VMware nella configurazione degli hyperscaler

NetApp Solutions

NetApp
April 26, 2024

Sommario

Configurazione dell’ambiente di virtualizzazione nel cloud provider 1
Implementare e configurare l’ambiente di virtualizzazione su AWS 2
Implementare e configurare l’ambiente di virtualizzazione su Azure 18
Implementare e configurare l’ambiente di virtualizzazione su Google Cloud Platform (GCP) 26

Configurazione dell’ambiente di virtualizzazione nel cloud provider

I dettagli su come configurare l’ambiente di virtualizzazione in ciascuno degli hyperscaler supportati sono illustrati qui.

AWS/VMC

Questa sezione descrive come configurare e gestire VMware Cloud su AWS SDDC e utilizzarlo in combinazione con le opzioni disponibili per la connessione dello storage NetApp.

> Lo storage in-guest è l'unico metodo supportato per connettere Cloud Volumes ONTAP ad AWS VMC.

Il processo di installazione può essere suddiviso nei seguenti passaggi:

- Implementazione e configurazione di VMware Cloud per AWS
- Connetti VMware Cloud a FSX ONTAP

Visualizza i dettagli "Procedura di configurazione per VMC".

Azure/AVS

Questa sezione descrive come configurare e gestire Azure VMware Solution e utilizzarla in combinazione con le opzioni disponibili per la connessione dello storage NetApp.

> Lo storage in-guest è l'unico metodo supportato per connettere Cloud Volumes ONTAP alla soluzione VMware Azure.

Il processo di installazione può essere suddiviso nei seguenti passaggi:

- Registrare il provider di risorse e creare un cloud privato
- Connettersi a un gateway di rete virtuale ExpressRoute nuovo o esistente
- Convalidare la connettività di rete e accedere al cloud privato

Visualizza i dettagli "Procedura di configurazione per AVS".

GCP/GCVE

Questa sezione descrive come configurare e gestire GCVE e utilizzarlo in combinazione con le opzioni disponibili per la connessione dello storage NetApp.

> Lo storage in-guest è l'unico metodo supportato per connettere Cloud Volumes ONTAP e Cloud Volumes Services a GCVE.

Il processo di installazione può essere suddiviso nei seguenti passaggi:

- Implementare e configurare GCVE
- Attiva accesso privato a GCVE

Visualizza i dettagli "Procedura di configurazione per GCVE".

Implementare e configurare l'ambiente di virtualizzazione su AWS

Come per i servizi on-premise, la pianificazione di VMware Cloud su AWS è

fondamentale per un ambiente pronto per la produzione di successo per la creazione di macchine virtuali e la migrazione.

Questa sezione descrive come configurare e gestire VMware Cloud su AWS SDDC e utilizzarlo in combinazione con le opzioni disponibili per la connessione dello storage NetApp.

> Lo storage in-guest è attualmente l'unico metodo supportato per connettere Cloud Volumes ONTAP (CVO) ad AWS VMC.

Il processo di installazione può essere suddiviso nei seguenti passaggi:

Implementare e configurare VMware Cloud per AWS

"VMware Cloud su AWS" Offre un'esperienza nativa nel cloud per i carichi di lavoro basati su VMware nell'ecosistema AWS. Ogni VMware Software-Defined Data Center (SDDC) viene eseguito in un Amazon Virtual Private Cloud (VPC) e fornisce uno stack VMware completo (incluso vCenter Server), networking software-defined NSX-T, storage vSAN software-defined e uno o più host ESXi che forniscono risorse di calcolo e storage ai carichi di lavoro.

Questa sezione descrive come configurare e gestire VMware Cloud su AWS e utilizzarlo in combinazione con Amazon FSX per NetApp ONTAP e/o Cloud Volumes ONTAP su AWS con storage in-guest.

> Lo storage in-guest è attualmente l'unico metodo supportato per connettere Cloud Volumes ONTAP (CVO) ad AWS VMC.

Il processo di configurazione può essere suddiviso in tre parti:

Registrati per un account AWS

Registratevi per un "Account Amazon Web Services".

Per iniziare, è necessario un account AWS, supponendo che non ne sia già stato creato uno. Nuovi o esistenti, per eseguire molte operazioni di questa procedura sono necessari privilegi amministrativi nell'account. Vedi questo "collegamento" Per ulteriori informazioni sulle credenziali AWS.

Registrati per un account My VMware

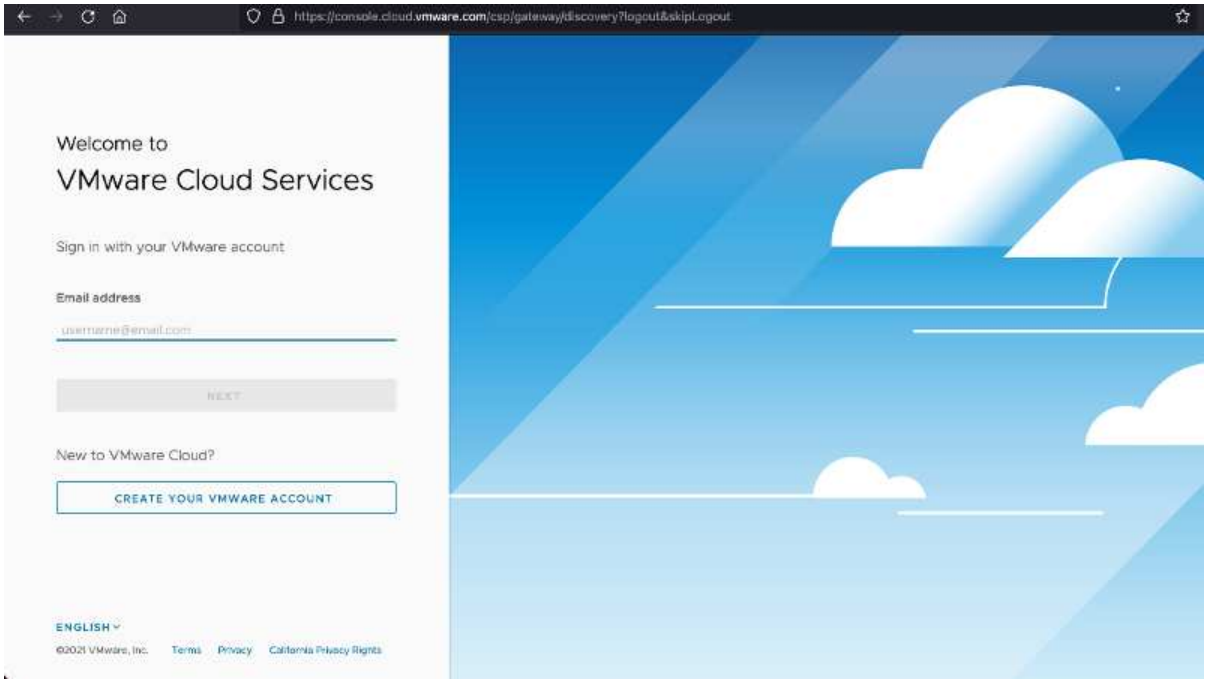
Registratevi per un "Il mio VMware" account.

Per accedere al portfolio cloud di VMware (incluso VMware Cloud su AWS), è necessario un account cliente VMware o un account My VMware. Se non lo si è già fatto, creare un account VMware "qui".

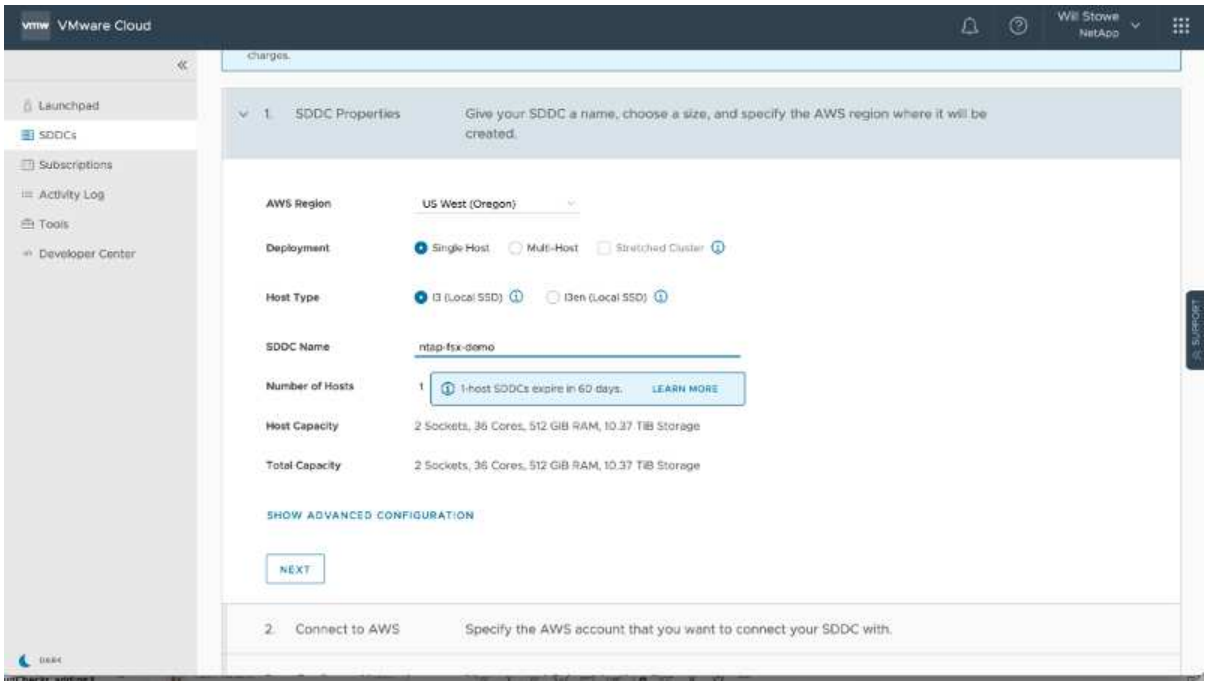
Provisioning di SDDC in VMware Cloud

Una volta configurato l'account VMware e eseguito il dimensionamento corretto, l'implementazione di un Software-Defined Data Center è il passaggio successivo più ovvio per l'utilizzo del servizio VMware Cloud su AWS. Per creare un SDDC, scegliere una regione AWS per ospitarla, assegnare un nome all'SDDC e specificare quanti host ESXi si desidera che l'SDDC contenga. Se non si dispone già di un account AWS, è comunque possibile creare un SDDC di configurazione iniziale contenente un singolo host ESXi.

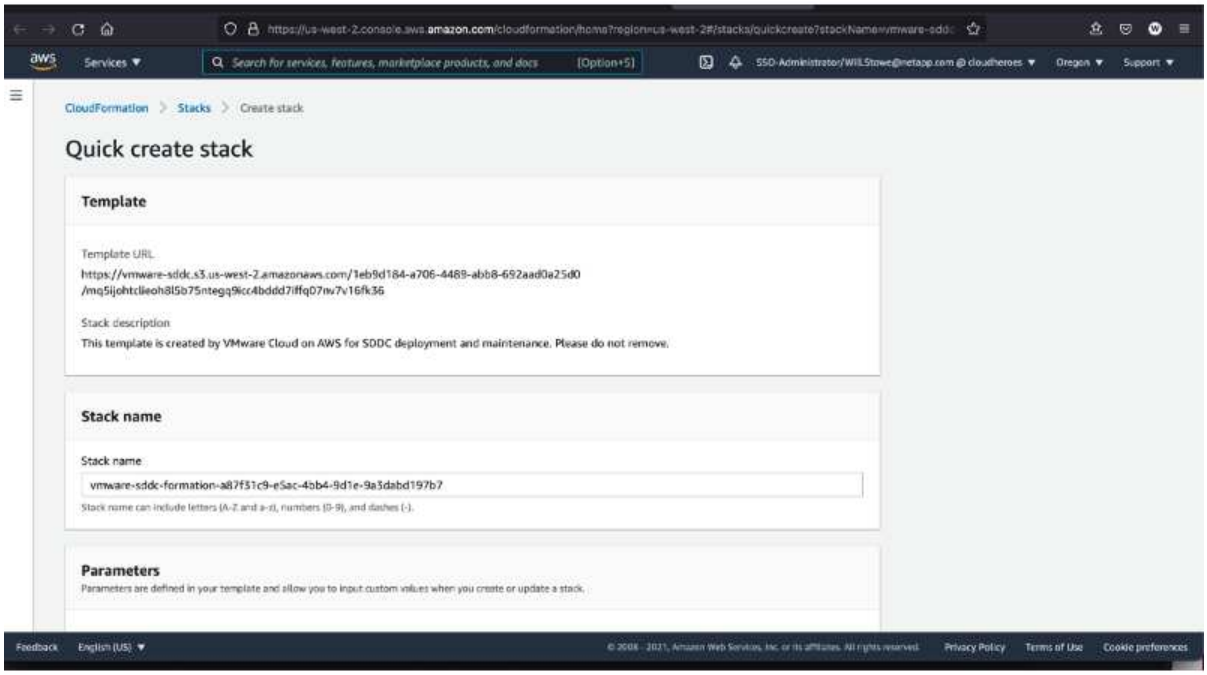
1. Accedere a VMware Cloud Console utilizzando le credenziali VMware esistenti o create di recente.

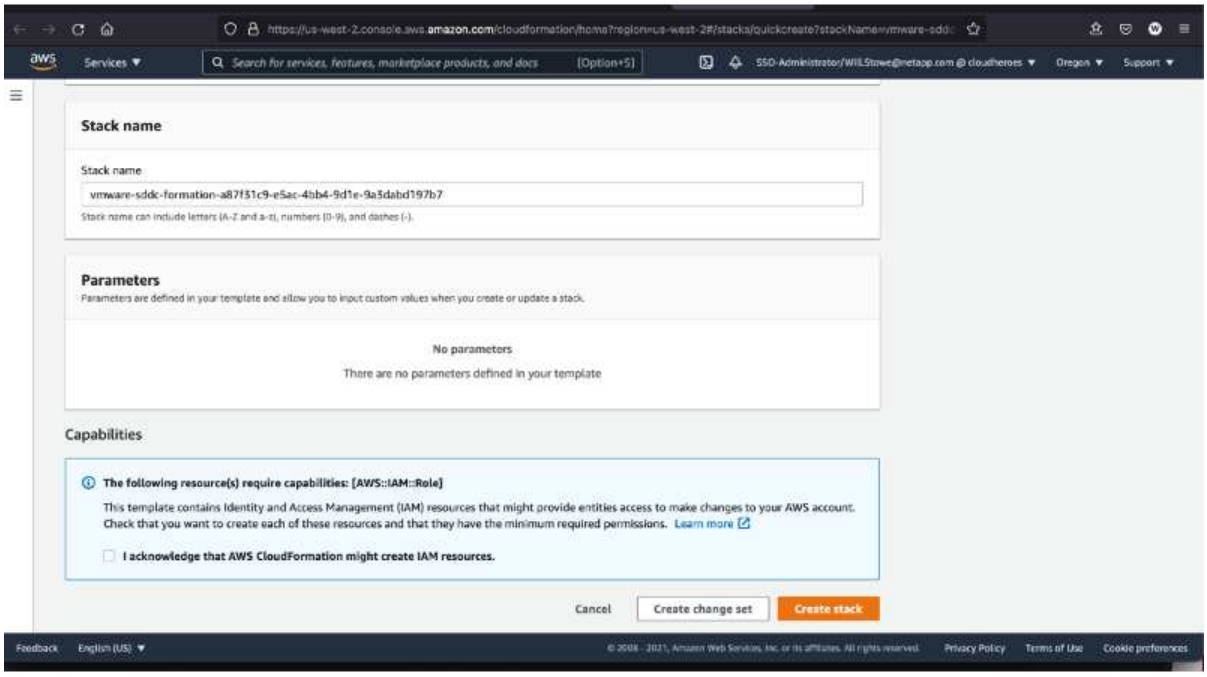


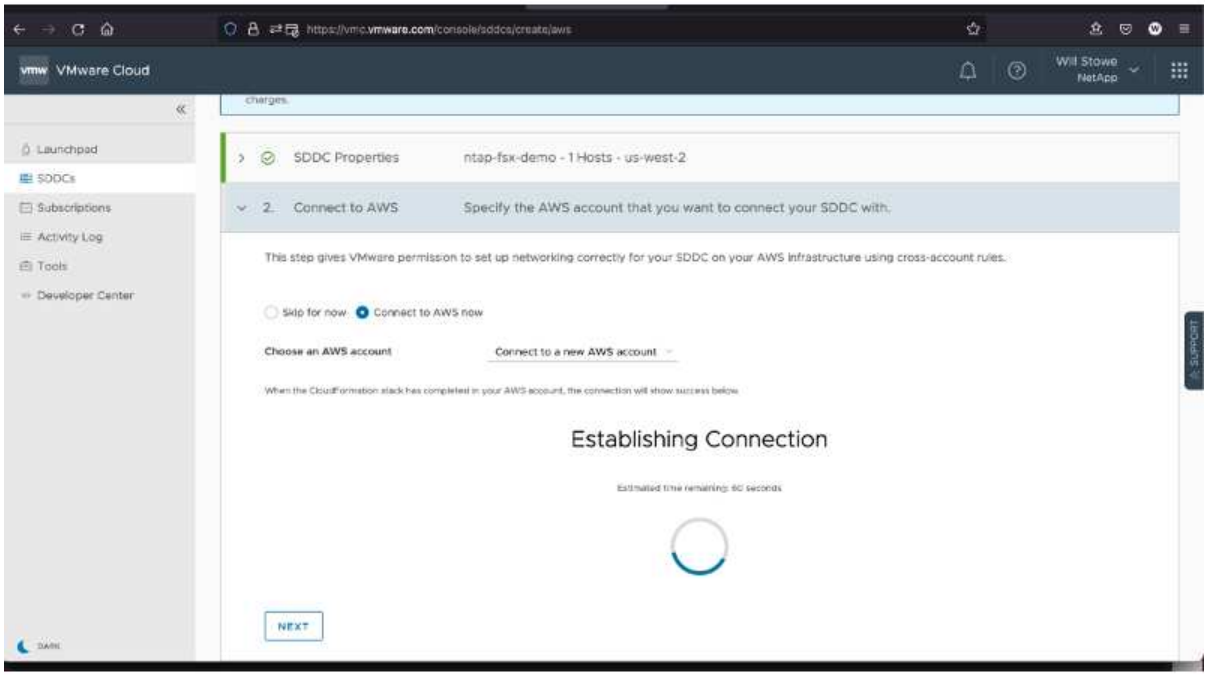
2. Configurare la regione AWS, l'implementazione, il tipo di host e il nome SDDC:

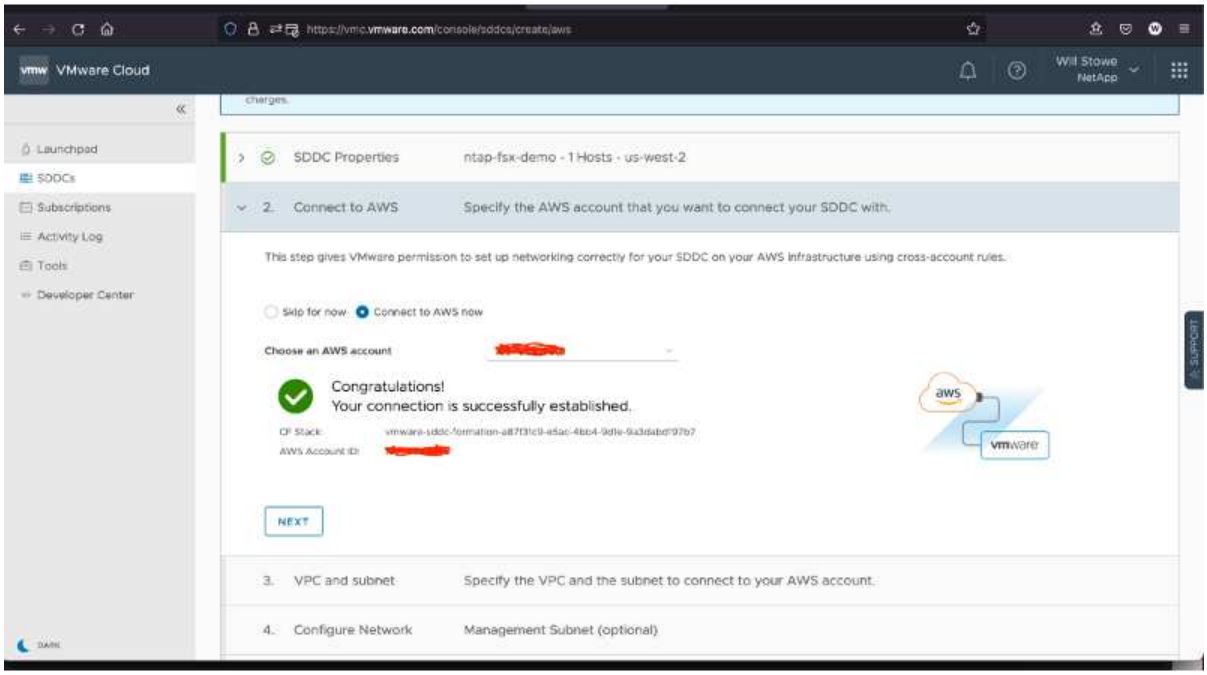


3. Connettersi all’account AWS desiderato ed eseguire lo stack di formazione cloud AWS.



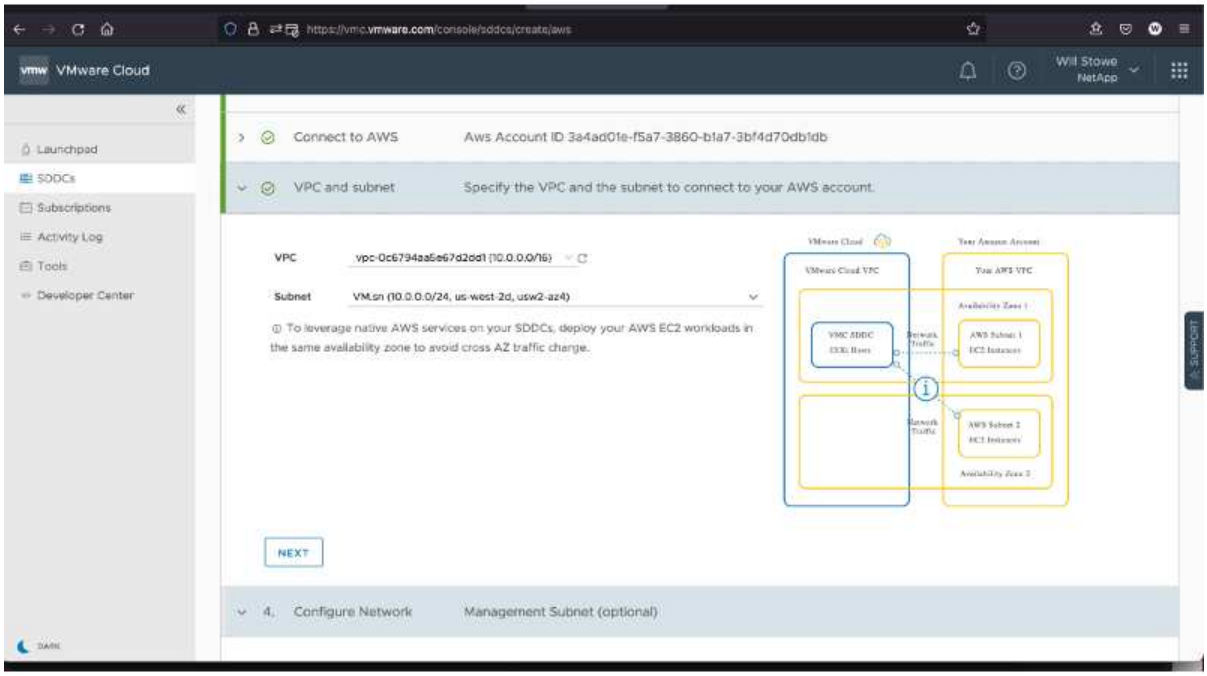




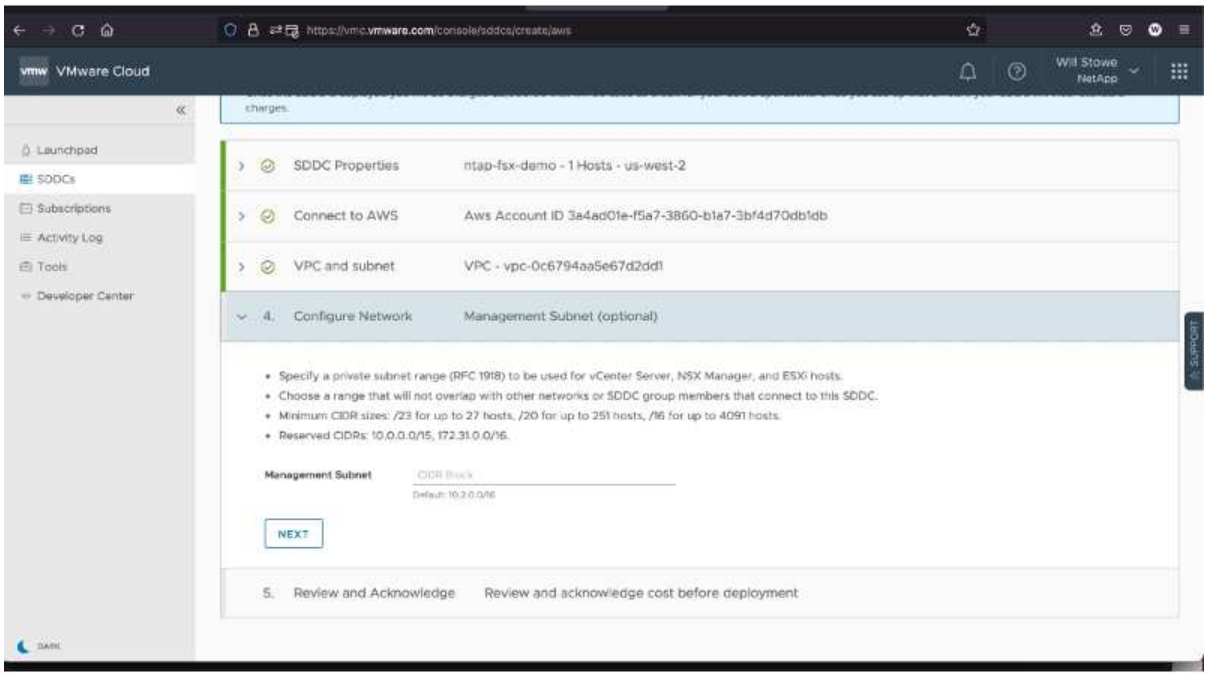


In questa convalida viene utilizzata la configurazione a host singolo.

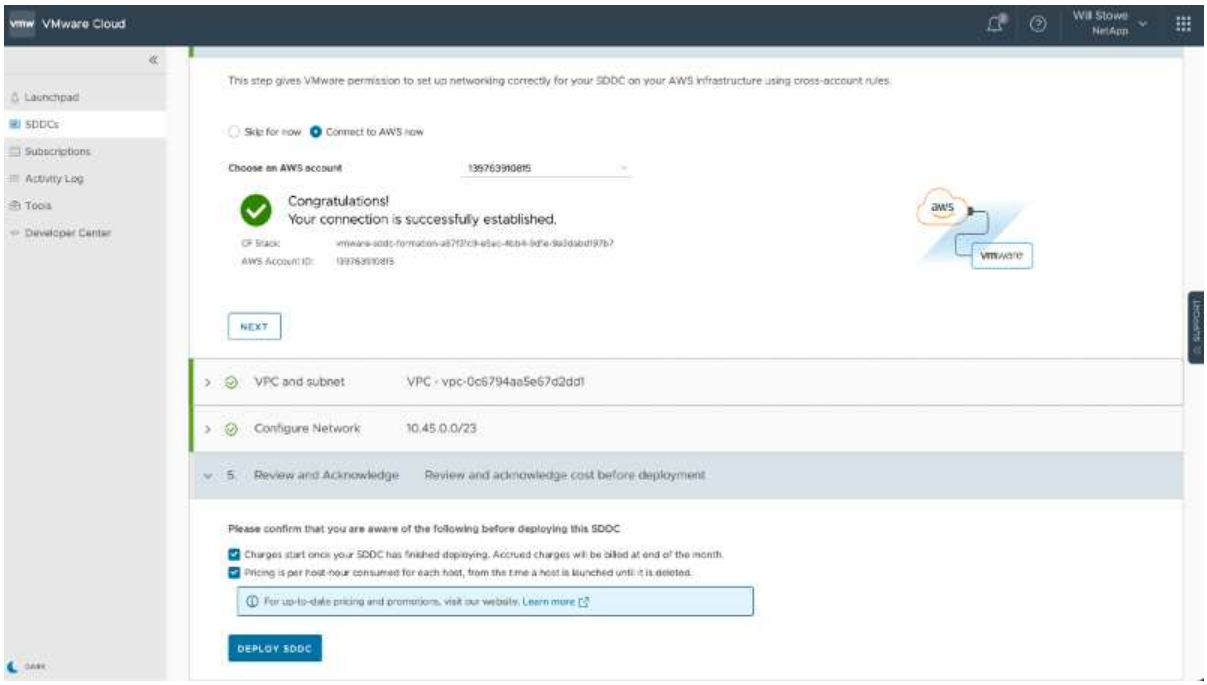
4. Selezionare il VPC AWS desiderato per la connessione dell'ambiente VMC.



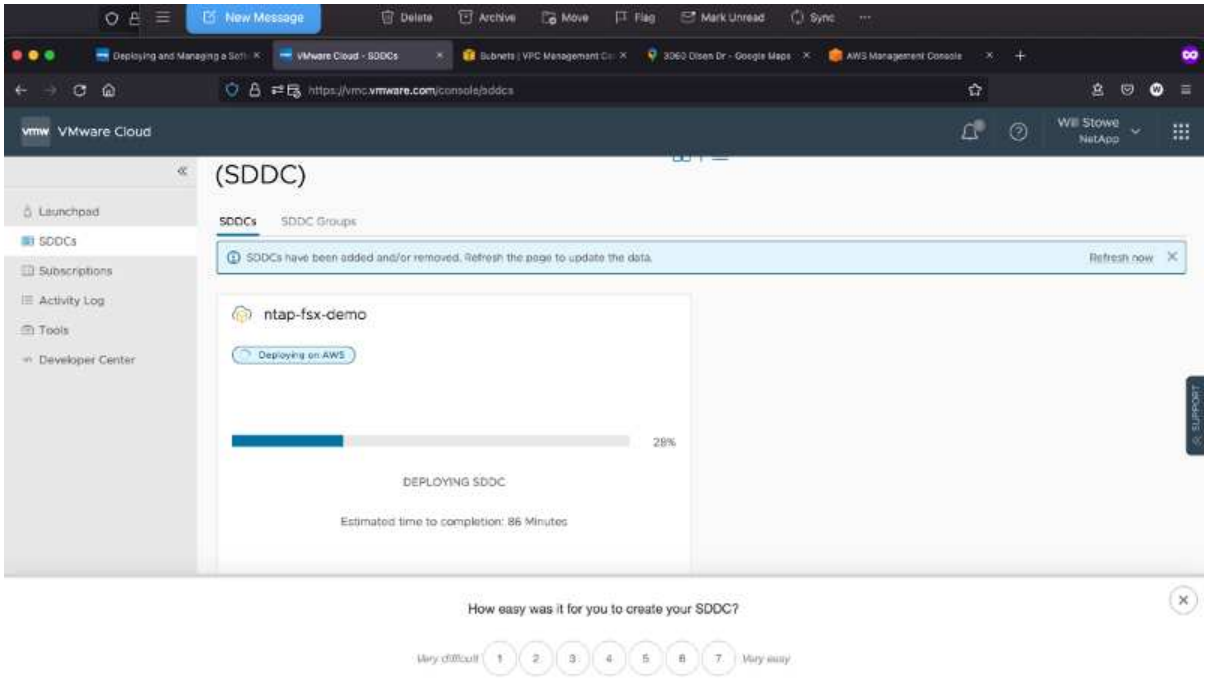
5. Configurare la subnet di gestione VMC; questa subnet contiene servizi gestiti da VMC come vCenter, NSX e così via. Non scegliere uno spazio di indirizzi sovrapposto con altre reti che necessitano di connettività all'ambiente SDDC. Infine, seguire le raccomandazioni per la dimensione CIDR indicate di seguito.



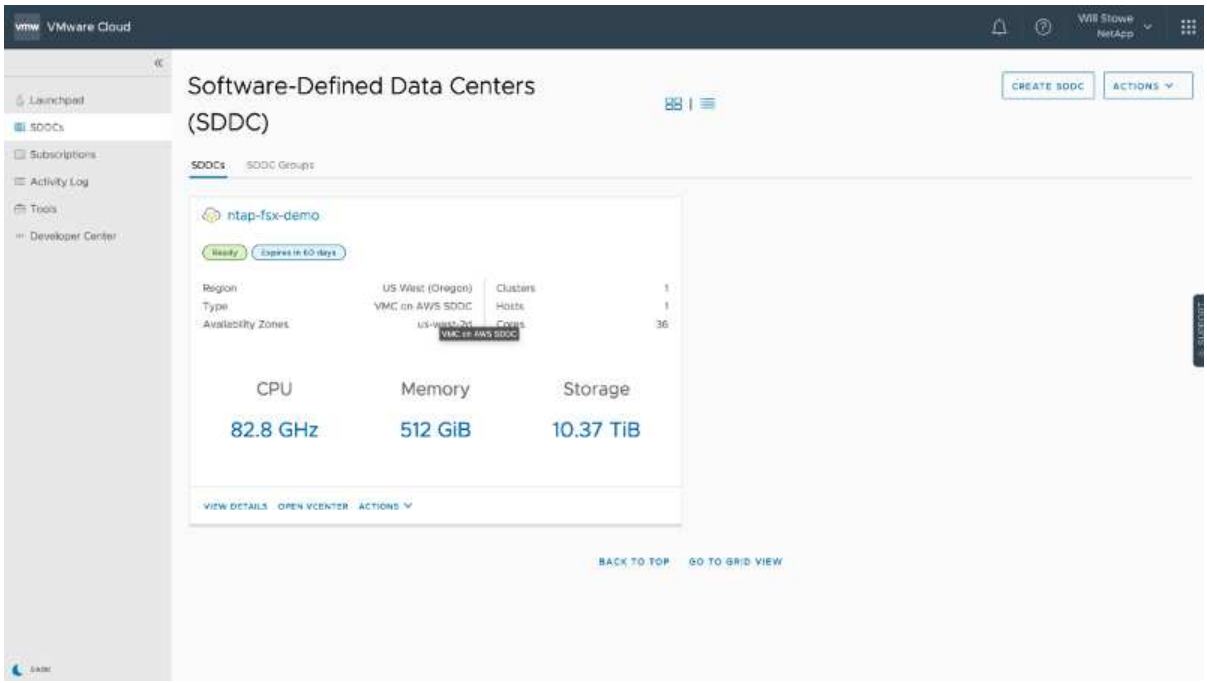
6. Esaminare e riconoscere la configurazione SDDC, quindi fare clic su Deploy the SDDC (implementa SDDC).



Il completamento del processo di implementazione richiede in genere circa due ore.



7. Al termine dell'operazione, SDDC è pronto per l'uso.

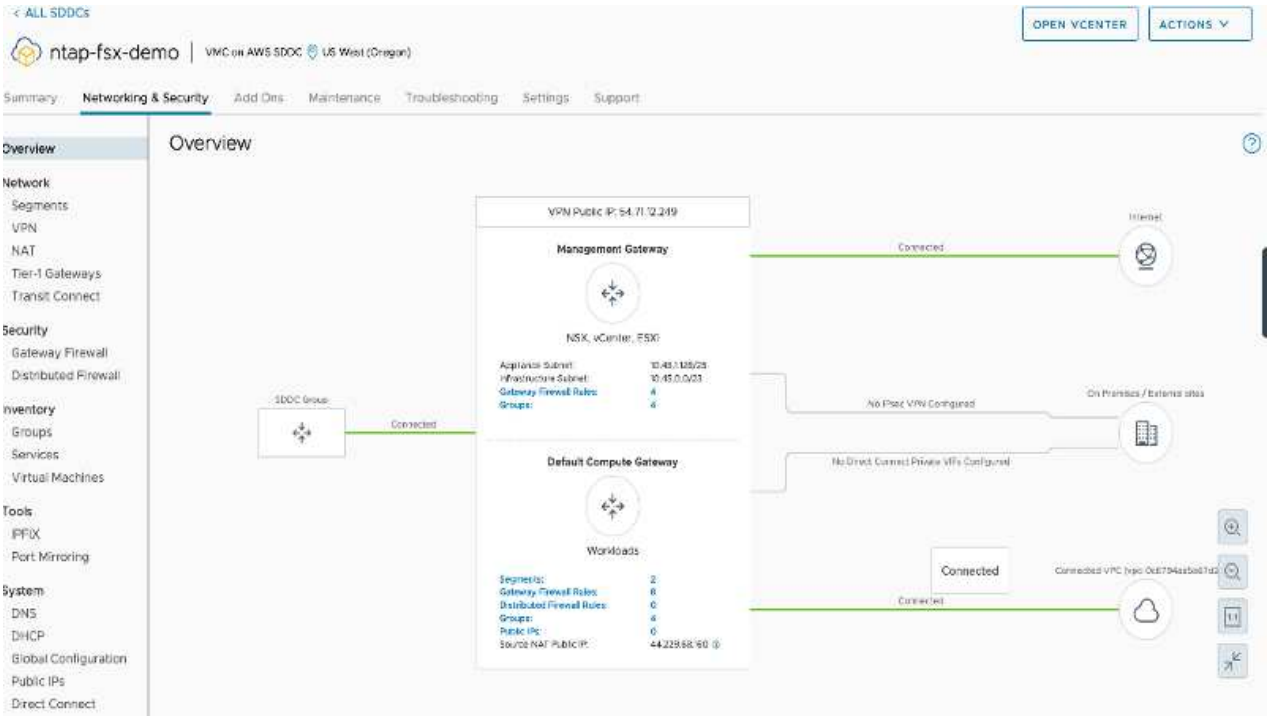


Per una guida dettagliata sull'implementazione di SDDC, vedere "Implementare un SDDC dalla console VMC".

Connetti VMware Cloud a FSX ONTAP

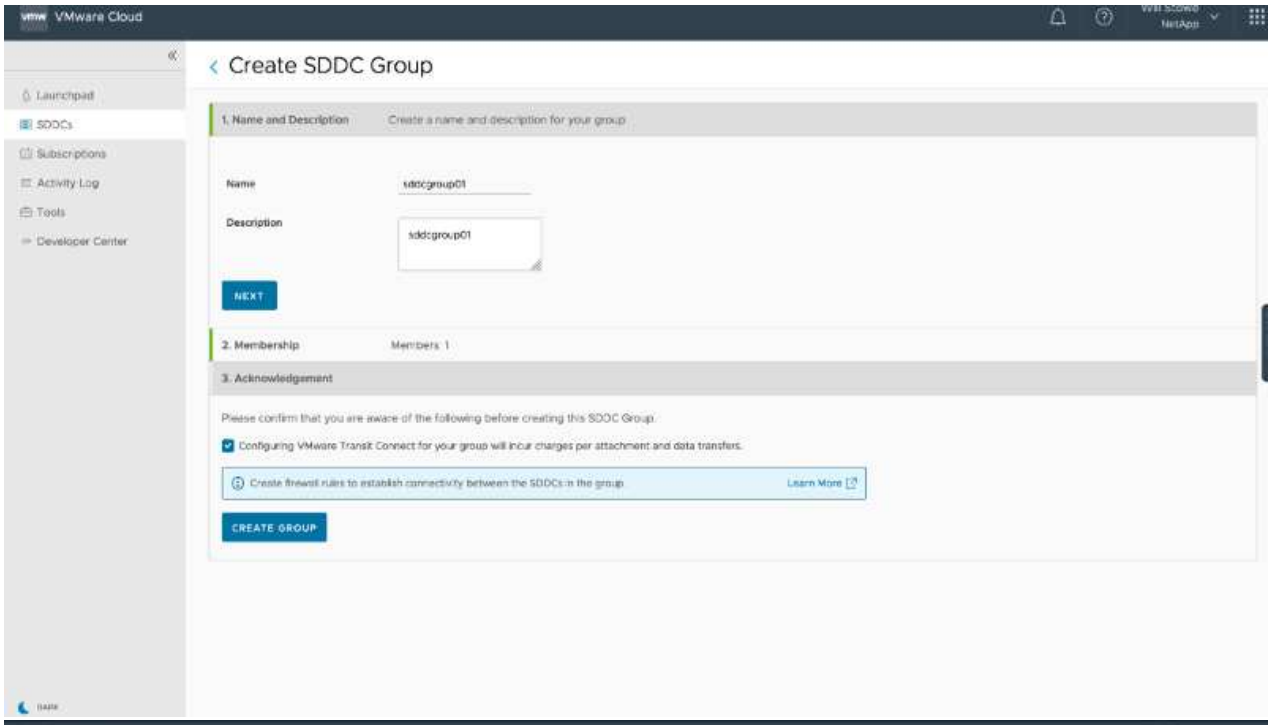
Per connettere VMware Cloud a FSX ONTAP, attenersi alla seguente procedura:

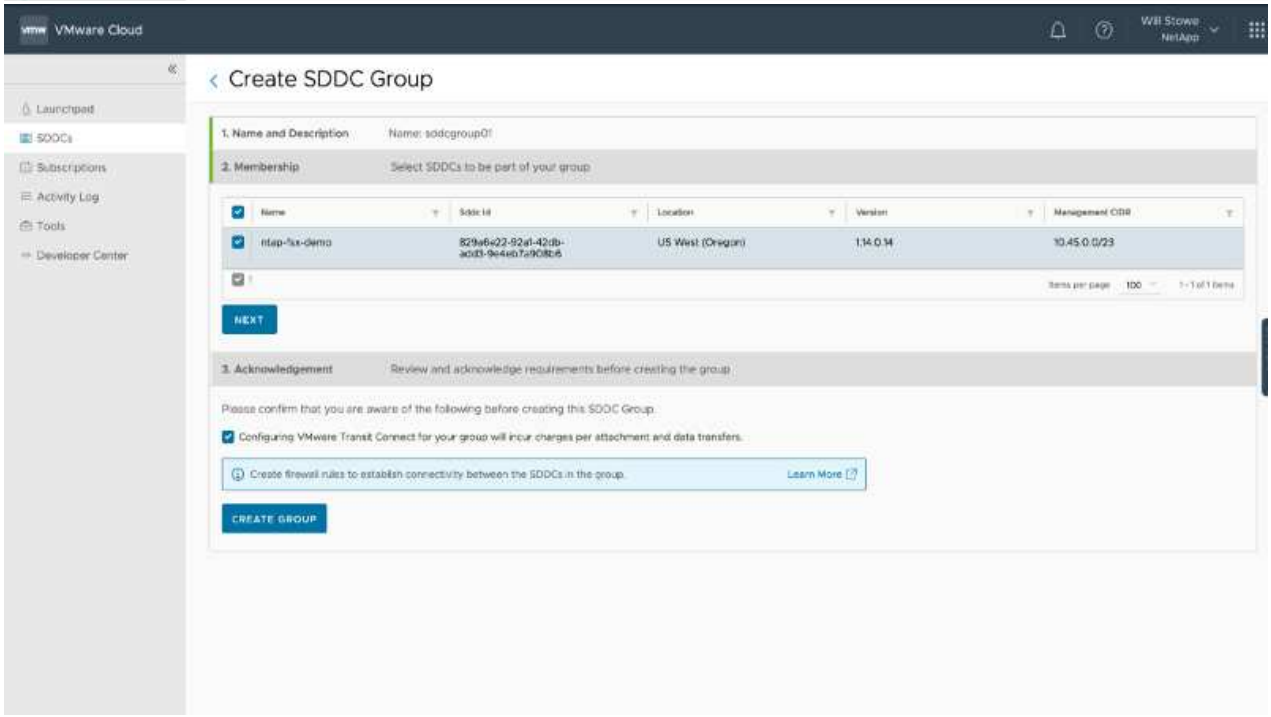
1. Una volta completata l'implementazione di VMware Cloud e connessa ad AWS VPC, è necessario implementare Amazon FSX per NetApp ONTAP in un nuovo VPC anziché nel VPC collegato originale (vedere la schermata riportata di seguito). FSX (IP mobili NFS e SMB) non è accessibile se viene implementato nel VPC connesso. Tenere presente che gli endpoint ISCSI come Cloud Volumes ONTAP funzionano correttamente dal VPC connesso.

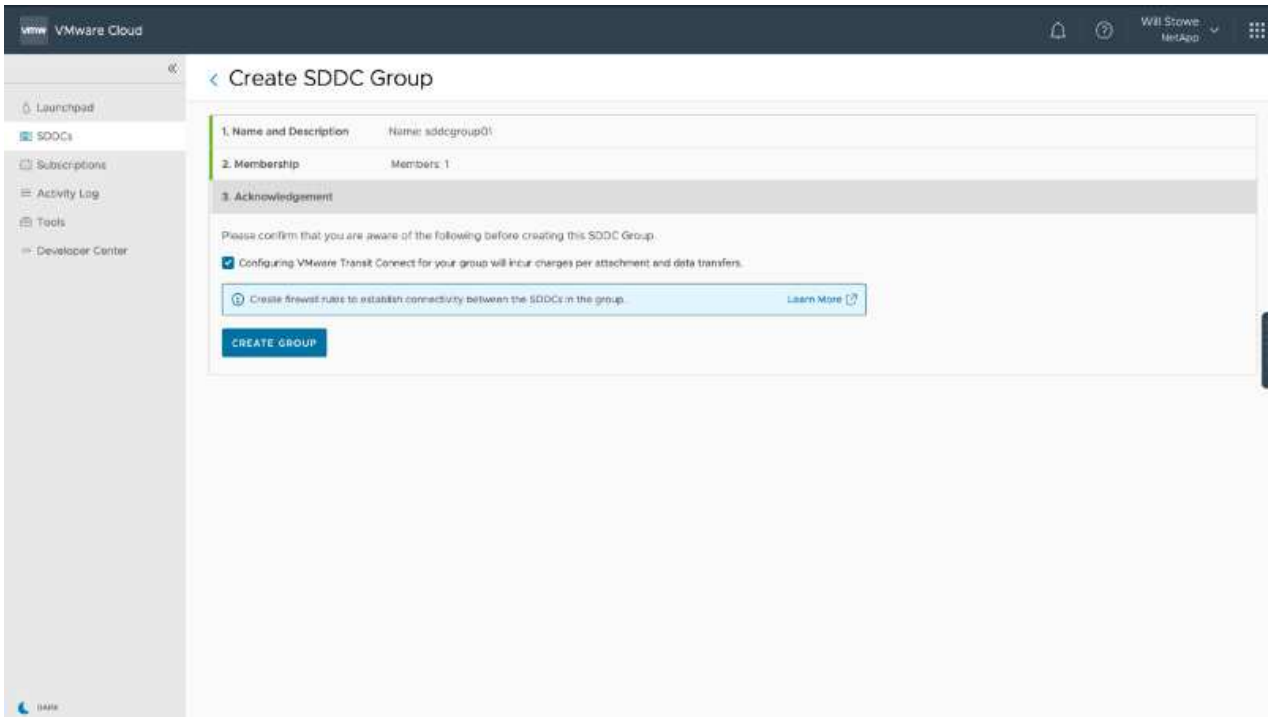


2. Implementare un VPC aggiuntivo nella stessa regione, quindi implementare Amazon FSX per NetApp ONTAP nel nuovo VPC.

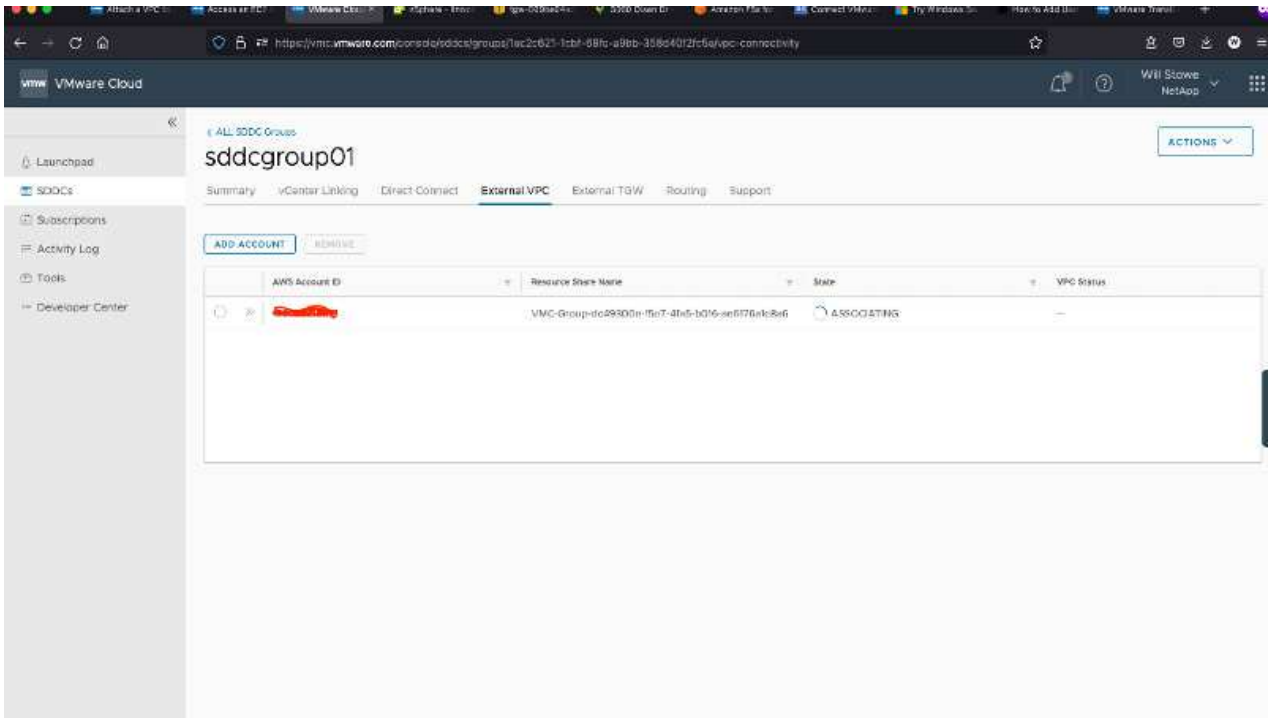
   La configurazione di un gruppo SDDC nella console VMware Cloud abilita le opzioni di configurazione di rete necessarie per connettersi al nuovo VPC in cui viene implementato FSX. Nella fase 3, verificare che l'opzione "Configurazione di VMware Transit Connect per il gruppo comporterà costi per allegato e trasferimento dati" sia selezionata, quindi scegliere Crea gruppo. Il completamento del processo può richiedere alcuni minuti.

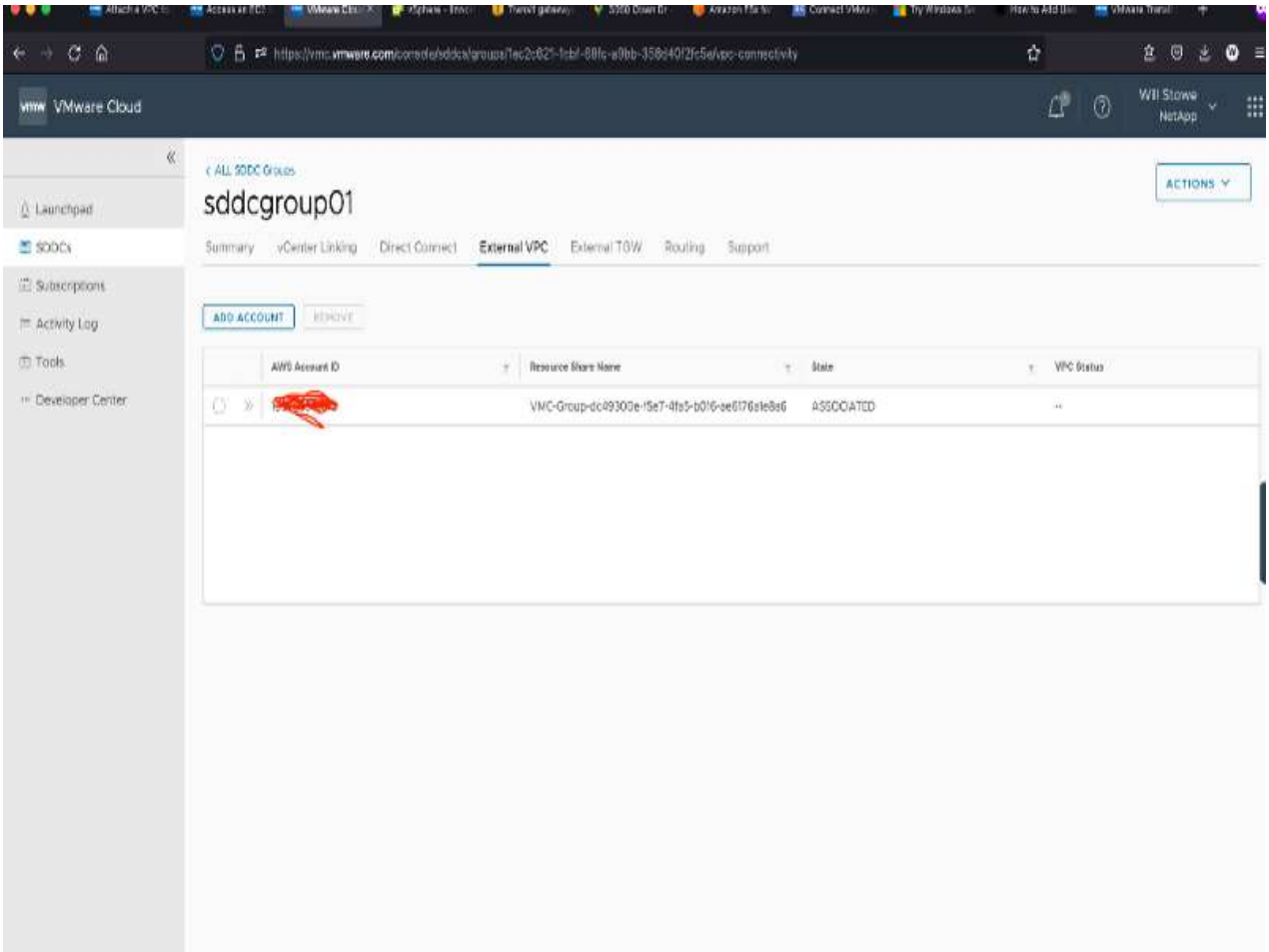

VMware Cloud
Will Stowe
NetApp
Launchpad
SDDCs
Subscriptions
Activity Log
Tools
Developer Center
Create SDDC Group
1. Name and Description
Create a name and description for your group
Name
sddcgroup01
Description
sddcgroup01
NEXT
2. Membership
Members: 1
3. Acknowledgement
Please confirm that you are 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

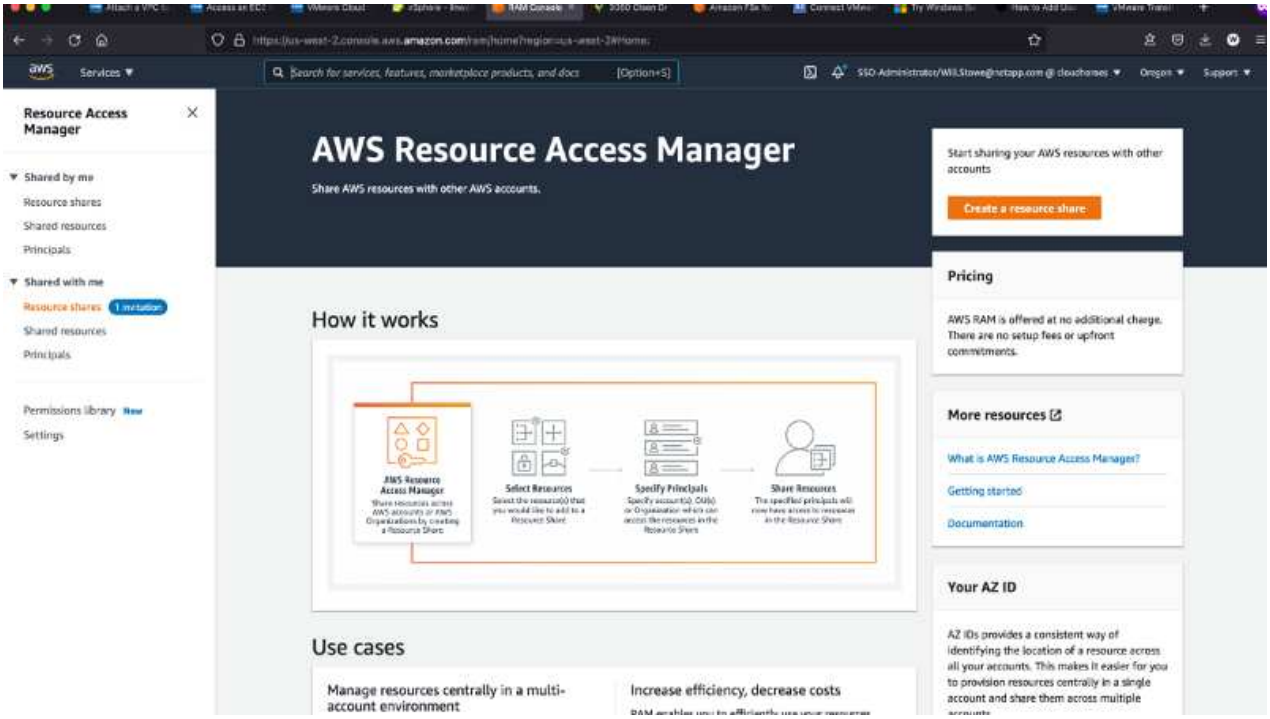


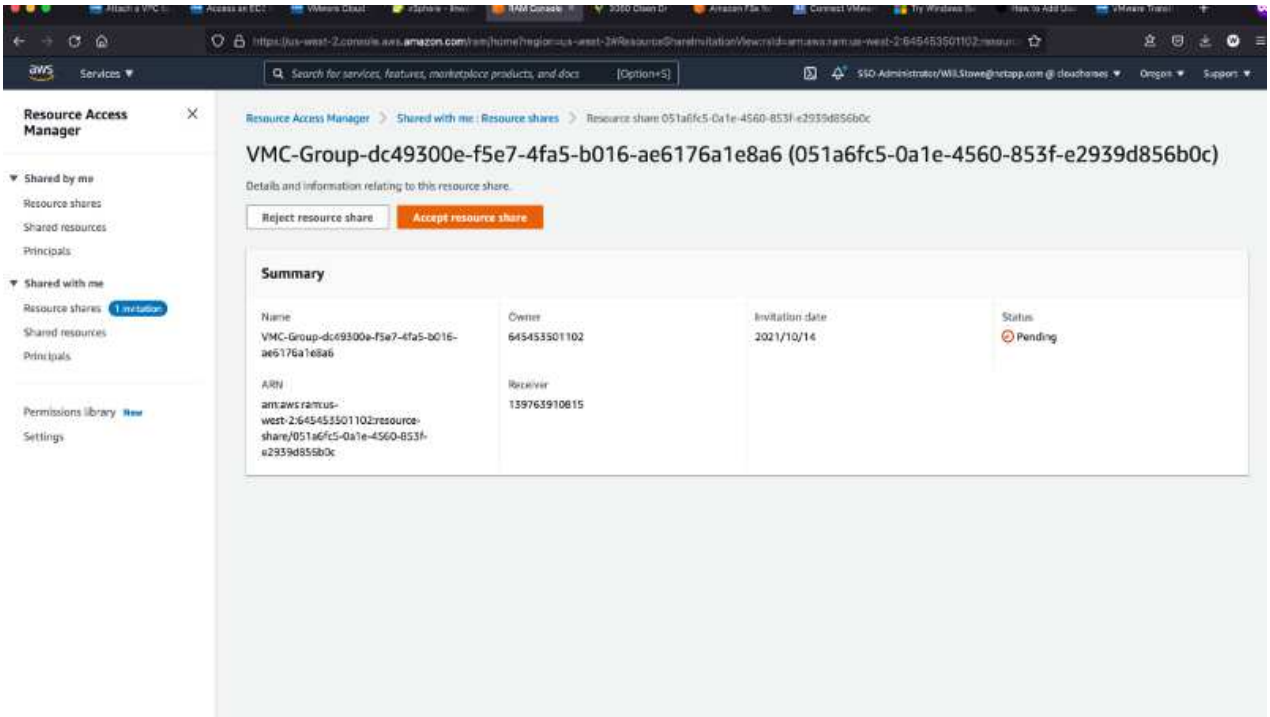
3. Collegare il VPC appena creato al gruppo SDDC appena creato. Selezionare la scheda External VPC (VPC esterno) e seguire le istruzioni "Istruzioni per il collegamento di un VPC esterno" al gruppo. Il completamento di questo processo può richiedere da 10 a 15 minuti.



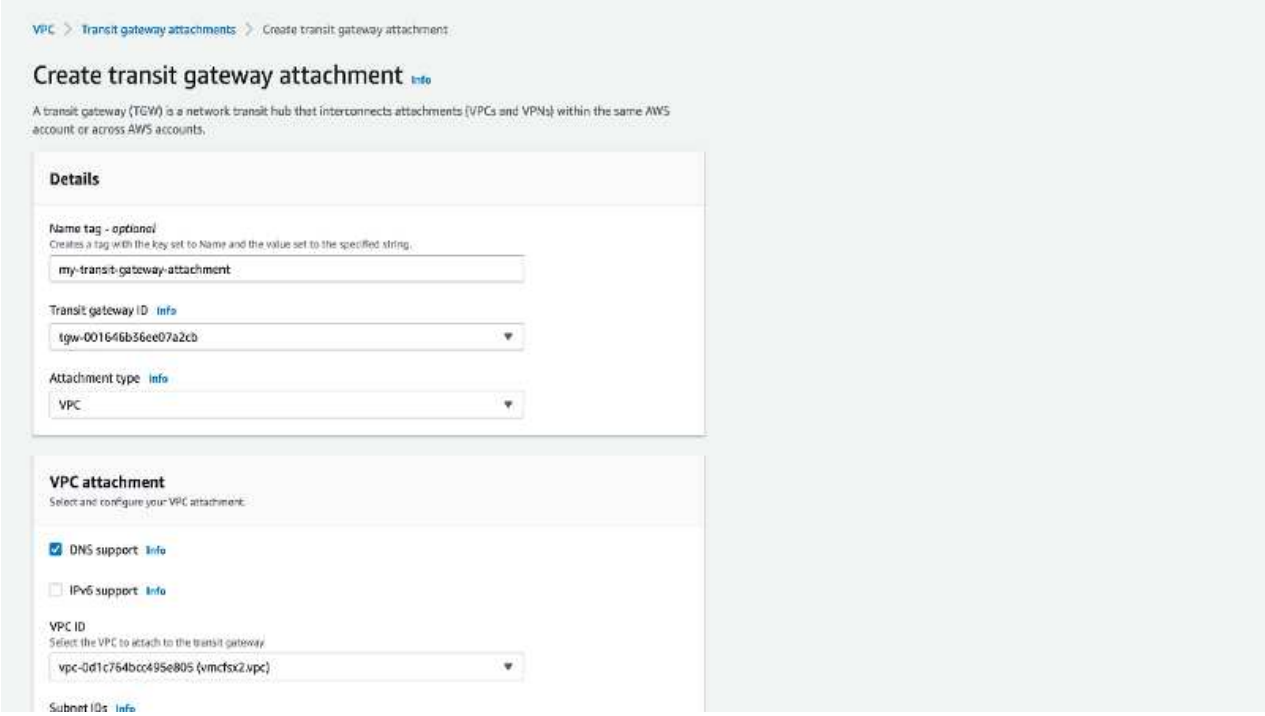


4. Nell'ambito del processo VPC esterno, viene richiesto tramite la console AWS di accedere a una nuova risorsa condivisa tramite Resource Access Manager. La risorsa condivisa è "AWS Transit Gateway" Gestito da VMware Transit Connect.

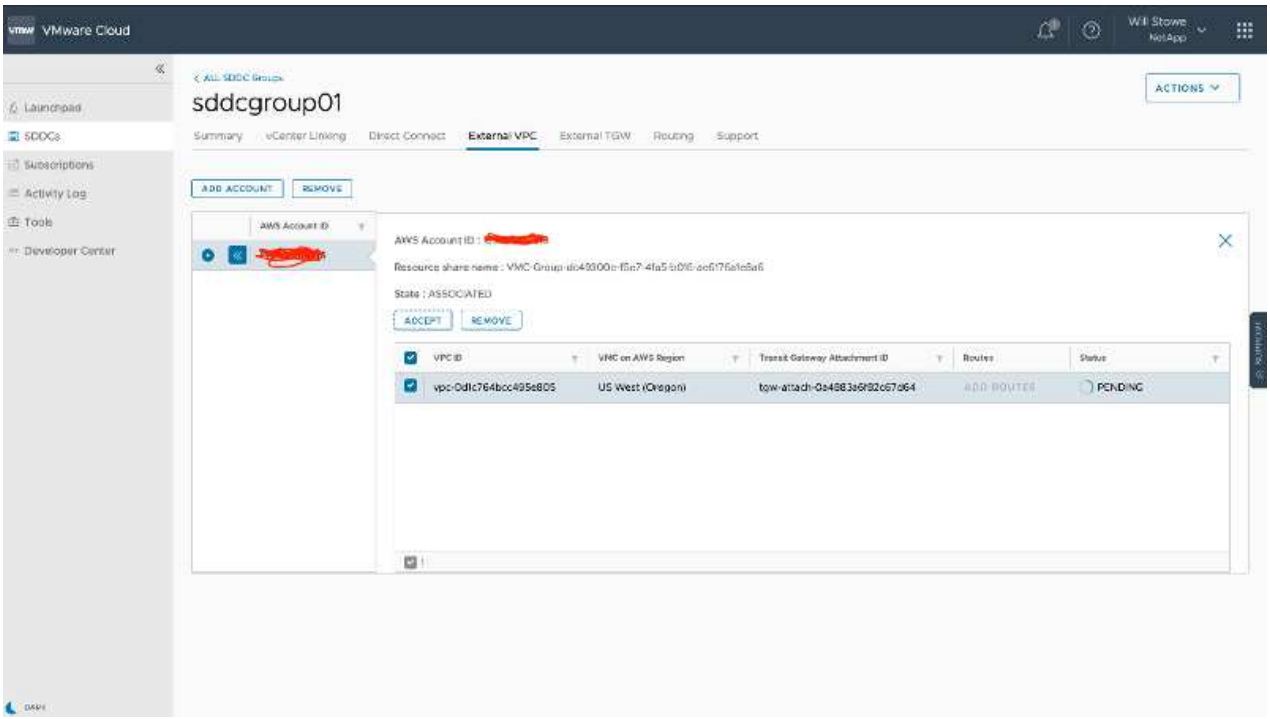




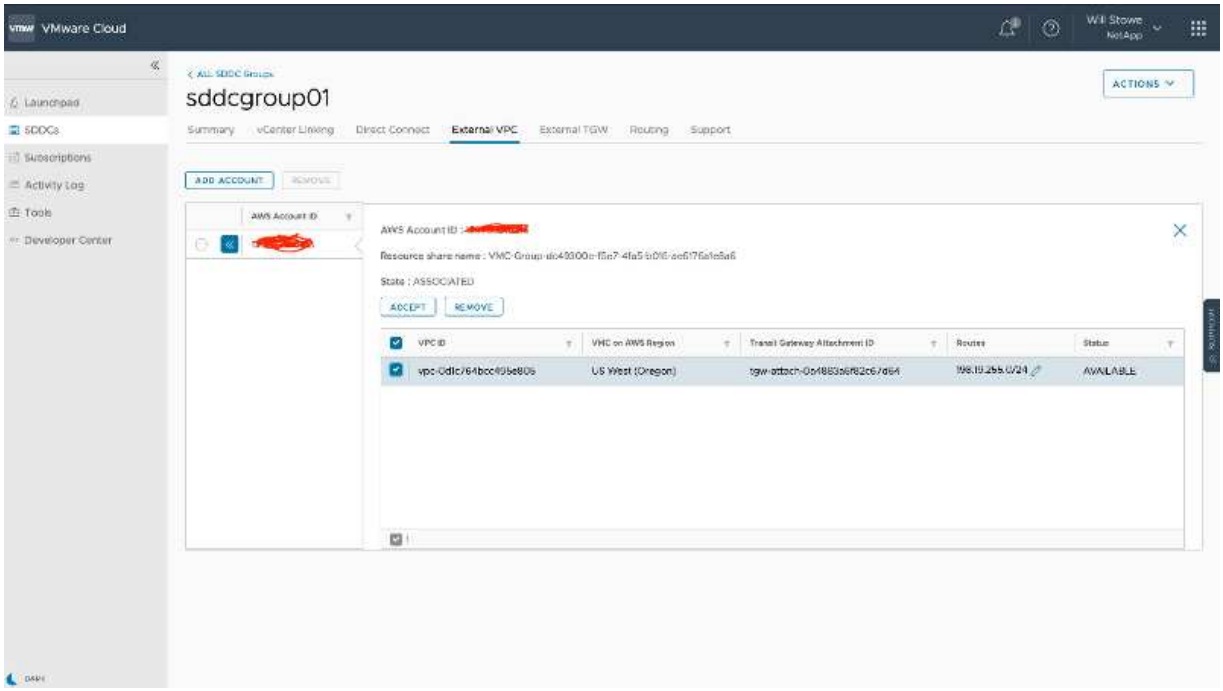
5. Creare l'allegato del gateway di transito.



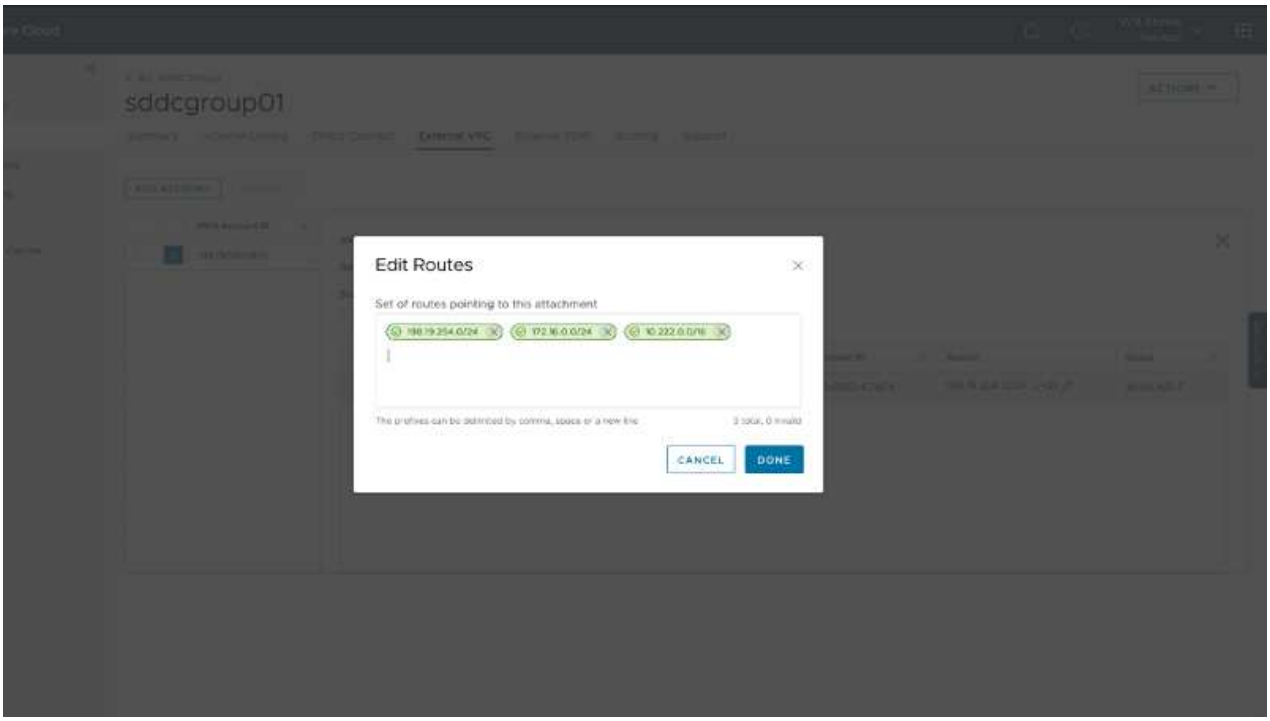
6. Sulla console VMC, accettare l'allegato VPC. Il completamento di questo processo può richiedere circa 10 minuti.



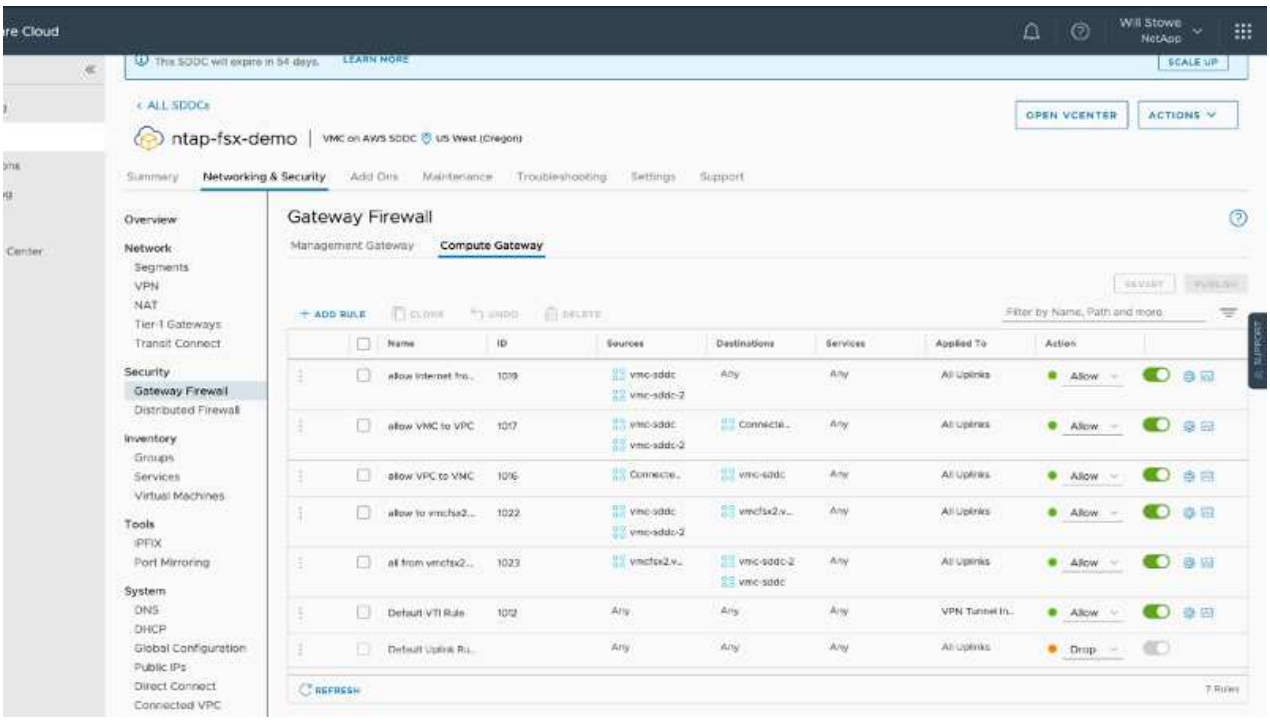
7. Nella scheda External VPC (VPC esterno), fare clic sull'icona di modifica nella colonna routes (percorsi) e aggiungere i seguenti percorsi richiesti:
   - Un percorso per l'intervallo IP mobile per Amazon FSX per NetApp ONTAP "IP mobili".
   - Route per l'intervallo IP mobile per Cloud Volumes ONTAP (se applicabile).
   - Un percorso per lo spazio di indirizzi VPC esterno appena creato.



8. Infine, consentire il traffico bidirezionale "regole del firewall" Per l'accesso a FSX/CVO. Seguire queste istruzioni "passaggi dettagliati" Per le regole firewall del gateway di calcolo per la connettività dei carichi di lavoro SDDC.



9. Una volta configurati i gruppi di firewall per il gateway di gestione e di calcolo, è possibile accedere a vCenter come segue:



Il passaggio successivo consiste nel verificare che Amazon FSX ONTAP o Cloud Volumes ONTAP sia configurato in base ai requisiti e che i volumi siano configurati per trasferire i componenti di storage da vSAN per ottimizzare l'implementazione.

Implementare e configurare l’ambiente di virtualizzazione su Azure

Come per la soluzione VMware di Azure on-premise, la pianificazione è fondamentale per un ambiente pronto per la produzione di successo per la creazione di macchine virtuali e la migrazione.

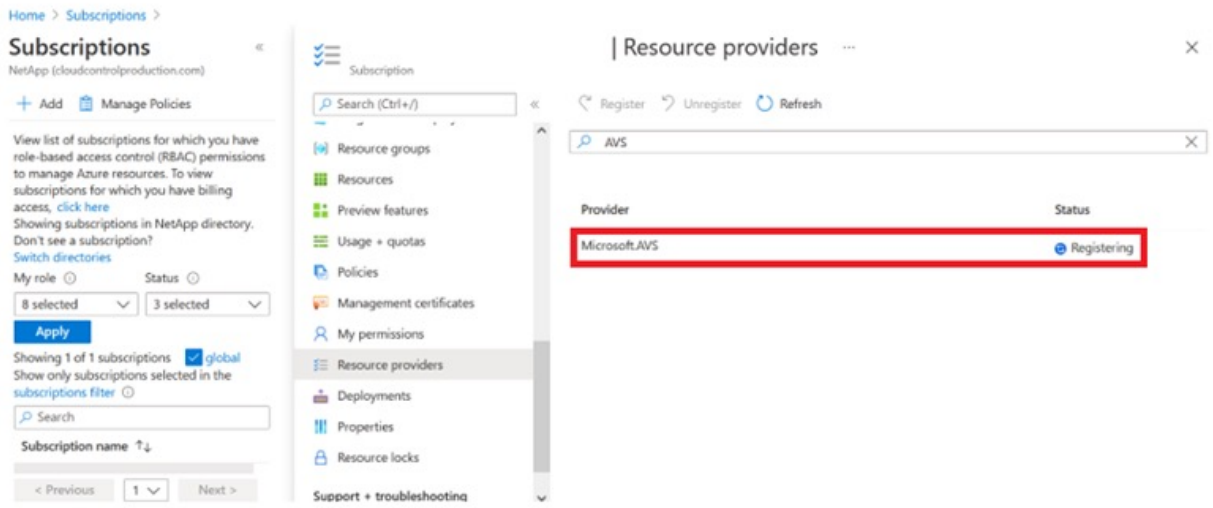
Questa sezione descrive come configurare e gestire Azure VMware Solution e utilizzarla in combinazione con le opzioni disponibili per la connessione dello storage NetApp.

Il processo di installazione può essere suddiviso nei seguenti passaggi:

Registrare il provider di risorse e creare un cloud privato

Per utilizzare Azure VMware Solution, registrare innanzitutto il provider di risorse nell'abbonamento identificato:

1. Accedi al portale Azure.
2. Nel menu del portale Azure, selezionare tutti i servizi.
3. Nella finestra di dialogo tutti i servizi, inserire l'abbonamento e selezionare Abbonamenti.
4. Per visualizzare, selezionare l'abbonamento dall'elenco.
5. Selezionare Resource Providers (Provider di risorse) e immettere Microsoft.AVS nella ricerca.
6. Se il provider di risorse non è registrato, selezionare Registra.

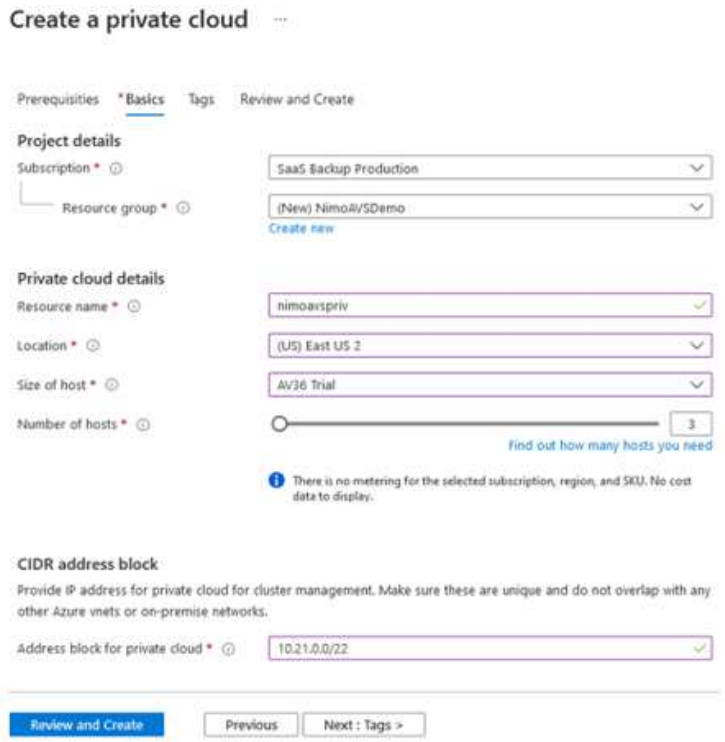


Provider	Status
Microsoft.OperationsManagement	Registered
Microsoft.Compute	Registered
Microsoft.ContainerService	Registered
Microsoft.ManagedIdentity	Registered
Microsoft.AVS	Registered
Microsoft.OperationalInsights	Registered
Microsoft.GuestConfiguration	Registered

7. Una volta registrato il provider di risorse, creare un cloud privato Azure VMware Solution utilizzando il portale Azure.
8. Accedi al portale Azure.
9. Selezionare Crea una nuova risorsa.
10. Nella casella di testo Cerca nel marketplace, immettere Azure VMware Solution e selezionarla dai risultati.
11. Nella pagina Azure VMware Solution, selezionare Create (Crea).
12. Nella scheda Basics (informazioni di base), immettere i valori nei campi e selezionare Review (esamina) + Create (Crea).

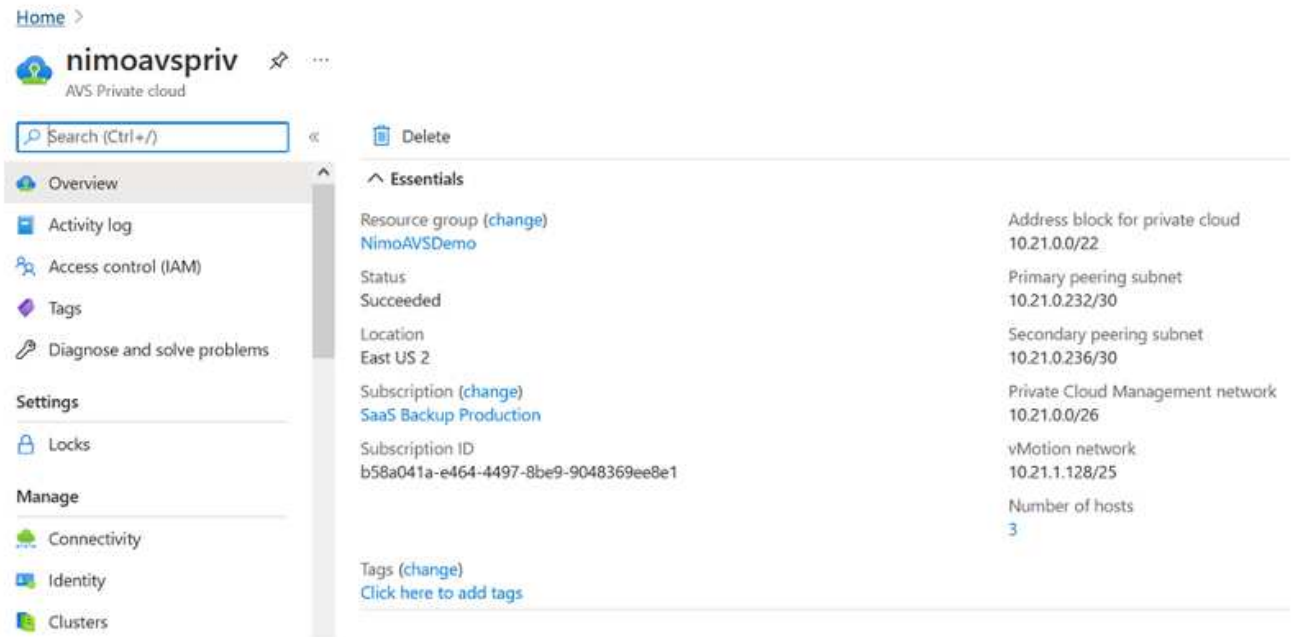
Note:

- Per un rapido avvio, raccogliere le informazioni necessarie durante la fase di pianificazione.
- Selezionare un gruppo di risorse esistente o creare un nuovo gruppo di risorse per il cloud privato. Un gruppo di risorse è un container logico in cui le risorse Azure vengono distribuite e gestite.
- Assicurarsi che l'indirizzo CIDR sia univoco e non si sovrapponga ad altre reti virtuali Azure o on-premise. Il CIDR rappresenta la rete di gestione del cloud privato e viene utilizzato per i servizi di gestione del cluster, come vCenter Server e NSX-T Manager. NetApp consiglia di utilizzare uno spazio di indirizzi /22. In questo esempio, viene utilizzato 10.21.0.0/22.



Il processo di provisioning richiede circa 4-5 ore. Una volta completato il processo, verificare che l'implementazione abbia avuto esito positivo accedendo al cloud privato dal portale Azure. Al termine dell'implementazione viene visualizzato lo stato riuscito.

Un cloud privato Azure VMware Solution richiede una rete virtuale Azure. Poiché Azure VMware Solution non supporta vCenter on-premise, sono necessari ulteriori passaggi per l'integrazione con un ambiente on-premise esistente. È inoltre necessaria la configurazione di un circuito ExpressRoute e di un gateway di rete virtuale. In attesa del completamento del provisioning del cluster, creare una nuova rete virtuale o utilizzarne una esistente per connettersi alla soluzione VMware Azure.



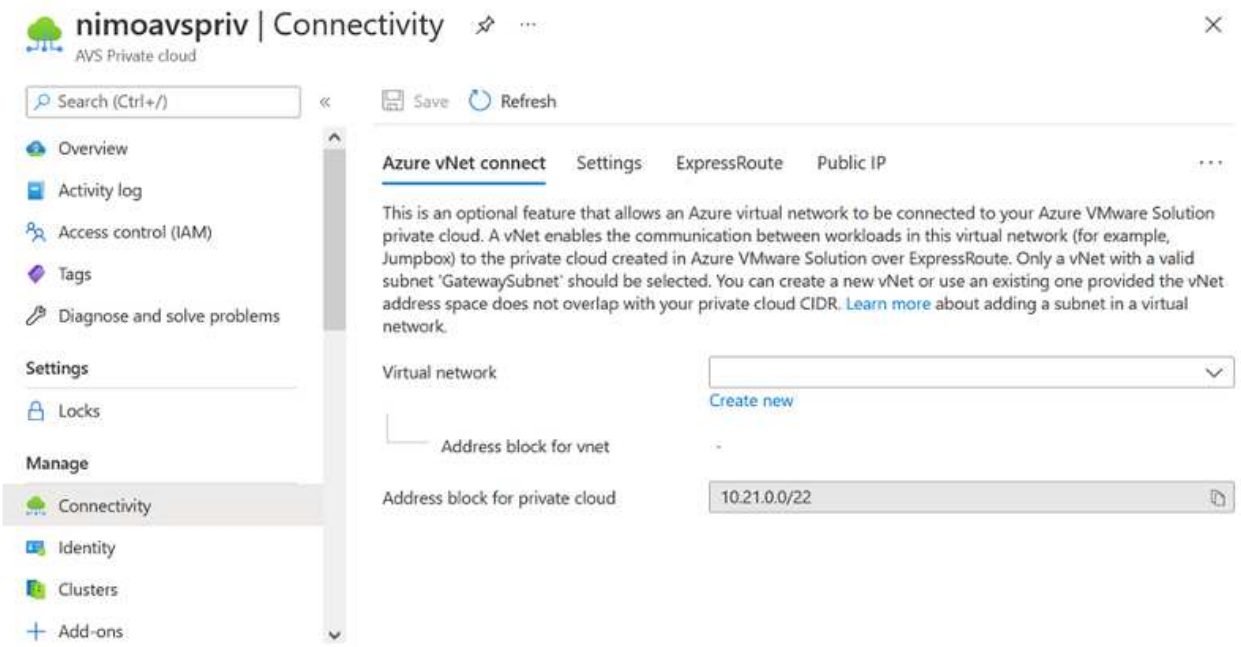
Connettersi a un gateway di rete virtuale ExpressRoute nuovo o esistente

Per creare una nuova rete virtuale Azure (VNET), selezionare la scheda Azure VNET Connect. In alternativa, è possibile crearne una manualmente dal portale Azure utilizzando la procedura guidata Create Virtual Network (Crea rete virtuale):

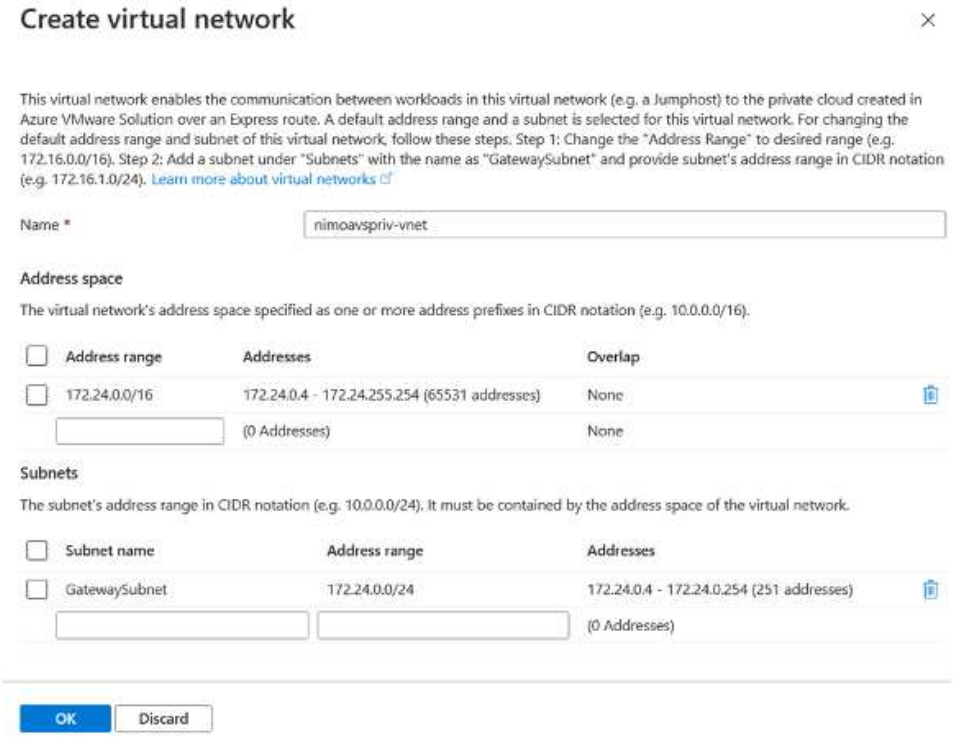
1. Accedere al cloud privato Azure VMware Solution e alla connettività sotto l'opzione Manage (Gestisci).
2. Selezionare Azure VNET Connect.
3. Per creare un nuovo VNET, selezionare l'opzione Create New (Crea nuovo).

   Questa funzione consente di connettere un VNET al cloud privato Azure VMware Solution. VNET consente la comunicazione tra i carichi di lavoro in questa rete virtuale creando automaticamente i componenti necessari (ad esempio, jump box, servizi condivisi come Azure NetApp Files e Cloud Volume ONTAP) al cloud privato creato in Azure VMware Solution su ExpressRoute.

   Nota: lo spazio degli indirizzi VNET non deve sovrapporsi al CIDR del cloud privato.



4. Fornire o aggiornare le informazioni per il nuovo VNET e selezionare OK.

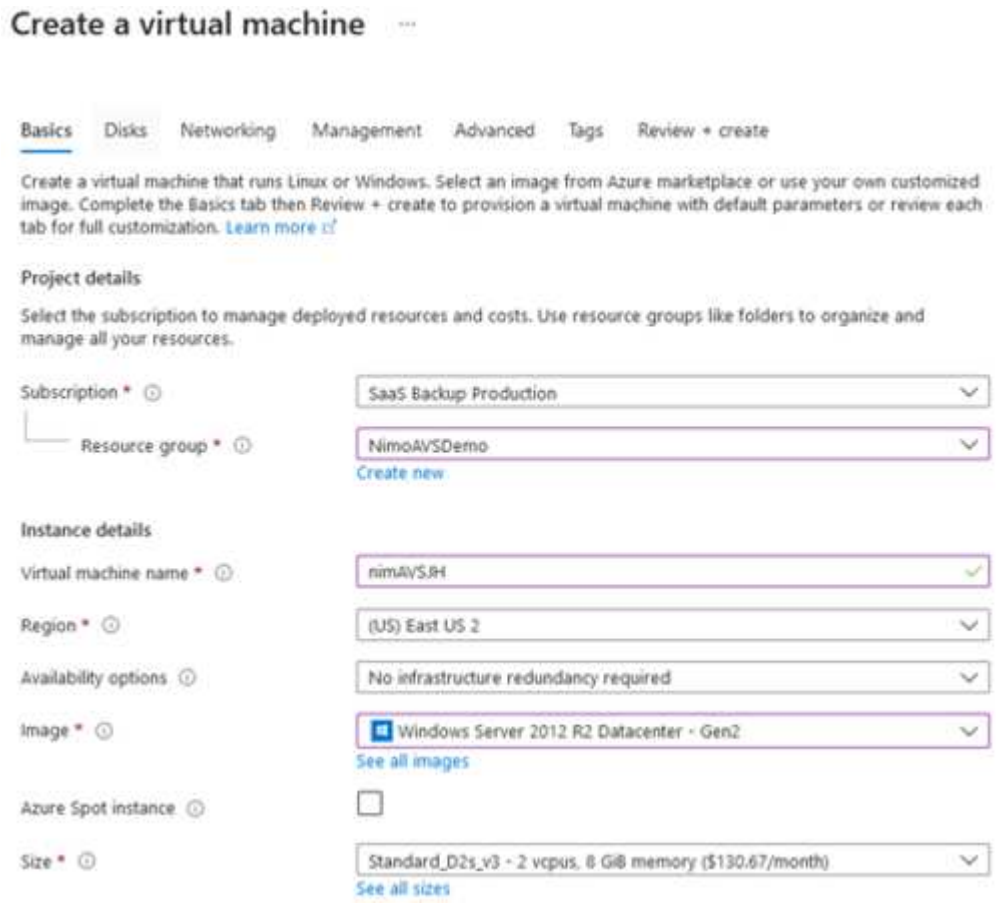


La rete VNET con l'intervallo di indirizzi e la subnet del gateway forniti viene creata nel gruppo di risorse e di abbonamento designato.

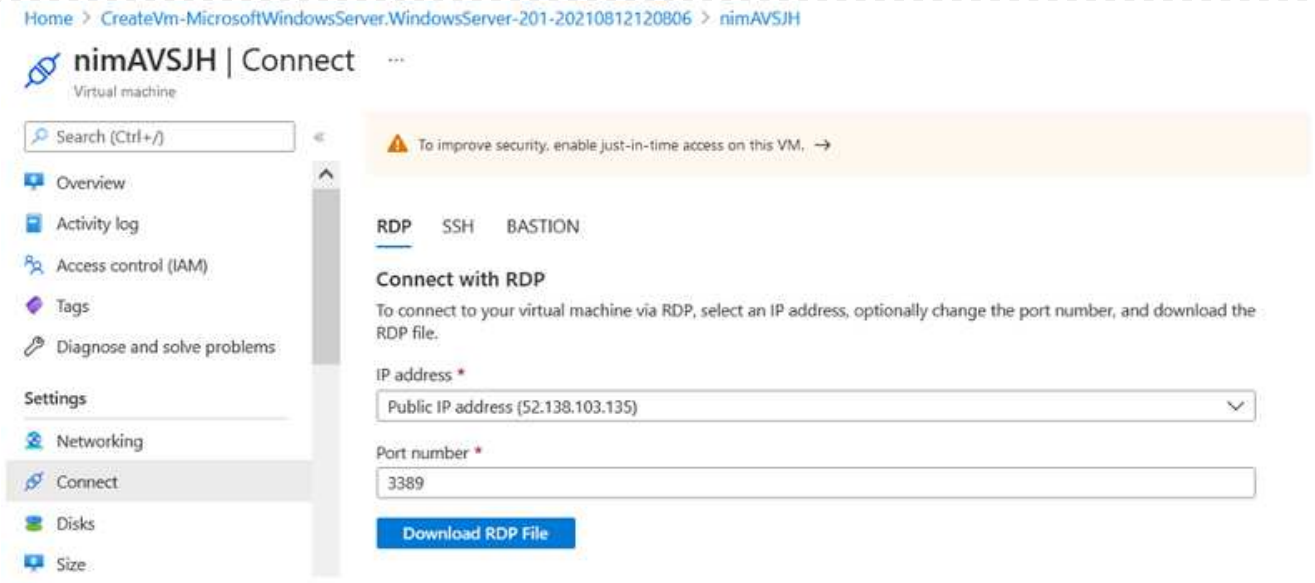
> Se si crea un VNET manualmente, creare un gateway di rete virtuale con lo SKU appropriato e ExpressRoute come tipo di gateway. Una volta completata l'implementazione, collegare la connessione ExpressRoute al gateway di rete virtuale contenente il cloud privato Azure VMware Solution utilizzando la chiave di autorizzazione. Per ulteriori informazioni, vedere "Configura il networking per il tuo cloud privato VMware in Azure".

Convalidare la connessione di rete e l'accesso al cloud privato Azure VMware Solution

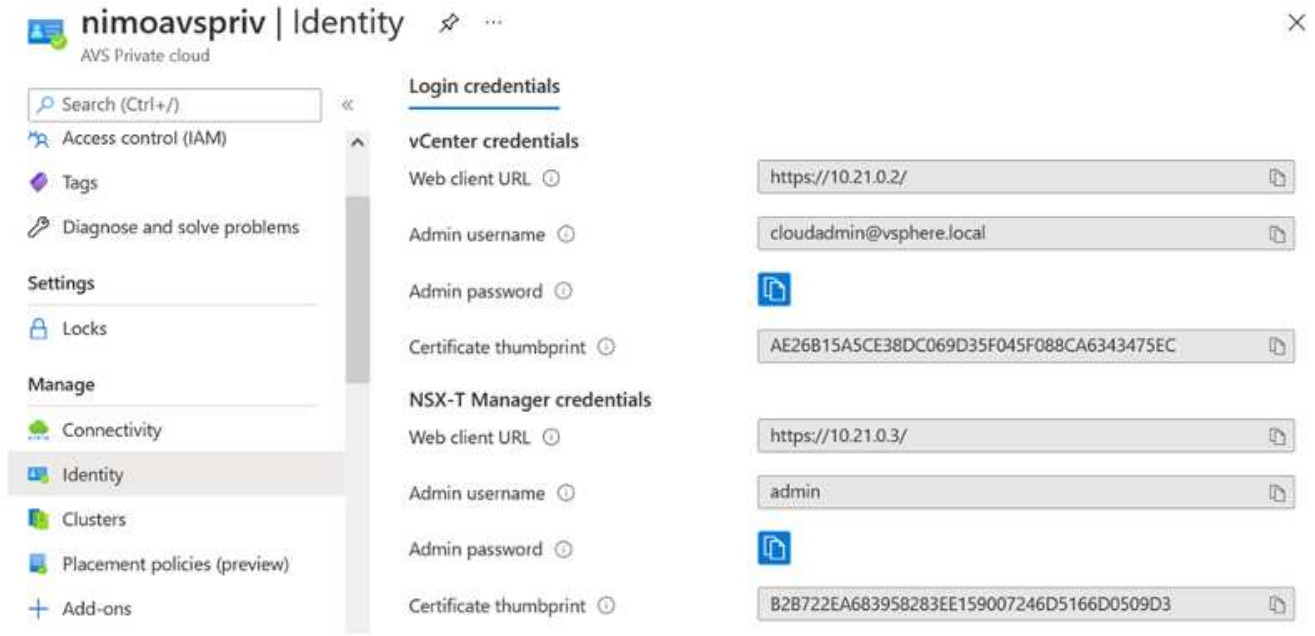
Azure VMware Solution non consente di gestire un cloud privato con VMware vCenter on-premise. Per connettersi all'istanza di Azure VMware Solution vCenter è invece necessario un host jump. Creare un host jump nel gruppo di risorse designato e accedere a Azure VMware Solution vCenter. Questo host jump dovrebbe essere una macchina virtuale Windows sulla stessa rete virtuale creata per la connettività e dovrebbe fornire l'accesso a vCenter e NSX Manager.



Una volta eseguito il provisioning della macchina virtuale, utilizzare l'opzione Connect (Connetti) per accedere a RDP.

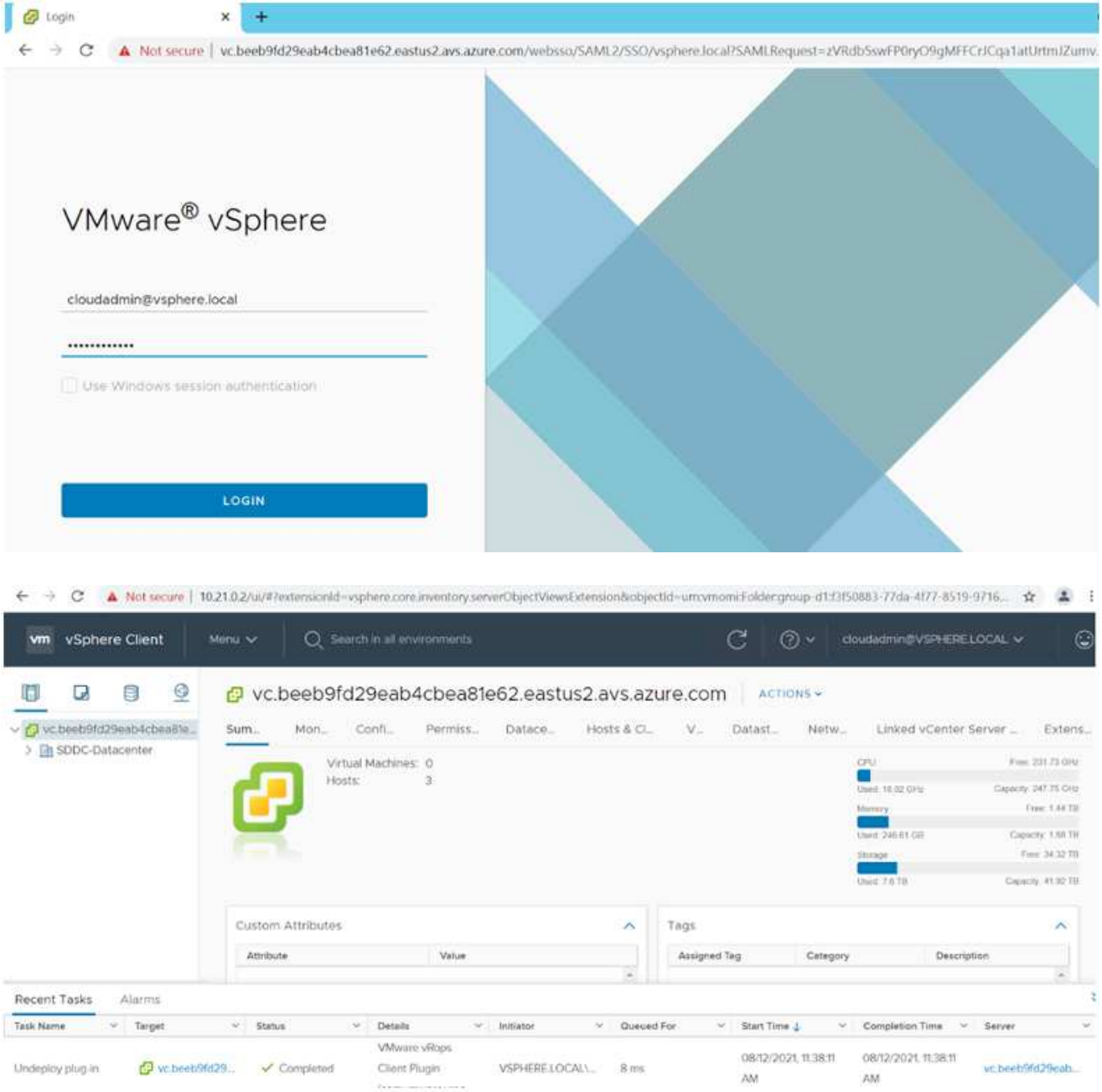


Accedere a vCenter da questa nuova macchina virtuale host jump utilizzando l'utente amministratore cloud . Per accedere alle credenziali, accedere al portale Azure e selezionare Identity (identità) (sotto l'opzione Manage (Gestisci) nel cloud privato). Da qui è possibile copiare gli URL e le credenziali utente per il cloud privato vCenter e NSX-T Manager.



Nella macchina virtuale Windows, aprire un browser e accedere all'URL del client Web vCenter e utilizzare il nome utente admin come **cloudadmin@vsphere.local** e incollare la password copiata. Allo stesso modo, è possibile accedere al gestore NSX-T anche utilizzando l'URL del client Web e utilizzare il nome utente admin e incollare la password copiata per creare nuovi segmenti o modificare i gateway tier esistenti.

Gli URL del client Web sono diversi per ogni SDDC fornito.



Azure VMware Solution SDDC è ora implementato e configurato. Sfrutta ExpressRoute Global Reach per connettere l'ambiente on-premise al cloud privato Azure VMware Solution. Per ulteriori informazioni, vedere "Ambienti on-premise peer per Azure VMware Solution".

Implementare e configurare l'ambiente di virtualizzazione su Google Cloud Platform (GCP)

Come avviene per le applicazioni on-premise, la pianificazione di Google Cloud VMware Engine (GCVE) è fondamentale per un ambiente pronto per la produzione di successo per la creazione di macchine virtuali e la migrazione.

Questa sezione descrive come configurare e gestire GCVE e utilizzarlo in combinazione con le opzioni disponibili per la connessione dello storage NetApp.

Il processo di installazione può essere suddiviso nei seguenti passaggi:

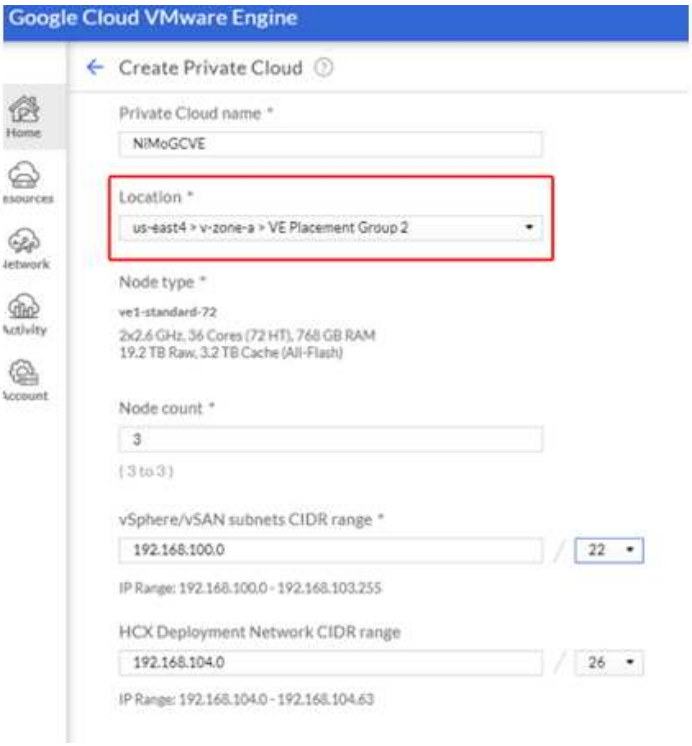
Distribuire e configurare GCVE

Per configurare un ambiente GCVE su GCP, accedere alla console GCP e al portale VMware Engine.

Fare clic sul pulsante "New Private Cloud" (nuovo cloud privato) e immettere la configurazione desiderata per il cloud privato GCVE. In "posizione", assicurarsi di implementare il cloud privato nella stessa regione/zona in cui viene implementato CVS/CVO, per garantire le migliori performance e la latenza più bassa.

Prerequisiti:

- Configurare il ruolo IAM di VMware Engine Service Admin
- "Abilitare l'accesso API VMware Engine e la quota del nodo"
- Assicurati che la gamma CIDR non si sovrapponga a nessuna delle tue subnet on-premise o cloud. L'intervallo CIDR deve essere /27 o superiore.



Nota: La creazione di un cloud privato può richiedere da 30 minuti a 2 ore.

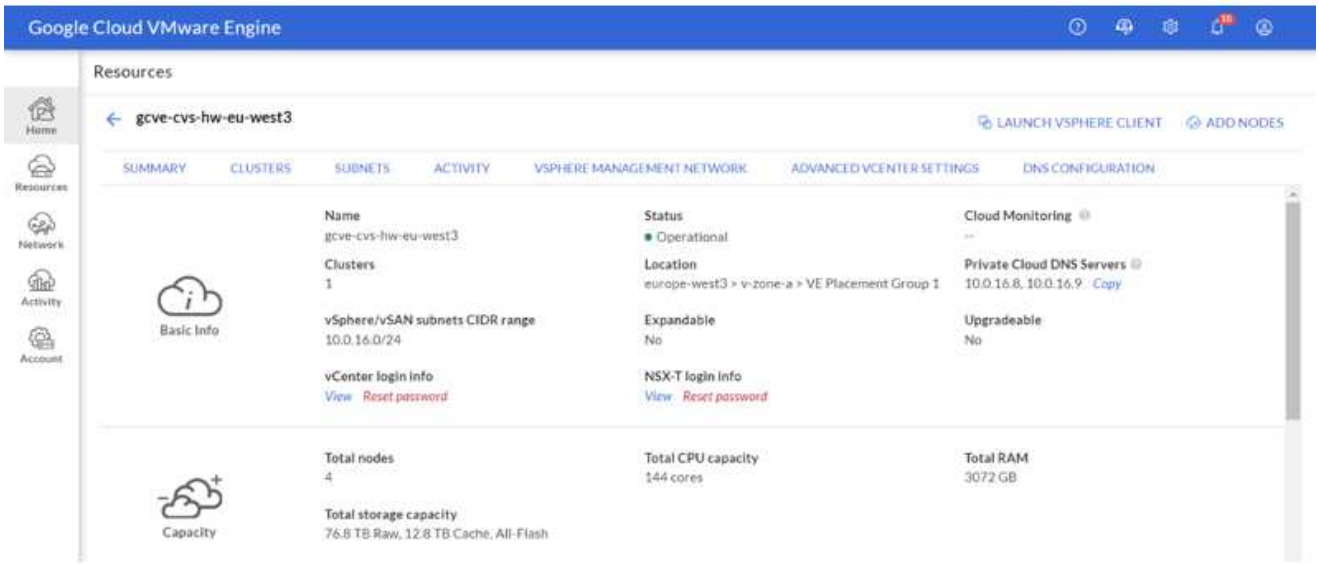
Attiva accesso privato a GCVE

Una volta eseguito il provisioning del cloud privato, configurare l'accesso privato al cloud privato per una connessione con percorso dati a bassa latenza e throughput elevato.

In questo modo, la rete VPC in cui sono in esecuzione le istanze di Cloud Volumes ONTAP sarà in grado di comunicare con il cloud privato GCVE. Per eseguire questa operazione, seguire la "Documentazione GCP". Per il servizio volume cloud, stabilire una connessione tra VMware Engine e Cloud Volumes Service eseguendo un peering una tantum tra i progetti host del tenant. Per informazioni dettagliate, seguire questa procedura "collegamento".

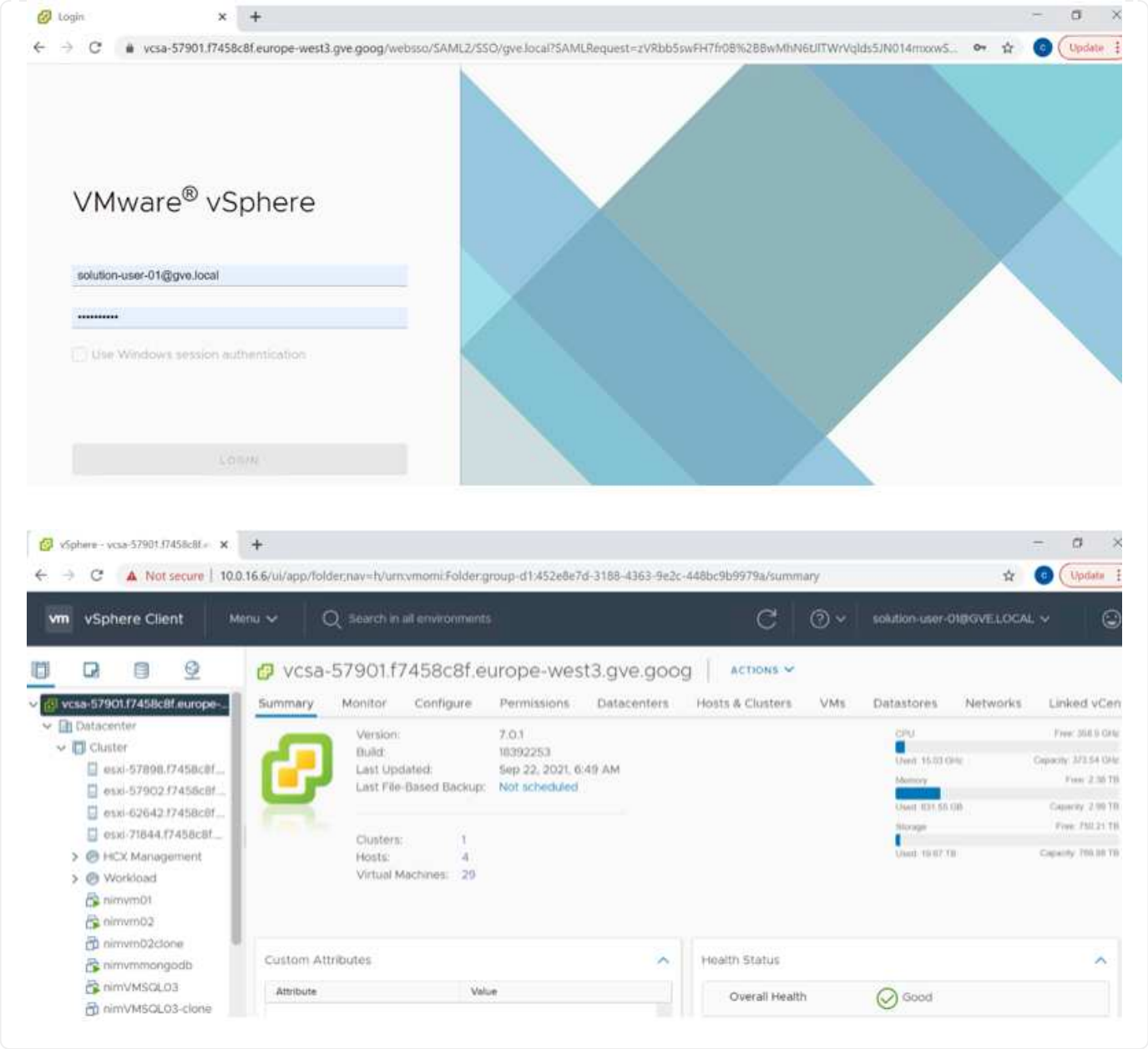
Tenant P	Service	Region	Routing Mode	Peered Project ID	Peered VPC	VPC Peering Sta...	Region Status
ke841388caa56b...	VPC Network	europe-west3	Global	cv-performance-te...	cloud-volumes-vpc	Active	Connected
jbd729510b3ebbf...	NetApp CVS	europe-west3	Global	y2b6c17202af6dc...	netapp-tenant-vpc	Active	Connected

Accedere a vcenter utilizzando CloudOwner@gve.local utente. Per accedere alle credenziali, accedere al portale VMware Engine, andare a risorse e selezionare il cloud privato appropriato. Nella sezione Basic info (informazioni di base), fare clic sul collegamento View (Visualizza) per le informazioni di accesso vCenter (vCenter Server, HCX Manager) o NSX-T (NSX Manager).



In una macchina virtuale Windows, aprire un browser e accedere all'URL del client Web vCenter E utilizzare il nome utente admin come CloudOwner@gve.local e incollare la password copiata. Allo stesso modo, è possibile accedere al gestore NSX-T anche utilizzando l'URL del client Web e utilizzare il nome utente admin e incollare la password copiata per creare nuovi segmenti o modificare i gateway tier esistenti.

Per la connessione da una rete on-premise al cloud privato VMware Engine, sfrutta la VPN cloud o l'interconnessione cloud per una connettività appropriata e assicurati che le porte richieste siano aperte. Per informazioni dettagliate, seguire questa procedura "collegamento".



Implementare il datastore supplementare del servizio volume cloud di NetApp in GCVE

Fare riferimento a. "Procedura per implementare un datastore NFS supplementare con CVS NetApp in GCVE"