"。クラウドボリュームサービスの場合は、テナントホストプロジェクト間で 1 回限りのピアリングを実行して、VMware エンジンと Cloud Volumes Service 間の接続を確立します。詳細な手順については、次の手順を実行してください "[リンク](#)"。

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

[CloudOwner@gve.local](#) ユーザを使用して vCenter にサインインします。クレデンシャルにアクセスするには、VMware Engine ポータルにアクセスし、Resources にアクセスして、適切なプライベートクラウドを選択します。[Basic info] セクションで、vCenter ログイン情報（vCenter Server、HCX Manager）または NSX ログイン情報（NSX Manager）の [View] リンクをクリックします。

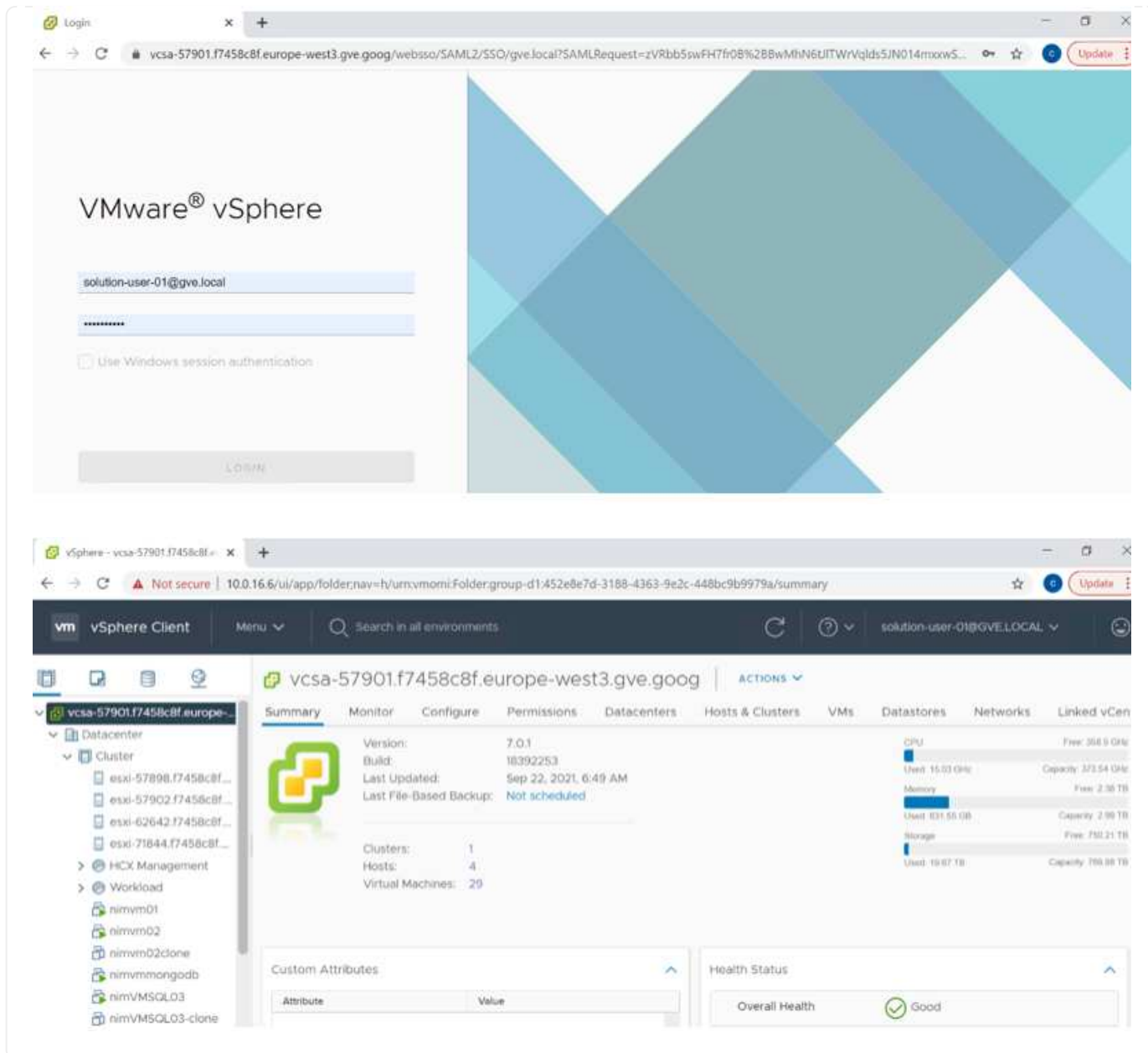
The screenshot shows the Google Cloud VMware Engine (GCVE) console. The top navigation bar includes 'Home', 'Resources', 'Network', 'Activity', and 'Account'. The main content area is titled 'Resources' and shows details for a private cloud instance named 'gcve-cvs-hw-eu-west3'. The instance is in the 'Operational' status and is located in 'europe-west3 > v-zone-a > VE Placement Group 1'. The console displays various configuration details and capacity information.

Section	Item	Value
Basic Info	Name	gcve-cvs-hw-eu-west3
	Status	Operational
	Location	europe-west3 > v-zone-a > VE Placement Group 1
	Cloud Monitoring	Private Cloud DNS Servers: 10.0.16.8, 10.0.16.9
vSphere/vSAN	Subnets CIDR range	10.0.16.0/24
	Expandable	No
	vCenter login info	View / Reset password
	NSX-T login info	View / Reset password
Capacity	Total nodes	4
	Total storage capacity	76.8 TB Raw, 12.8 TB Cache, All-Flash

Windows 仮想マシンでブラウザを開き、vCenter Web Client の URL にアクセスします admin ユーザのユーザ名として [CloudOwner@gve.local](#) を使用し、コピーしたパスワードを貼り付けます。同様に、Web クライアントの URL を使用して NSX Manager にアクセスすることもできます admin ユーザ名を使用し、コピーしたパスワードを貼り付けて新しいセグメントを作成したり、既存の階層ゲートウェイを変更したりできます。

オンプレミスネットワークから VMware Engine プライベートクラウドに接続する場合は、クラウド VPN または Cloud Interconnect を利用して適切な接続を行い、必要なポートが開いていることを確認します。詳細な手順については、次の手順を実行してください "[リンク](#)"。





## NetApp Cloud Volume Serviceの補完的データストアをGCVEに導入

を参照してください "手順を使用して、NetApp CVSを使用した補完的NFSデータストアをGCVEに導入します"

## 著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

## 商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。