



Migration von Workloads auf Azure/AVS

NetApp Solutions

NetApp
April 26, 2024

Inhalt

Migration von Workloads auf Azure/AVS	1
TR-4940: Migration von Workloads auf Azure NetApp Files Datastore mithilfe von VMware HCX -	
QuickStart Guide	1

Migration von Workloads auf Azure/AVS

TR-4940: Migration von Workloads auf Azure NetApp Files Datastore mithilfe von VMware HCX - QuickStart Guide

Autor(en): NetApp Solutions Engineering

Übersicht: Migration von Virtual Machines mit VMware HCX, Azure NetApp Files Datastores und Azure VMware Lösung

Eine der gängigsten Anwendungsfälle für die Azure VMware Lösung und den Azure NetApp Files Datastore ist die Migration von VMware Workloads. VMware HCX ist eine bevorzugte Option und bietet verschiedene Migrationsmechanismen zum Verschieben von On-Premises-Virtual Machines (VMs) und deren Daten in Azure NetApp Files Datastores.

VMware HCX ist primär eine Migrationsplattform, die entwickelt wurde, um die Migration von Applikationen, die Ausbalancierung von Workloads und sogar Business Continuity Cloud-übergreifend zu vereinfachen. Es ist im Rahmen von Azure VMware Solution Private Cloud enthalten und bietet viele Möglichkeiten zum Migrieren von Workloads und kann für Disaster-Recovery-(DR-)Vorgänge genutzt werden.

Dieses Dokument enthält eine Schritt-für-Schritt-Anleitung zur Bereitstellung von Azure NetApp Files Datastore. Anschließend werden die Komponenten von VMware HCX heruntergeladen, implementiert und konfiguriert, einschließlich aller Hauptkomponenten vor Ort und der Seite der Azure VMware Lösung, einschließlich Interconnect, Netzwerkerweiterung und WAN-Optimierung, um verschiedene VM-Migrationsmechanismen zu ermöglichen.



VMware HCX arbeitet mit jedem Datenspeichertyp zusammen, da die Migration auf VM-Ebene erfolgt. Dieses Dokument eignet sich daher für bestehende NetApp Kunden sowie für Kunden anderer Anbieter, die eine Implementierung der Azure NetApp Files Lösung mit Azure VMware als kostengünstige VMware Cloud-Implementierung planen.

Allgemeine Schritte

Diese Liste enthält grundlegende Schritte, die für die Installation und Konfiguration von HCX Cloud Manager auf der Azure Cloud-Seite und die Installation von HCX Connector vor Ort erforderlich sind:

1. Installieren Sie HCX über das Azure-Portal.
2. Laden Sie das Installationsprogramm für die HCX Connector Open Virtualization Appliance (OVA) im lokalen VMware vCenter Server herunter und implementieren Sie es.
3. HCX mit dem Lizenzschlüssel aktivieren.
4. Verbinden Sie den lokalen VMware HCX Connector mit der Azure VMware-Lösung HCX Cloud Manager.
5. Sie konfigurieren das Netzwerkprofil, das Computing-Profil und das Service-Mesh.
6. (Optional) Sie können eine Netzwerkerweiterung vornehmen, um bei Migrationen eine erneute IP-Adresse zu vermeiden.
7. Validieren des Appliance-Status und Sicherstellen der Möglichkeit der Migration
8. Migration der VM-Workloads

Voraussetzungen

Bevor Sie beginnen, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind. Weitere Informationen finden Sie unter "[Verlinken](#)". Nachdem die Voraussetzungen, einschließlich der Konnektivität, vorhanden sind, konfigurieren und aktivieren Sie HCX, indem Sie den Lizenzschlüssel aus dem Azure VMware-Lösungsportal generieren. Nach dem Herunterladen des OVA-Installationsprogramms gehen Sie wie unten beschrieben mit der Installation vor.

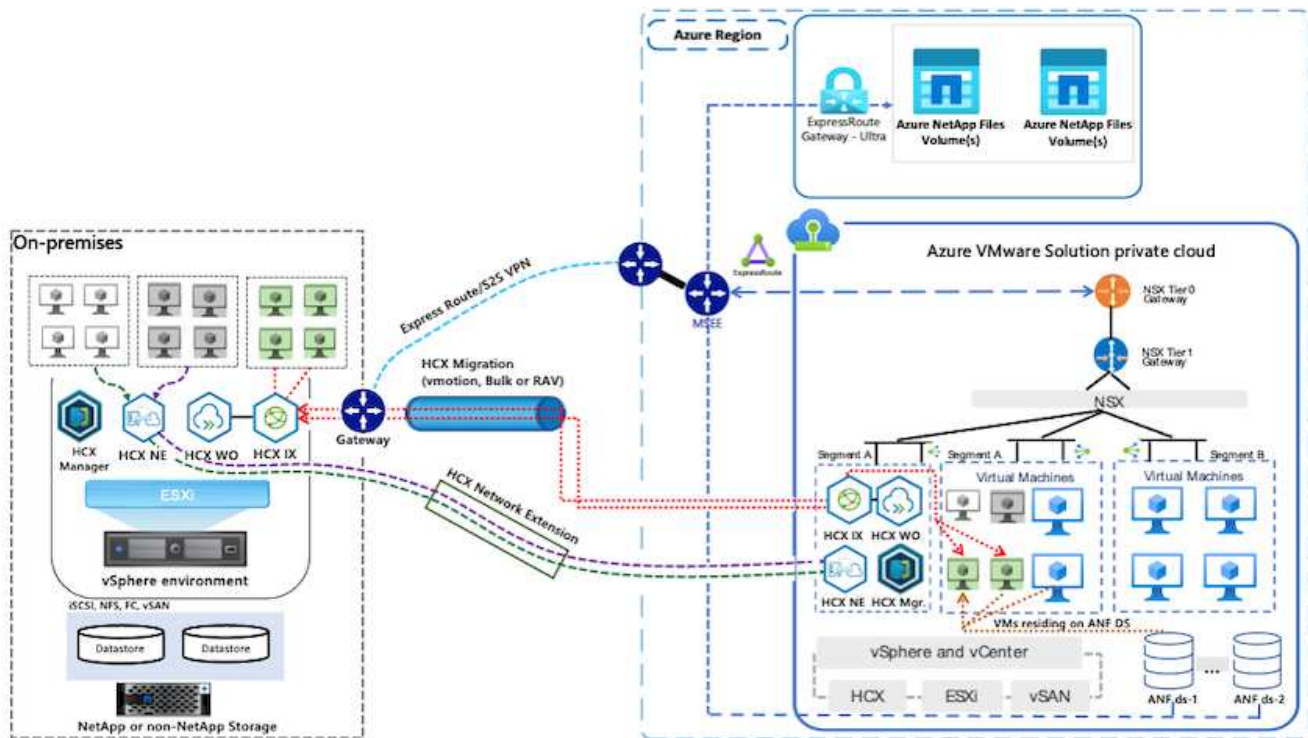


HCX Advanced ist die Standardoption und die VMware HCX Enterprise Edition ist auch über ein Support-Ticket erhältlich und wird ohne zusätzliche Kosten unterstützt.

- Nutzen Sie ein bereits softwaredefiniertes Datacenter (SDDC) einer Azure VMware Lösung oder erstellen Sie mithilfe dieses Modells eine Private Cloud "[Link von NetApp](#)" Oder hier "[Microsoft-Link](#)".
- Die Migration von VMs und zugehörigen Daten vom lokalen Datacenter mit VMware vSphere erfordert Netzwerkkonnektivität vom Datacenter zur SDDC-Umgebung. Vor der Migration von Workloads "[Richten Sie eine Site-to-Site-VPN- oder Express-Route-globale REACH-Verbindung ein](#)" Zwischen der lokalen Umgebung und der jeweiligen Private Cloud verschieben.
- Der Netzwerkpfad von der lokalen VMware vCenter Server Umgebung zur Private Cloud der Azure VMware Lösung muss die Migration von VMs mithilfe von vMotion unterstützen.
- Stellen Sie sicher, dass die erforderlichen "[Firewall-Regeln und -Ports](#)" Sind für vMotion Traffic zwischen dem lokalen vCenter Server und SDDC vCenter zulässig. In der Private Cloud ist das Routing im vMotion Netzwerk standardmäßig konfiguriert.
- Das Azure NetApp Files NFS-Volume sollte als Datastore in der Azure VMware-Lösung eingebunden werden. Befolgen Sie die in diesem Schritt beschriebenen Schritte "[Verlinken](#)" Um Azure NetApp Files-Datenspeicher an Azure VMware Solutions Hosts anzuschließen.

Übergeordnete Architektur

Die für diese Validierung verwendete Lab-Umgebung wurde zu Testzwecken über ein Site-to-Site-VPN verbunden, das On-Premises-Konnektivität mit der Azure VMware Lösung ermöglicht.



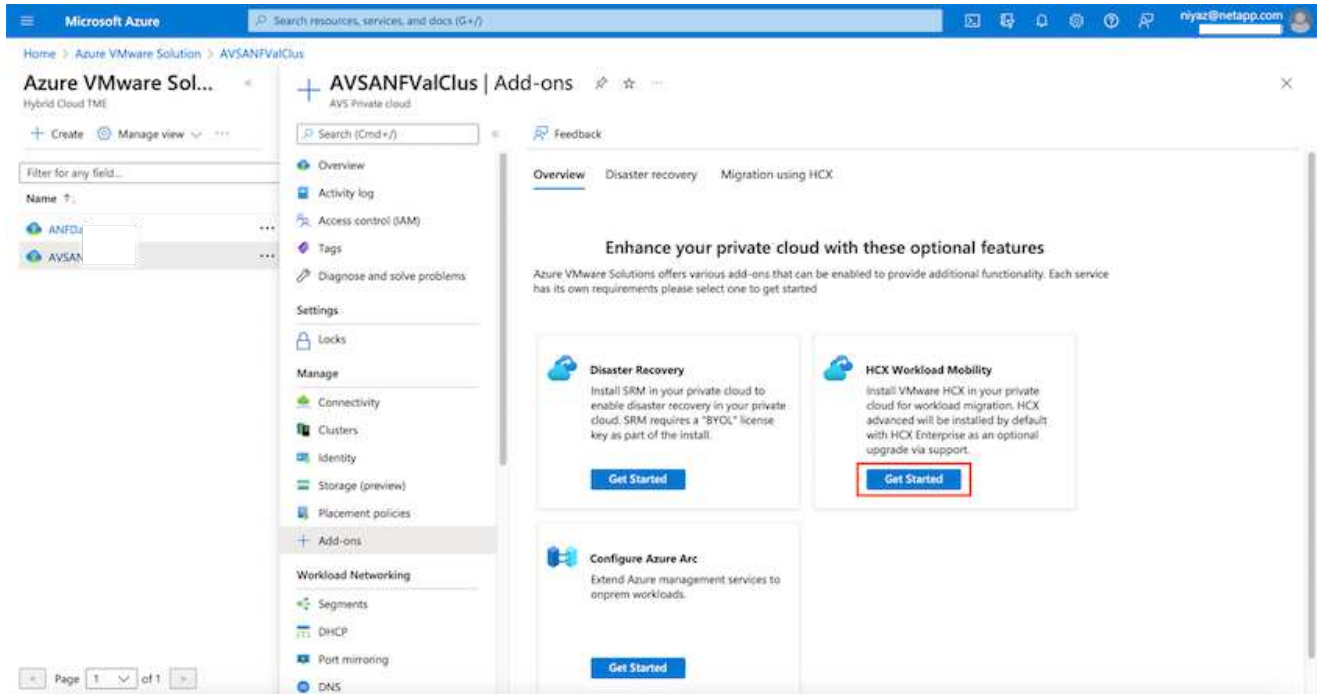
Lösungsimplementierung

Führen Sie die folgenden Schritte aus, um die Implementierung dieser Lösung abzuschließen:

Schritt 1: Installieren Sie HCX über Azure Portal mit der Option Add-ons

Gehen Sie wie folgt vor, um die Installation durchzuführen:

1. Melden Sie sich im Azure-Portal an und greifen Sie auf die Private Cloud der Azure VMware Lösung zu.
2. Wählen Sie die entsprechende private Cloud aus, und greifen Sie auf Add-ons zu. Dazu navigieren Sie zu **Verwalten > Add-ons**.
3. Klicken Sie im Bereich HCX Workload Mobility auf **Get Started**.



1. Wählen Sie die Option **Ich stimme den Allgemeinen Geschäftsbedingungen** zu und klicken Sie auf **Aktivieren und Bereitstellen**.



Die Standardbereitstellung ist HCX Advanced. Öffnen Sie eine Support-Anfrage, um die Enterprise Edition zu aktivieren.



Die Implementierung dauert etwa 25 bis 30 Minuten.

Microsoft Azure

Search resources, services, and docs (G+/f)

Home > Azure VMware Solution > AVSANFValClus

Azure VMware Sol...

Hybrid Cloud TME

+ Create Manage view ...

Filter for any field...

Name ↑

- ANFD
- AVSA

AVSANFValClus | Add-ons

Search (Ctrl+F)

Feedback

Overview Disaster recovery **Migration using HCX**

HCX is an application mobility platform that is designed for simplifying application migration, workload rebalancing, and business continuity across data centers and clouds. [Learn more.](#)

☒ I agree with terms and conditions.
By selecting above, you hereby acknowledge that HCX is not FedRamp compliant at this time and to be used at own risk.

HCX plan ⓘ HCX Advanced

Enable and deploy

Settings

- Locks

Manage

- Connectivity
- Clusters
- Identity
- Storage (preview)
- Placement policies

+ Add-ons

Workload Networking

- Segments
- DHCP
- Port mirroring
- DNS

Page 1 of 1

Schritt 2: Stellen Sie das Installationsprogramm OVA im lokalen vCenter Server bereit

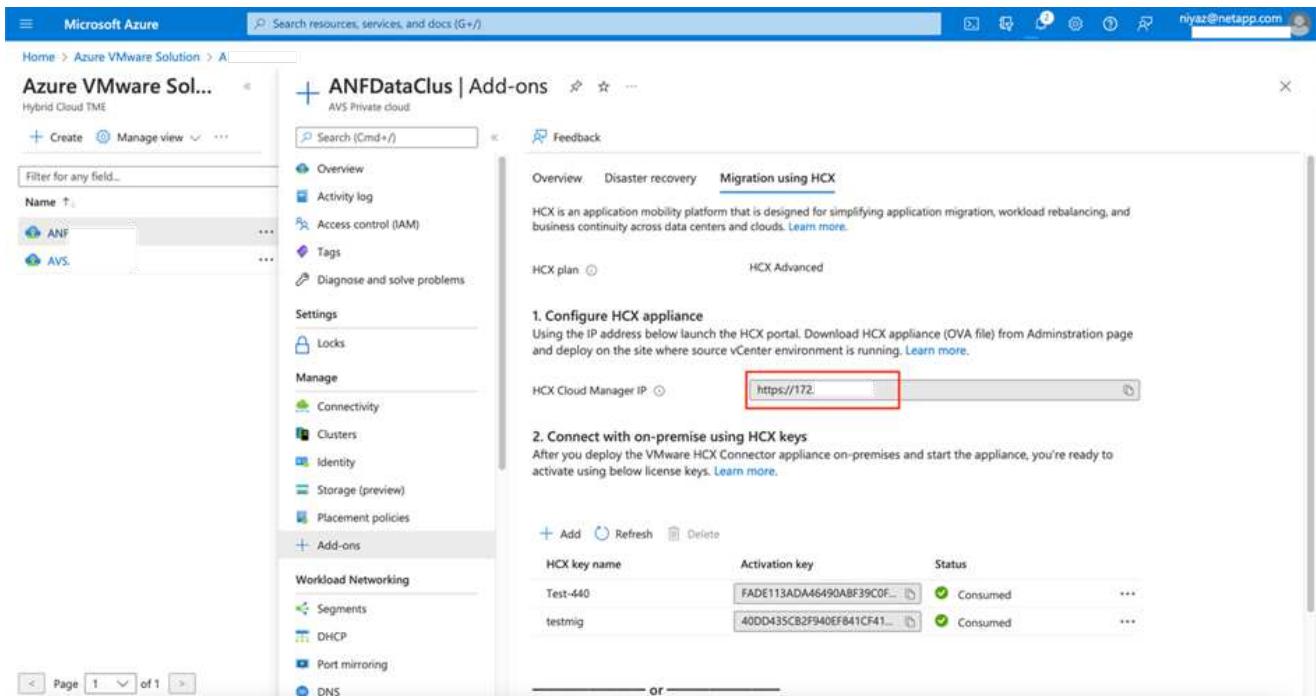
Damit der On-Premises Connector eine Verbindung zum HCX Manager in Azure VMware herstellen kann, müssen in der On-Premises-Umgebung die entsprechenden Firewall-Ports geöffnet sein.

So laden Sie den HCX Connector auf dem lokalen vCenter Server herunter und installieren ihn:

1. Wählen Sie im Azure-Portal die Azure-VMware-Lösung aus, wählen Sie die Private Cloud aus, und wählen Sie **Verwalten > Add-ons > Migration** mit HCX aus. Kopieren Sie das HCX-Cloud-Manager-Portal, um die OVA-Datei herunterzuladen.



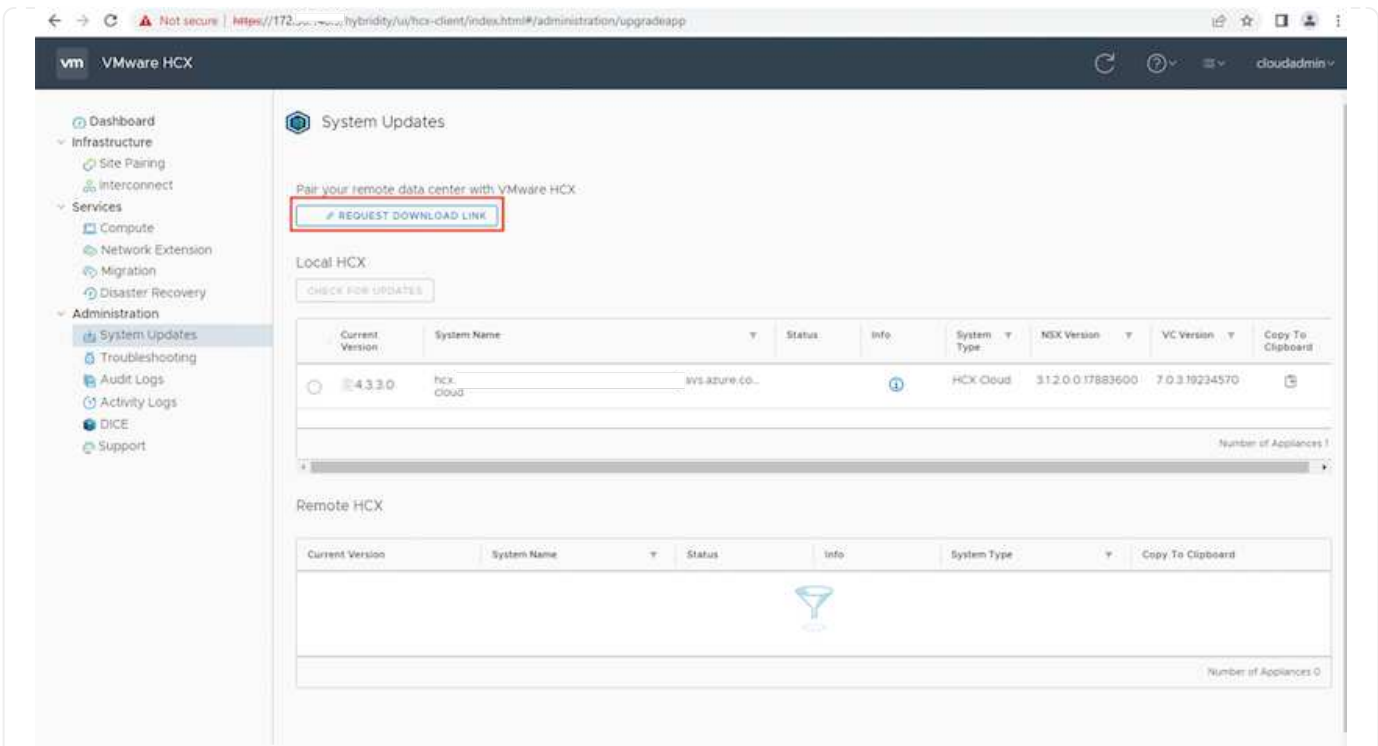
Verwenden Sie die standardmäßigen CloudAdmin-Benutzeranmeldeinformationen für den Zugriff auf das HCX-Portal.



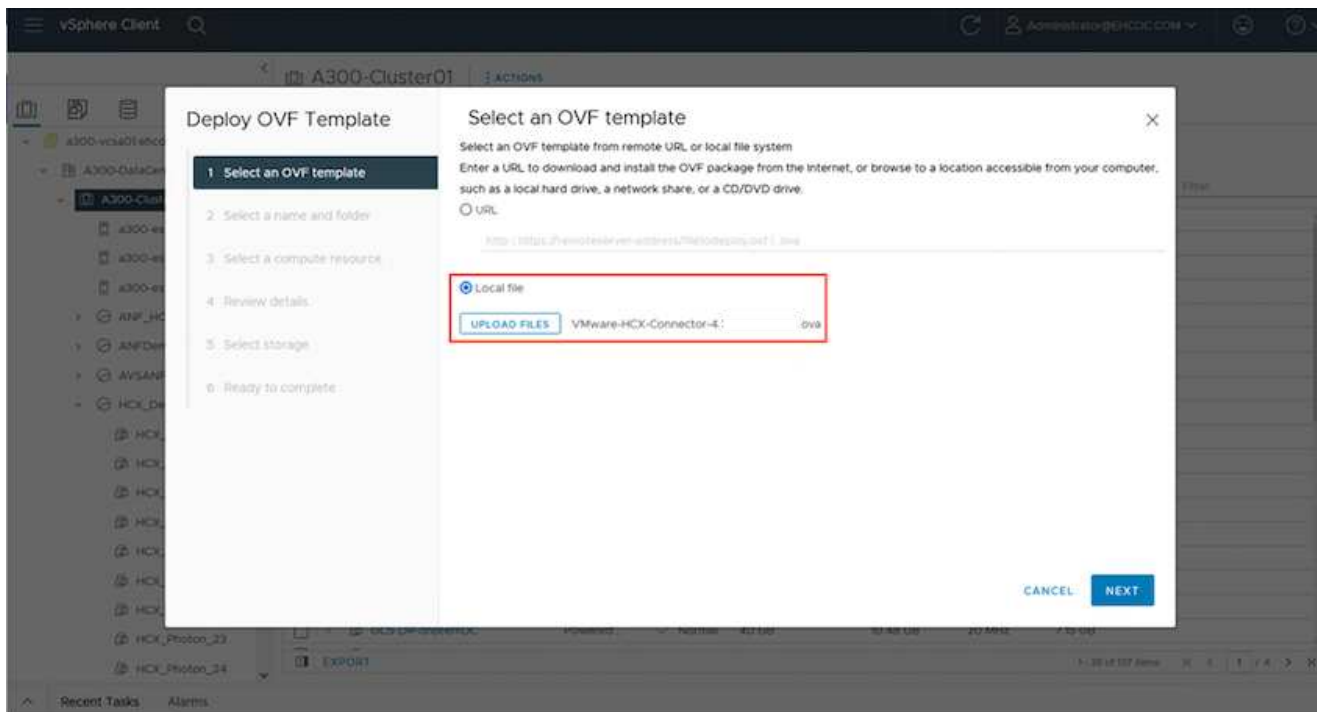
1. Nachdem Sie über den Jumphost auf das HCX-Portal mit cloudadmin@vsphere.local zugegriffen haben, navigieren Sie zu **Administration > Systemaktualisierungen** und klicken Sie auf **Download anfordern Link**.



Laden Sie entweder den Link zur OVA herunter oder kopieren Sie ihn in einen Browser, um den Download-Prozess der OVA-Datei von VMware HCX Connector zu starten, um sie auf dem lokalen vCenter Server bereitzustellen.



1. Nachdem die OVA heruntergeladen wurde, stellen Sie sie in der lokalen VMware vSphere Umgebung mithilfe der Option **Deploy OVF Template** bereit.



1. Geben Sie alle erforderlichen Informationen für die OVA-Bereitstellung ein, klicken Sie auf **Weiter** und klicken Sie dann auf **Fertig stellen**, um die OVA des VMware HCX-Connectors bereitzustellen.



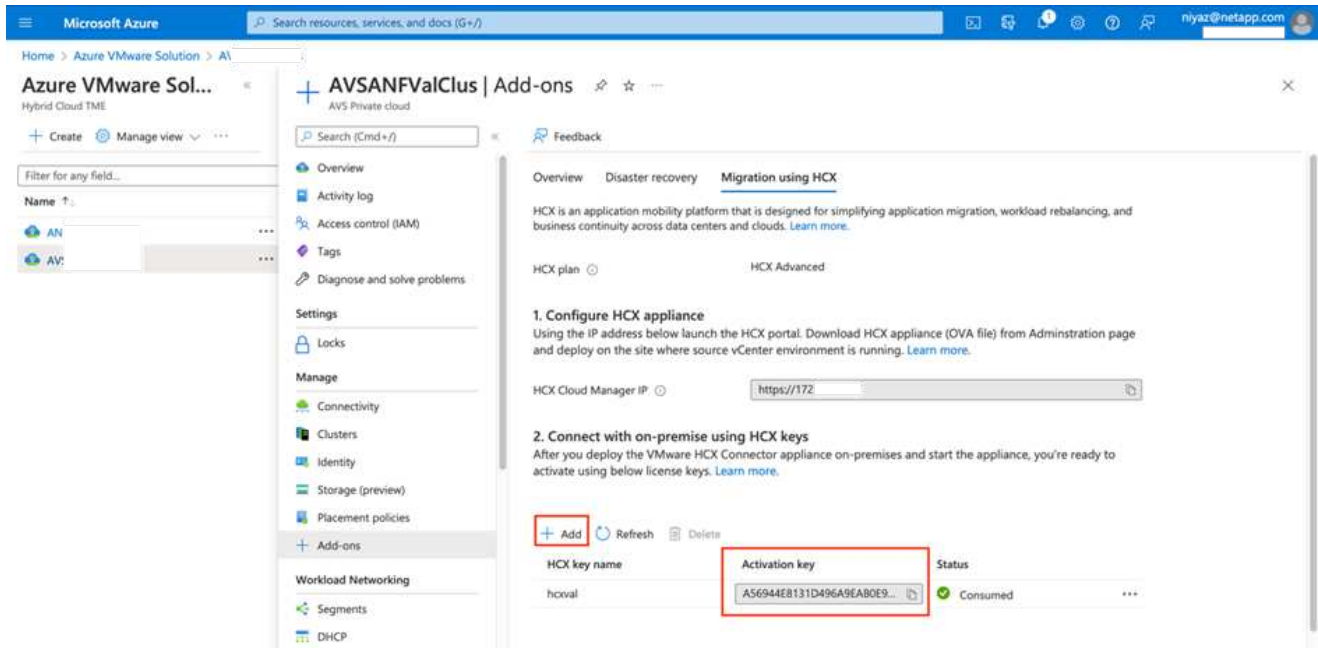
Schalten Sie die virtuelle Appliance manuell ein.

Eine Schritt-für-Schritt-Anleitung finden Sie im "[VMware HCX-Benutzerhandbuch](#)".

Schritt 3: HCX Connector mit dem Lizenzschlüssel aktivieren

Nachdem Sie den VMware HCX Connector OVA vor Ort bereitgestellt und das Gerät gestartet haben, führen Sie die folgenden Schritte aus, um den HCX Connector zu aktivieren. Generieren Sie den Lizenzschlüssel aus dem Azure VMware Lösungs-Portal und aktivieren Sie ihn in VMware HCX Manager.

1. Wählen Sie im Azure-Portal die Azure VMware-Lösung, wählen Sie die Private Cloud aus und wählen Sie **Verwalten > Add-ons > Migration Using HCX** aus.
2. Klicken Sie unter **Verbindung mit On-Premise mit HCX-Tasten** auf **Hinzufügen** und kopieren Sie den Aktivierungsschlüssel.



Für jeden bereitgestellten HCX-Connector vor Ort ist ein separater Schlüssel erforderlich.

1. Melden Sie sich beim lokalen VMware HCX Manager unter an "<https://hcxmanagerIP:9443>" Administratordaten werden verwendet.



Verwenden Sie das während der OVA-Bereitstellung definierte Passwort.

1. Geben Sie in der Lizenzierung den aus Schritt 3 kopierten Schlüssel ein und klicken Sie auf **Aktivieren**.



Der HCX-Connector sollte über einen Internetzugang verfügen.

1. Geben Sie unter **Datacenter Location** den nächstgelegenen Standort für die Installation des VMware HCX Managers vor Ort an. Klicken Sie Auf **Weiter**.
2. Aktualisieren Sie unter **Systemname** den Namen und klicken Sie auf **Weiter**.
3. Klicken Sie Auf **Ja, Weiter**.
4. Geben Sie unter **Connect Your vCenter** den vollständig qualifizierten Domännennamen (FQDN) oder die IP-Adresse des vCenter Servers und die entsprechenden Anmeldeinformationen an und klicken Sie auf **Continue**.



Verwenden Sie den FQDN, um Verbindungsprobleme später zu vermeiden.

1. Geben Sie unter * SSO/PSC konfigurieren* den FQDN oder die IP-Adresse des Plattform-Services-Controllers an und klicken Sie auf **Weiter**.



Geben Sie den VMware vCenter Server FQDN oder die IP-Adresse ein.

1. Überprüfen Sie, ob die eingegebenen Informationen korrekt sind, und klicken Sie auf **Neustart**.
2. Nach dem Neustart der Dienste wird vCenter Server auf der angezeigten Seite grün angezeigt. Sowohl vCenter Server als auch SSO müssen über die entsprechenden Konfigurationsparameter verfügen, die mit der vorherigen Seite übereinstimmen sollten.



Dieser Vorgang dauert etwa 10 bis 20 Minuten, und das Plug-in wird dem vCenter Server hinzugefügt.

The screenshot displays the VMware HCX Manager dashboard. The top navigation bar includes 'vm HCX Manager', 'Dashboard', 'Appliance Summary', 'Configuration', and 'Administration'. The main content area is titled 'VMware-HCX-440' and shows the following details:

- FQDN:** VMware-HCX-440.ehcdc.com
- IP Address:** 172.2
- Version:** 4.4.1.0
- Uptime:** 20 days, 21 hours, 9 minutes
- Current Time:** Tuesday, 13 September 2022 07:44:11 PM UTC

On the right, resource usage is shown with progress bars:

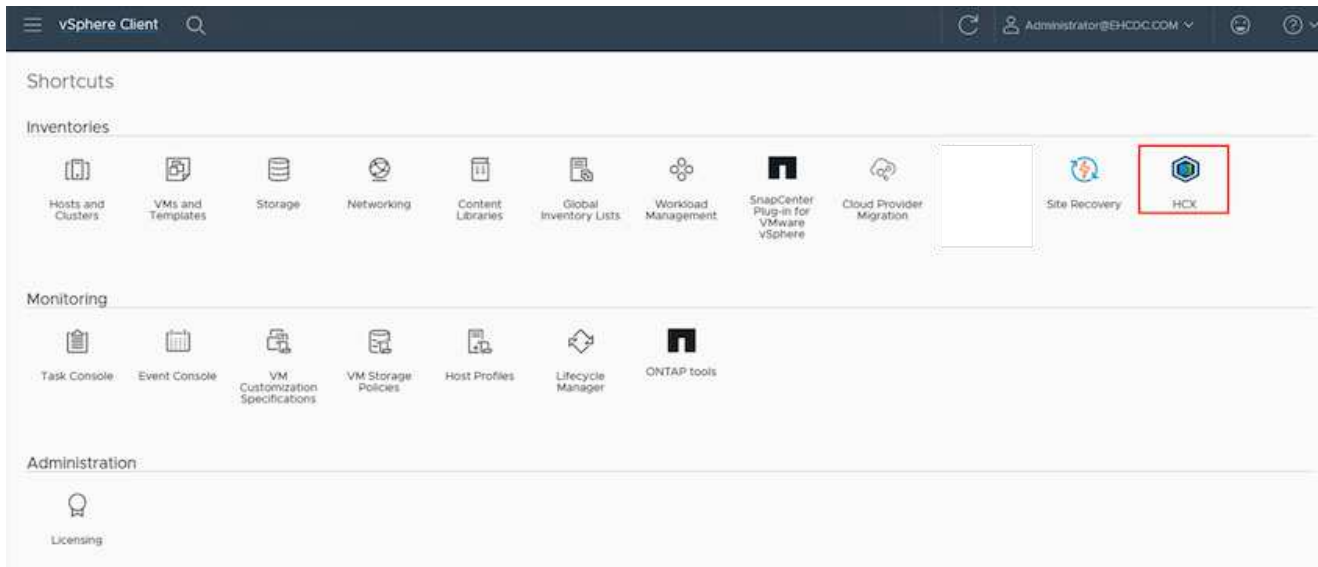
- CPU:** Used 1407 MHz, Free 688 MHz, Capacity 2095 MHz, 67%.
- Memory:** Used 9691 MB, Free 2316 MB, Capacity 12008 MB, 81%.
- Storage:** Used 29G, Free 98G, Capacity 127G, 23%.

Below these are three configuration sections: NSX, vCenter, and SSO. Each section has a 'MANAGE' button. The vCenter and SSO sections show the FQDN 'https://a300-vcso01.ehcdc.com' and a green status indicator, which is highlighted by a red rectangle in the image.

Schritt 4: Verbinden Sie den lokalen VMware HCX Connector mit der Azure VMware-Lösung HCX Cloud Manager

Nachdem HCX Connector sowohl in der lokalen als auch in der Azure VMware-Lösung installiert wurde, konfigurieren Sie die private Cloud der lokalen VMware HCX Connector for Azure VMware-Lösung, indem Sie die Paarung hinzufügen. Gehen Sie wie folgt vor, um die Standortpaarung zu konfigurieren:

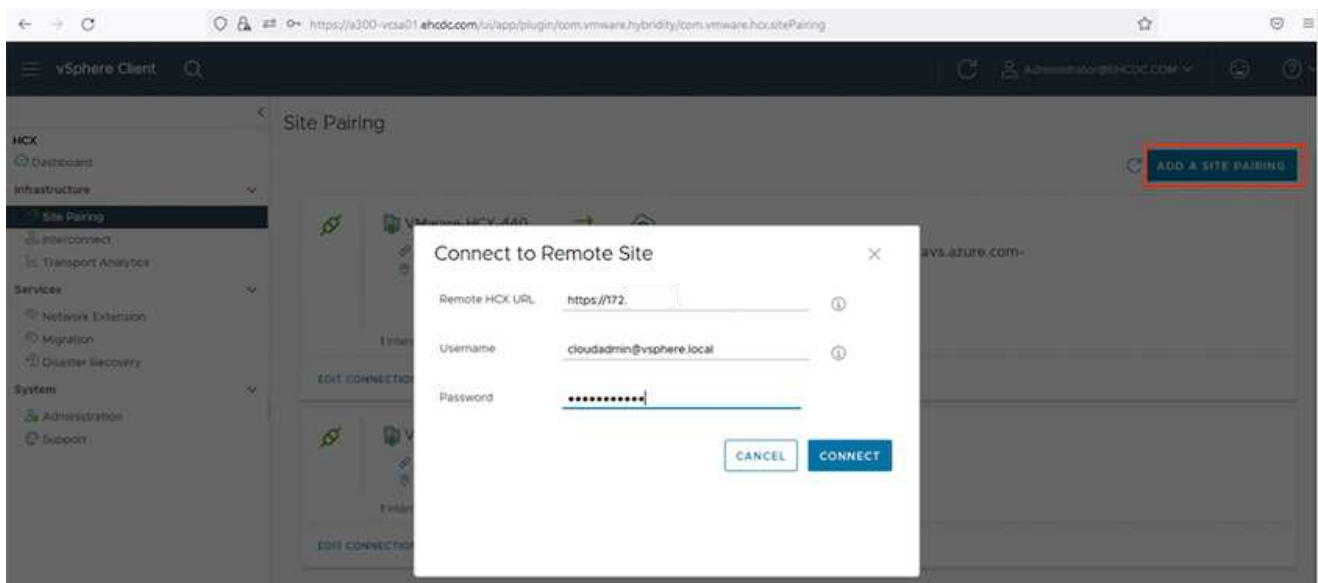
1. Um ein Standortpaar zwischen der lokalen vCenter Umgebung und der Azure VMware Solution SDDC zu erstellen, melden Sie sich beim lokalen vCenter Server an und greifen Sie auf das neue HCX vSphere Web Client Plug-in zu.



1. Klicken Sie unter Infrastruktur auf **Site Pairing hinzufügen**.



Geben Sie die URL oder IP-Adresse der Azure VMware Solution HCX Cloud Manager und die Anmeldedaten für CloudAdmin-Rolle für den Zugriff auf die private Cloud ein.

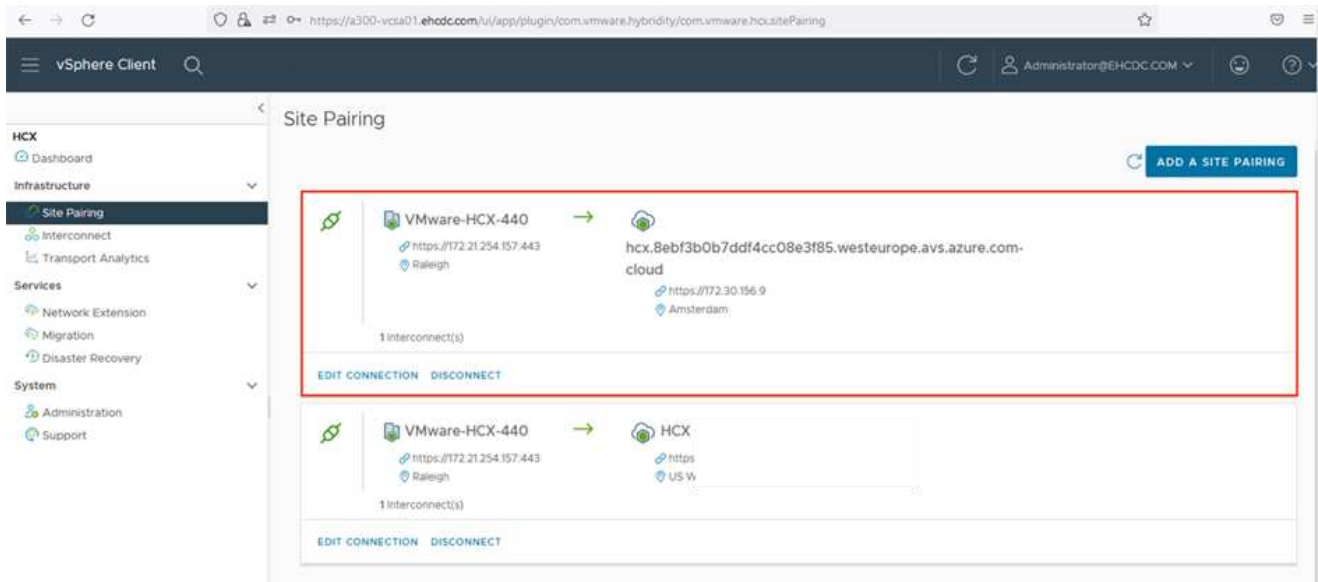


1. Klicken Sie Auf **Verbinden**.



VMware HCX Connector muss über Port 443 zu HCX Cloud Manager IP weiterleiten können.

1. Nach der Erstellung der Kopplung steht die neu konfigurierte Standortpairing auf dem HCX Dashboard zur Verfügung.



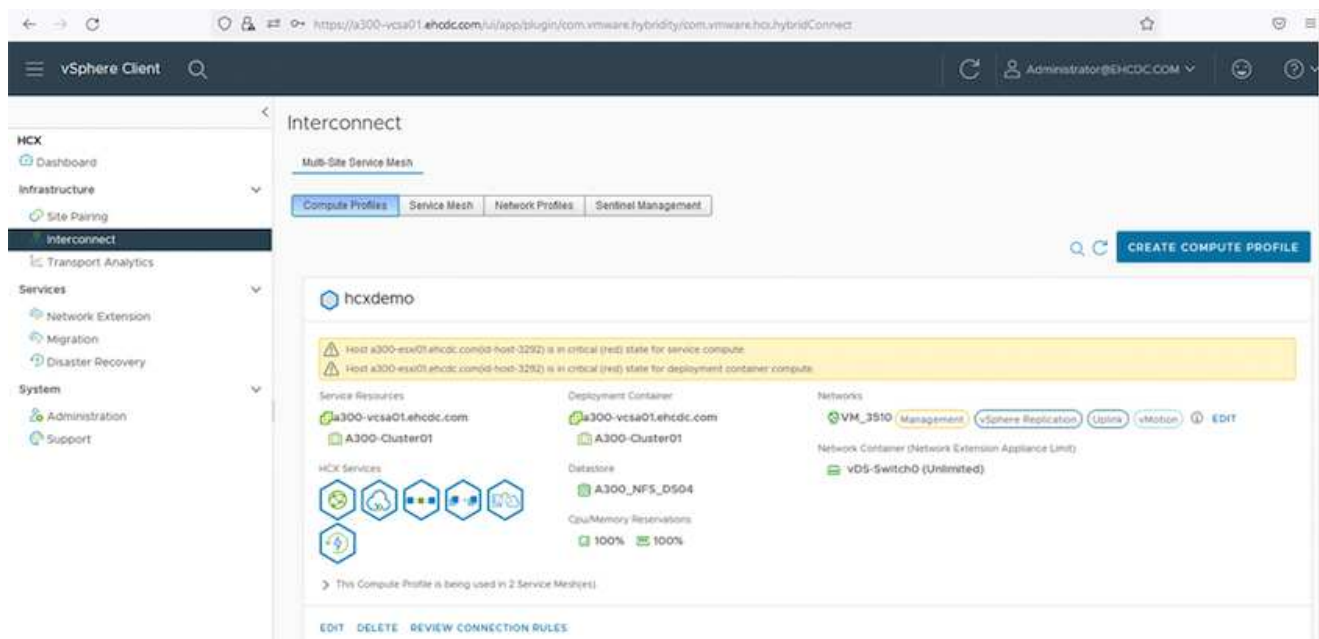
Schritt 5: Netzwerkprofil, Computing-Profil und Service-Mesh konfigurieren

Die VMware HCX Interconnect Service Appliance bietet Replizierungs- und vMotion-basierte Migrationsfunktionen über das Internet und private Verbindungen zum Zielstandort. Das Interconnect bietet Verschlüsselung, Traffic Engineering und VM-Mobilität. Um eine Interconnect Service Appliance zu erstellen, gehen Sie wie folgt vor:

1. Wählen Sie unter Infrastruktur die Option **Interconnect > Multi-Site Service Mesh > Compute Profiles > Create Compute Profile** aus.



Die Computing-Profile definieren die Implementierungsparameter einschließlich der Appliances, die bereitgestellt werden und welche Teile des VMware Datacenters für den HCX-Service verfügbar sind.

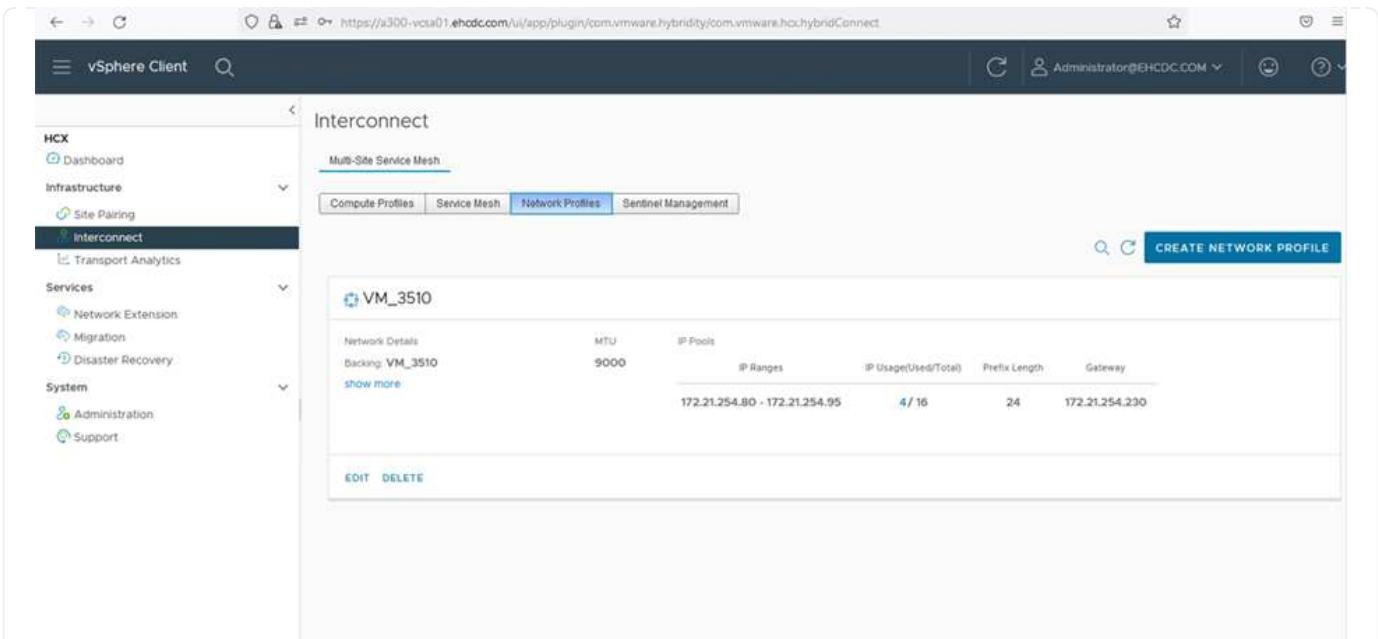


1. Erstellen Sie nach dem Erstellen des Rechenprofils die Netzwerkprofile, indem Sie **Multi-Site Service Mesh > Netzwerkprofil > Netzwerkprofil erstellen** auswählen.

Das Netzwerkprofil definiert einen Bereich von IP-Adressen und Netzwerken, die von HCX für seine virtuellen Appliances verwendet werden.



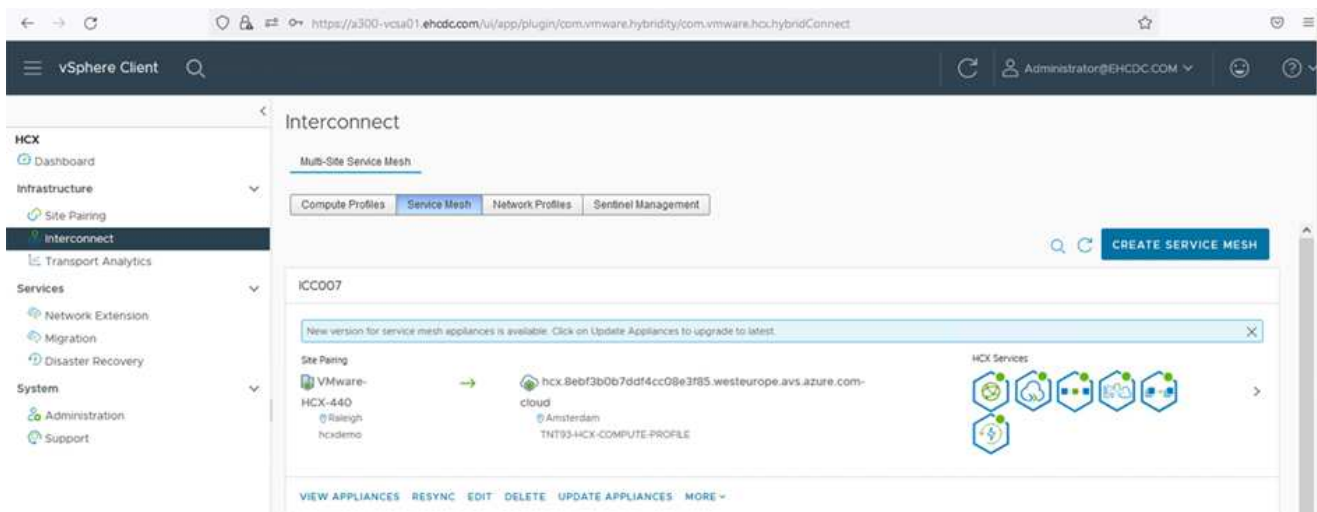
Für diesen Schritt werden mindestens zwei IP-Adressen benötigt. Diese IP-Adressen werden den Interconnect Appliances vom Managementnetzwerk zugewiesen.



1. Derzeit wurden die Computing- und Netzwerkprofile erfolgreich erstellt.
2. Erstellen Sie das Service Mesh, indem Sie in der Option **Interconnect** die Registerkarte **Service Mesh** auswählen und die On-Premises- und Azure SDDC-Sites auswählen.
3. Das Service Mesh gibt ein lokales und entferntes Compute- und Netzwerkprofilpaar an.



Im Rahmen dieses Prozesses werden die HCX-Appliances sowohl an den Quell- als auch an den Zielstandorten bereitgestellt und automatisch konfiguriert, um eine sichere Transportstruktur zu erstellen.



1. Dies ist der letzte Konfigurationsschritt. Die Implementierung sollte also fast 30 Minuten dauern. Nach der Konfiguration des Service-Mesh ist die Umgebung bereit, wobei die IPsec-Tunnel erfolgreich erstellt wurden, um die Workload-VMs zu migrieren.

Schritt 6: Migration von Workloads

Workloads können mithilfe verschiedener VMware HCX Migrationstechnologien bidirektional zwischen lokalen und Azure SDDCs migriert werden. VMs können mithilfe von mehreren Migrationstechnologien wie HCX Bulk Migration, HCX vMotion, HCX Cold Migration, HCX Replication Assisted vMotion (erhältlich mit HCX Enterprise Edition) und HCX OS Assisted Migration (erhältlich mit der HCX Enterprise Edition) in und von VMware HCX Enterprise Edition verschoben werden.

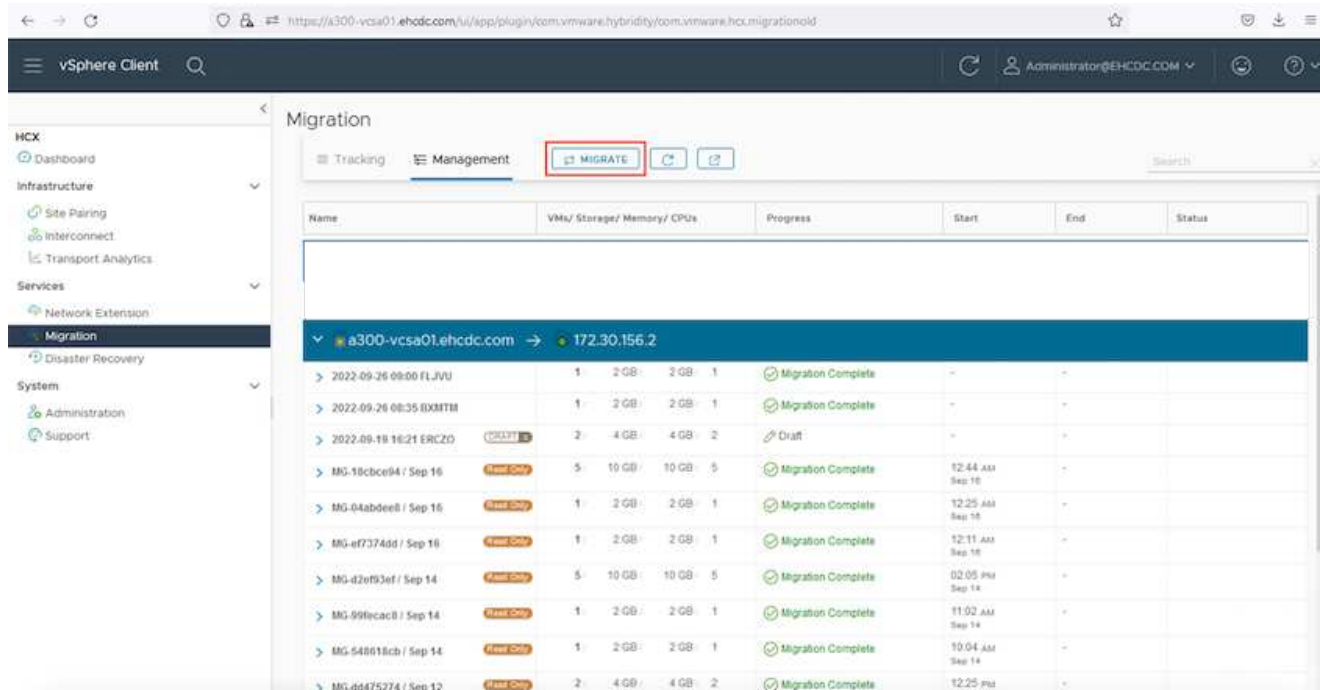
Weitere Informationen zu verschiedenen HCX-Migrationsmechanismen finden Sie unter ["Migrationstypen von VMware HCX"](#).

Massenmigration

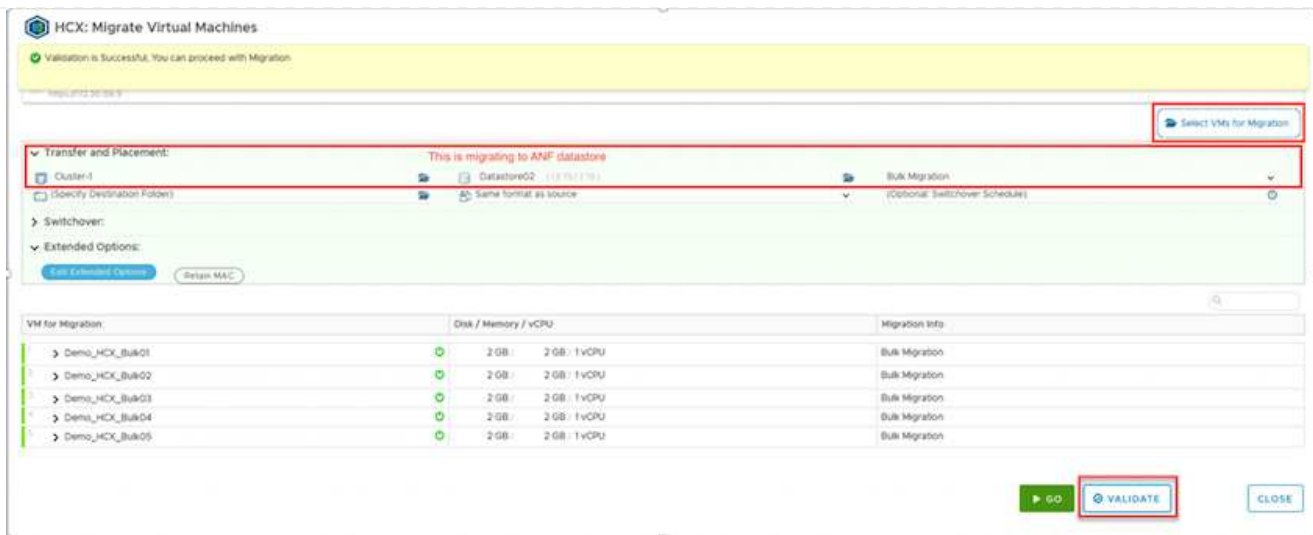
In diesem Abschnitt wird der Migrationsmechanismus für große Datenmengen beschrieben. Während einer Massenmigration nutzt die Funktion zur Massenmigration von HCX vSphere Replication, um Festplattendateien zu migrieren und die VM auf der vSphere HCX-Zielinstanz neu zu erstellen.

Um VM-Massenmigrationen zu initiieren, führen Sie die folgenden Schritte aus:

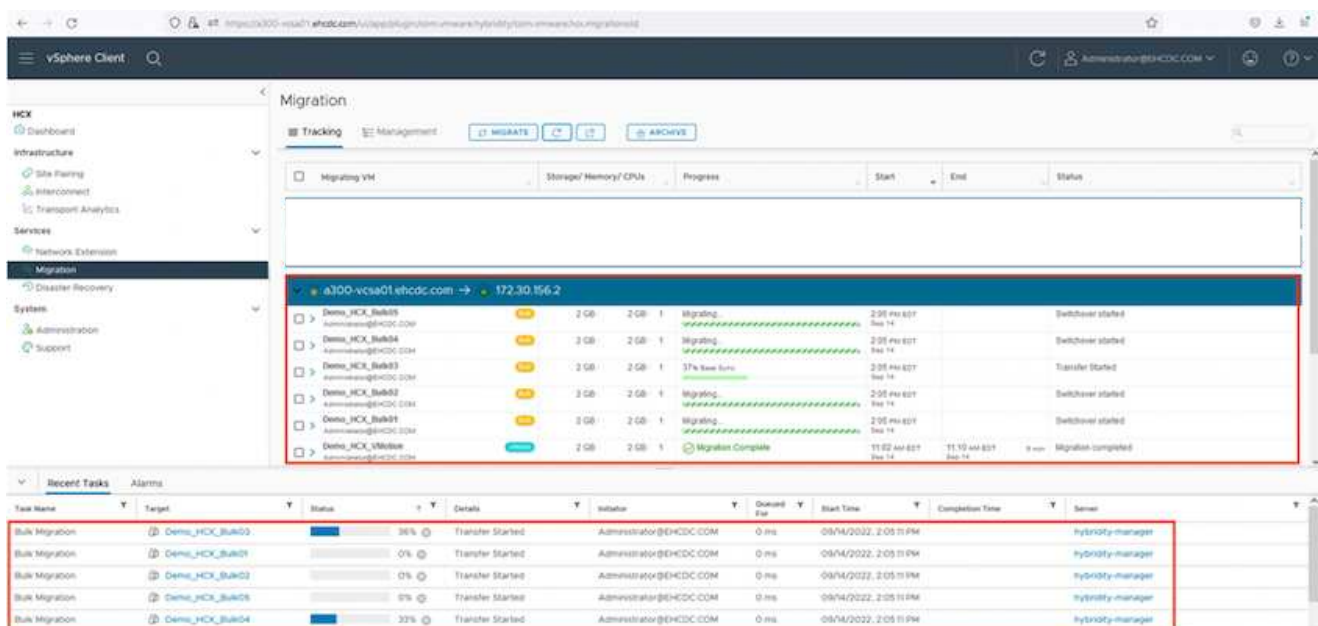
1. Öffnen Sie die Registerkarte * Migrate* unter **Services > Migration**.



1. Wählen Sie unter **Remote-Standortverbindung** die Verbindung mit dem Remote-Standort aus und wählen Sie die Quelle und das Ziel aus. In diesem Beispiel wird als Ziel der SDDC HCX-Endpunkt der Azure VMware-Lösung verwendet.
2. Klicken Sie auf **Select VMs for Migration**. Hier wird eine Liste aller lokalen VMs angezeigt. Wählen Sie die VMs basierend auf dem Ausdruck Match:value aus und klicken Sie auf **Add**.
3. Aktualisieren Sie im Abschnitt **Transfer und Platzierung** die Pflichtfelder (**Cluster, Storage, Ziel und Netzwerk**), einschließlich des Migrationsprofils, und klicken Sie auf **Validieren**.

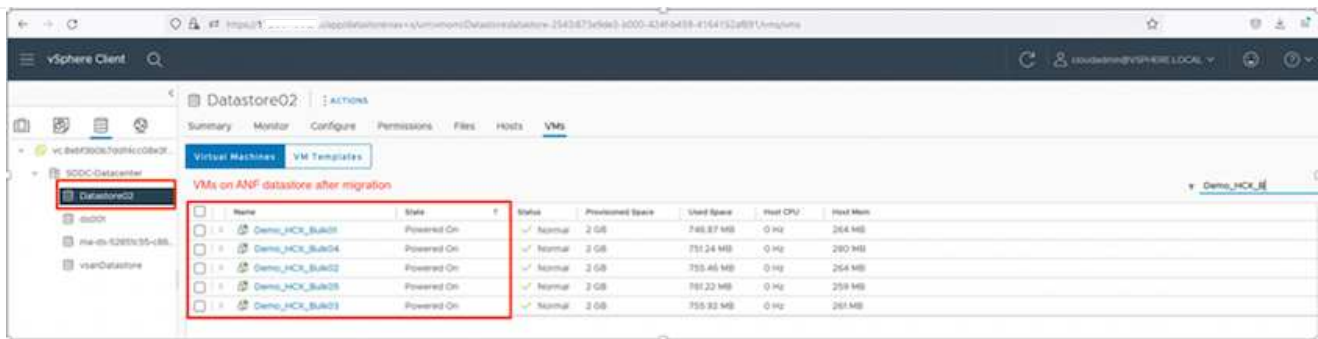


1. Nachdem die Validierungsprüfungen abgeschlossen sind, klicken Sie auf **Go**, um die Migration zu starten.



Während dieser Migration wird auf dem angegebenen Azure NetApp Files Datastore im Ziel-vCenter eine Platzhalterfestplatte erstellt, um die Daten der Quell-VM-Festplatte auf die Platzhalterfestplatten replizieren zu können. HBR wird ausgelöst, um eine vollständige Synchronisierung zum Ziel zu ermöglichen. Nach Abschluss der Baseline wird basierend auf dem RPO-Zyklus (Recovery Point Objective) eine inkrementelle Synchronisierung durchgeführt. Nach Abschluss der vollständigen/inkrementellen Synchronisierung wird die Umschaltung automatisch ausgelöst, es sei denn, ein bestimmter Zeitplan ist festgelegt.

1. Nach Abschluss der Migration können Sie dies durch Zugriff auf das SDDC Ziel-vCenter validieren.

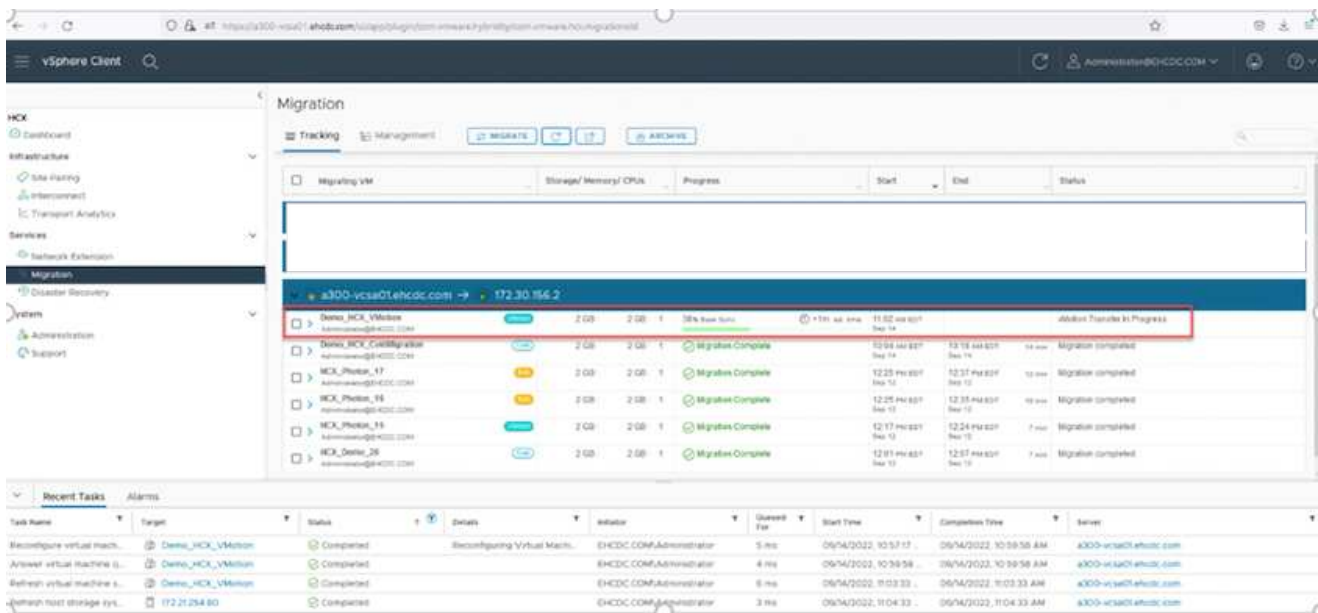


Weitere und detaillierte Informationen zu verschiedenen Migrationsoptionen und zur Migration von Workloads von On-Premises-Systemen zur Azure VMware Lösung mithilfe von HCX finden Sie unter ["VMware HCX-Benutzerhandbuch"](#).

Wenn Sie mehr über diesen Prozess erfahren möchten, sehen Sie sich das folgende Video an:

[Workload-Migration mithilfe von HCX](#)

Hier sehen Sie einen Screenshot der HCX vMotion Option.



Wenn Sie mehr über diesen Prozess erfahren möchten, sehen Sie sich das folgende Video an:

[HCX vMotion](#)



Stellen Sie sicher, dass für die Migration ausreichend Bandbreite zur Verfügung steht.



Der Ziel-ANF-Datastore sollte über genügend Speicherplatz für die Migration verfügen.

Schlussfolgerung

Ganz gleich, ob Sie nur auf All-Cloud- oder Hybrid Cloud-Umgebungen abzielen und Daten in On-Premises-Storage eines beliebigen Typs oder Anbieters speichern – Azure NetApp Files und HCX bieten hervorragende

Optionen für die Implementierung und Migration der Applikations-Workloads und senken gleichzeitig die TCO, da die Datenanforderungen nahtlos auf die Applikationsebene integriert sind. Wie auch immer der Anwendungsfall ist: Wählen Sie Azure VMware Lösung zusammen mit Azure NetApp Files, um schnell von den Vorteilen der Cloud zu profitieren, eine konsistente Infrastruktur und Abläufe vor Ort und in mehreren Clouds, bidirektionale Portabilität von Workloads und Kapazität und Performance der Enterprise-Klasse. Es handelt sich dabei um denselben bekannten Prozess und dieselben Verfahren, die zum Verbinden des Storage und zur Migration von VMs mithilfe von VMware vSphere Replication, VMware vMotion oder sogar NFS (Network File Copy) verwendet werden.

Erkenntnisse Aus

Zu den wichtigsten Punkten dieses Dokuments gehören:

- Sie können Azure NetApp Files nun als Datastore auf dem Azure VMware Solution SDDC verwenden.
- Daten lassen sich problemlos von lokalen Systemen zu Azure NetApp Files Datastores migrieren.
- Erweitern und verkleinern Sie den Azure NetApp Files-Datastore einfach, um die Kapazitäts- und Performance-Anforderungen während der Migration zu erfüllen.

Wo Sie weitere Informationen finden

Weitere Informationen zu den in diesem Dokument beschriebenen Daten finden Sie unter den folgenden Links:

- Dokumentation der Azure VMware Lösung

["https://docs.microsoft.com/en-us/azure/azure-vmware/"](https://docs.microsoft.com/en-us/azure/azure-vmware/)

- Azure NetApp Files-Dokumentation

["https://docs.microsoft.com/en-us/azure/azure-netapp-files/"](https://docs.microsoft.com/en-us/azure/azure-netapp-files/)

- VMware HCX-Benutzerhandbuch

["https://docs.vmware.com/en/VMware-HCX/4.4/hcx-user-guide/GUID-BFD7E194-CFE5-4259-B74B-991B26A51758.html"](https://docs.vmware.com/en/VMware-HCX/4.4/hcx-user-guide/GUID-BFD7E194-CFE5-4259-B74B-991B26A51758.html)

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 IRGEND EINER 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.