TR 4942: Migrieren Sie Workloads mit VMware HCX zum FSx ONTAP Datenspeicher

NetApp public and hybrid cloud solutions

NetApp
August 18, 2025

This PDF was generated from https://docs.netapp.com/de-de/netapp-solutions-cloud/vmware/vmw-aws-vmc-migrate-hcx.html on August 18, 2025. Always check docs.netapp.com for the latest.

Inhalt

TR 4942: Migrieren Sie Workloads mit VMware HCX zum FSx ONTAP Datenspeicher . . . 1
Übersicht: Migrieren virtueller Maschinen mit VMware HCX, FSx ONTAP -Zusatzdatenspeichern und VMware Cloud . . . 1
Lösungsbereitstellung . . . 3
Abschluss . . . 19
Imbiss . . . 19
Wo Sie weitere Informationen finden . . . 19

TR 4942: Migrieren Sie Workloads mit VMware HCX zum FSx ONTAP Datenspeicher

Ein häufiger Anwendungsfall für VMware Cloud (VMC) auf Amazon Web Services (AWS) mit seinem zusätzlichen NFS-Datenspeicher auf Amazon FSx ONTAP ist die Migration von VMware-Workloads. VMware HCX ist eine bevorzugte Option und bietet verschiedene Migrationsmethoden zum Verschieben lokaler virtueller Maschinen (VMs) und ihrer Daten, die auf allen von VMware unterstützten Datenspeichern ausgeführt werden, in VMC-Datenspeicher, einschließlich zusätzlicher NFS-Datenspeicher auf FSx ONTAP.

Übersicht: Migrieren virtueller Maschinen mit VMware HCX, FSx ONTAP -Zusatzdatenspeichern und VMware Cloud

VMware HCX ist in erster Linie eine Mobilitätsplattform, die die Workload-Migration, die Workload-Neuverteilung und die Geschäftskontinuität über Clouds hinweg vereinfachen soll. Es ist Teil von VMware Cloud auf AWS und bietet zahlreiche Möglichkeiten zur Migration von Workloads und kann für Disaster Recovery (DR)-Vorgänge verwendet werden.

Dieses Dokument bietet eine Schritt-für-Schritt-Anleitung zum Bereitstellen und Konfigurieren von VMware HCX, einschließlich aller Hauptkomponenten, vor Ort und auf der Cloud-Rechenzentrumsseite, wodurch verschiedene VM-Migrationsmechanismen ermöglicht werden.

Weitere Informationen finden Sie unter "VMware HCX-Benutzerhandbuch" Und "Checkliste B installieren – HCX mit einer VMware Cloud on AWS SDDC-Zielumgebung" .

Schritte auf hoher Ebene

Diese Liste enthält die wichtigsten Schritte zum Installieren und Konfigurieren von VMware HCX:

1. Aktivieren Sie HCX für das VMC-Software-Defined Data Center (SDDC) über die VMware Cloud Services Console.
2. Laden Sie das OVA-Installationsprogramm für den HCX Connector herunter und stellen Sie es auf dem lokalen vCenter Server bereit.
3. Aktivieren Sie HCX mit einem Lizenzschlüssel.
4. Koppeln Sie den lokalen VMware HCX Connector mit VMC HCX Cloud Manager.
5. Konfigurieren Sie das Netzwerkprofil, das Computeprofil und das Service Mesh.
6. (Optional) Führen Sie eine Netzwerkerweiterung durch, um das Netzwerk zu erweitern und eine erneute IP-Vergabe zu vermeiden.
7. Überprüfen Sie den Gerätestatus und stellen Sie sicher, dass eine Migration möglich ist.
8. Migrieren Sie die VM-Workloads.

Voraussetzungen

Bevor Sie beginnen, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind. Weitere Informationen finden Sie unter "Vorbereitung der Installation" . Nachdem die Voraussetzungen, einschließlich der Konnektivität, erfüllt sind, konfigurieren und aktivieren Sie HCX, indem Sie einen Lizenzschlüssel von der VMware HCX-Konsole bei VMC generieren. Nachdem HCX aktiviert wurde, wird das vCenter-Plug-in bereitgestellt und kann zur Verwaltung über die vCenter-Konsole aufgerufen werden.

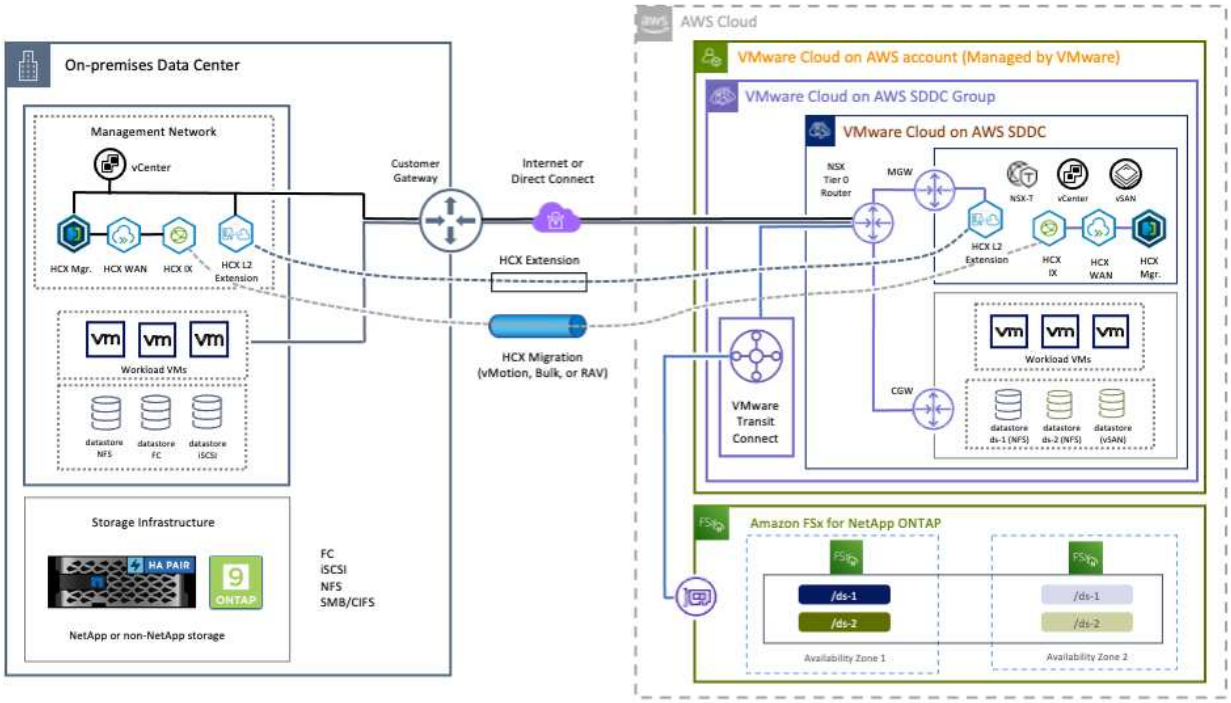
Die folgenden Installationsschritte müssen abgeschlossen sein, bevor Sie mit der Aktivierung und Bereitstellung von HCX fortfahren:

1. Verwenden Sie ein vorhandenes VMC SDDC oder erstellen Sie ein neues SDDC, indem Sie Folgendes befolgen:"NetApp Link" oder das "VMware-Link" .
2. Der Netzwerkpfad von der lokalen vCenter-Umgebung zum VMC SDDC muss die Migration von VMs mithilfe von vMotion unterstützen.
3. Stellen Sie sicher, dass die erforderlichen "Firewall-Regeln und Ports" sind für vMotion-Datenverkehr zwischen dem lokalen vCenter Server und dem SDDC vCenter zulässig.
4. Das FSx ONTAP NFS-Volume sollte als zusätzlicher Datenspeicher im VMC SDDC gemountet werden. Um die NFS-Datenspeicher an den entsprechenden Cluster anzuhängen, folgen Sie den Schritten in diesem"NetApp Link" oder das "VMware-Link" .

High-Level-Architektur

Zu Testzwecken wurde die für diese Validierung verwendete lokale Laborumgebung über ein Site-to-Site-VPN mit AWS VPC verbunden, was eine lokale Konnektivität mit AWS und mit VMware Cloud SDDC über ein externes Transit-Gateway ermöglichte. Der Datenverkehr für die HCX-Migration und Netzwerkerweiterung fließt über das Internet zwischen lokalen Standorten und dem VMware Cloud-Ziel-SDDC. Diese Architektur kann so geändert werden, dass private virtuelle Schnittstellen von Direct Connect verwendet werden.

Das folgende Bild zeigt die Architektur auf hoher Ebene.



Lösungsbereitstellung

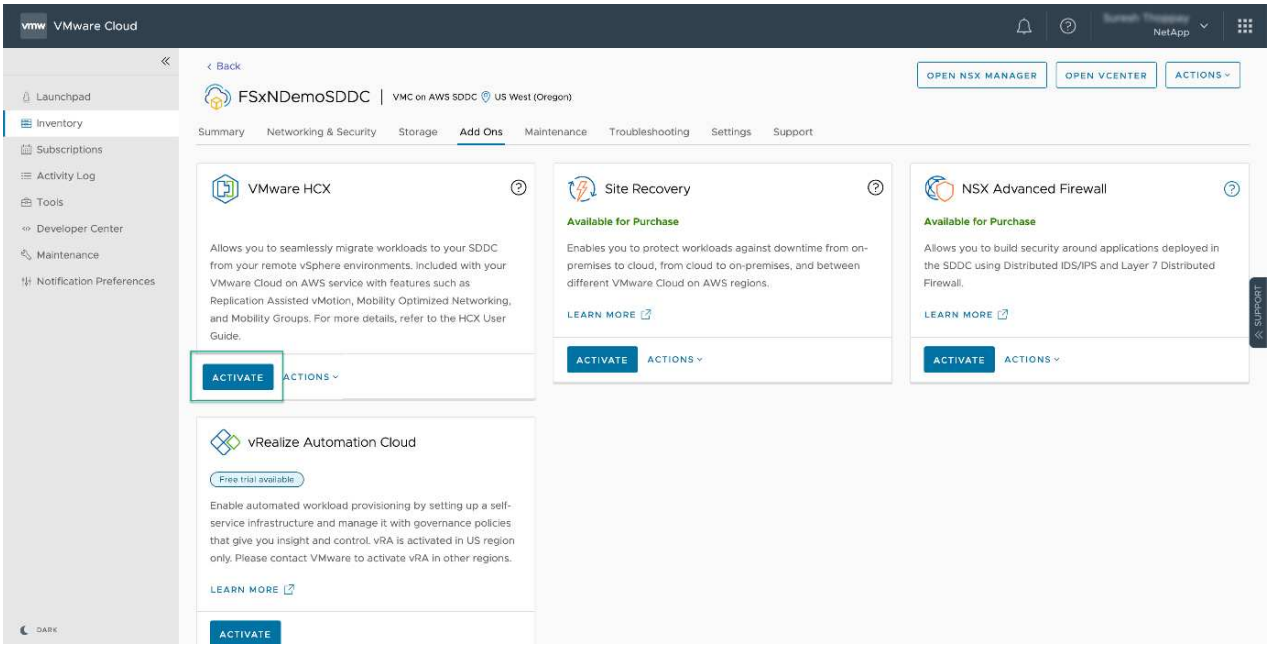
Befolgen Sie die Schritte, um die Bereitstellung dieser Lösung abzuschließen:

Schritt 1: Aktivieren Sie HCX über VMC SDDC mithilfe der Add-Ons-Option

Führen Sie zur Durchführung der Installation die folgenden Schritte aus:

1. Melden Sie sich bei der VMC-Konsole an unter "vmc.vmware.com" und greifen Sie auf das Inventar zu.
2. Um das entsprechende SDDC auszuwählen und auf Add-Ons zuzugreifen, klicken Sie auf „Details zum SDDC anzeigen“ und wählen Sie die Registerkarte „Add-Ons“ aus.
3. Klicken Sie auf „Für VMware HCX aktivieren“.

> Dieser Schritt kann bis zu 25 Minuten dauern.

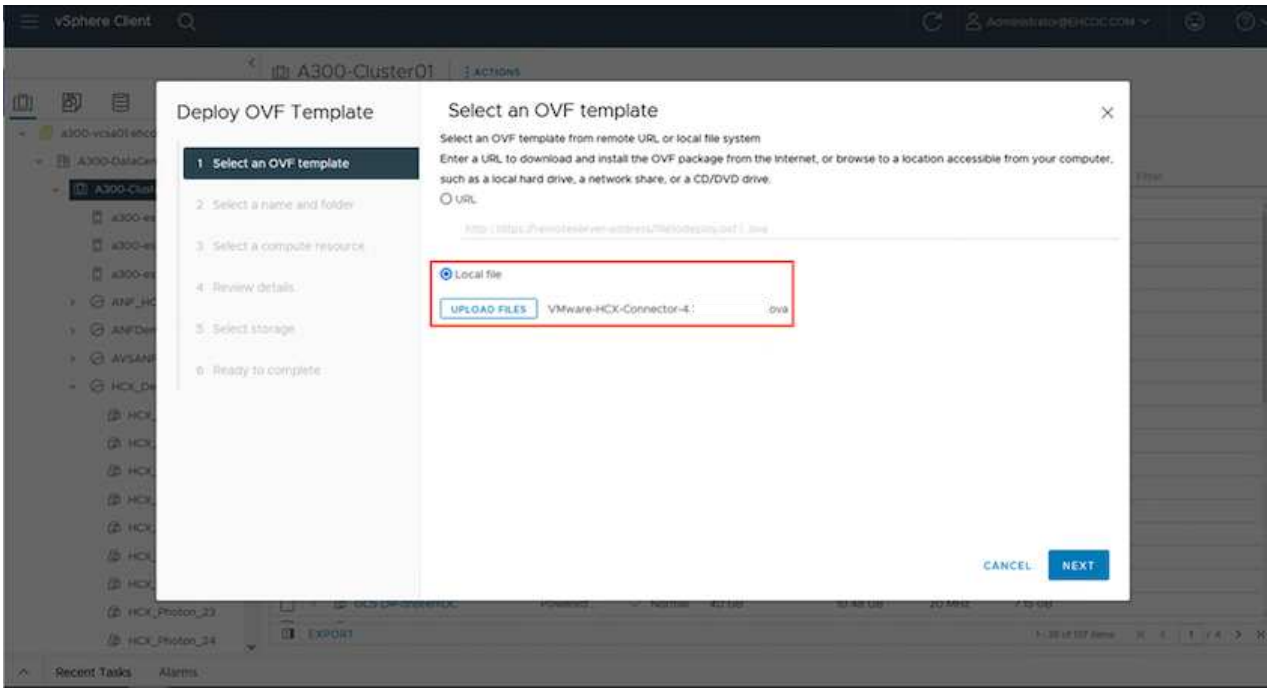


4. Nachdem die Bereitstellung abgeschlossen ist, validieren Sie die Bereitstellung, indem Sie bestätigen, dass HCX Manager und die zugehörigen Plug-Ins in der vCenter-Konsole verfügbar sind.
5. Erstellen Sie die entsprechenden Management Gateway-Firewalls, um die für den Zugriff auf HCX Cloud Manager erforderlichen Ports zu öffnen. HCX Cloud Manager ist jetzt für HCX-Vorgänge bereit.

Schritt 2: Bereitstellen der OVA-Installationsdatei im lokalen vCenter Server

Damit der lokale Connector mit dem HCX Manager in VMC kommunizieren kann, stellen Sie sicher, dass die entsprechenden Firewall-Ports in der lokalen Umgebung geöffnet sind.

1. Navigieren Sie von der VMC-Konsole zum HCX-Dashboard, gehen Sie zu „Administration“ und wählen Sie die Registerkarte „Systemaktualisierung“ aus. Klicken Sie auf „Download-Link für das OVA-Image des HCX Connector anfordern“.
2. Nachdem Sie den HCX Connector heruntergeladen haben, stellen Sie die OVA auf dem lokalen vCenter Server bereit. Klicken Sie mit der rechten Maustaste auf „vSphere-Cluster“ und wählen Sie die Option „OVF-Vorlage bereitstellen“.

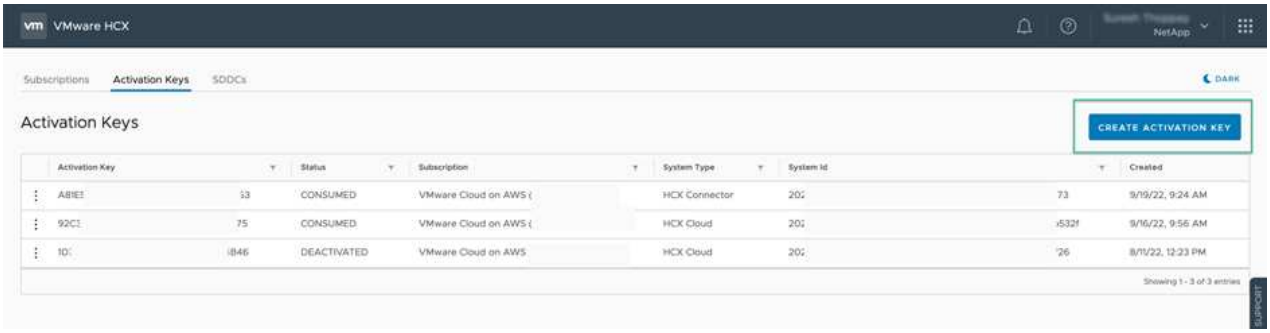


3. Geben Sie die erforderlichen Informationen in den Assistenten „OVF-Vorlage bereitstellen“ ein, klicken Sie auf „Weiter“ und dann auf „Fertig stellen“, um die VMware HCX Connector OVA bereitzustellen.
4. Schalten Sie die virtuelle Appliance manuell ein. Eine Schritt-für-Schritt-Anleitung finden Sie unter "VMware HCX-Benutzerhandbuch" .

Schritt 3: HCX Connector mit dem Lizenzschlüssel aktivieren

Nachdem Sie die VMware HCX Connector OVA vor Ort bereitgestellt und die Appliance gestartet haben, führen Sie die folgenden Schritte aus, um HCX Connector zu aktivieren. Generieren Sie den Lizenzschlüssel von der VMware HCX-Konsole bei VMC und geben Sie die Lizenz während der Einrichtung des VMware HCX-Connectors ein.

1. Gehen Sie in der VMware Cloud Console zu „Inventar“, wählen Sie das SDDC aus und klicken Sie auf „Details anzeigen“. Klicken Sie auf der Registerkarte „Add-Ons“ in der Kachel „VMware HCX“ auf „HCX öffnen“.
2. Klicken Sie auf der Registerkarte „Aktivierungsschlüssel“ auf „Aktivierungsschlüssel erstellen“. Wählen Sie als Systemtyp „HCX-Connector“ aus und klicken Sie auf „Bestätigen“, um den Schlüssel zu generieren. Kopieren Sie den Aktivierungsschlüssel.



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

3. Melden Sie sich beim lokalen VMware HCX Connector an unter `"https://hcxconnectorIP:9443"` mit Administratoranmeldeinformationen.

> Verwenden Sie das während der OVA-Bereitstellung definierte Kennwort.

4. Geben Sie im Abschnitt „Lizenzierung“ den in Schritt 2 kopierten Aktivierungsschlüssel ein und klicken Sie auf „Aktivieren“.

> Damit die Aktivierung erfolgreich abgeschlossen werden kann, muss der lokale HCX-Connector über einen Internetzugang verfügen.

5. Geben Sie unter „Rechenzentrumsstandort“ den gewünschten Speicherort für die lokale Installation des VMware HCX Managers an. Klicken Sie auf „Weiter“.
6. Aktualisieren Sie unter „Systemname“ den Namen und klicken Sie auf „Fortfahren“.
7. Wählen Sie „Ja“ und dann „Weiter“.
8. Geben Sie unter „Verbinden Sie Ihr vCenter“ die IP-Adresse oder den vollqualifizierten Domänennamen (FQDN) und die Anmeldeinformationen für den vCenter-Server ein und klicken Sie auf „Fortfahren“.

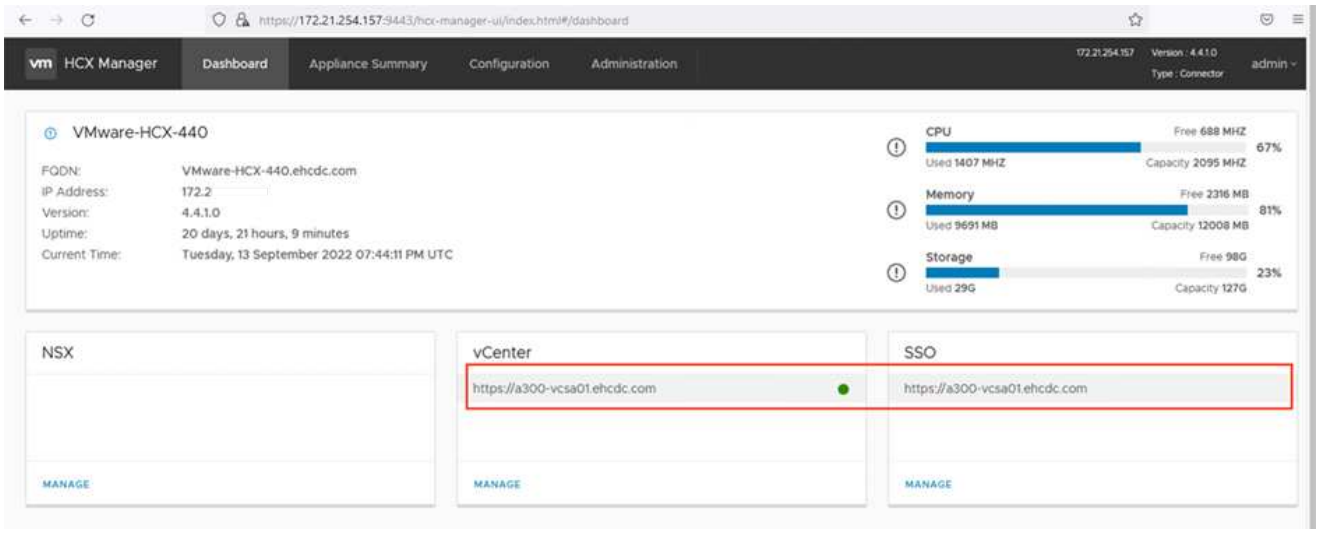
> Verwenden Sie den FQDN, um spätere Kommunikationsprobleme zu vermeiden.

9. Geben Sie unter „SSO/PSC konfigurieren“ den FQDN oder die IP-Adresse des Platform Services Controllers ein und klicken Sie auf „Fortfahren“.

Geben Sie die IP-Adresse oder den FQDN des vCenter-Servers ein.

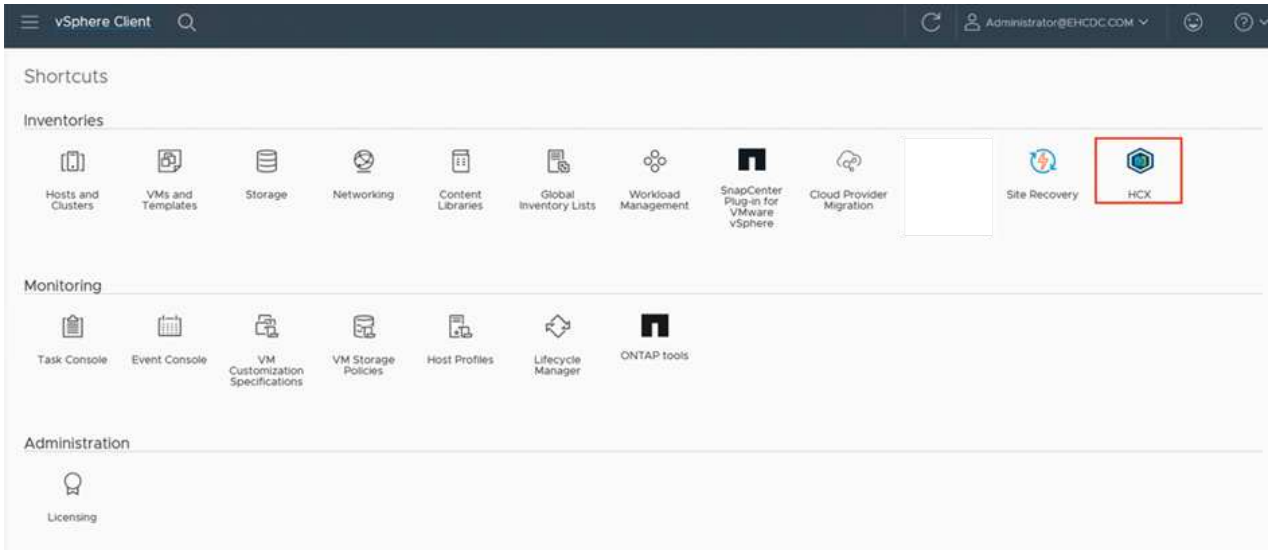
10. Überprüfen Sie, ob die Informationen richtig eingegeben wurden, und klicken Sie auf „Neu starten“.
11. Nach Abschluss wird der vCenter Server grün angezeigt. Sowohl der vCenter Server als auch SSO müssen über die richtigen Konfigurationsparameter verfügen, die mit denen auf der vorherigen Seite übereinstimmen sollten.

Dieser Vorgang sollte etwa 10–20 Minuten dauern und das Plug-In sollte dem vCenter Server hinzugefügt werden.

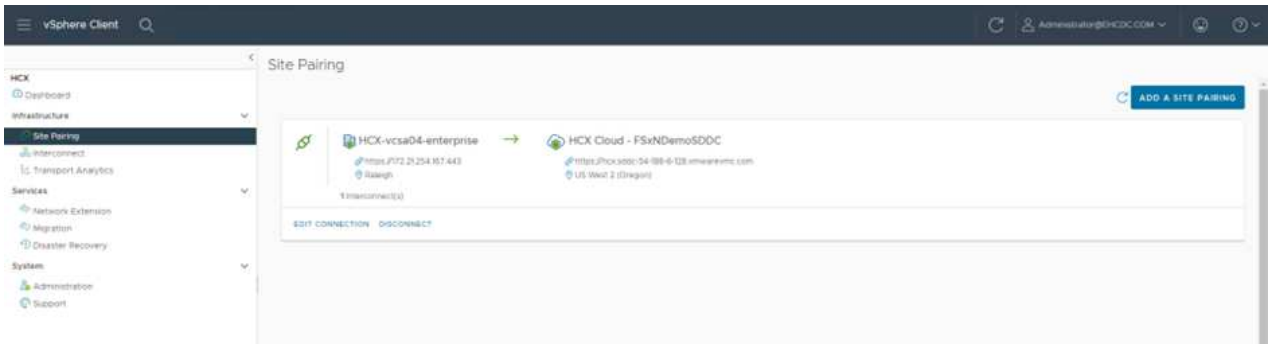


Schritt 4: Koppeln Sie den lokalen VMware HCX Connector mit dem VMC HCX Cloud Manager

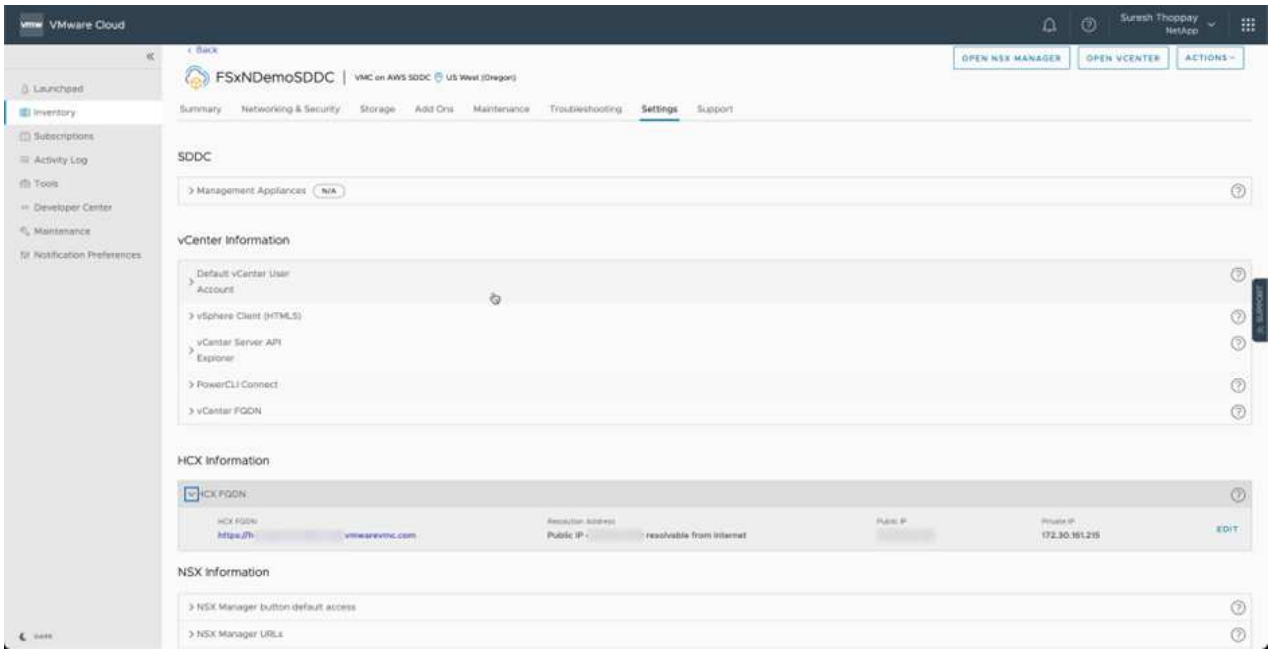
1. Um ein Site-Paar zwischen dem lokalen vCenter Server und dem VMC SDDC zu erstellen, melden Sie sich beim lokalen vCenter Server an und greifen Sie auf das HCX vSphere Web Client Plug-in zu.

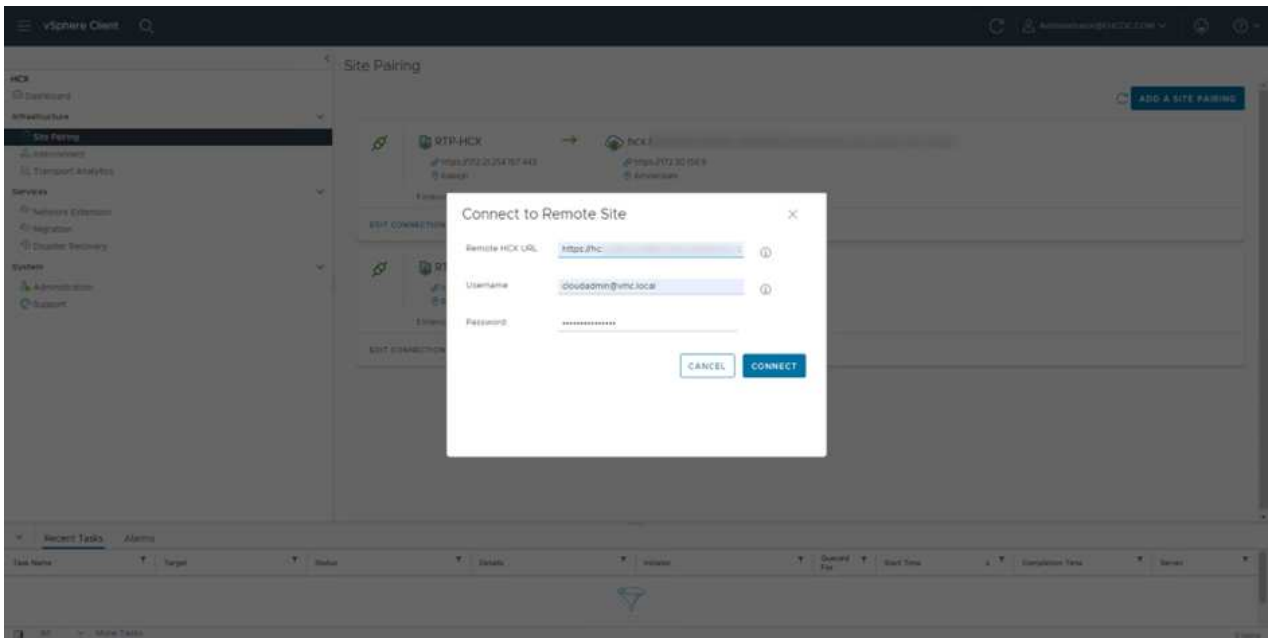


2. Klicken Sie unter „Infrastruktur“ auf „Site-Paarung hinzufügen“. Geben Sie zur Authentifizierung der Remote-Site die URL oder IP-Adresse des VMC HCX Cloud Managers und die Anmeldeinformationen für die CloudAdmin-Rolle ein.



HCX-Informationen können von der SDDC-Einstellungsseite abgerufen werden.





3. Klicken Sie auf „Verbinden“, um die Site-Kopplung zu starten.

> VMware HCX Connector muss über Port 443 mit der HCX Cloud Manager-IP kommunizieren können.

4. Nachdem die Kopplung erstellt wurde, ist die neu konfigurierte Site-Kopplung auf dem HCX-Dashboard verfügbar.

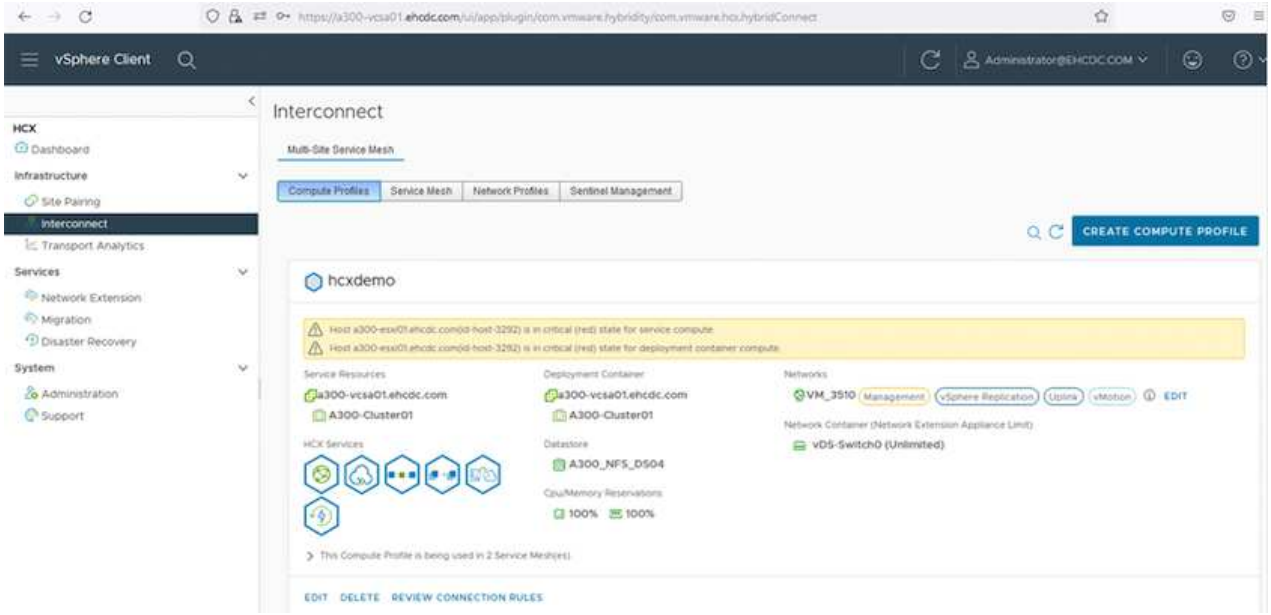
Schritt 5: Konfigurieren Sie das Netzwerkprofil, das Compute-Profil und das Service Mesh

Das VMware HCX Interconnect (HCX-IX)-Gerät bietet sichere Tunnelfunktionen über das Internet und private Verbindungen zum Zielstandort, die Replikations- und vMotion-basierte Funktionen ermöglichen. Die Verbindung bietet Verschlüsselung, Verkehrstechnik und ein SD-WAN. Führen Sie die folgenden Schritte aus, um die HCI-IX Interconnect Appliance zu erstellen:

1. Wählen Sie unter „Infrastruktur“ die Optionen „Interconnect“ > „Multi-Site Service Mesh“ > „Compute-Profile“ > „Compute-Profil erstellen“ aus.

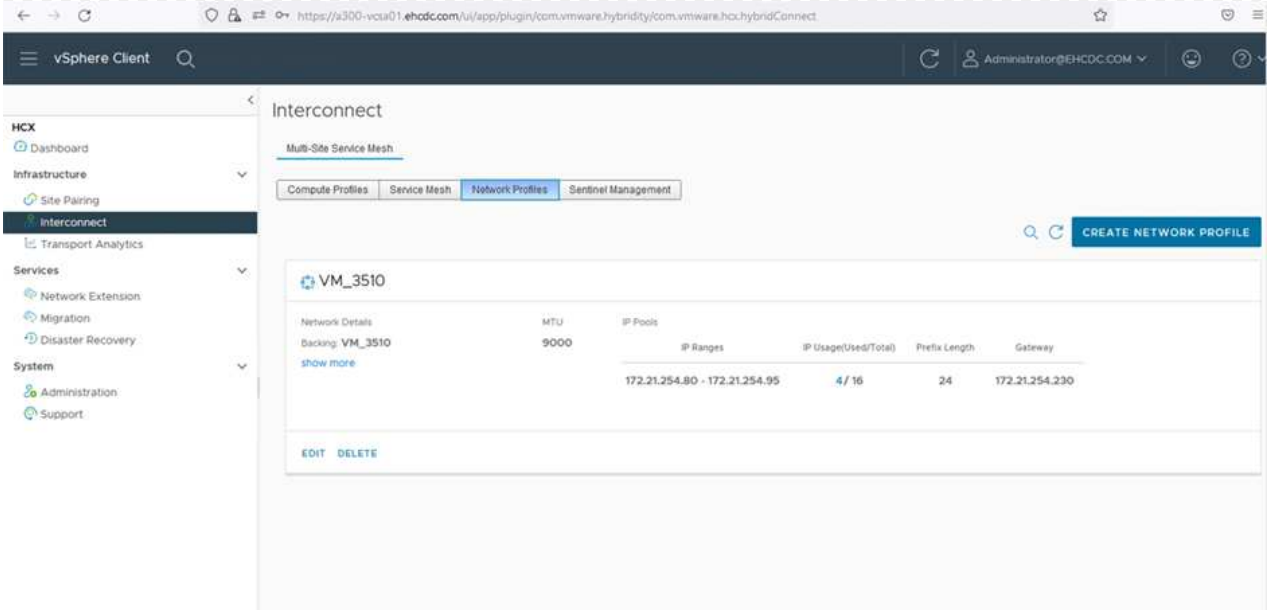
   > Rechenprofile enthalten die Rechen-, Speicher- und Netzwerkbereitstellungsparameter, die zum Bereitstellen einer virtuellen Interconnect-Appliance erforderlich sind. Sie geben auch an, auf welchen Teil des VMware-Rechenzentrums der HCX-Dienst zugreifen kann.

   Ausführliche Anweisungen finden Sie unter "Erstellen eines Compute-Profils" .



2. Nachdem das Compute-Profil erstellt wurde, erstellen Sie das Netzwerkprofil, indem Sie Multi-Site Service Mesh > Netzwerkprofile > Netzwerkprofil erstellen auswählen.
3. Das Netzwerkprofil definiert einen Bereich von IP-Adressen und Netzwerken, die von HCX für seine virtuellen Appliances verwendet werden.

   > Dies erfordert zwei oder mehr IP-Adressen. Diese IP-Adressen werden vom Verwaltungsnetzwerk an virtuelle Appliances zugewiesen.

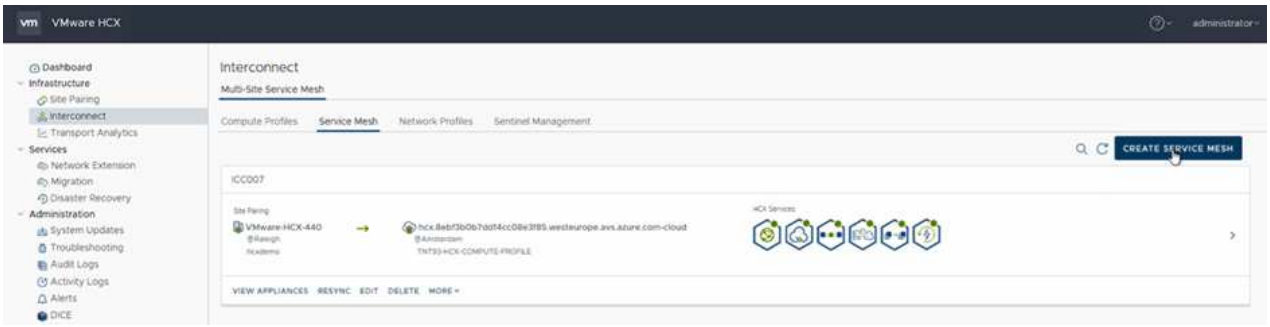


Ausführliche Anweisungen finden Sie unter "Erstellen eines Netzwerkprofils" .

> Wenn Sie über das Internet eine Verbindung mit einem SD-WAN herstellen, müssen Sie im Abschnitt „Netzwerk und Sicherheit“ öffentliche IPs reservieren.

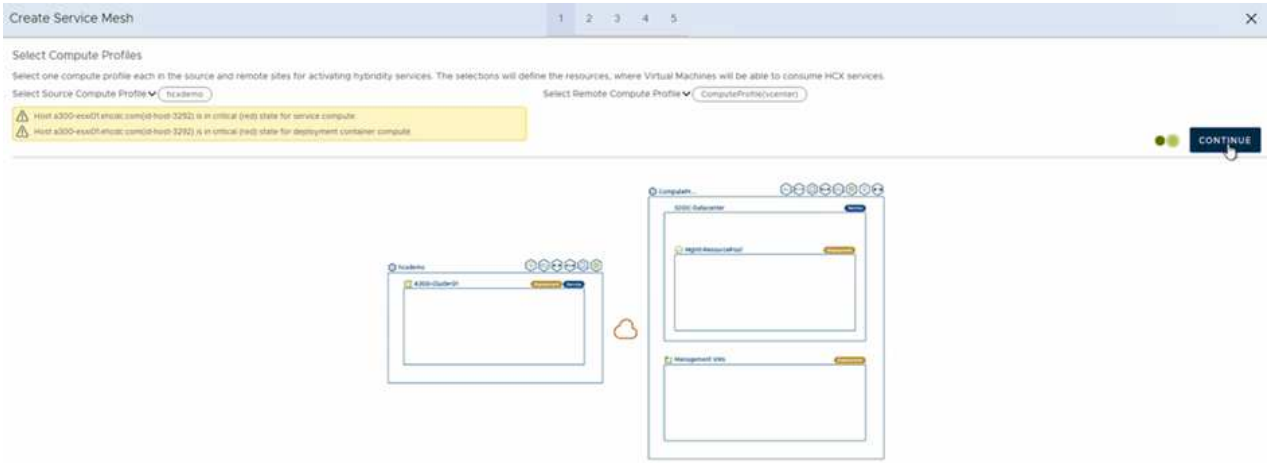
4. Um ein Service Mesh zu erstellen, wählen Sie die Registerkarte „Service Mesh“ innerhalb der Option „Interconnect“ und wählen Sie lokale und VMC SDDC-Sites aus.

   Das Service-Mesh erstellt ein lokales und ein Remote-Compute- und Netzwerkprofilpaar.

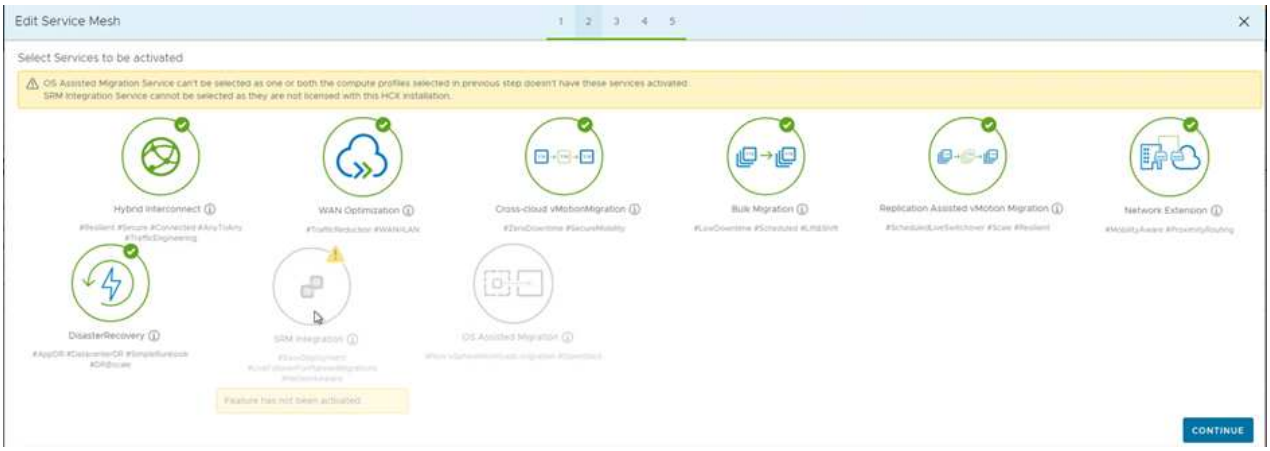


> Teil dieses Prozesses ist die Bereitstellung von HCX-Geräten, die sowohl auf den Quell- als auch auf den Zielstandorten automatisch konfiguriert werden und so ein sicheres Transport-Fabric erstellen.

5. Wählen Sie die Quell- und Remote-Compute-Profile aus und klicken Sie auf „Fortfahren“.

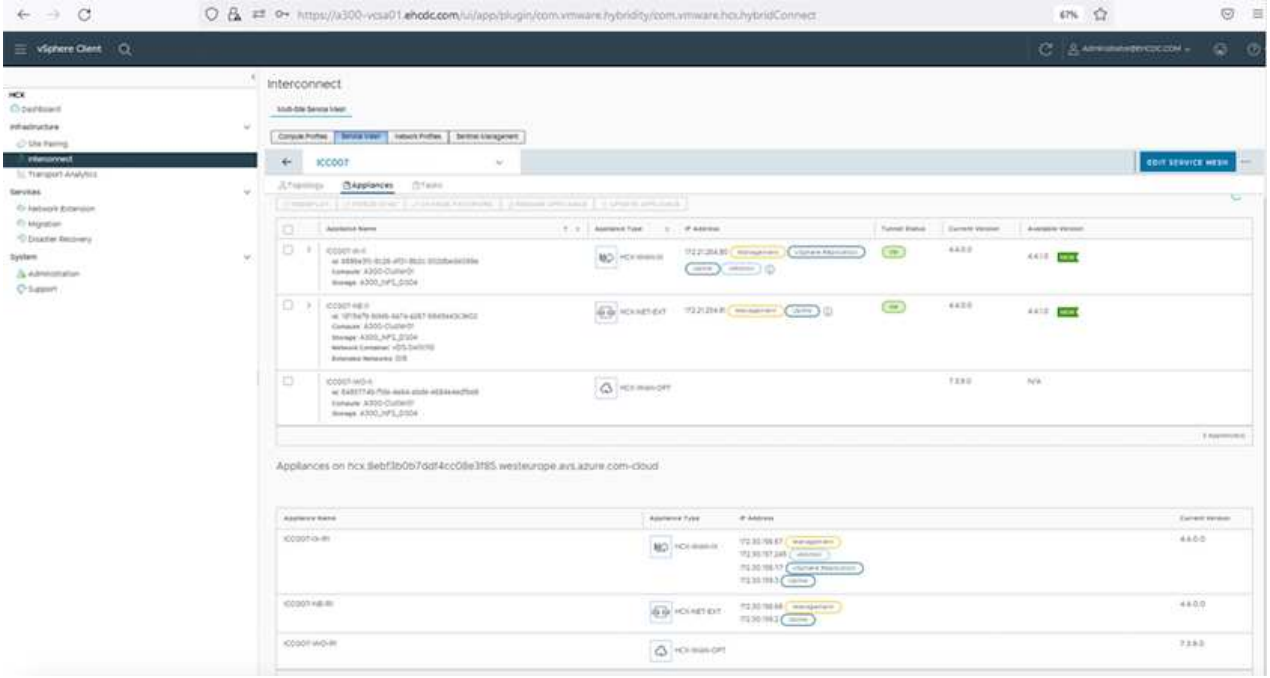


6. Wählen Sie den zu aktivierenden Dienst aus und klicken Sie auf „Weiter“.



> Für Replication Assisted vMotion Migration, SRM Integration und OS Assisted Migration ist eine HCX Enterprise-Lizenz erforderlich.

7. Geben Sie dem Service Mesh einen Namen und klicken Sie auf „Fertig stellen“, um mit dem Erstellungsprozess zu beginnen. Die Bereitstellung sollte etwa 30 Minuten dauern. Nachdem das Service Mesh konfiguriert wurde, wurden die virtuelle Infrastruktur und das Netzwerk erstellt, die zum Migrieren der Workload-VMs erforderlich sind.


vSphere Client
Interconnect
ICC007
EDIT SERVICE MESH
Appliances
Appliances on hcx.8ebf3b0b7ddf4cc08e3f85.westeurope.avs.azure.com-cloud

Schritt 6: Migrieren von Workloads

HCX bietet bidirektionale Migrationsdienste zwischen zwei oder mehr unterschiedlichen Umgebungen wie lokalen Umgebungen und VMC SDDCs. Anwendungs-Workloads können mithilfe einer Vielzahl von Migrationstechnologien wie HCX-Massenmigration, HCX vMotion, HCX Cold Migration, HCX Replication Assisted vMotion (verfügbar mit HCX Enterprise Edition) und HCX OS Assisted Migration (verfügbar mit HCX Enterprise Edition) zu und von HCX-aktivierten Sites migriert werden.

Weitere Informationen zu verfügbaren HCX-Migrationstechnologien finden Sie unter "VMware HCX-Migrationstypen"

Das HCX-IX-Gerät verwendet den Mobility Agent-Dienst, um vMotion-, Cold- und Replication Assisted vMotion (RAV)-Migrationen durchzuführen.

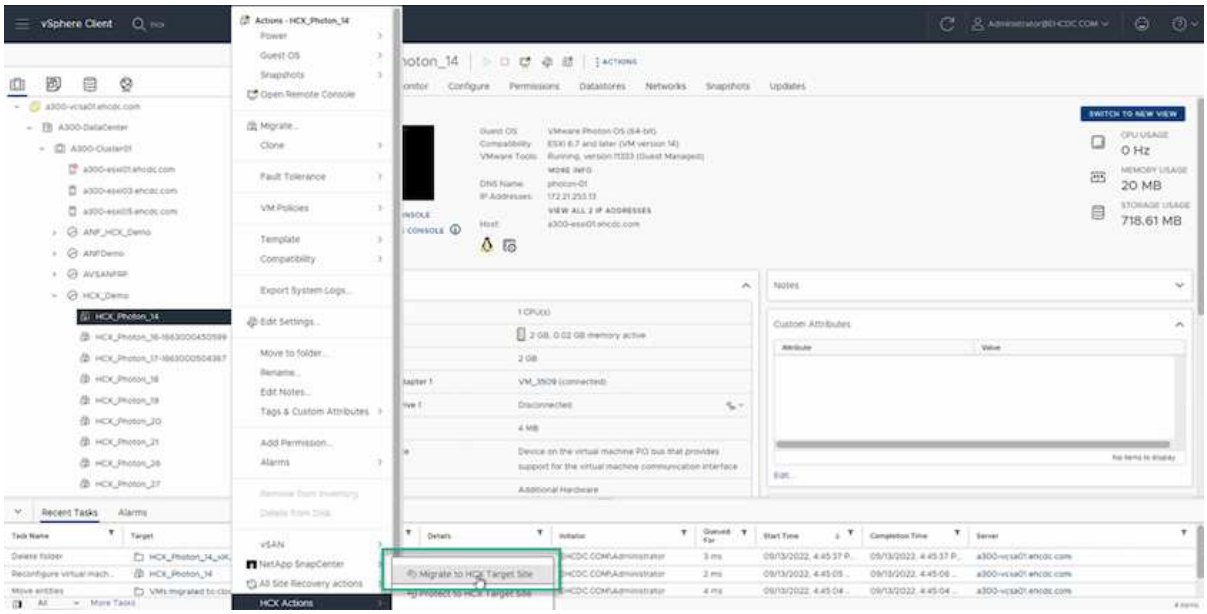
> Die HCX-IX-Appliance fügt den Mobility Agent-Dienst als Hostobjekt im vCenter Server hinzu. Die in diesem Objekt angezeigten Prozessor-, Speicher-, Speicher- und Netzwerkressourcen stellen nicht den tatsächlichen Verbrauch auf dem physischen Hypervisor dar, auf dem die IX-Appliance gehostet wird.

VMware HCX vMotion

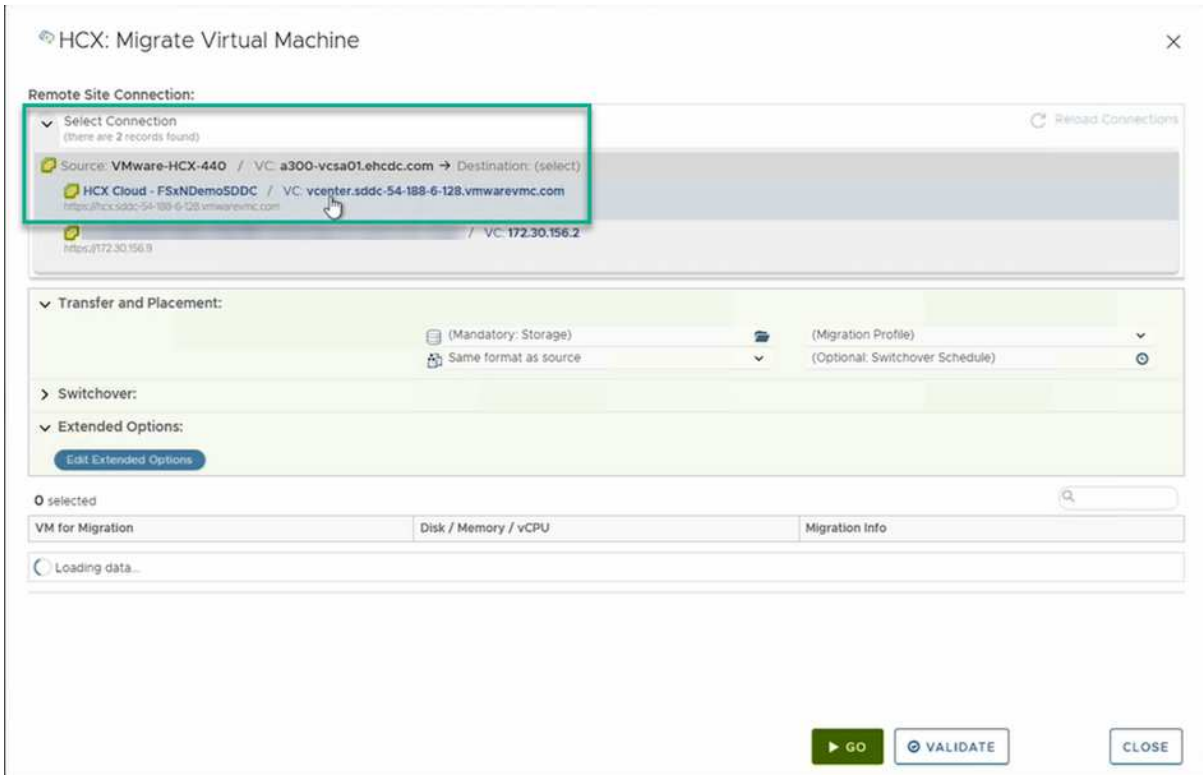
In diesem Abschnitt wird der HCX vMotion-Mechanismus beschrieben. Diese Migrationstechnologie verwendet das VMware vMotion-Protokoll, um eine VM zu VMC SDDC zu migrieren. Die Migrationsoption vMotion wird zum Migrieren des VM-Status jeweils einer einzelnen VM verwendet. Bei dieser Migrationsmethode kommt es zu keiner Dienstunterbrechung.

> Die Netzwerkerweiterung sollte vorhanden sein (für die Portgruppe, an die die VM angeschlossen ist), um die VM zu migrieren, ohne dass eine Änderung der IP-Adresse erforderlich ist.

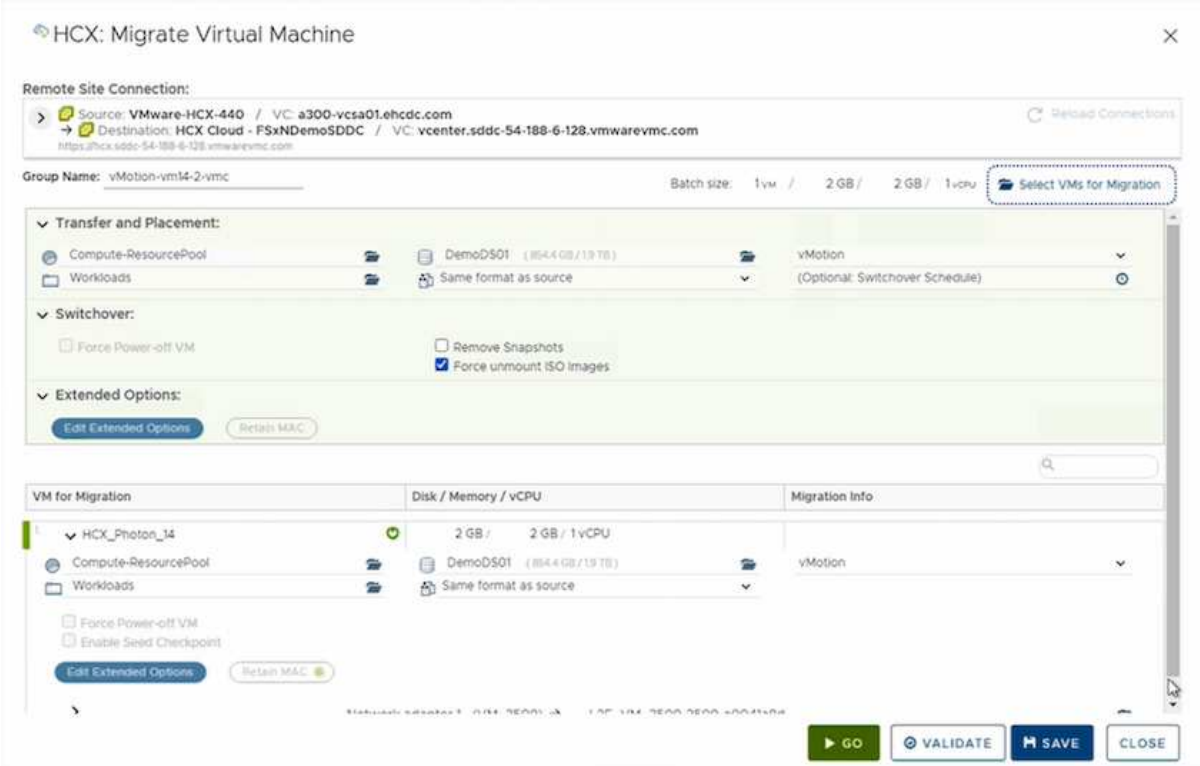
1. Gehen Sie im lokalen vSphere-Client zu „Inventar“, klicken Sie mit der rechten Maustaste auf die zu migrierende VM und wählen Sie „HCX-Aktionen“ > „Zu HCX-Zielsite migrieren“.



2. Wählen Sie im Assistenten „Virtuelle Maschine migrieren“ die Remote-Site-Verbindung (Ziel-VMC-SDDC) aus.



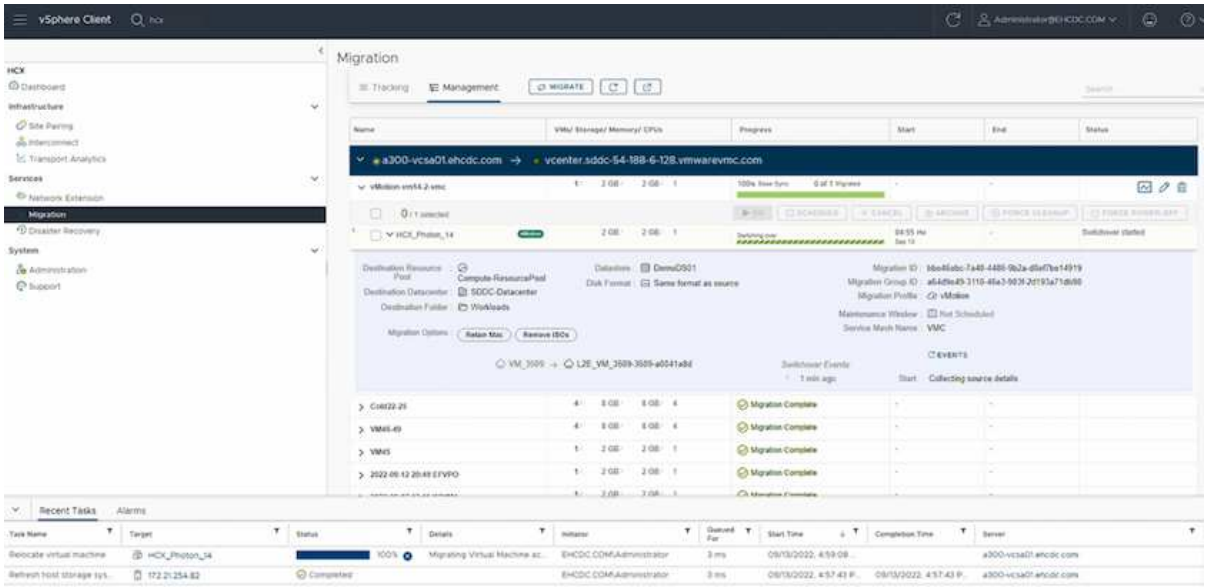
3. Fügen Sie einen Gruppennamen hinzu und aktualisieren Sie unter „Übertragung und Platzierung“ die Pflichtfelder (Cluster, Speicher und Zielnetzwerk). Klicken Sie auf „Validieren“.



4. Klicken Sie nach Abschluss der Validierungsprüfungen auf „Los“, um die Migration zu starten.

Die vMotion-Übertragung erfasst den aktiven Speicher der VM, ihren Ausführungsstatus, ihre IP-Adresse und ihre MAC-Adresse. Weitere Informationen zu den Anforderungen und Einschränkungen von HCX vMotion finden Sie unter "VMware HCX vMotion und Cold Migration verstehen" .

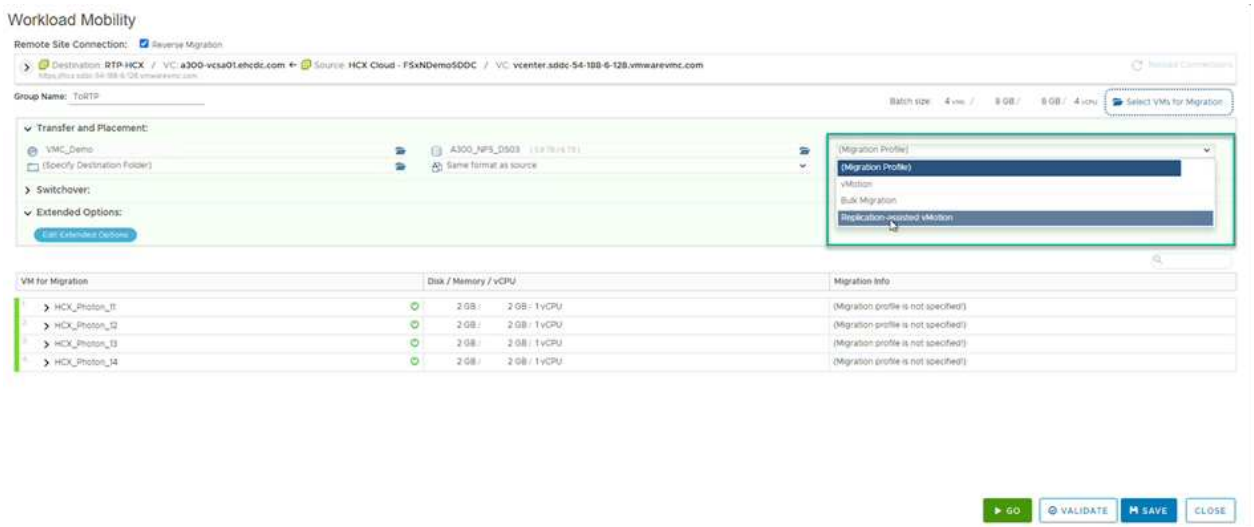
5. Sie können den Fortschritt und den Abschluss von vMotion über das Dashboard „HCX > Migration“ überwachen.



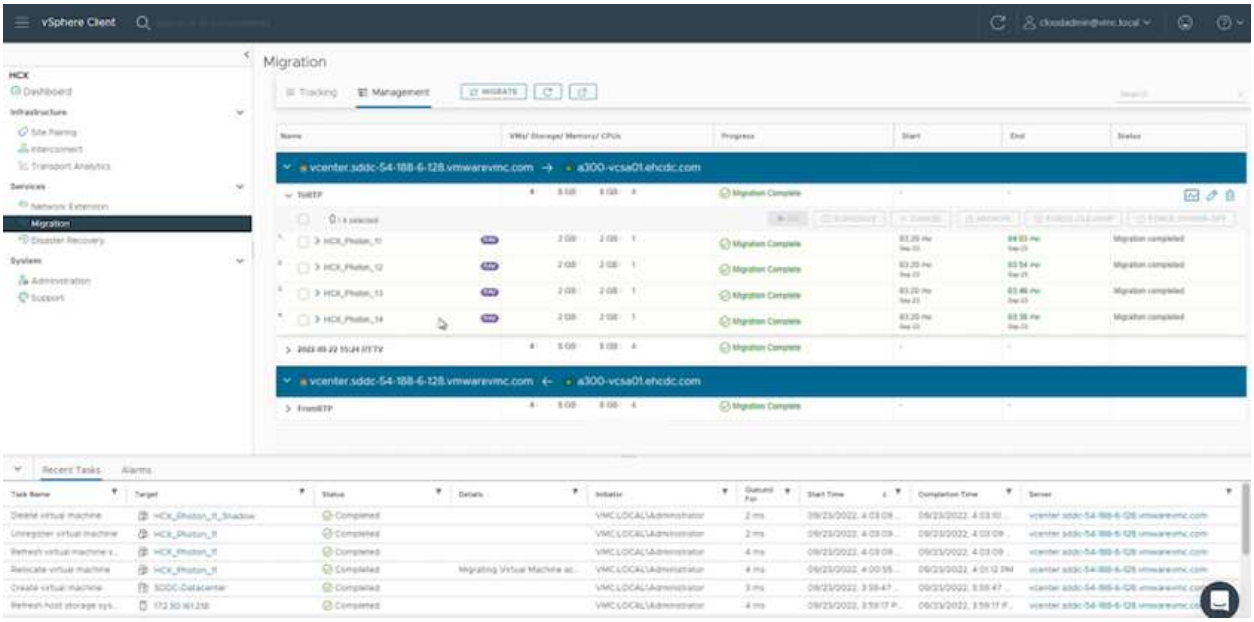
VMware Replication Assisted vMotion

Wie Sie vielleicht der VMware-Dokumentation entnommen haben, kombiniert VMware HCX Replication Assisted vMotion (RAV) die Vorteile von Massenmigration und vMotion. Bei der Massenmigration wird vSphere Replication verwendet, um mehrere VMs parallel zu migrieren. Die VM wird während der Umschaltung neu gestartet. HCX vMotion migriert ohne Ausfallzeiten, wird jedoch seriell jeweils eine VM in einer Replikationsgruppe durchgeführt. RAV repliziert die VM parallel und hält sie bis zum Umschaltfenster synchron. Während des Umschaltvorgangs wird jeweils eine VM migriert, ohne dass es zu Ausfallzeiten für die VM kommt.

Der folgende Screenshot zeigt das Migrationsprofil als Replication Assisted vMotion.



Die Dauer der Replikation kann im Vergleich zur vMotion einer kleinen Anzahl von VMs länger sein. Synchronisieren Sie mit RAV nur die Deltas und schließen Sie den Speicherinhalt ein. Nachfolgend sehen Sie einen Screenshot des Migrationsstatus. Er zeigt, dass die Startzeit der Migration für jede VM gleich ist, die Endzeit jedoch unterschiedlich ist.



Weitere Informationen zu den HCX-Migrationsoptionen und zur Migration von Workloads von lokalen

Standorten zu VMware Cloud on AWS mithilfe von HCX finden Sie im "VMware HCX-Benutzerhandbuch" .

VMware HCX vMotion erfordert eine Durchsatzkapazität von 100 Mbit/s oder mehr.

Der Zieldatenspeicher von VMC FSx ONTAP muss über ausreichend Speicherplatz für die Migration verfügen.

Abschluss

Unabhängig davon, ob Sie eine reine Cloud oder eine Hybrid-Cloud anstreben und Ihre Daten sich auf Speichersystemen beliebiger Art/Anbieter vor Ort befinden, bieten Amazon FSx ONTAP und HCX hervorragende Optionen zum Bereitstellen und Migrieren der Workloads bei gleichzeitiger Reduzierung der Gesamtbetriebskosten, indem die Datenanforderungen nahtlos in die Anwendungsebene integriert werden. Wählen Sie für jeden Anwendungsfall VMC zusammen mit dem FSx ONTAP -Datenspeicher, um die Vorteile der Cloud schnell zu nutzen, eine konsistente Infrastruktur und Vorgänge vor Ort und in mehreren Clouds zu nutzen, Workloads in beide Richtungen zu portieren und Kapazität und Leistung auf Unternehmensniveau zu erreichen. Es handelt sich um denselben bekannten Prozess und dieselben bekannten Verfahren, die zum Verbinden des Speichers und Migrieren von VMs mithilfe der VMware vSphere-Replikation, VMware vMotion oder sogar NFC-Kopie verwendet werden.

Imbiss

Zu den wichtigsten Punkten dieses Dokuments gehören:

- Sie können jetzt Amazon FSx ONTAP als Datenspeicher mit VMC SDDC verwenden.
- Sie können Daten problemlos von jedem lokalen Rechenzentrum zu VMC migrieren, das mit FSx ONTAP -Datenspeicher läuft
- Sie können den FSx ONTAP Datenspeicher problemlos vergrößern und verkleinern, um die Kapazitäts- und Leistungsanforderungen während der Migrationsaktivität zu erfüllen.

Wo Sie weitere Informationen finden

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

- VMware Cloud-Dokumentation

  "https://docs.vmware.com/en/VMware-Cloud-on-AWS/"

- Amazon FSx ONTAP Dokumentation

  "https://docs.aws.amazon.com/fsx/latest/ONTAPGuide"

  VMware HCX-Benutzerhandbuch

- "https://techdocs.broadcom.com/us/en/vmware-cis/hcx/vmware-hcx/4-10/vmware-hcx-user-guide-4-10.html"

Copyright-Informationen

Copyright © 2025 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.