VMware in der Konfiguration von Hyperscalern

NetApp Solutions

NetApp
April 24, 2024

This PDF was generated from https://docs.netapp.com/de-de/netapp-solutions/ehc/aws-setup.html on April 24, 2024. Always check docs.netapp.com for the latest.

Inhalt

Konfiguration der Virtualisierungsumgebung beim Cloud-Provider 1
Implementieren und Konfigurieren der Virtualisierungsumgebung auf AWS 3
Implementieren und Konfigurieren der Virtualisierungsumgebung auf Azure 18
Implementieren und Konfigurieren der Virtualisierungsumgebung auf der Google Cloud Platform (GCP) . . 27

Konfiguration der Virtualisierungsumgebung beim Cloud-Provider

Im Folgenden werden Details zur Konfiguration der Virtualisierungsumgebung für jeden der unterstützten Hyperscaler erläutert.

AWS/VMC

In diesem Abschnitt wird beschrieben, wie Sie VMware Cloud auf AWS SDDC einrichten und managen und es in Kombination mit den verfügbaren Optionen zur Verbindung von NetApp Storage nutzen.

> Der in-Guest Storage ist die einzige unterstützte Methode zur Verbindung von Cloud Volumes ONTAP mit AWS VMC.

Der Einrichtungsvorgang kann in die folgenden Schritte unterteilt werden:

- Implementieren und Konfigurieren von VMware Cloud für AWS
- Verbinden Sie VMware Cloud mit FSX ONTAP

Details anzeigen "Konfigurationsschritte für VMC".

Azure/AVS

In diesem Abschnitt wird beschrieben, wie Sie Azure VMware Lösung einrichten und managen und in Kombination mit den verfügbaren Optionen für die Verbindung von NetApp Storage verwenden.

> Der in-Guest-Speicher ist die einzige unterstützte Methode zur Verbindung von Cloud Volumes ONTAP mit Azure VMware-Lösung.

Der Einrichtungsvorgang kann in die folgenden Schritte unterteilt werden:

- Registrieren Sie den Ressourcenanbieter und erstellen Sie eine Private Cloud
- Stellen Sie eine Verbindung zu einem neuen oder vorhandenen virtuellen ExpressRoute Netzwerk-Gateway her
- Netzwerkverbindung validieren und auf Private Cloud zugreifen

Details anzeigen "Konfigurationsschritte für AVS".

GCP/GCVE

In diesem Abschnitt wird beschrieben, wie Sie GCVE einrichten und managen und in Kombination mit den verfügbaren Optionen zum Verbinden von NetApp Storage verwenden.

> Der in-Guest-Speicher ist die einzige unterstützte Methode zum Verbinden von Cloud Volumes ONTAP und Cloud Volumes Services mit GCVE.

Der Einrichtungsvorgang kann in die folgenden Schritte unterteilt werden:

- Bereitstellen und Konfigurieren von GCVE
- Aktivieren Sie den privaten Zugriff auf GCVE

Details anzeigen "Konfigurationsschritte für GCVE".

Implementieren und Konfigurieren der Virtualisierungsumgebung auf AWS

Wie auch bei lokalen Systemen ist die Planung von VMware Cloud auf AWS von entscheidender Bedeutung für eine erfolgreiche produktionsbereite Umgebung zur Erstellung von VMs und Migration.

In diesem Abschnitt wird beschrieben, wie Sie VMware Cloud auf AWS SDDC einrichten und managen und es in Kombination mit den verfügbaren Optionen zur Verbindung von NetApp Storage nutzen.

> Im-Gast-Storage ist derzeit die einzige unterstützte Methode zur Verbindung von Cloud Volumes ONTAP (CVO) mit AWS VMC.

Der Einrichtungsvorgang kann in die folgenden Schritte unterteilt werden:

Implementieren und Konfigurieren von VMware Cloud for AWS

"VMware Cloud auf AWS" Für VMware-basierte Workloads im AWS Ecosystem bietet es ein Cloud-natives Arbeiten. Jedes softwaredefinierte VMware Datacenter (SDDC) wird in einer Amazon Virtual Private Cloud (VPC) ausgeführt und bietet einen vollständigen VMware Stack (einschließlich vCenter Server), softwaredefiniertes NSX-T Networking, softwaredefinierten vSAN Storage sowie einen oder mehrere ESXi Hosts, die Computing- und Storage-Ressourcen für Ihre Workloads bereitstellen.

In diesem Abschnitt wird beschrieben, wie Sie VMware Cloud auf AWS einrichten und managen und in Kombination mit Amazon FSX für NetApp ONTAP und/oder Cloud Volumes ONTAP auf AWS mit in-Guest Storage verwenden.

> Im-Gast-Storage ist derzeit die einzige unterstützte Methode zur Verbindung von Cloud Volumes ONTAP (CVO) mit AWS VMC.

Der Einrichtungsprozess kann in drei Teile unterteilt werden:

Für ein AWS Konto registrieren

Für ein registrieren "Amazon Web Services Konto".

Sie brauchen ein AWS-Konto, um zu beginnen, vorausgesetzt, es gibt nicht bereits erstellt. Neu oder bereits vorhanden, Sie benötigen Administratorrechte im Konto für viele Schritte in diesem Verfahren. Siehe das "Verlinken" Weitere Informationen zu AWS Zugangsdaten.

Für einen My VMware Account registrieren

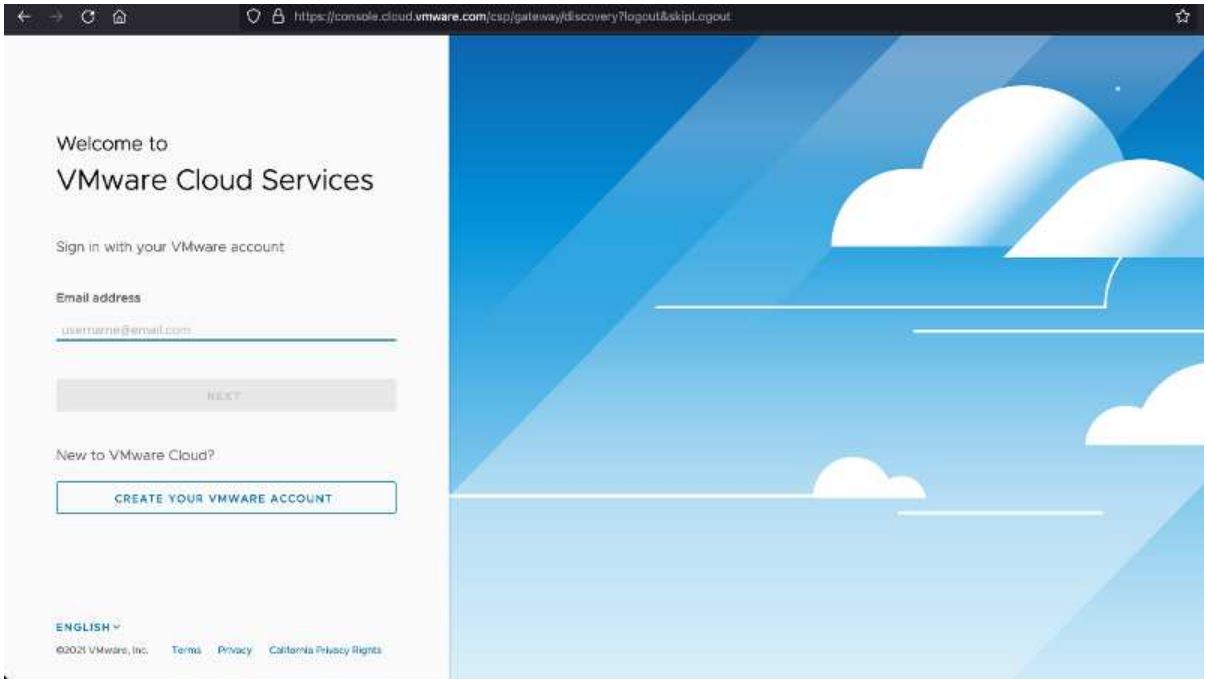
Für A registrieren "Meine VMware" Konto.

Für den Zugriff auf das Cloud-Portfolio von VMware (einschließlich VMware Cloud auf AWS) benötigen Sie ein VMware-Kundenkonto oder ein My VMware-Konto. Falls noch nicht geschehen, erstellen Sie ein VMware-Konto "Hier".

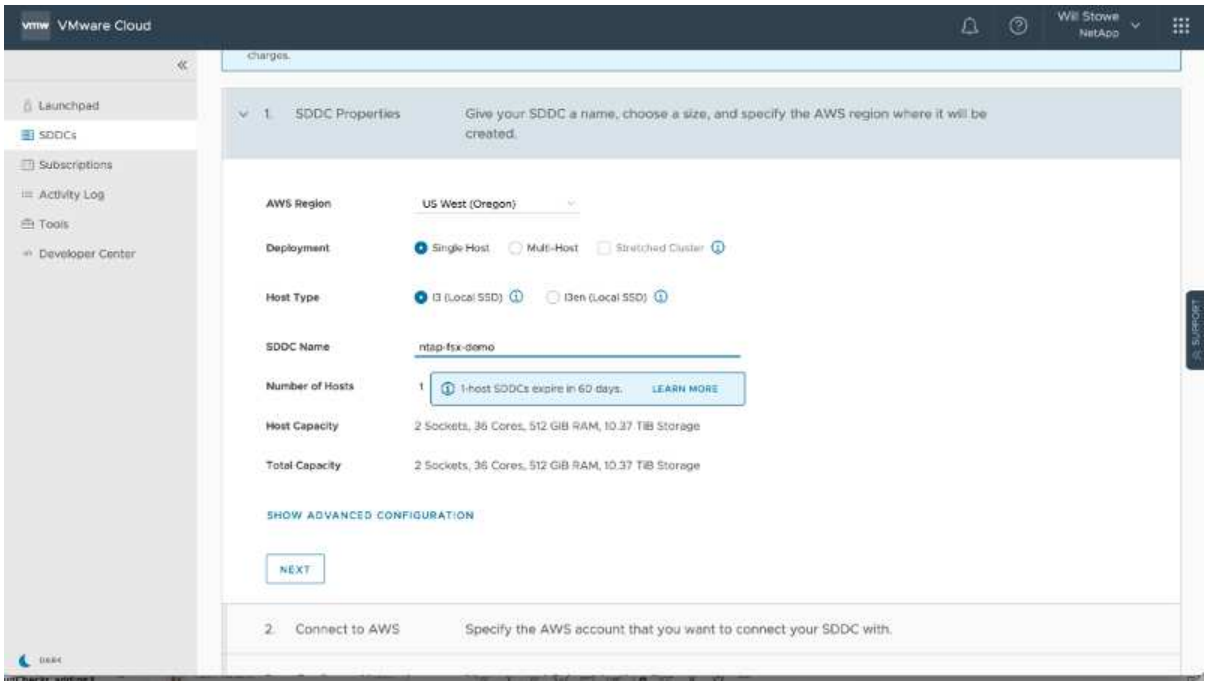
Bereitstellung von SDDC in VMware Cloud

Nach der Konfiguration des VMware Kontos und der ordnungsgemäßen Größenbestimmung ist die Implementierung eines softwaredefinierten Datacenters der nächste Schritt auf dem Weg zur Nutzung des VMware Cloud auf AWS Service. Wenn Sie ein SDDC erstellen möchten, wählen Sie eine AWS Region zum Hosten aus, geben Sie dem SDDC einen Namen und legen Sie fest, wie viele ESXi Hosts das SDDC enthalten soll. Wenn Sie noch kein AWS Konto haben, können Sie dennoch ein SDDC mit einer Starterkonfiguration erstellen, das einen einzelnen ESXi Host enthält.

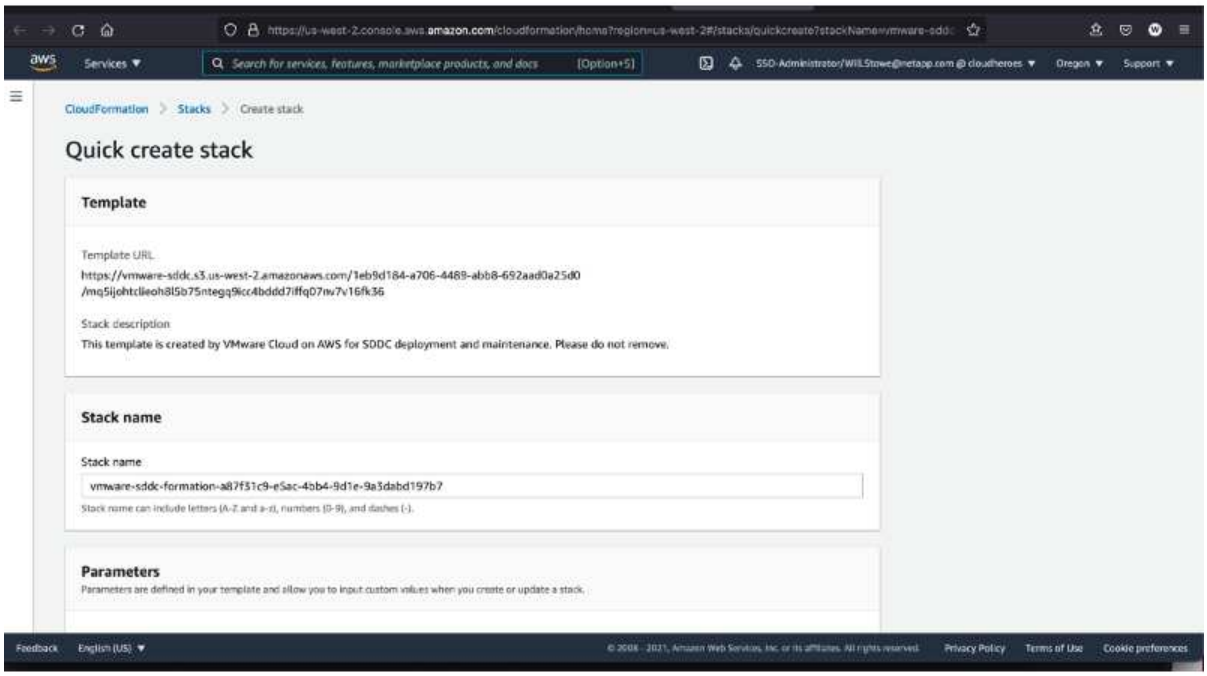
1. Melden Sie sich mit Ihren vorhandenen oder neu erstellten VMware Zugangsdaten bei der VMware Cloud Console an.

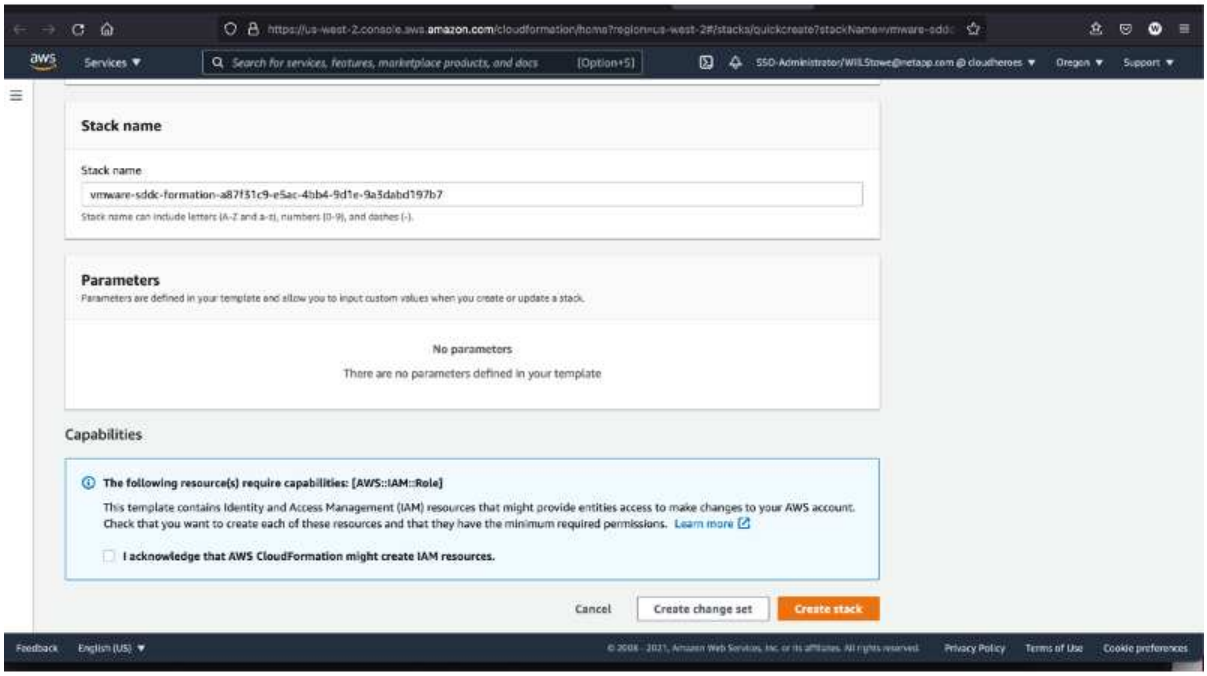


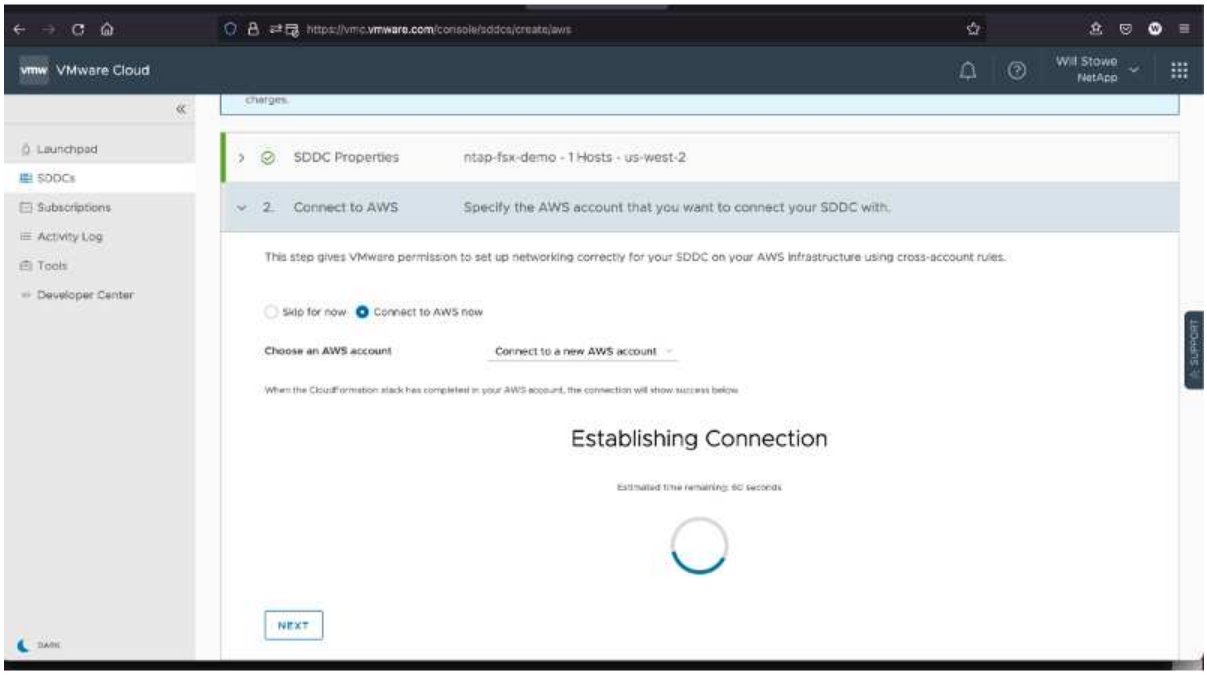
2. Konfigurieren Sie die AWS Region, die Implementierung und den Host-Typ sowie den SDDC-Namen:

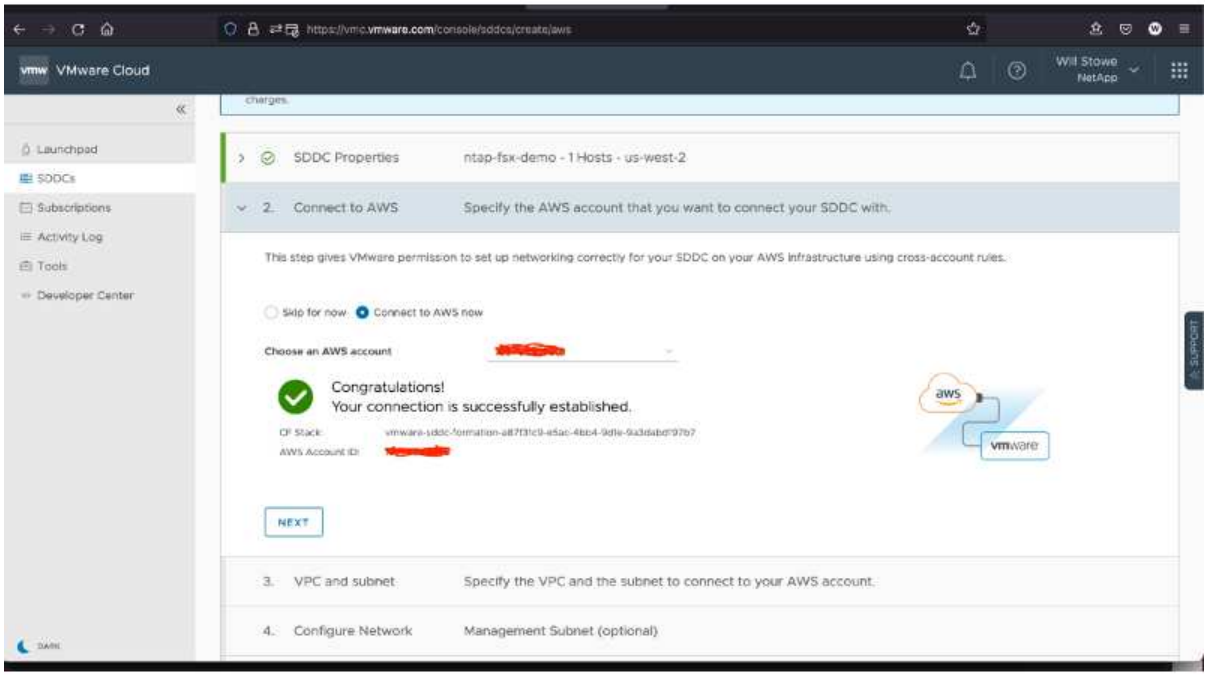


3. Stellen Sie eine Verbindung mit dem gewünschten AWS Konto her und führen Sie den AWS Cloud-Formationstack aus.



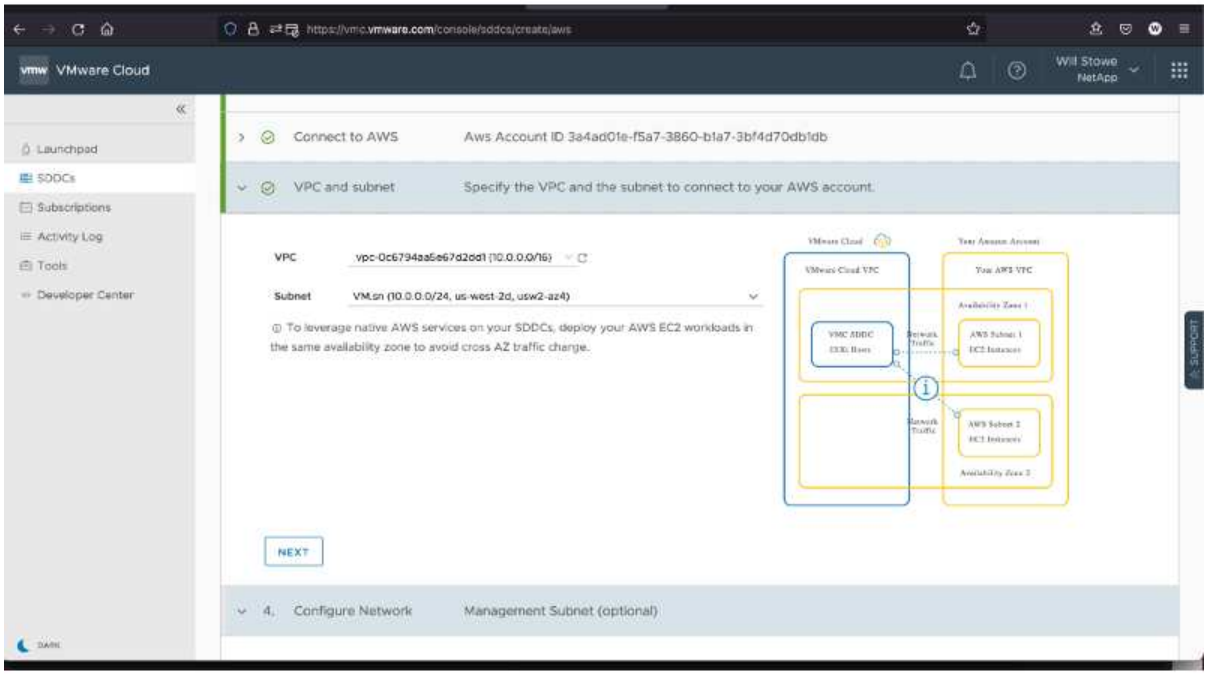

Stack name
Stack name
vmware-sddc-formation-a87f51c9-e5ac-4bb4-9d1e-9a3dabd197b7
Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).
Parameters
Parameters are defined in your template and allow you to input custom values when you create or update a stack.
No parameters
There 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


VMware Cloud
Launchpad
SDDCs
Subscriptions
Activity Log
Tools
Developer Center
SDDC Properties
ntap-fsx-demo - 1 Hosts - us-west-2
2. Connect to AWS
Specify the AWS account that you want to connect your SDDC with.
This step gives VMware permission to set up networking correctly for your SDDC on your AWS infrastructure using cross-account rules.
Skip for now
Connect to AWS now
Choose an AWS account
Connect to a new AWS account
Establishing Connection
NEXT

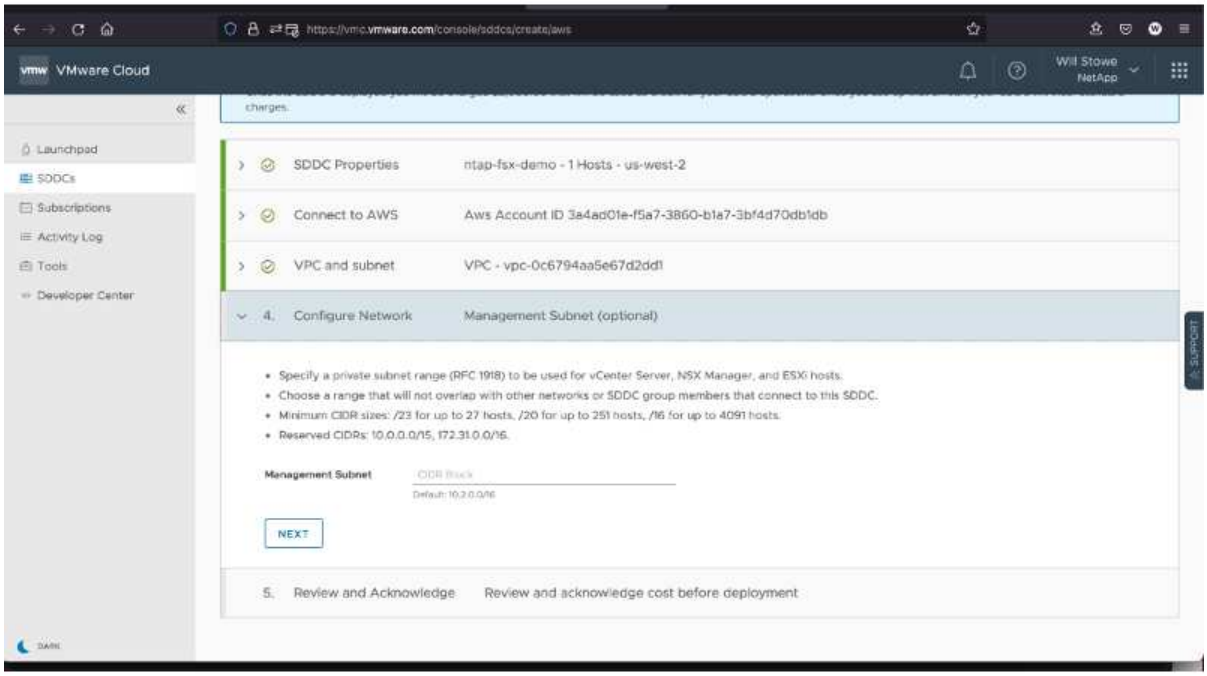


In dieser Validierung wird Single-Host-Konfiguration verwendet.

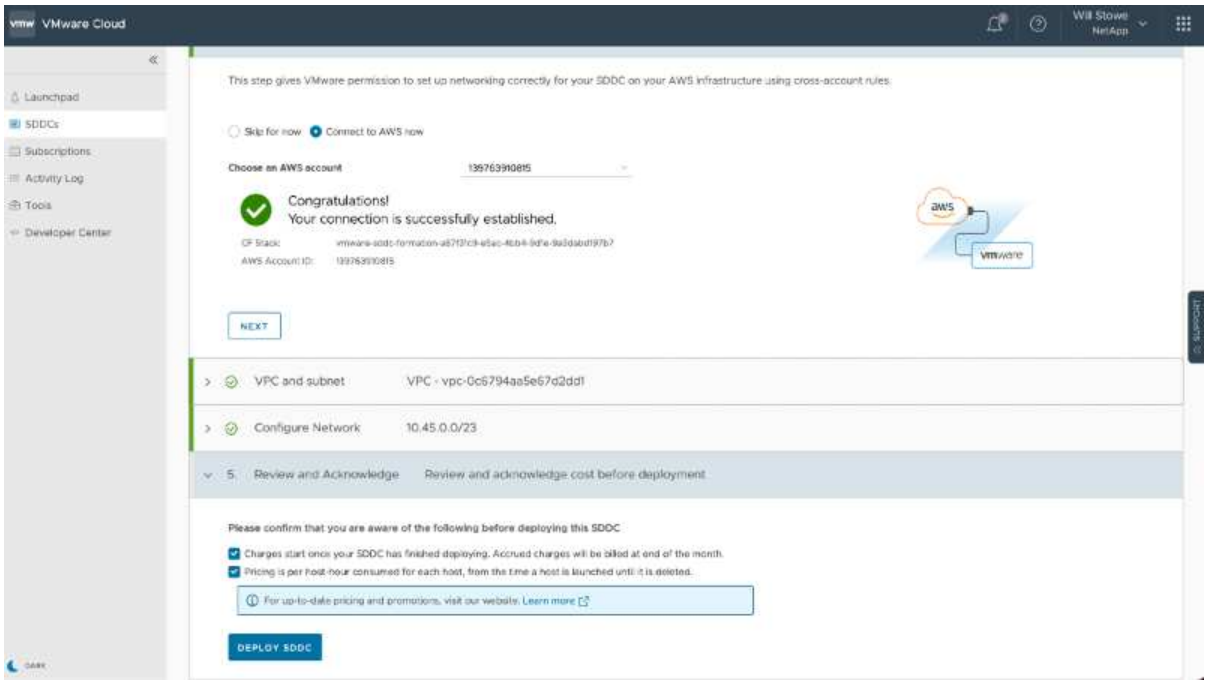
4. Wählen Sie die gewünschte AWS VPC aus, mit der die VMC-Umgebung verbunden werden soll.



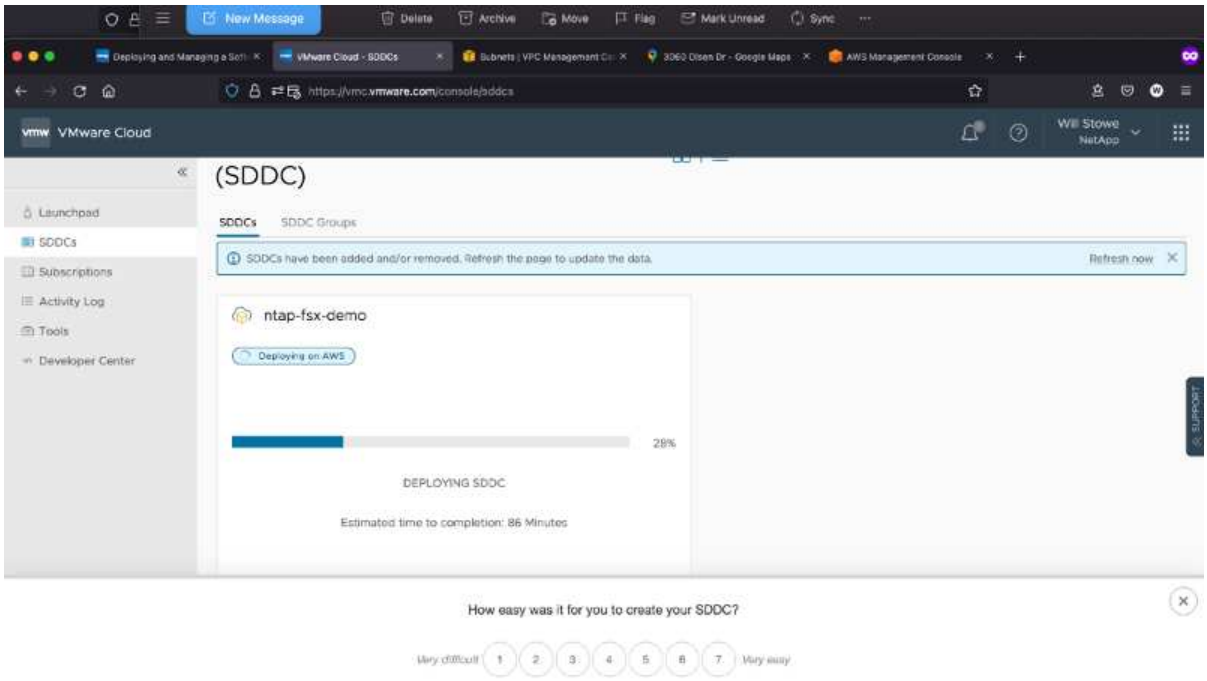
5. VMC-Managementsubnetz konfigurieren: Dieses Subnetz enthält von VMC gemanagte Services wie vCenter, NSX usw. Wählen Sie keinen überlappenden Adressraum mit anderen Netzwerken, die Verbindung zur SDDC-Umgebung benötigen. Folgen Sie abschließend den unten aufgeführten Empfehlungen für CIDR-Größe.



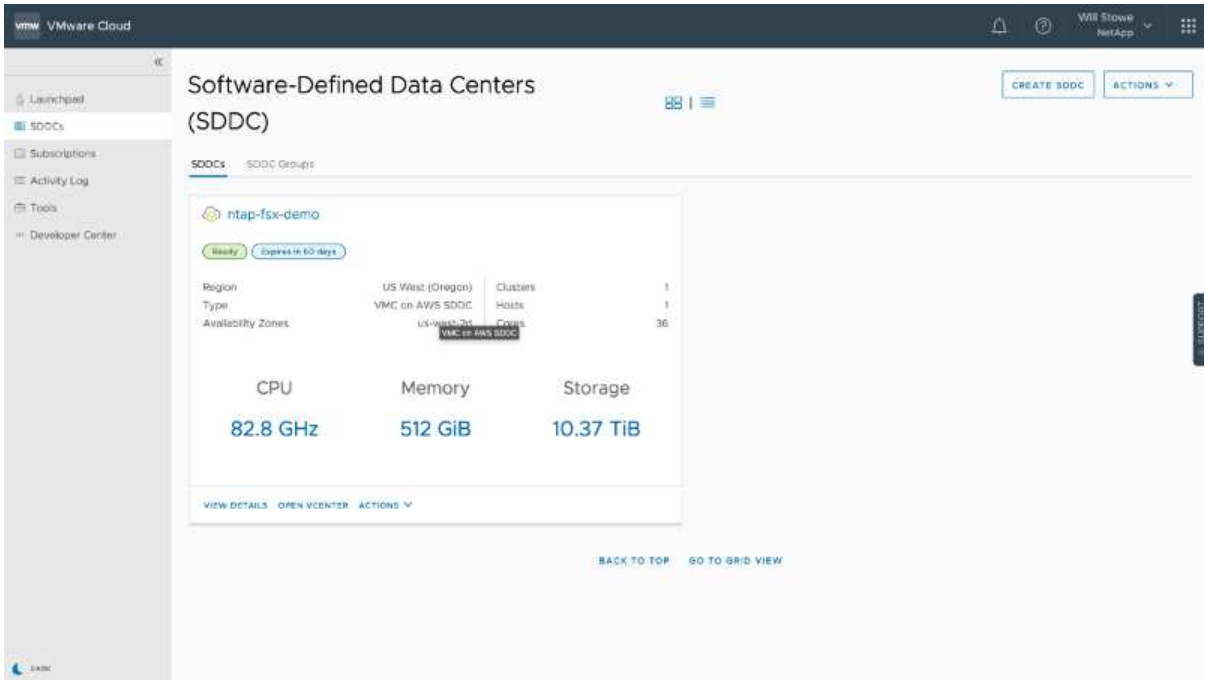
6. Prüfen und bestätigen Sie die SDDC-Konfiguration und klicken Sie dann auf Bereitstellen des SDDC.



Die Implementierung dauert normalerweise etwa zwei Stunden.



7. Nach Abschluss der Fertigstellung ist das SDDC einsatzbereit.

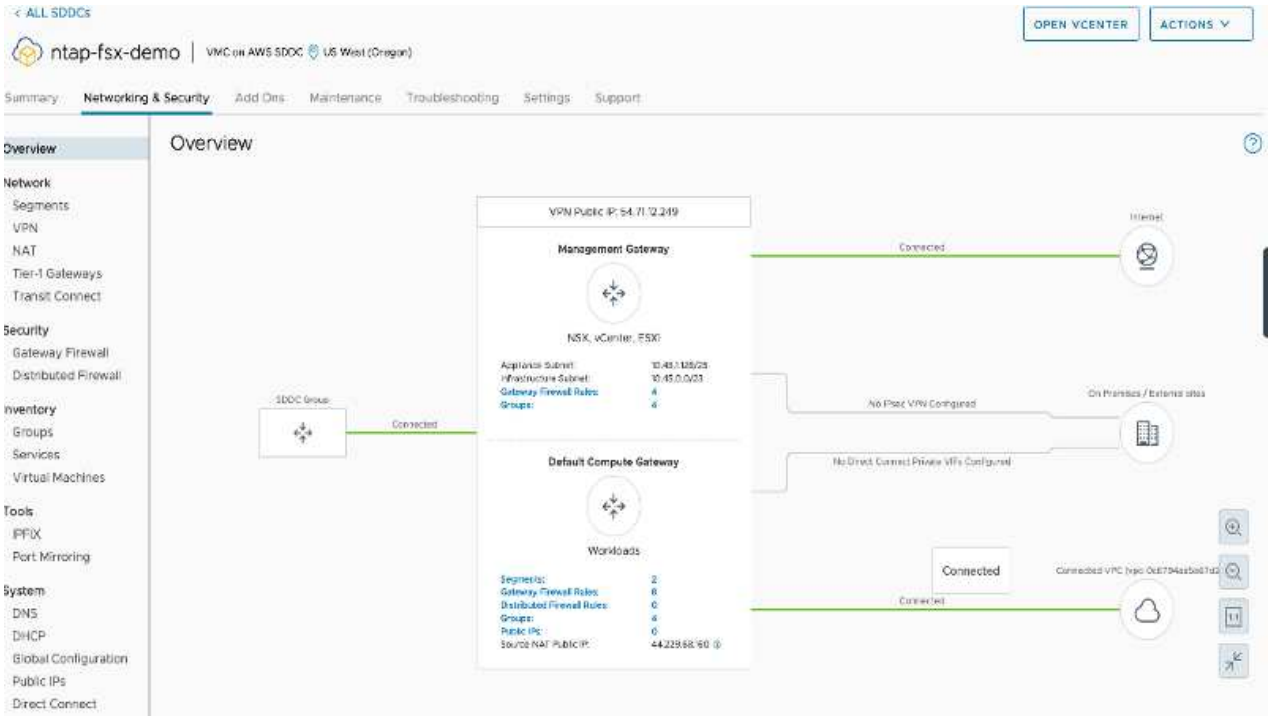


Einen Schritt-für-Schritt-Leitfaden zur SDDC-Implementierung finden Sie unter "Implementieren Sie ein SDDC über die VMC-Konsole".

Verbinden Sie VMware Cloud mit FSX ONTAP

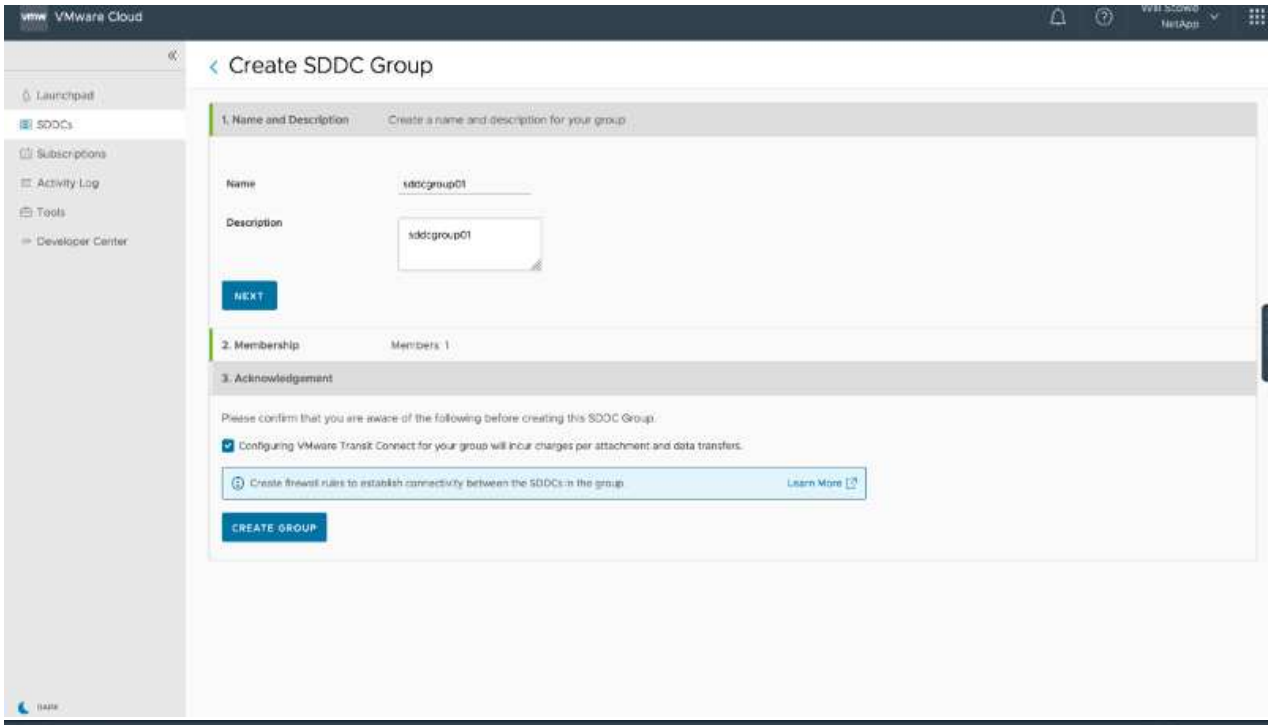
So verbinden Sie VMware Cloud mit FSX ONTAP:

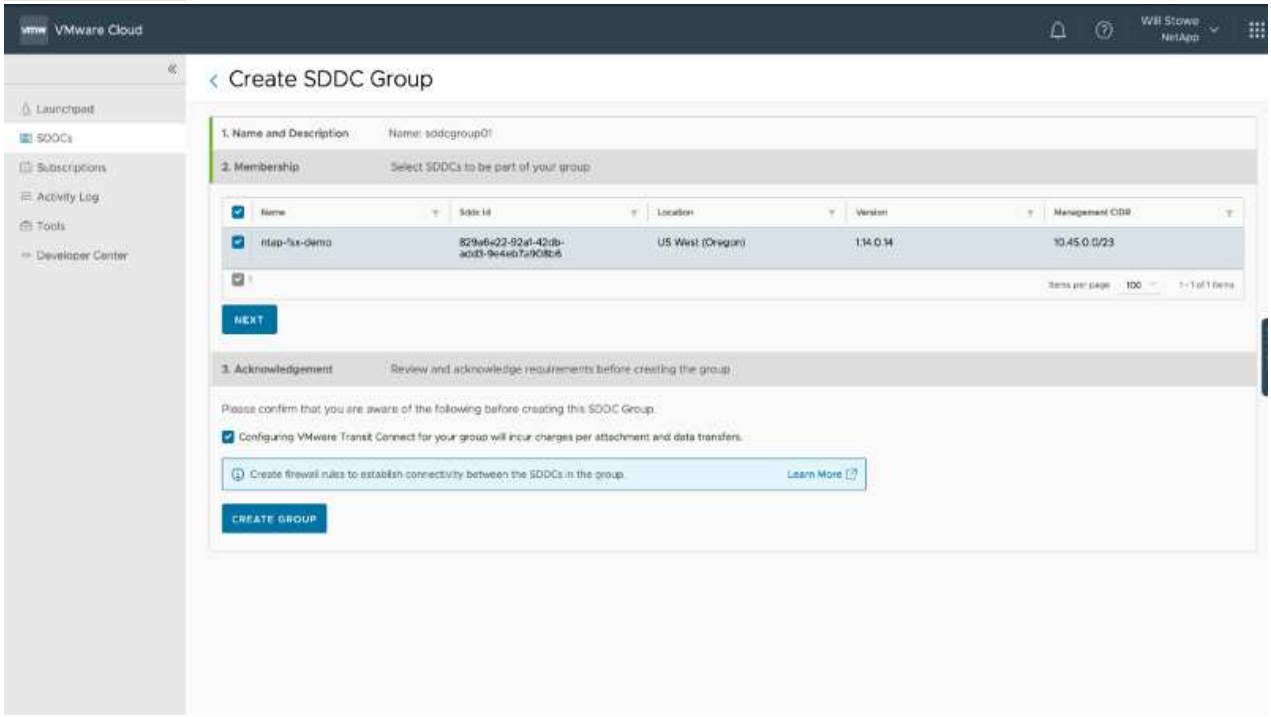
1. Wenn die VMware Cloud Implementierung abgeschlossen und mit AWS VPC verbunden ist, müssen Sie Amazon FSX für NetApp ONTAP in ein neues VPC anstatt in der mit der Integration verbundenen VPC implementieren (siehe Abbildung unten). FSX (NFS- und SMB-fließende IPs) ist nicht zugänglich, wenn sie in der verbundenen VPC implementiert werden. ISCSI-Endpunkte wie Cloud Volumes ONTAP funktionieren genauso gut wie die verbundene VPC.

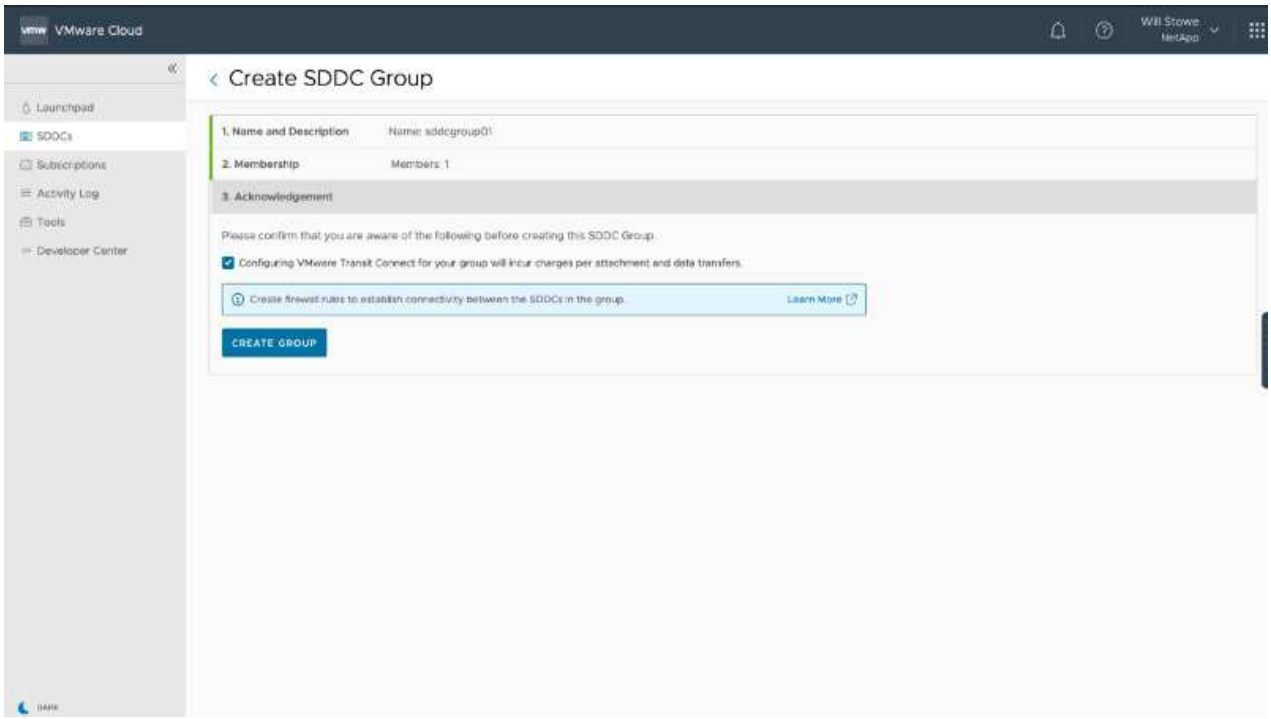


2. Eine zusätzliche VPC in derselben Region implementieren und dann Amazon FSX für NetApp ONTAP in die neue VPC implementieren.

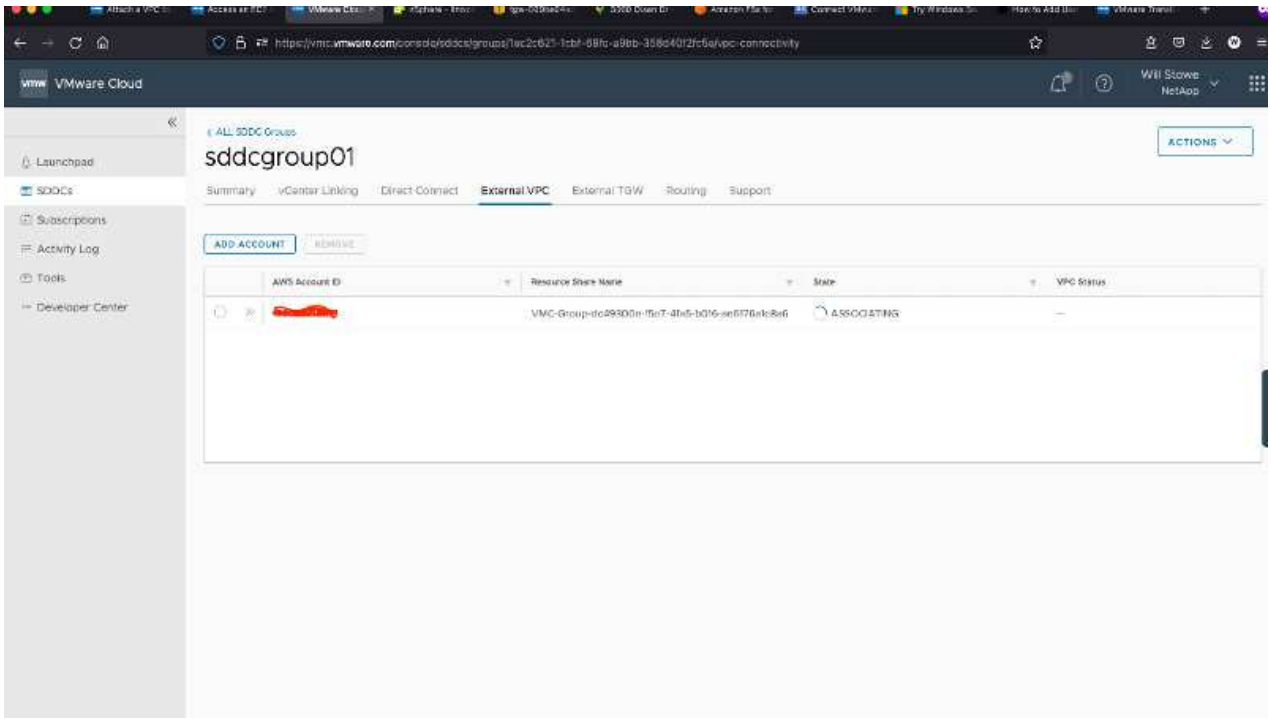
   Die Konfiguration einer SDDC-Gruppe in der VMware Cloud Konsole ermöglicht die erforderlichen Netzwerkkonfigurationsoptionen für die Verbindung zur neuen VPC, bei der FSX implementiert wird. Überprüfen Sie in Schritt 3, ob „VMware Transit Connect für Ihre Gruppe konfigurieren“ Gebühren pro Anlage und Datenübertragung anfällt und wählen Sie „Gruppe erstellen“. Dieser Vorgang kann einige Minuten dauern.

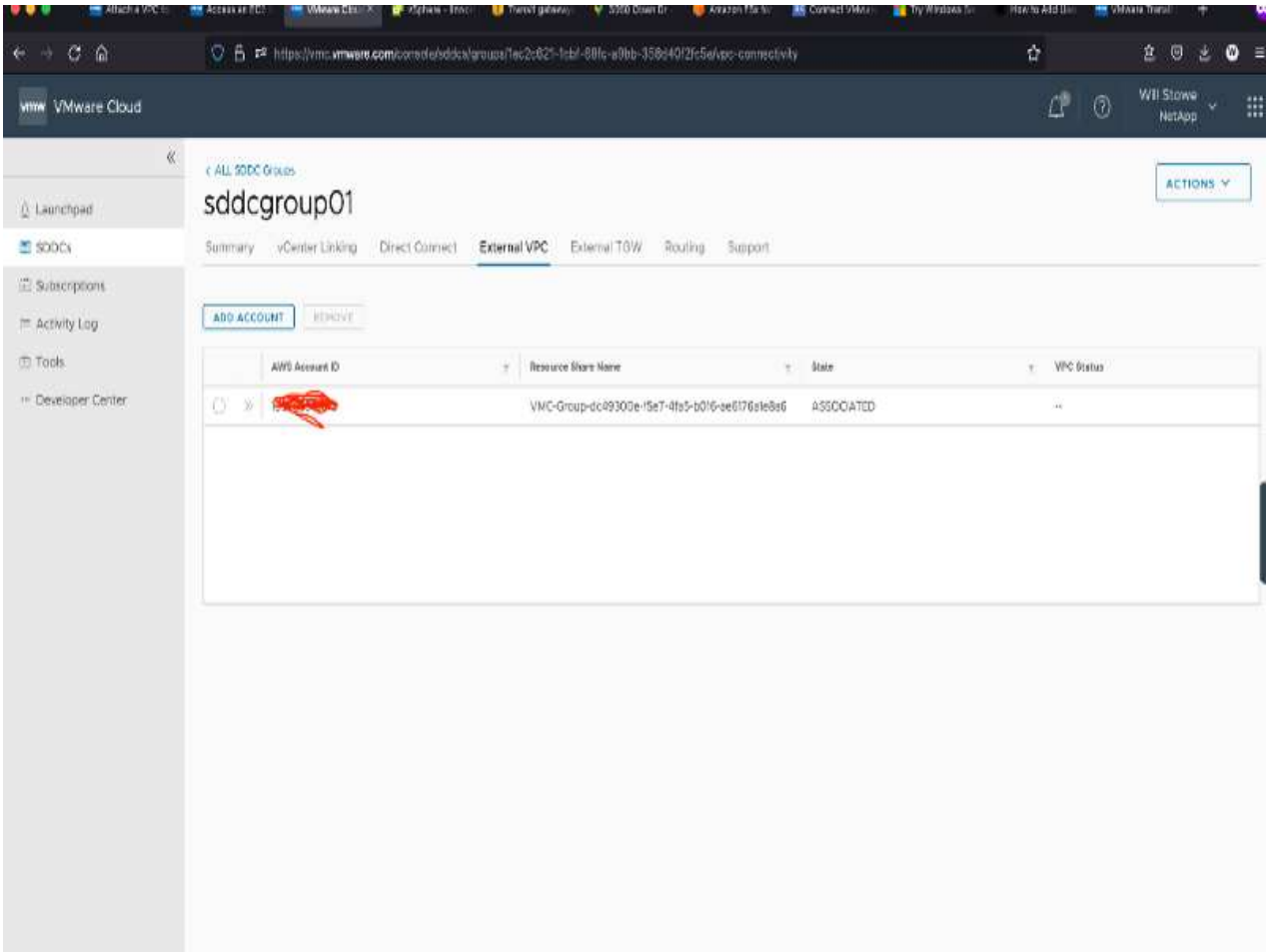

VMware Cloud
Will Stowe
NetApp
Launchpad
SDDCs
Subscriptions
Activity Log
Tools
Developer Center
Create SDDC Group
1. Name and Description
Create a name and description for your group
Name
sddcgroup01
Description
sddcgroup01
NEXT
2. Membership
Members: 1
3. Acknowledgement
Please confirm that you are 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
Will 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
Name
Sddc Id
Location
Version
Management CIDR
ntap-fsx-demo
829a6a22-92a1-42db-acd3-9e4eb7a908b6
US West (Oregon)
1.14.0.14
10.45.0.0/23
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

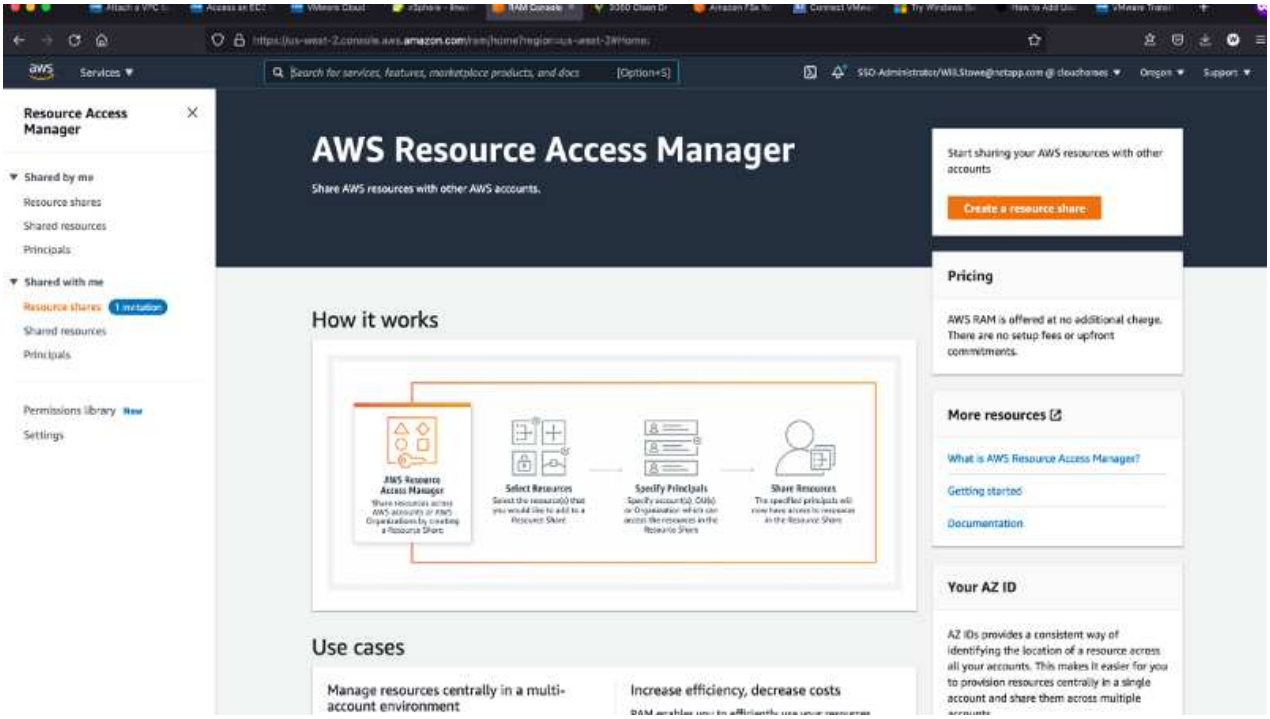


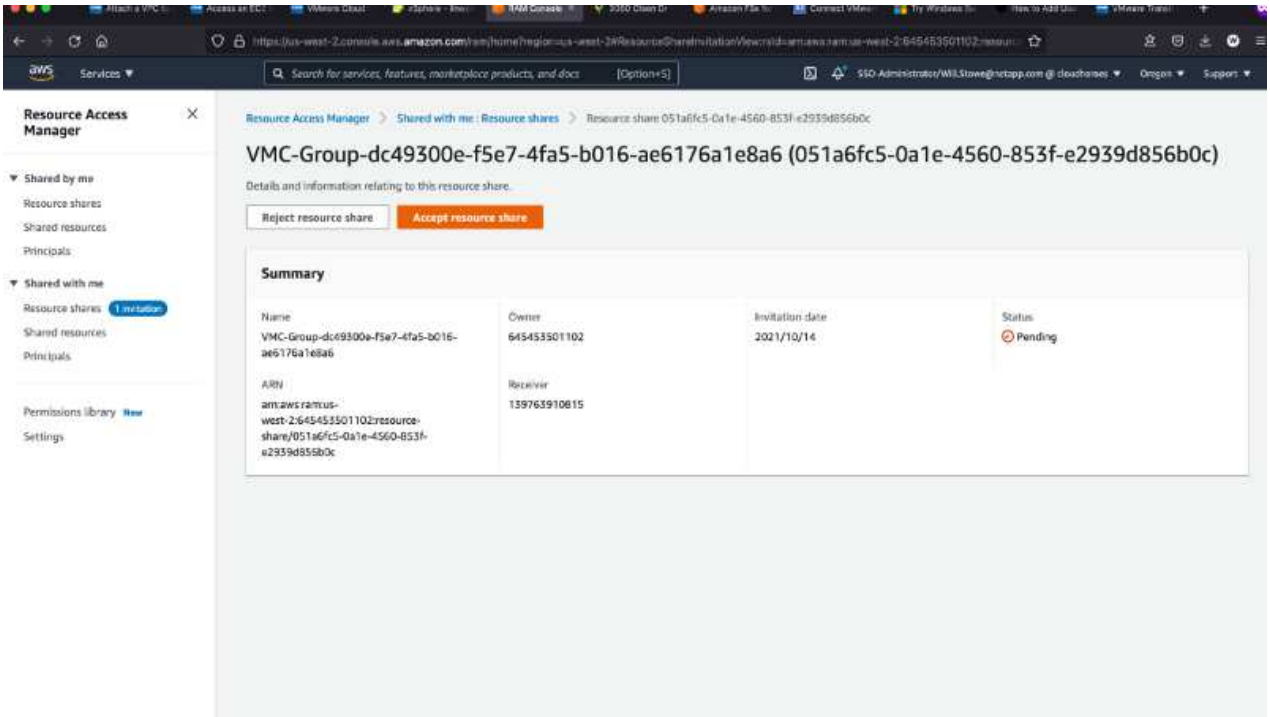
3. Binden Sie die neu erstellte VPC an die gerade erstellte SDDC-Gruppe. Wählen Sie die Registerkarte External VPC aus, und folgen Sie der "Anweisungen zum Anschließen eines externen VPC" Für die Gruppe. Dieser Vorgang kann 10 bis 15 Minuten in Anspruch nehmen.



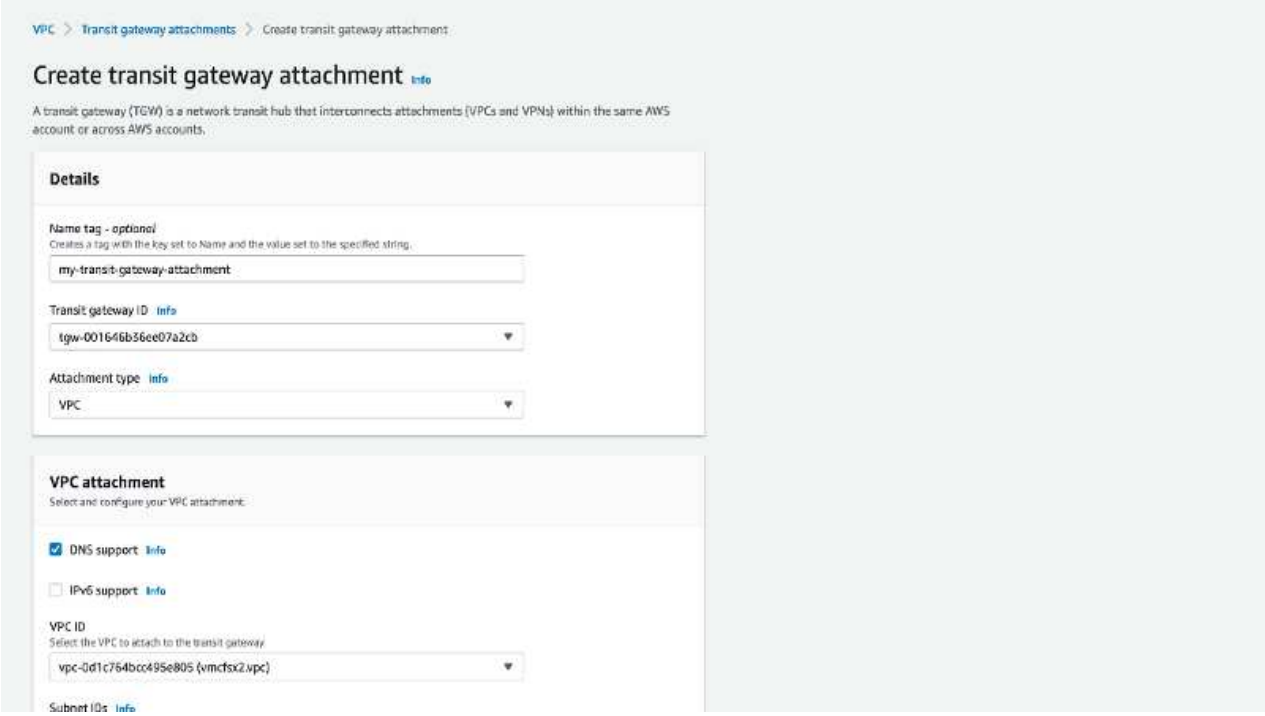


4. Im Rahmen des externen VPC-Prozesses werden Sie über die AWS-Konsole zu einer neuen, gemeinsam genutzten Ressource über den Resource Access Manager aufgefordert. Die gemeinsam genutzte Ressource ist die "AWS Transit Gateway" Management über VMware Transit Connect

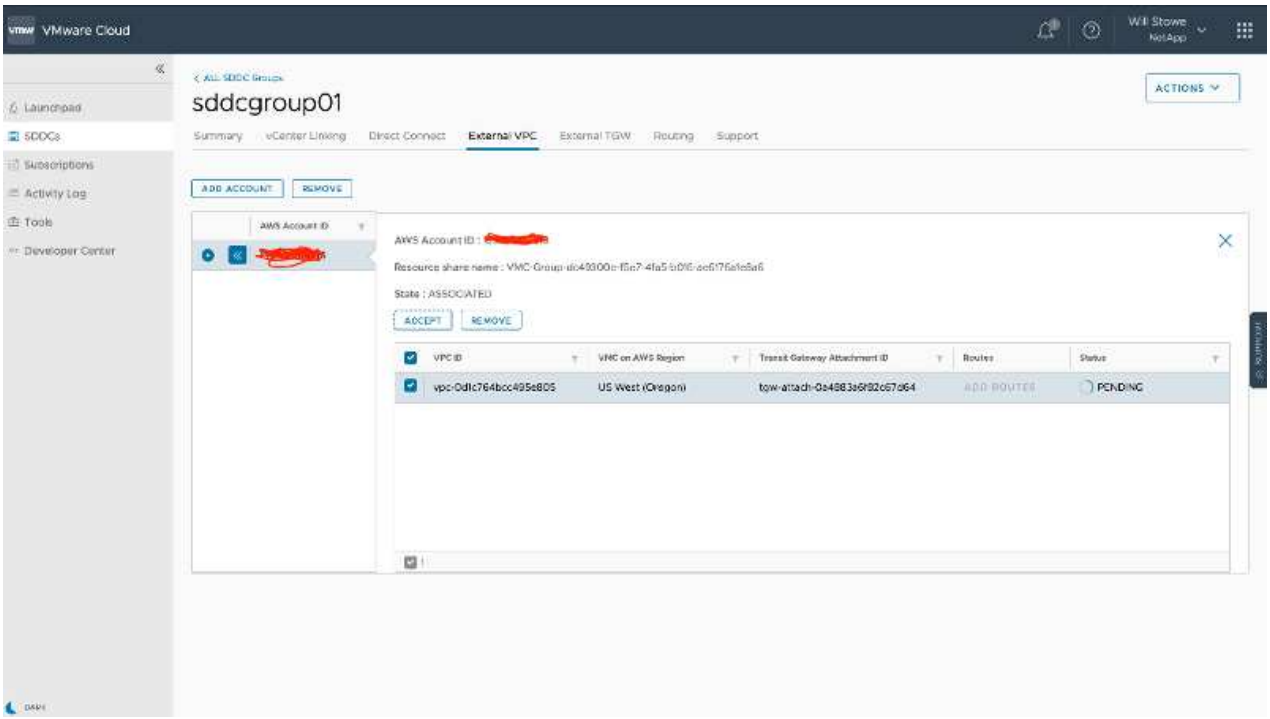




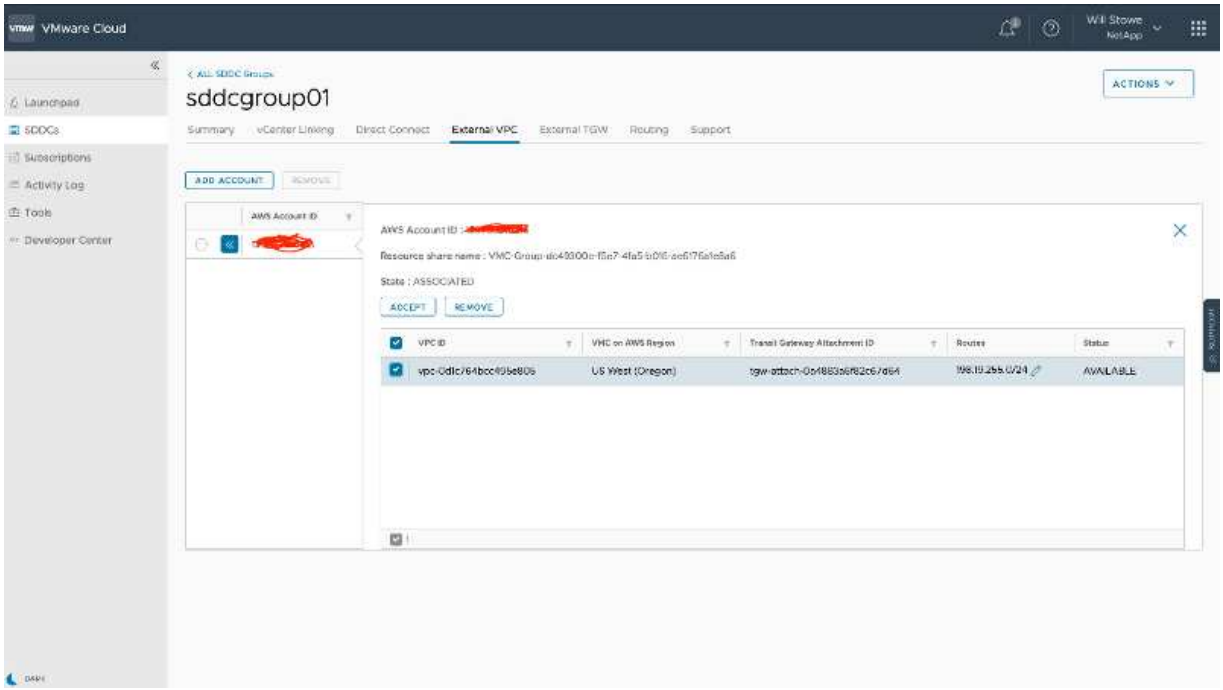
5. Erstellen Sie den Transit Gateway-Anhang.



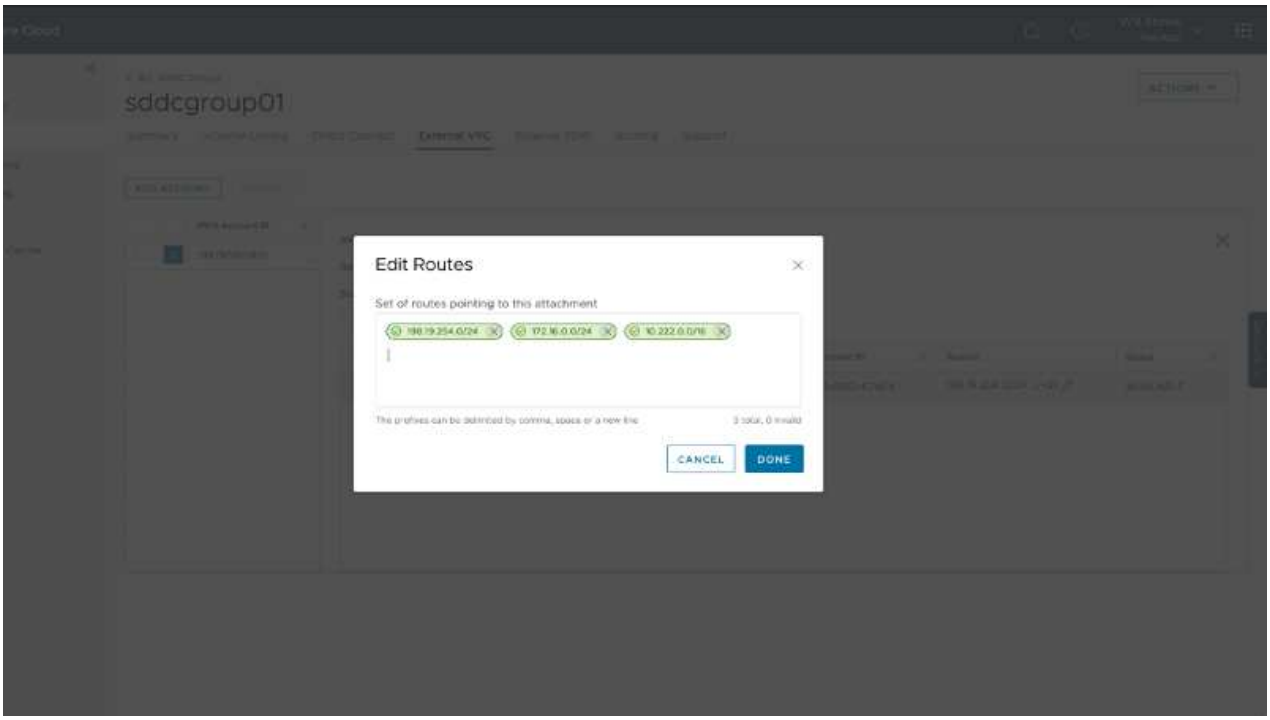
6. Nehmen Sie wieder an der VMC-Konsole die VPC-Anlage an. Dieser Vorgang dauert etwa 10 Minuten.



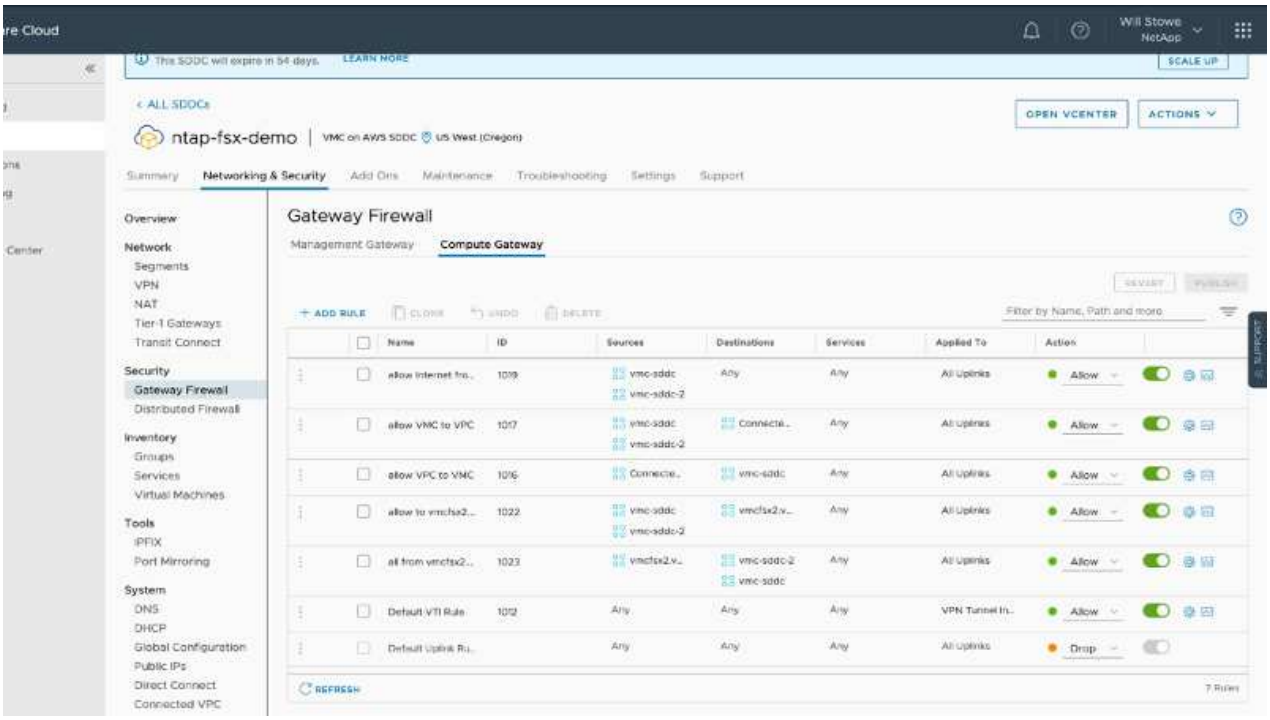
7. Klicken Sie auf der Registerkarte External VPC auf das Bearbeiten-Symbol in der Spalte Routen und fügen Sie die folgenden erforderlichen Routen hinzu:
   - Eine Route für den unverankerten IP-Bereich für Amazon FSX für NetApp ONTAP "Fließende IPs".
   - Eine Route für den unverankerten IP-Bereich für Cloud Volumes ONTAP (falls zutreffend).
   - Eine Route für den neu erstellten externen VPC-Adressraum.



8. Außerdem bidirektionalen Datenverkehr zulassen "Firewall-Regeln" Für den Zugriff auf FSX/CVO. Befolgen Sie diese "Detaillierte Schritte" Für die Firewall des Computing-Gateways für die SDDC-Workload-Konnektivität.



9. Nachdem die Firewall-Gruppen sowohl für das Management- als auch für das Computing-Gateway konfiguriert wurden, ist der Zugriff auf vCenter wie folgt möglich:



Als nächsten Schritt müssen Sie überprüfen, ob Amazon FSX ONTAP oder Cloud Volumes ONTAP je nach Ihren Anforderungen konfiguriert ist und dass die Volumes bereitgestellt werden, um Storage-Komponenten aus vSAN auszulagern, um die Implementierung zu optimieren.

Implementieren und Konfigurieren der Virtualisierungsumgebung auf Azure

Wie bei On-Premises-Systemen ist die Planung von Azure VMware Lösungen für eine erfolgreiche produktionsbereite Umgebung für das Erstellen von VMs und die Migration von großer Bedeutung.

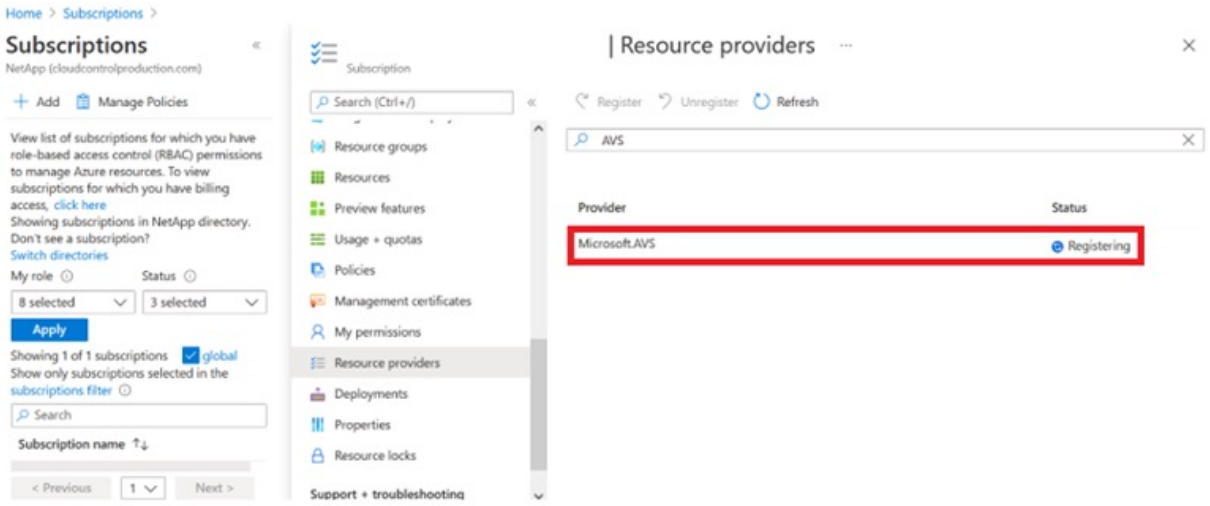
In diesem Abschnitt wird beschrieben, wie Sie Azure VMware Lösung einrichten und managen und in Kombination mit den verfügbaren Optionen für die Verbindung von NetApp Storage verwenden.

Der Einrichtungsvorgang kann in die folgenden Schritte unterteilt werden:

Registrieren Sie den Ressourcenanbieter und erstellen Sie eine Private Cloud

Für die Nutzung der Azure VMware Lösung müssen Sie zunächst den Ressourcenanbieter im angegebenen Abonnement registrieren:

1. Melden Sie sich im Azure Portal an.
2. Wählen Sie im Menü Azure-Portal die Option Alle Services aus.
3. Geben Sie im Dialogfeld „Alle Services“ das Abonnement ein, und wählen Sie anschließend Abonnements aus.
4. Wählen Sie das Abonnement aus der Abonnementliste aus, um es anzuzeigen.
5. Wählen Sie Ressourcenanbieter aus, und geben Sie Microsoft.AVS in die Suche ein.
6. Wenn der Ressourcenanbieter nicht registriert ist, wählen Sie Registrieren.

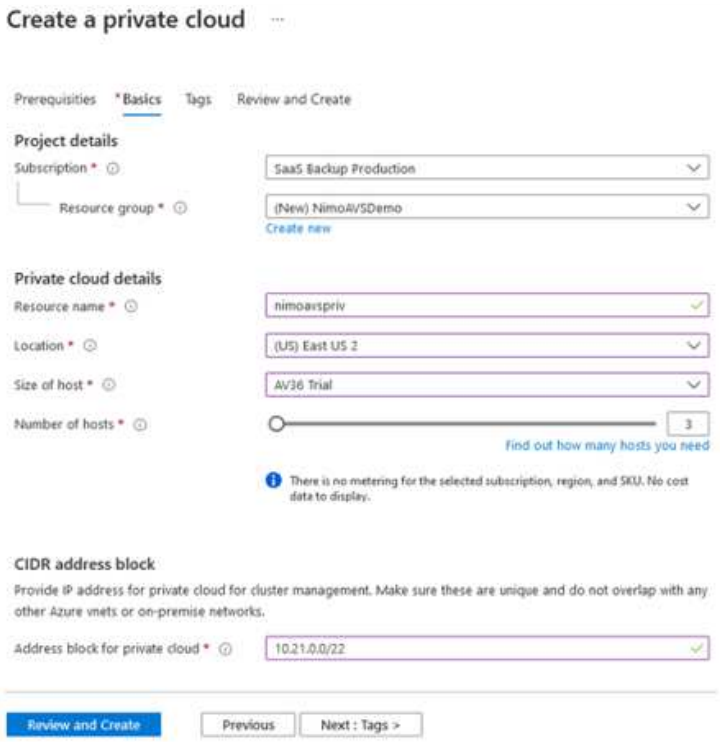


Provider	Status
Microsoft.OperationsManagement	Registered
Microsoft.Compute	Registered
Microsoft.ContainerService	Registered
Microsoft.ManagedIdentity	Registered
Microsoft.AVS	Registered
Microsoft.OperationalInsights	Registered
Microsoft.GuestConfiguration	Registered

7. Nachdem der Ressourcenanbieter registriert ist, erstellen Sie über das Azure-Portal eine Private Cloud für eine Azure VMware-Lösung.
8. Melden Sie sich im Azure Portal an.
9. Wählen Sie Neue Ressource erstellen.
10. Geben Sie im Textfeld „Search the Marketplace“ die Azure VMware Lösung ein und wählen Sie sie aus den Ergebnissen aus.
11. Wählen Sie auf der Seite Azure VMware Lösung die Option Erstellen.
12. Geben Sie auf der Registerkarte Grundlagen die Werte in die Felder ein, und wählen Sie Überprüfen + Erstellen.

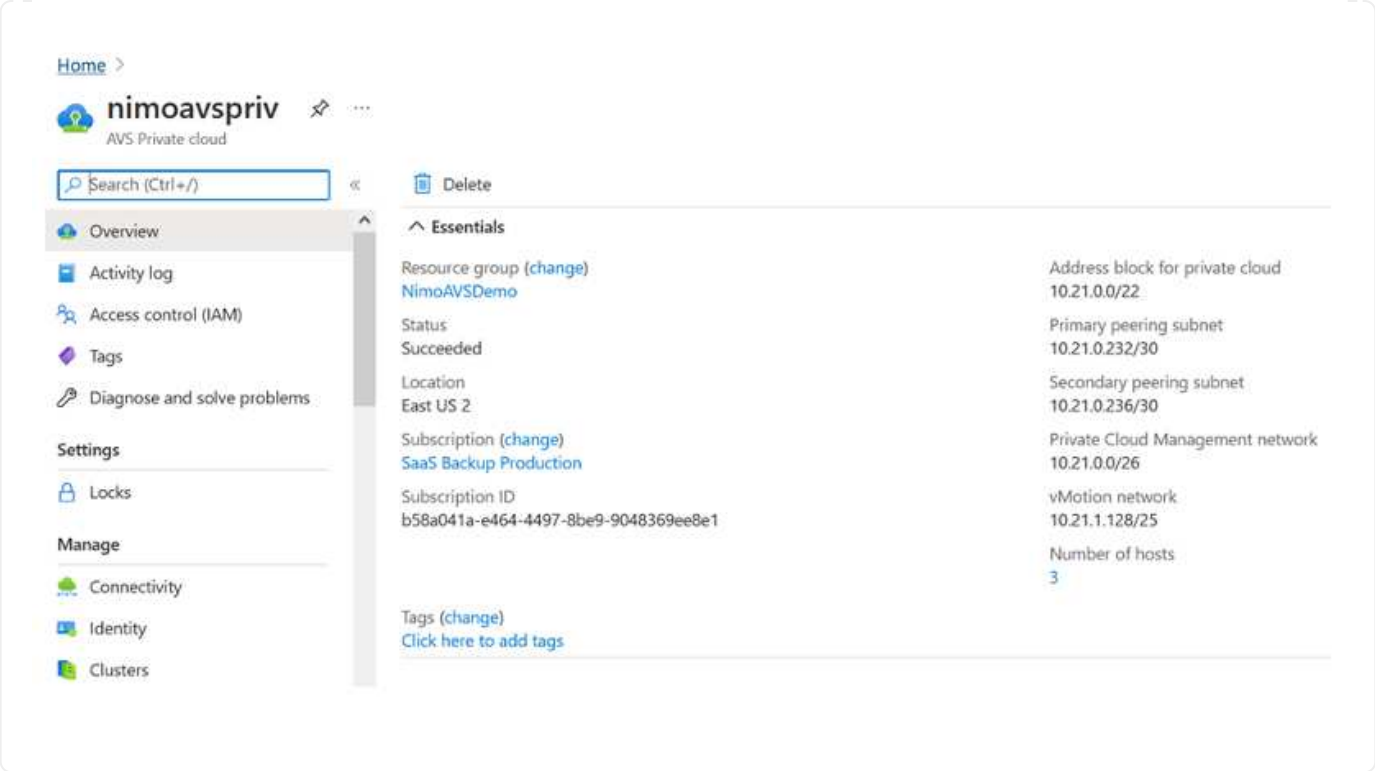
Hinweise:

- Für einen schnellen Start müssen Sie die erforderlichen Informationen während der Planungsphase erfassen.
- Wählen Sie eine vorhandene Ressourcengruppe aus oder erstellen Sie eine neue Ressourcengruppe für die private Cloud. Eine Ressourcengruppe ist ein logischer Container, in dem die Azure Ressourcen implementiert und gemanagt werden.
- Stellen Sie sicher, dass die CIDR-Adresse einzigartig ist und nicht mit anderen virtuellen Azure Netzwerken oder On-Premises-Netzwerken überlappt. Das CIDR stellt das private Cloud-Managementnetzwerk dar und wird für Cluster-Managementservices wie vCenter Server und NSX-T Manager verwendet. NetApp empfiehlt die Verwendung eines Adressspeichers unter /22. In diesem Beispiel wird 10.21.0.0/22 verwendet.



Die Bereitstellung dauert ungefähr 4 bis 5 Stunden. Nach Abschluss des Prozesses muss überprüft werden, ob die Implementierung erfolgreich war. Greifen Sie über das Azure-Portal auf die Private Cloud zu. Nach Abschluss der Bereitstellung wird ein Status von erfolgreich angezeigt.

Eine Private Cloud für eine Azure VMware Lösung erfordert ein virtuelles Azure Netzwerk. Da die Azure VMware Lösung vCenter vor Ort nicht unterstützt, sind für die Integration in eine vorhandene lokale Umgebung zusätzliche Schritte erforderlich. Zudem ist die Einrichtung einer ExpressRoute-Verbindung und eines virtuellen Netzwerk-Gateways erforderlich. Während Sie warten, bis die Cluster-Bereitstellung abgeschlossen ist, erstellen Sie ein neues virtuelles Netzwerk oder verwenden Sie ein vorhandenes für die Verbindung mit Azure VMware Lösung.


Home >
nimoavspriv
AVS Private cloud
Search (Ctrl+/)
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Locks
Manage
Connectivity
Identity
Clusters
Delete
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

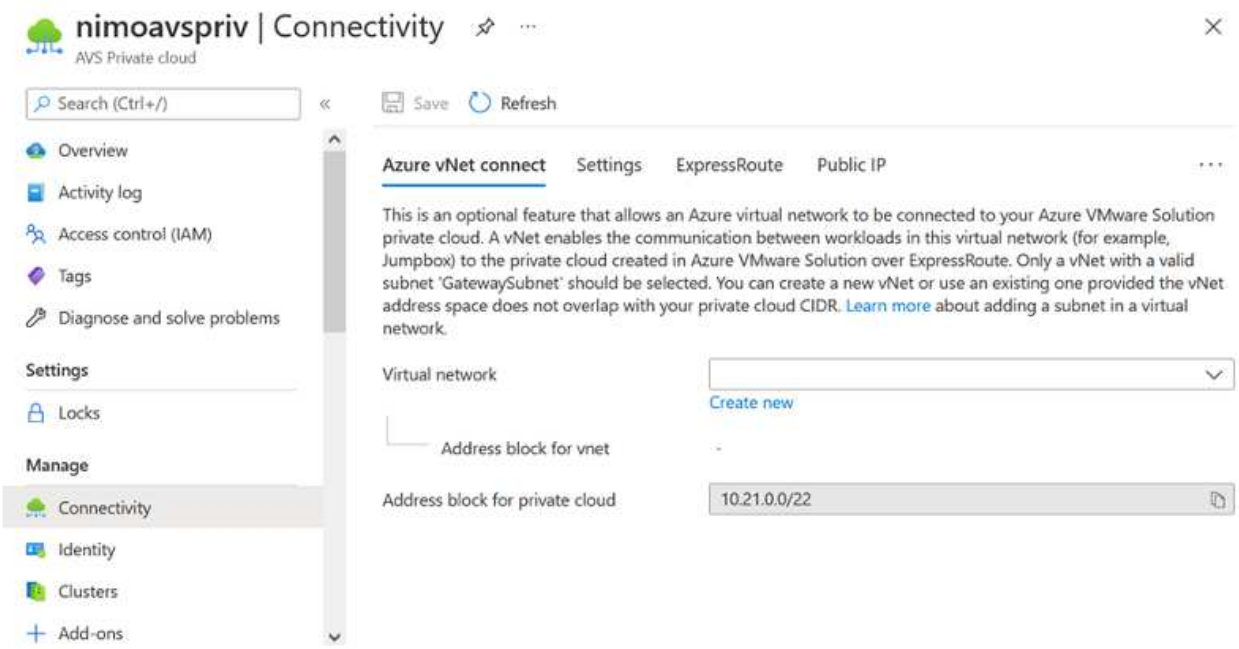
Stellen Sie eine Verbindung zu einem neuen oder vorhandenen virtuellen ExpressRoute Netzwerk-Gateway her

Um ein neues Azure Virtual Network (vnet) zu erstellen, wählen Sie die Registerkarte Azure vnet Connect aus. Alternativ können Sie aus dem Azure-Portal eine manuell erstellen mit dem Assistenten zum Erstellen von virtuellen Netzwerken:

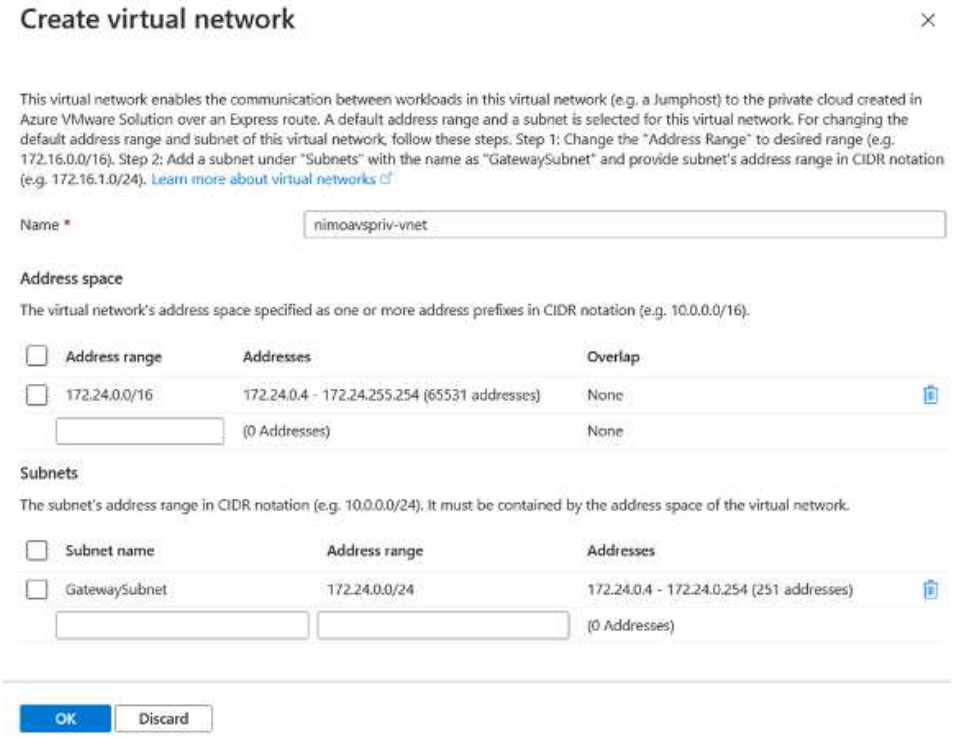
1. Gehen Sie zur Azure VMware Solution Private Cloud und greifen Sie unter Manage auf Konnektivität zu.
2. Wählen Sie Azure vnet Connect aus.
3. Um ein neues vnet zu erstellen, wählen Sie die Option Neue erstellen.

   Mit dieser Funktion kann ein vnet mit der Azure VMware-Lösung Private Cloud verbunden werden. Vnet ermöglicht die Kommunikation zwischen Workloads in diesem virtuellen Netzwerk, indem die erforderlichen Komponenten automatisch erstellt werden (z. B. Sprungbox, Shared Services wie Azure NetApp Files und Cloud Volume ONTAP) in der in Azure VMware Lösung erstellten Private Cloud über ExpressRoute.

   Hinweis: der vnet-Adressraum sollte sich nicht mit der privaten Cloud CIDR überschneiden.



4. Geben Sie die Informationen für die neue vnet ein, oder aktualisieren Sie sie, und wählen Sie OK.

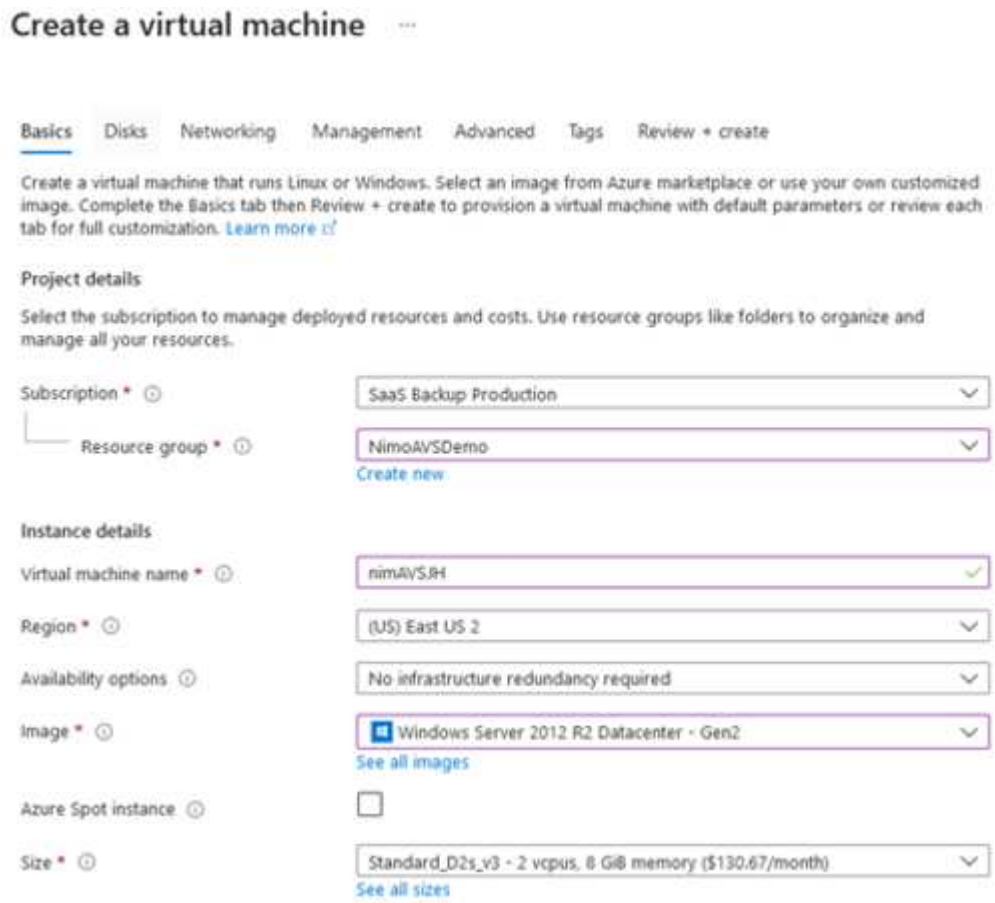


Das vnet mit dem angegebenen Adressbereich und Gateway Subnetz wird in der designierten Abonnement- und Ressourcengruppe erstellt.

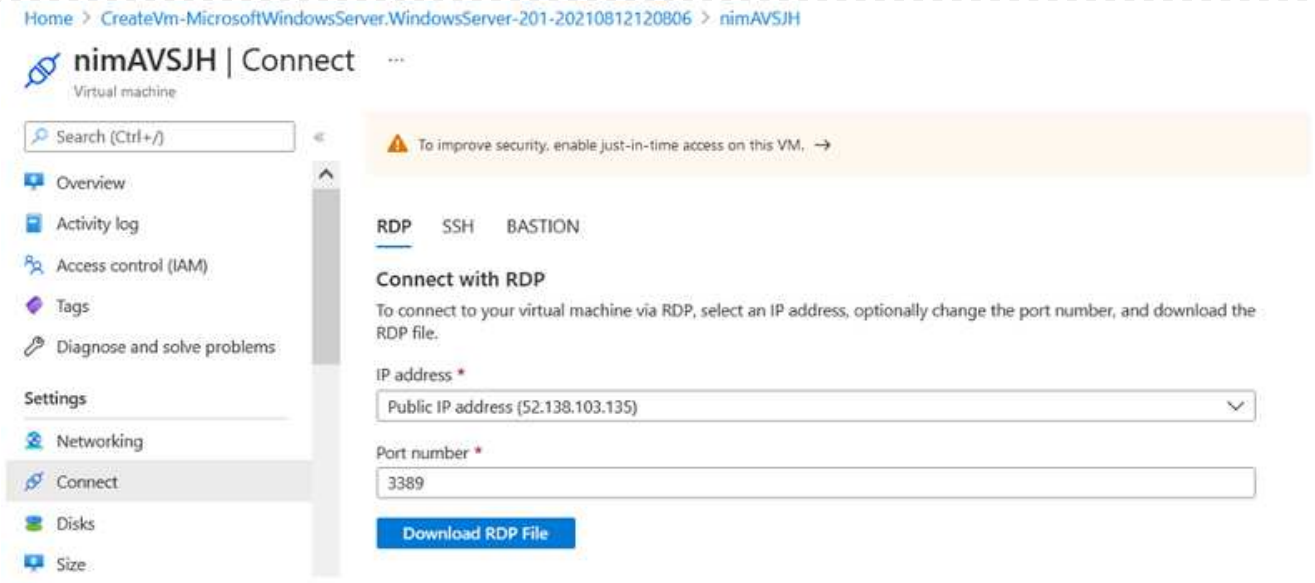
> Wenn Sie ein vnet manuell erstellen, erstellen Sie ein virtuelles Netzwerk-Gateway mit der entsprechenden SKU und ExpressRoute als Gateway-Typ. Nach Abschluss der Implementierung verbinden Sie die ExpressRoute Verbindung mit dem virtuellen Netzwerk-Gateway mit der Private Cloud der Azure VMware Lösung über den Autorisierungsschlüssel. Weitere Informationen finden Sie unter "Konfigurieren Sie das Networking für Ihre VMware Private Cloud in Azure".

Netzwerkverbindung und Zugriff auf Azure VMware Solution Private Cloud validieren

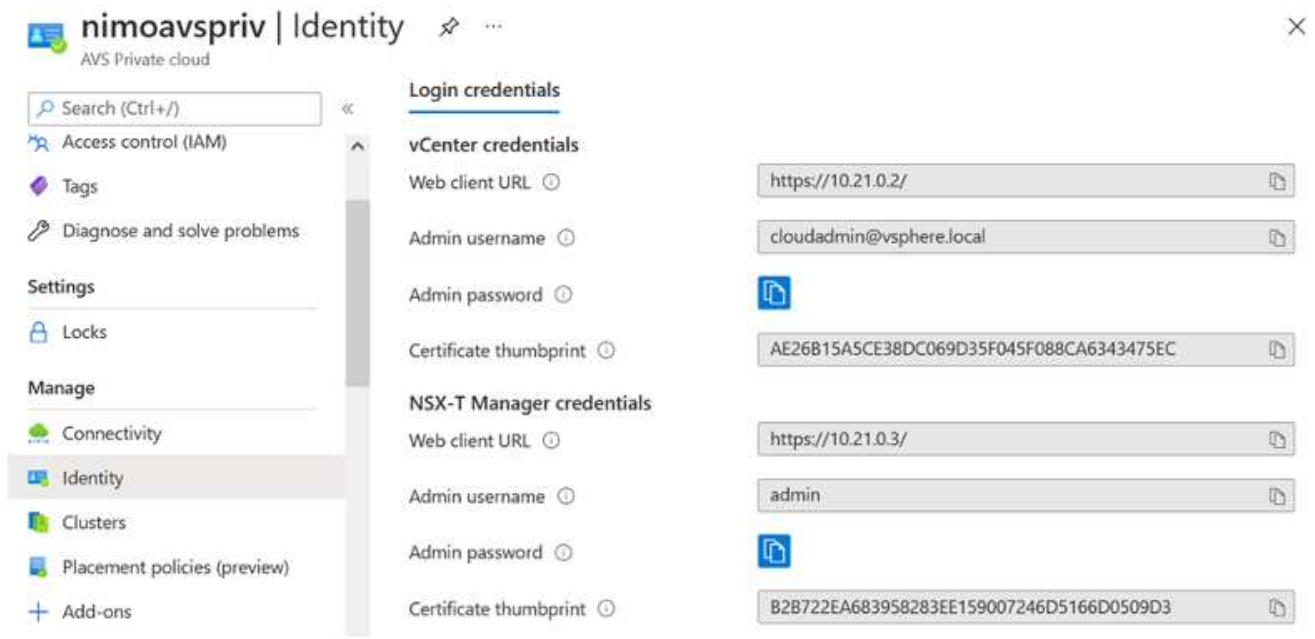
Mit der Azure VMware Lösung können Sie eine Private Cloud nicht über VMware vCenter vor Ort managen. Stattdessen ist zum Herstellen der Verbindung mit der vCenter Instanz der Azure VMware Lösung ein Sprunglink auf den Host erforderlich. Erstellen Sie einen Sprunghost in der angegebenen Ressourcengruppe und melden Sie sich bei Azure VMware Solution vCenter an. Dieser Jump-Host sollte eine Windows VM in demselben virtuellen Netzwerk sein, das für die Konnektivität erstellt wurde und sowohl vCenter als auch den NSX Manager nutzen sollte.



Nachdem die virtuelle Maschine bereitgestellt wurde, verwenden Sie die Option Verbinden, um auf RDP zuzugreifen.

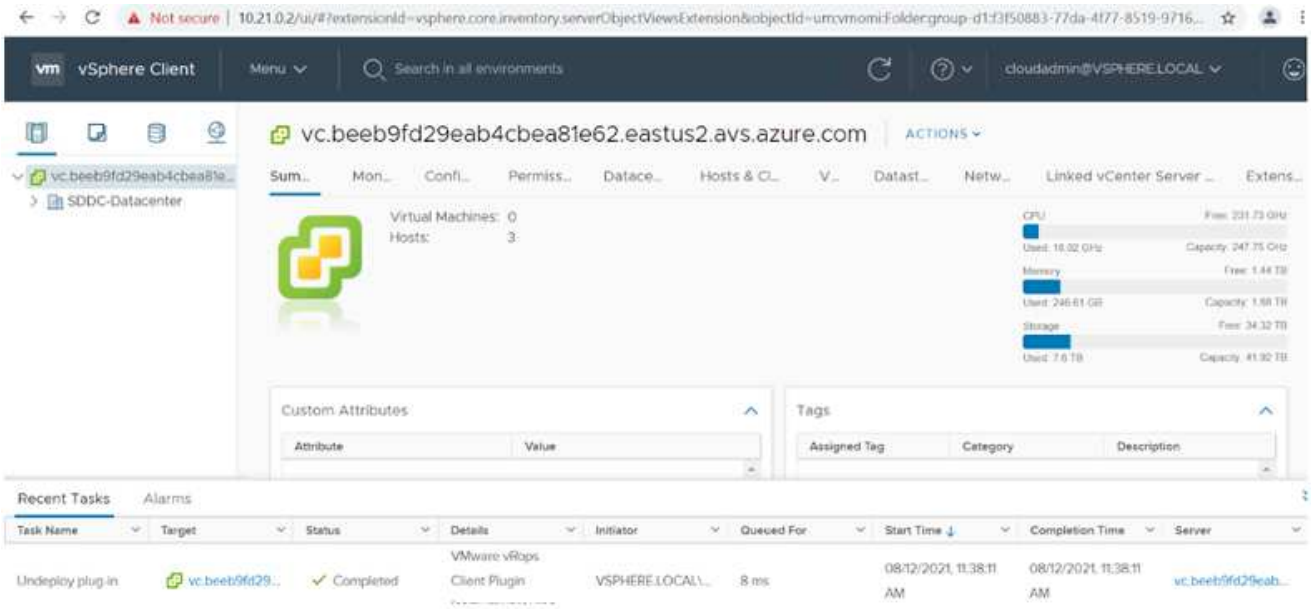


Melden Sie sich von dieser neu erstellten Jump-Host-virtuellen Maschine mit dem Cloud-Admin-Benutzer in vCenter an. Rufen Sie zum Zugreifen auf die Anmeldedaten im Azure-Portal auf und navigieren Sie zu „Identity“ (Identitäts-Management (über die Option „Manage“ in der Private Cloud). Die URLs und Benutzeranmeldeinformationen für die private Cloud vCenter und NSX-T Manager können hier kopiert werden.



Öffnen Sie in der virtuellen Windows-Maschine einen Browser, und navigieren Sie zur vCenter Web-Client-URL Und verwenden Sie den Admin-Benutzernamen als **cloudadmin@vsphere.local** und fügen Sie das kopierte Passwort ein. Auf ähnliche Weise kann auch NSX-T-Manager über die Web-Client-URL zugegriffen werden Und verwenden Sie den Admin-Benutzernamen und fügen Sie das kopierte Passwort ein, um neue Segmente zu erstellen oder die vorhandenen Tier-Gateways zu ändern.

> Die Web-Client-URLs sind für jede bereitgestellte SDDC unterschiedlich.



Die Azure VMware Lösung SDDC ist jetzt implementiert und konfiguriert. Nutzung von ExpressRoute Global REACH zur Verbindung der lokalen Umgebung mit der Private Cloud der Azure VMware Lösung Weitere Informationen finden Sie unter "Erstellen Sie Peer-on-Premises-Umgebungen mit der Azure VMware Lösung".

Implementieren und Konfigurieren der Virtualisierungsumgebung auf der Google Cloud Platform (GCP)

Wie bei vor Ort ist die Planung der Google Cloud VMware Engine (GCVE) entscheidend für eine erfolgreiche produktionsbereite Umgebung für das Erstellen von VMs und die Migration.

In diesem Abschnitt wird beschrieben, wie Sie GCVE einrichten und managen und in Kombination mit den verfügbaren Optionen zum Verbinden von NetApp Storage verwenden.

Der Einrichtungsvorgang kann in die folgenden Schritte unterteilt werden:

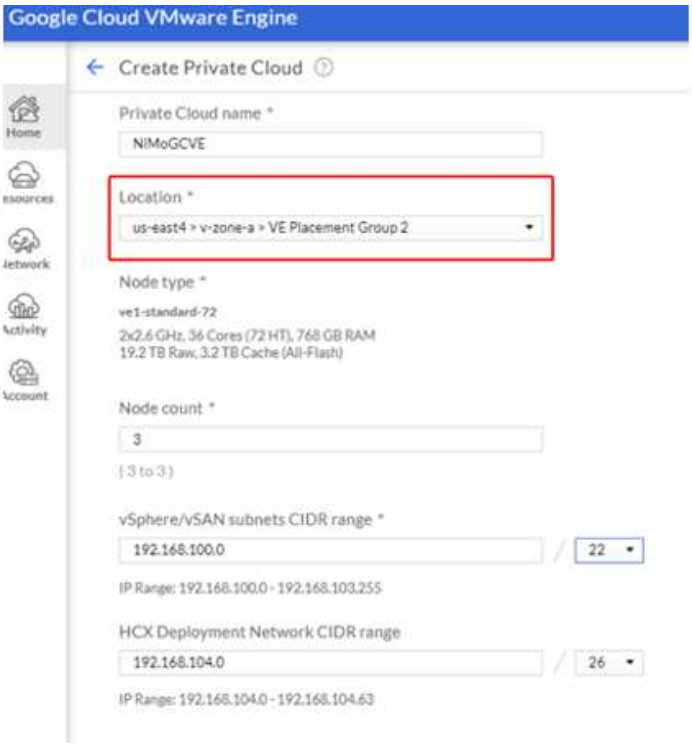
GCVE bereitstellen und konfigurieren

Um eine GCVE-Umgebung auf GCP zu konfigurieren, melden Sie sich bei der GCP-Konsole an und greifen Sie auf das VMware Engine-Portal zu.

Klicken Sie auf die Schaltfläche „Neue private Cloud“ und geben Sie die gewünschte Konfiguration für die GCVE Private Cloud ein. Achten Sie beim „Standort“ darauf, die Private Cloud in derselben Region/Zone, in der CVS/CVO implementiert wird, zu implementieren, um die beste Performance und die niedrigste Latenz zu gewährleisten.

Voraussetzungen:

- Einrichtung der IAM-Rolle des VMware Engine Service Admin
- "VMware Engine-API-Zugriff und Node-Kontingent aktivieren"
- Stellen Sie sicher, dass der CIDR-Bereich nicht mit Ihren lokalen oder Cloud-Subnetzen überlappt. Der CIDR-Bereich muss /27 oder höher sein.



Hinweis: Die Erstellung einer privaten Cloud kann zwischen 30 Minuten und 2 Stunden dauern.

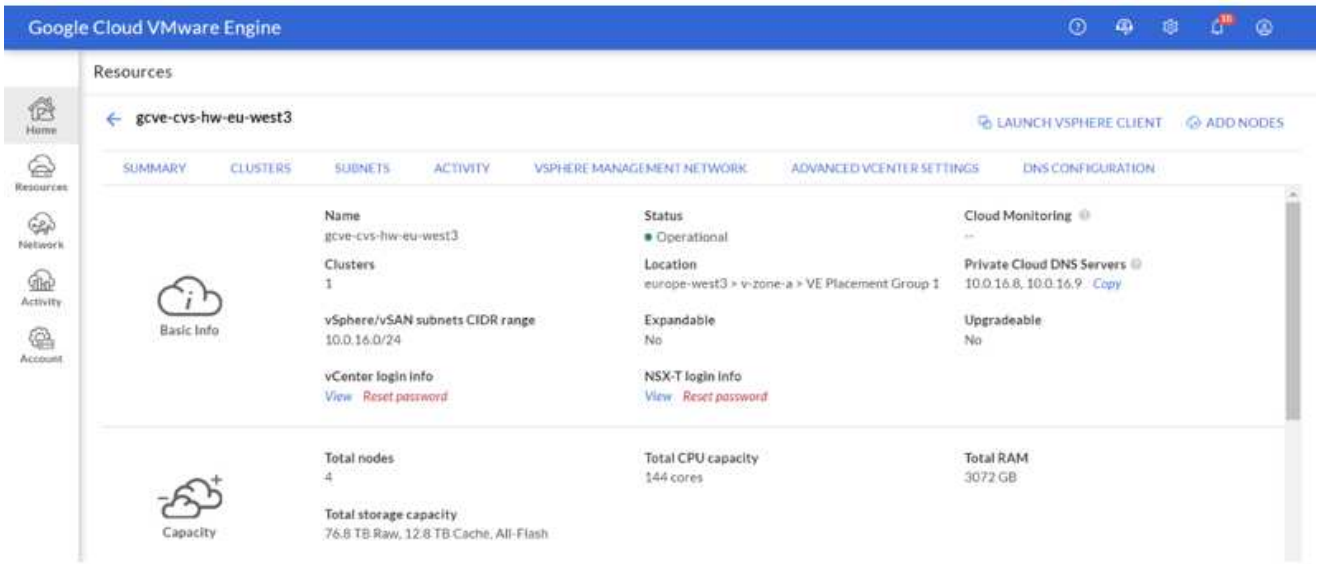
Aktivieren Sie den privaten Zugriff auf GCVE

Konfigurieren Sie nach der Bereitstellung der Private Cloud den privaten Zugriff auf die Private Cloud für eine Verbindung mit hohem Durchsatz und niedriger Latenz.

Dadurch wird sichergestellt, dass das VPC-Netzwerk, auf dem Cloud Volumes ONTAP-Instanzen ausgeführt werden, mit der GCVE Private Cloud kommunizieren kann. Folgen Sie dazu dem "GCP-Dokumentation". Richten Sie für den Cloud Volume Service eine Verbindung zwischen VMware Engine und Cloud Volumes Service ein, indem Sie einmalig zwischen den Mandanten-Host-Projekten Peering durchführen. Gehen Sie wie folgt vor, um ausführliche Schritte zu erhalten "Verlinken".

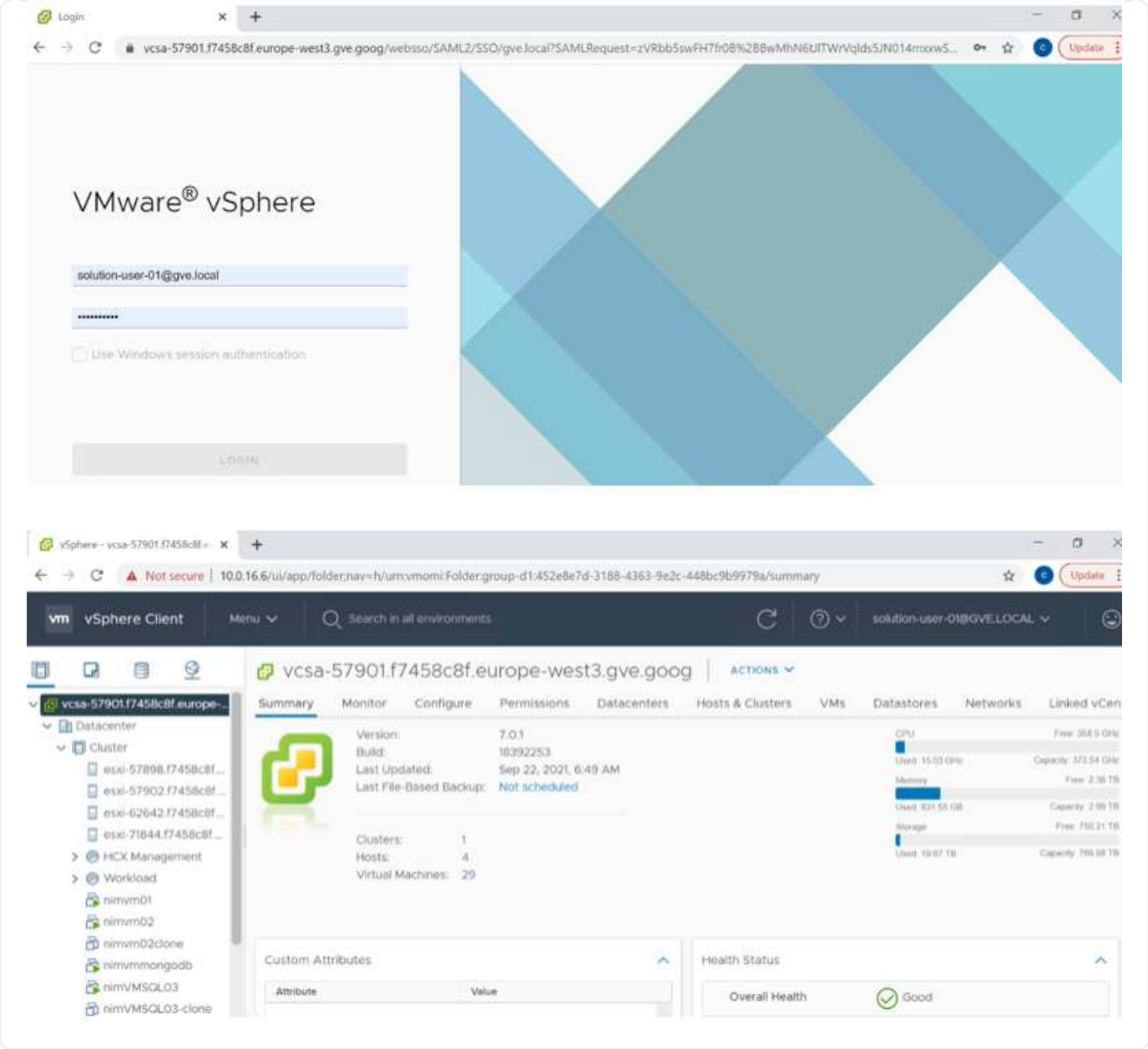
Tenant P	Service	Region	Routing Mode	Peered Project ID	Peered VPC	VPC Peering Sta...	Region Status
ke841388caa56b...	VPC Network	europe-west3	Global	cv-performance-te...	cloud-volumes-vpc	Active	Connected
jbd729510b3ebbf...	NetApp CVS	europe-west3	Global	y2b6c17202af6dc...	netapp-tenant-vpc	Active	Connected

Melden Sie sich mit dem CloudOwner@gve.local-Benutzer bei vcenter an. Rufen Sie das VMware Engine Portal auf, rufen Sie zu Ressourcen auf und wählen Sie die entsprechende Private Cloud aus. Klicken Sie im Abschnitt grundlegende Informationen auf den Link Anzeigen, um die vCenter-Anmeldedaten (vCenter Server, HCX Manager) oder NSX-T-Anmeldeinformationen (NSX Manager) anzuzeigen.



Öffnen Sie in einer virtuellen Windows-Maschine einen Browser, und navigieren Sie zur vCenter Web-Client-URL Verwenden Sie dann den Admin-Benutzernamen als CloudOwner@gve.local, und fügen Sie das kopierte Passwort ein. Auf ähnliche Weise kann auch NSX-T-Manager über die Web-Client-URL zugegriffen werden Und verwenden Sie den Admin-Benutzernamen und fügen Sie das kopierte Passwort ein, um neue Segmente zu erstellen oder die vorhandenen Tier-Gateways zu ändern.

Wenn Sie ein lokales Netzwerk zur Private Cloud der VMware Engine verbinden möchten, nutzen Sie Cloud-VPN oder Cloud Interconnect, um entsprechende Konnektivität zu erhalten und stellen sicher, dass die erforderlichen Ports geöffnet sind. Gehen Sie wie folgt vor, um ausführliche Schritte zu erhalten "Verlinken".



Stellen Sie zusätzlichen Datastore für den NetApp-Cloud-Volume-Service in GCVE bereit

Siehe "Verfahren zum Bereitstellen von zusätzlichem NFS-Datastore mit NetApp CVS zu GCVE"

Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.