



Migrating Workloads on GCP / GCVE

NetApp Solutions

NetApp
July 31, 2024

Table of Contents

- Migrating Workloads on GCP / GCVE 1
 - Migrate workloads to NetApp Cloud Volume Service datastore on Google Cloud VMware Engine using VMware HCX - Quickstart guide 1
 - VM Migration to NetApp Cloud Volume Service NFS Datastore on Google Cloud VMware Engine using Veeam Replication feature 16

Migrating Workloads on GCP / GCVE

Migrate workloads to NetApp Cloud Volume Service datastore on Google Cloud VMware Engine using VMware HCX - Quickstart guide

One of the most common use cases for the Google Cloud VMware Engine and Cloud Volume Service datastore is the migration of VMware workloads. VMware HCX is a preferred option and provides various migration mechanisms to move on-premises virtual machines (VMs) and its data to Cloud Volume Service NFS datastores.

Author(s): NetApp Solutions Engineering

Overview: Migrating virtual machines with VMware HCX, NetApp Cloud Volume Service datastores, and Google Cloud VMware Engine (GCVE)

VMware HCX is primarily a migration platform that is designed to simplify application migration, workload rebalancing, and even business continuity across clouds. It is included as part of Google Cloud VMware Engine Private Cloud and offers many ways to migrate workloads and can be used for disaster recovery (DR) operations.

This document provides step-by-step guidance for provisioning Cloud Volume Service datastore followed by downloading, deploying, and configuring VMware HCX, including all its main components in on-premises and the Google Cloud VMware Engine side including Interconnect, Network Extension, and WAN optimization for enabling various VM migration mechanisms.



VMware HCX works with any datastore type as the migration is at the VM level. Hence this document is applicable to existing NetApp customers and non-NetApp customers who are planning to deploy Cloud Volume Service with Google Cloud VMware Engine for a cost-effective VMware cloud deployment.

High-level steps

This list provides the high-level steps necessary to pair & Migrate the VMs to HCX Cloud Manager on the Google Cloud VMware Engine side from HCX Connector on-premises:

1. Prepare HCX through the Google VMware Engine portal.
2. Download and deploy the HCX Connector Open Virtualization Appliance (OVA) installer in the on-premises VMware vCenter Server.
3. Activate HCX with the license key.
4. Pair the on-premises VMware HCX Connector with Google Cloud VMware Engine HCX Cloud Manager.
5. Configure the network profile, compute profile, and service mesh.
6. (Optional) Perform network extension to avoid re-IP during migrations.
7. Validate the appliance status and ensure that migration is possible.
8. Migrate the VM workloads.

Prerequisites

Before you begin, make sure the following prerequisites are met. For more information, see this [link](#). After the prerequisites, including connectivity, are in place, download HCX license key from the Google Cloud VMware Engine portal. After the OVA installer is downloaded, proceed with the installation process as described below.

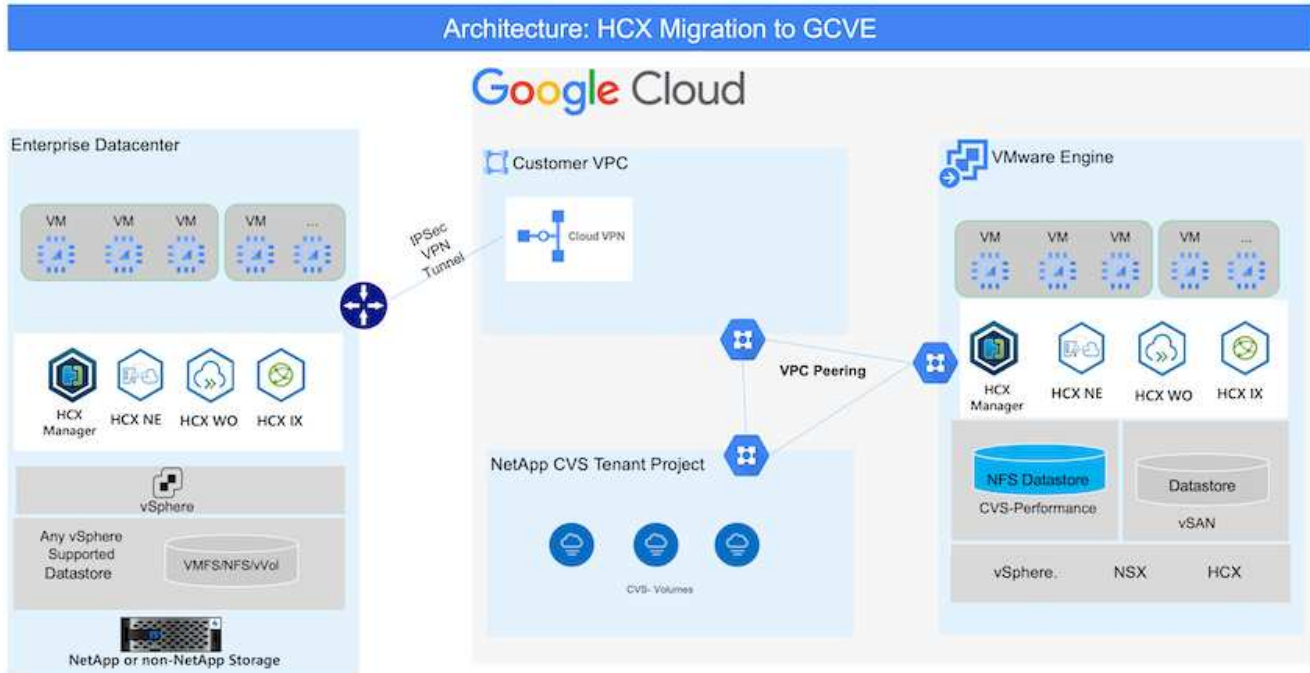


HCX advanced is the default option and VMware HCX Enterprise edition is also available through a support ticket and supported at no additional cost. Refer [this link](#)

- Use an existing Google Cloud VMware Engine software-defined data center (SDDC) or create a private cloud by using this [NetApp link](#) or this [Google link](#).
- Migration of VMs and associated data from the on-premises VMware vSphere-enabled data center requires network connectivity from the data center to the SDDC environment. Before migrating workloads, [set up a Cloud VPN or Cloud Interconnect connection](#) between the on-premises environment and the respective private cloud.
- The network path from on-premises VMware vCenter Server environment to the Google Cloud VMware Engine private cloud must support the migration of VMs by using vMotion.
- Make sure the required [firewall rules and ports](#) are allowed for vMotion traffic between the on-premises vCenter Server and SDDC vCenter.
- Cloud Volume Service NFS volume should be mounted as a datastore in Google Cloud VMware Engine. Follow the steps detailed in this [link](#) to attach Cloud Volume Service datastores to Google Cloud VMware Engines hosts.

High Level Architecture

For testing purposes, the lab environment from on-premises used for this validation was connected through a Cloud VPN, which allows on-premises connectivity to Google Cloud VPC.



For more detailed diagram on HCX, please refer [VMware link](#)

Solution Deployment

Follow the series of steps to complete the deployment of this solution:

Step 1: Prepare HCX through the Google VMware Engine Portal

HCX Cloud Manager component automatically gets installed as you provision private cloud with VMware Engine. To prepare for site pairing, complete the following steps:

1. Log in to the Google VMware Engine Portal and sign-in to the HCX Cloud Manager.

You can login to HCX Console either by clicking on the HCX version link
image::gcpd-hcx-image2.png[HCX Console access with link on GCVE resource]
or clicking on HCX FQDN under vSphere Management Network tab.
image::gcpd-hcx-image3.png[HCX Console access with FQDN link]

2. In HCX Cloud Manager, go to **Administration > System Updates**.
3. Click **Request download link** and download the OVA file.
image::gcpd-hcx-image4.png[Request download link]
4. Update HCX Cloud Manager to the latest version available from the HCX Cloud Manager UI.

Step 2: Deploy the installer OVA in the on-premises vCenter Server

For the on-premises Connector to connect to the HCX Manager in Google Cloud VMware Engine, make sure the appropriate firewall ports are open in the on-premises environment.

To download and install HCX Connector in the on-premises vCenter Server, complete the following steps:

1. Have the ova downloaded from the HCX Console on Google Cloud VMware Engine as stated in previous step.
2. After the OVA is downloaded, deploy it on to the on-premises VMware vSphere environment by using the **Deploy OVF Template** option.

The screenshot shows the 'Deploy OVF Template' wizard in vSphere. The wizard is at step 1: 'Select an OVF template'. The left sidebar shows the progress: 1. Select an OVF template (selected), 2. Select a name and folder, 3. Select a compute resource, 4. Review details, 5. Select storage, 6. Ready to complete. The main area is titled 'Select an OVF template' and contains the following text: 'Select an OVF template from remote URL or local file system. Enter a URL to download and install the OVF package from the internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.' There are two radio buttons: 'URL' (unselected) and 'Local file' (selected). Below the radio buttons is a text input field with the placeholder 'http://remoteserver-address/filetoinstall.ovf'. Below the input field is an 'UPLOAD FILES' button and a file name 'VMware-HCX-Connector-4.5.2.0-20914338.ova'. At the bottom right, there are 'CANCEL' and 'NEXT' buttons.

3. Enter all the required information for the OVA deployment, click **Next**, and then click **Finish** to deploy the VMware HCX connector OVA.



Power on the virtual appliance manually.

For step-by-step instructions, see the [VMware HCX User Guide](#).

Step 3: Activate HCX Connector with the license key

After you deploy the VMware HCX Connector OVA on-premises and start the appliance, complete the following steps to activate HCX Connector. Generate the license key from the Google Cloud VMware Engine portal and activate it in VMware HCX Manager.

1. From the VMware Engine portal, Click on Resources, select the private cloud, and **click on download icon under HCX Manager Cloud Version.**

image::gcpd-hcx-image6.png[Download HCX License]

Open Downloaded file and copy the License Key String.

2. Log into the on-premises VMware HCX Manager at "`https://hcxmanagerIP:9443`" using administrator credentials.



Use the hcxmanagerIP and password defined during the OVA deployment.

3. In the licensing, enter the key copied from step 3 and click **Activate**.



The on-premises HCX Connector should have internet access.

4. Under **Datacenter Location**, provide the nearest location for installing the VMware HCX Manager on-premises. Click **Continue**.

5. Under **System Name**, update the name and click **Continue**.

6. Click **Yes, Continue**.

7. Under **Connect your vCenter**, provide the fully qualified domain name (FQDN) or IP address of vCenter Server and the appropriate credentials and click **Continue**.



Use the FQDN to avoid connectivity issues later.

8. Under **Configure SSO/PSC**, provide the Platform Services Controller's(PSC) FQDN or IP address and click **Continue**.



For Embedded PSC, Enter the VMware vCenter Server FQDN or IP address.

9. Verify that the information entered is correct and click **Restart**.

10. After the services restart, vCenter Server is displayed as green on the page that appears. Both vCenter Server and SSO must have the appropriate configuration parameters, which should be the same as the previous page.



This process should take approximately 10 to 20 minutes and for the plug-in to be added to the vCenter Server.

HCX-RTP

IP Address: 172.21.254.155
Version: 4.5.2.0
Uptime: 13 days, 21 hours, 6 minutes
Current Time: Thursday, 16 February 2023 05:59:00 PM UTC



NSX

MANAGE

vCenter

<https://a300-vcsa01.ehcdc.com>

MANAGE

SSO

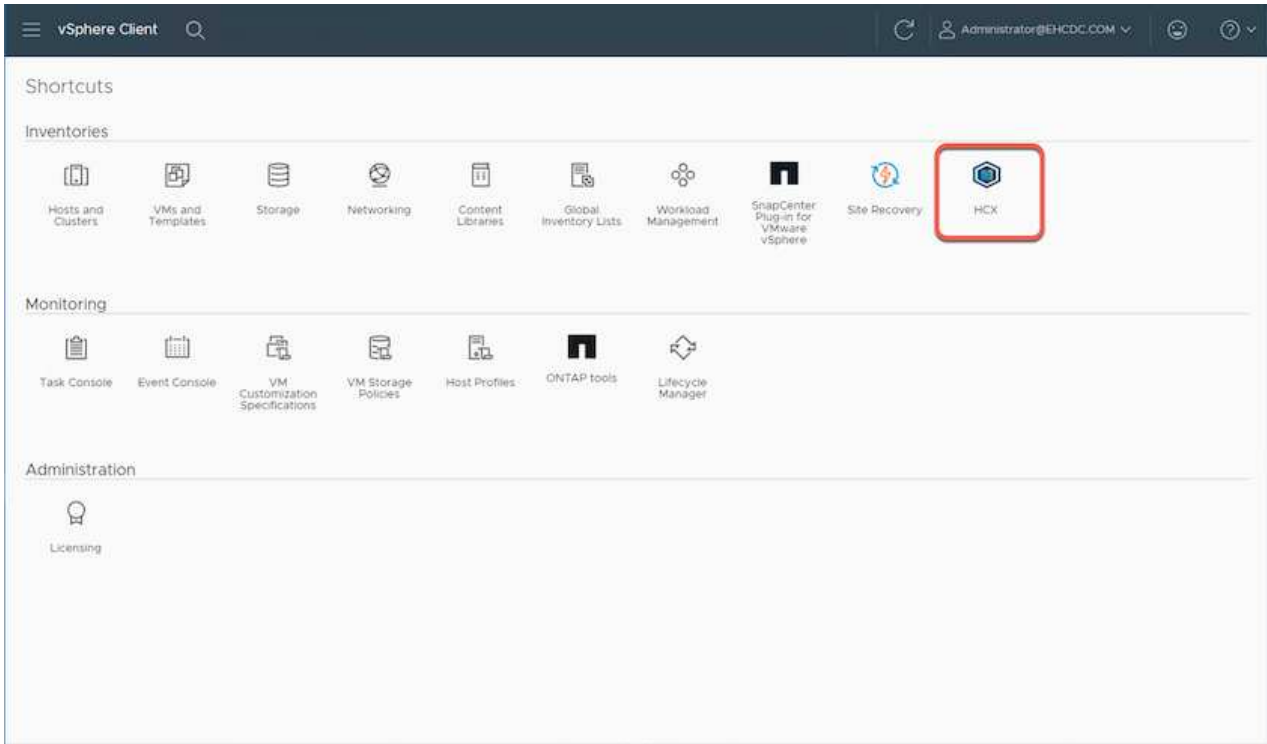
<https://a300-vcsa01.ehcdc.com>

MANAGE

Step 4: Pair on-premises VMware HCX Connector with Google Cloud VMware Engine HCX Cloud Manager

After HCX Connector is deployed and configured on on-premises vCenter, establish connection to Cloud Manager by adding the pairing. To configure the site pairing, complete the following steps:

1. To create a site pair between the on-premises vCenter environment and Google Cloud VMware Engine SDDC, log in to the on-premises vCenter Server and access the new HCX vSphere Web Client plug-in.



2. Under Infrastructure, click **Add a Site Pairing**.



Enter the Google Cloud VMware Engine HCX Cloud Manager URL or IP address and the credentials for user with Cloud-Owner-Role privileges for accessing the private cloud.

Connect to Remote Site



Remote HCX URL

https://hcx-58042.f7458c8f.europe-west3.g



Username

cloudowner@gve.local



Password

.....

CANCEL

CONNECT

3. Click **Connect**.





VMware HCX Connector must be able to route to HCX Cloud Manager IP over port 443.

4. After the pairing is created, the newly configured site pairing is available on the HCX Dashboard.

vSphere Client Administrator@EHCDC.COM

Site Pairing

ADD A SITE PAIRING

 HCX-RTP https://172.21254.155.443 Durham	→	 hcx-58042.f7458c8f.europe-west3.gve.goog-cloud https://10.0.16.13 Frankfurt
--	---	--

1 Interconnect(s)

EDIT CONNECTION DISCONNECT

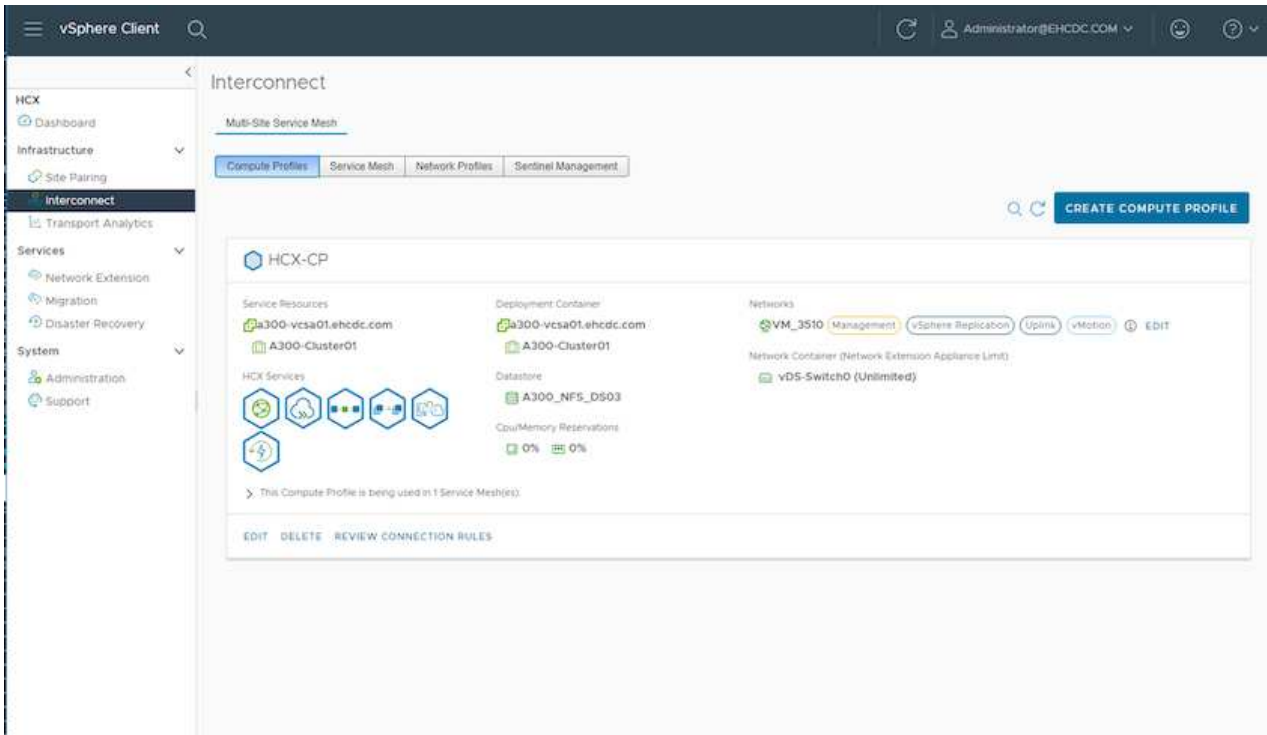
Step 5: Configure the network profile, compute profile, and service mesh

The VMware HCX Interconnect service appliance provides replication and vMotion-based migration capabilities over the internet and private connections to the target site. The interconnect provides encryption, traffic engineering, and VM mobility. To create an Interconnect service appliance, complete the followings steps:

1. Under Infrastructure, select **Interconnect > Multi-Site Service Mesh > Compute Profiles > Create Compute Profile**.



The compute profiles define the deployment parameters including the appliances that are deployed and which portion of the VMware data center are accessible to HCX service.

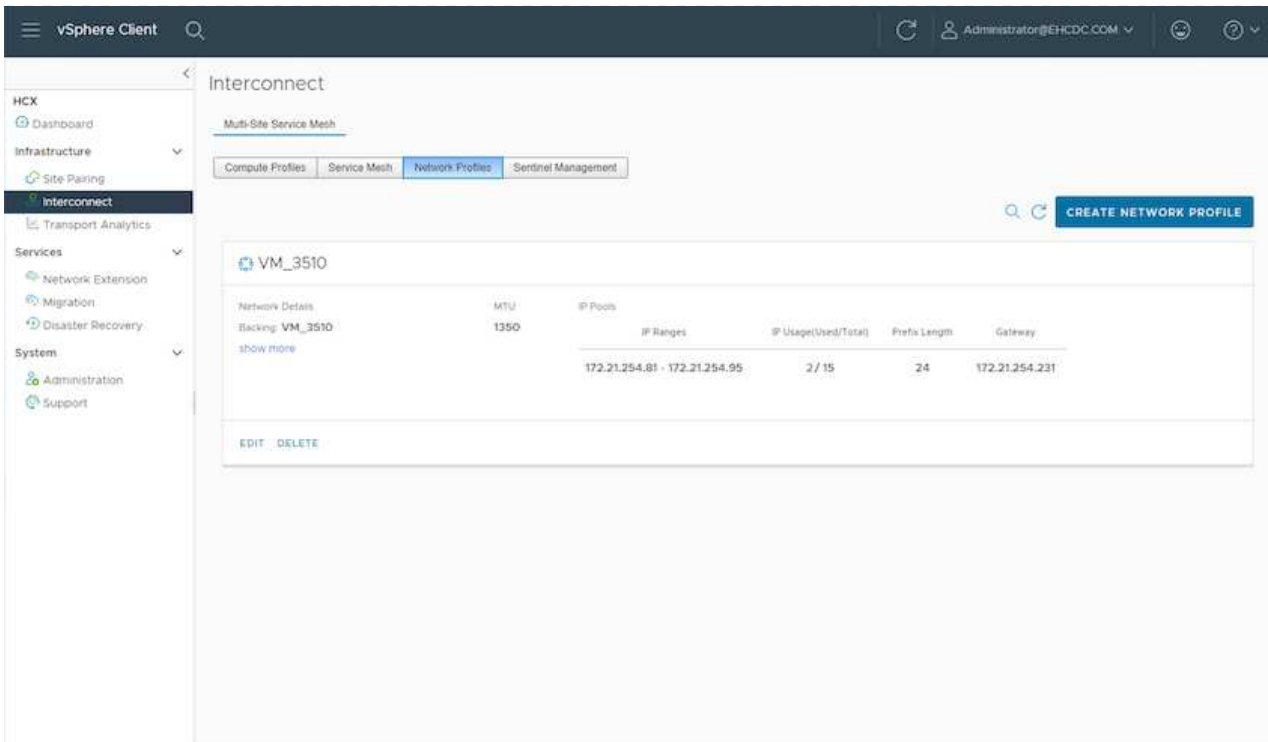


2. After the compute profile is created, create the network profiles by selecting **Multi-Site Service Mesh > Network Profiles > Create Network Profile**.

The network profile defines a range of IP address and networks that are used by HCX for its virtual appliances.



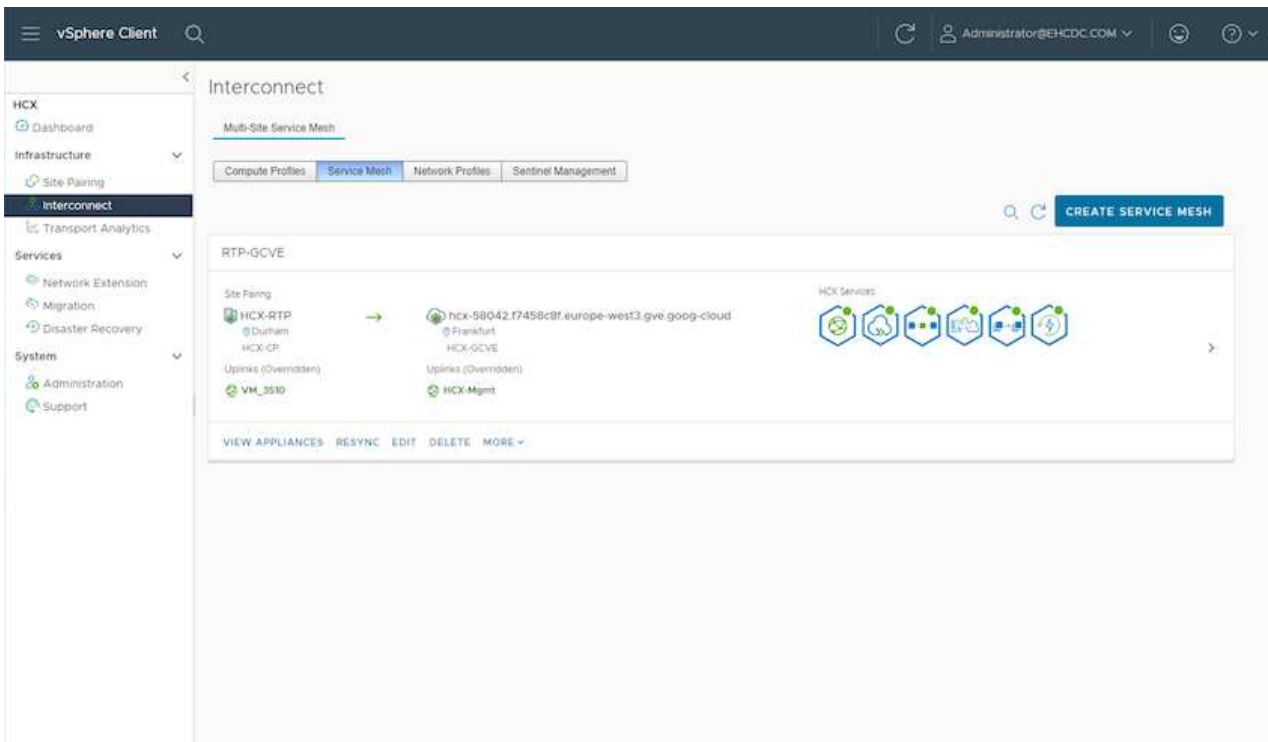
This step requires two or more IP addresses. These IP addresses are assigned from the management network to the Interconnect Appliances.



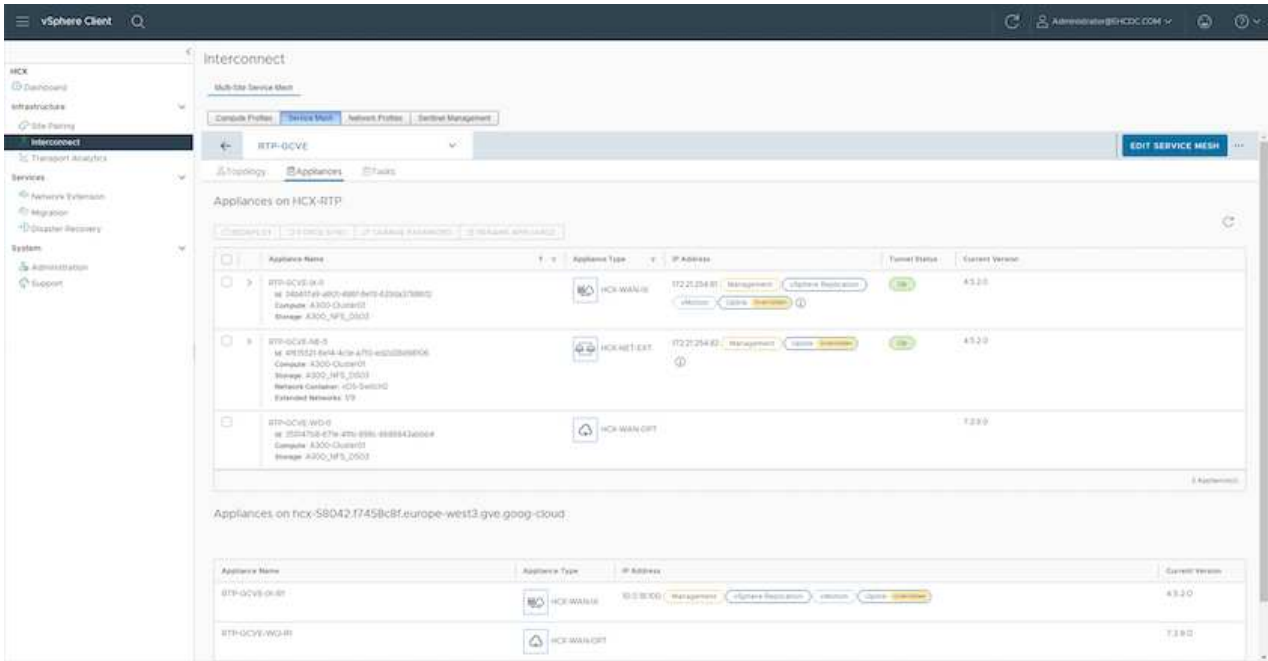
3. At this time, the compute and network profiles have been successfully created.
4. Create the Service Mesh by selecting the **Service Mesh** tab within the **Interconnect** option and select the on-premises and GCVE SDDC sites.
5. The Service Mesh specifies a local and remote compute and network profile pair.



As part of this process, the HCX appliances are deployed and automatically configured on both the source and target sites in order to create a secure transport fabric.



6. This is the final step of configuration. This should take close to 30 minutes to complete the deployment. After the service mesh is configured, the environment is ready with the IPsec tunnels successfully created to migrate the workload VMs.



Step 6: Migrate workloads

Workloads can be migrated bidirectionally between on-premises and GCVE SDDCs using various VMware HCX migration technologies. VMs can be moved to and from VMware HCX-activated entities using multiple migration technologies such as HCX bulk migration, HCX vMotion, HCX Cold migration, HCX Replication Assisted vMotion (available with HCX Enterprise edition), and HCX OS Assisted Migration (available with the HCX Enterprise edition).

To learn more about various HCX migration mechanisms, see [VMware HCX Migration Types](#).

The HCX-IX appliance uses the Mobility Agent service to perform vMotion, Cold, and Replication Assisted vMotion (RAV) migrations.



The HCX-IX appliance adds the Mobility Agent service as a host object in the vCenter Server. The processor, memory, storage and networking resources displayed on this object do not represent actual consumption on the physical hypervisor hosting the IX appliance.

HCX vMotion

This section describes the HCX vMotion mechanism. This migration technology uses the VMware vMotion protocol to migrate a VM to GCVE. The vMotion migration option is used for migrating the VM state of a single VM at a time. There is no service interruption during this migration method.



Network Extension should be in place (for the port group in which the VM is attached) in order to migrate the VM without the need to make an IP address change.

1. From the on-premises vSphere client, go to Inventory, right-click on the VM to be migrated, and select HCX Actions > Migrate to HCX Target Site.

The screenshot shows the vSphere Client interface for a VM named 'Move2GCVE'. The 'Actions' menu is open, and the 'Migrate to HCX Target Site' option is highlighted with a red box. The VM details panel shows the following information:

- Guest OS: VMware (Motion OS (64-bit))
- Compatibility: ESX-6.7 and later (VM version 16)
- VMware Tools: Running, version 1033 (Guest Managed)
- MOSE NPID: MOSE-NPID
- Phone ID: phone-01
- IP Address: 172.20.203.8
- VMX File: 2 IP ADDRESS02
- Host: 4300-xxxx@hcx.com

The 'Details' tab shows the following information:

- VCPU(s): 2 DR, 0 DR memory active
- RAM: 2 GB
- VM ID(s): VM_3500 (xxxxxxxx)
- Disconnection: Disconnected
- RAM: 4 MB
- Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
- Additional Hardware: ESX-6.7 and later (VM version 16)
- Host: 4300-Cluster01
- Host: 4300-xxxx@hcx.com
- Host: VM_3500
- Host: 4300-NPI_0003

The 'Recent Tasks' table shows the following information:

Task Name	Target	Status	Start Time	Completion Time	Owner
Power On virtual machine	vSAN	Completed	03/16/2023, 2:30:50	03/16/2023, 2:32:51 PM	4300-xxxx@hcx.com
Instance provisioning on	NetApp ONTAP tools	Completed	03/16/2023, 2:30:50	03/16/2023, 2:30:50	4300-xxxx@hcx.com
Move into resource pool	NetApp SnapCenter	Completed	03/16/2023, 2:30:33 F.	03/16/2023, 2:30:33 H.	4300-xxxx@hcx.com
Reconfigure virtual machi...	All Site Security actions	Completed	03/16/2023, 2:30:19 PM	03/16/2023, 2:30:30	4300-xxxx@hcx.com

2. In the Migrate Virtual Machine wizard, select the Remote Site Connection (target GCVE).

HCX: Migrate Virtual Machine

Remote Site Connection:

Source: HCX-RTP / VC: a300-vcsa01.ehcdc.com
Destination: hcx-58042.f7458c8f.europe-west3.gve.goog-cloud / VC: vcsa-57901.f7458c8f.europe-west3.gve.goog

Transfer and Placement:

(Mandatory: Compute Container) (Mandatory: Storage) (Migration Profile)
(Specify Destination Folder) Same format as source (Optional: Switchover Schedule)

Switchover:

Extended Options:
Edit Extended Options

VM for Migration	Disk / Memory / vCPU	Migration Info
Move2GCVE	2 GB / 2 GB / 1 vCPU	(Migration profile is not specified)

GO VALIDATE CLOSE

3. Update the mandatory fields (Cluster, Storage, and Destination Network), Click Validate.

HCX: Migrate Virtual Machine

Remote Site Connection:

Source: HCX-RTP / VC: a300-vcsa01.ehcdc.com
Destination: hcx-58042.f7458c8f.europe-west3.gve.goog-cloud / VC: vcsa-57901.f7458c8f.europe-west3.gve.goog

Transfer and Placement:

Workload: gcp-ve-4 (807.6 GB / 1 TB) vMotion
(Specify Destination Folder) Same format as source (Optional: Switchover Schedule)

Switchover:

Extended Options:
Edit Extended Options Retain MAC

VM for Migration	Disk / Memory / vCPU	Migration Info
Move2GCVE	2 GB / 2 GB / 1 vCPU	vMotion

Force Power-off VM
Enable Seed Checkpoint
Edit Extended Options Retain MAC

Network adapter 1 (VM_3509) → L2E_VM_3509-3509-a0041a8d

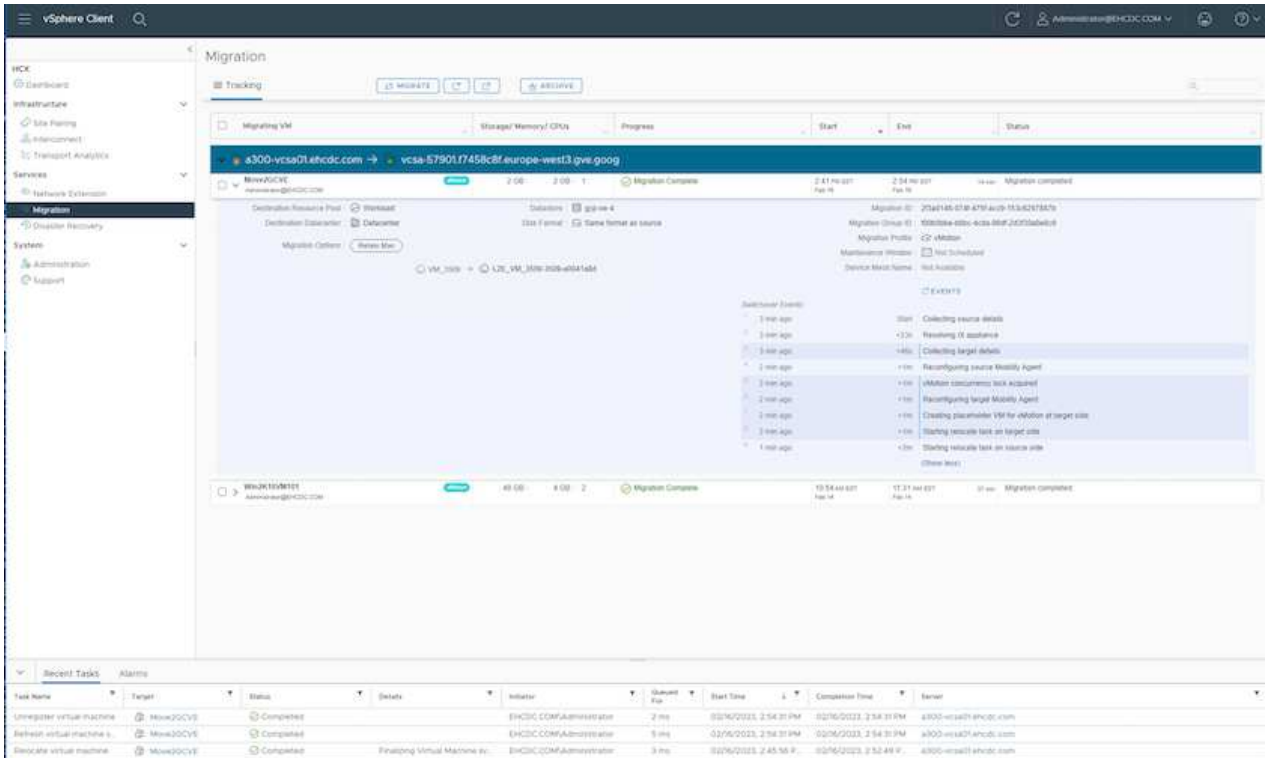
GO VALIDATE CLOSE

4. After the validation checks are complete, click Go to initiate the migration.



The vMotion transfer captures the VM active memory, its execution state, its IP address, and its MAC address. For more information about the requirements and limitations of HCX vMotion, see [Understanding VMware HCX vMotion and Cold Migration](#).

5. You can monitor the progress and completion of the vMotion from the HCX > Migration dashboard.



The target CVS NFS datastore should have sufficient space to handle the migration.

Conclusion

Whether you're targeting all-cloud or hybrid cloud and data residing on any type/vendor storage in on-premises, Cloud Volume Service and HCX provide excellent options to deploy and migrate the application workloads while reducing the TCO by making the data requirements seamless to the application layer. Whatever the use case, choose Google Cloud VMware Engine along with Cloud Volume Service for rapid realization of cloud benefits, consistent infrastructure, and operations across on-premises and multiple clouds, bidirectional portability of workloads, and enterprise-grade capacity and performance. It is the same familiar process and procedures used to connect the storage and migrate VMs using VMware vSphere Replication, VMware vMotion, or even network file copy (NFC).

Takeaways

The key points of this document include:

- You can now use Cloud Volume Service as a datastore on Google Cloud VMware Engine SDDC.
- You can easily migrate data from on-premises to Cloud Volume Service datastore.
- You can easily grow and shrink the Cloud Volume Service datastore to meet the capacity and performance requirements during migration activity.

Videos from Google and VMware for reference

From Google

- [Deploy HCX Connector with GCVE](#)
- [Configure HCX ServiceMesh with GCVE](#)
- [Migrate VM with HCX to GCVE](#)

From VMware

- [HCX Connector deployment for GCVE](#)
- [HCX ServiceMesh configuration for GCVE](#)
- [HCX Workload Migration to GCVE](#)

Where to find additional information

To learn more about the information described in this document, refer to the following website links:

- Google Cloud VMware Engine documentation

<https://cloud.google.com/vmware-engine/docs/overview>

- Cloud Volume Service documentation

<https://cloud.google.com/architecture/partners/netapp-cloud-volumes>

- VMware HCX User Guide

<https://docs.vmware.com/en/VMware-HCX/index.html>

VM Migration to NetApp Cloud Volume Service NFS Datastore on Google Cloud VMware Engine using Veeam Replication feature

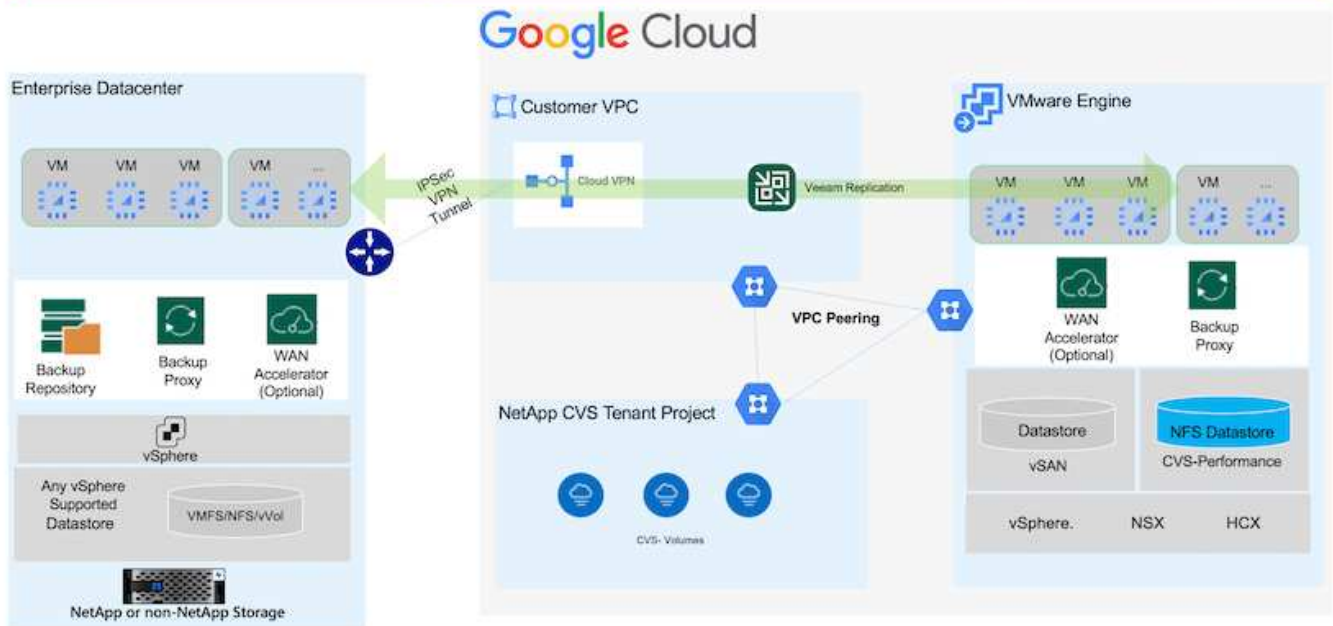
Customers who currently use Veeam for their data protection requirements continue using that solution to migrate the workloads to GCVE and enjoy the benefits of NetApp Cloud Volume Service NFS Datastores.

Overview

Authors: Suresh Thoppay, NetApp

VM Workloads running on VMware vSphere can be migrated to Google Cloud VMware Engine (GCVE) utilizing Veeam Replication feature.

This document provides a step-by-step approach for setting up and performing VM migration that uses NetApp Cloud Volume Service, Veeam, and the Google Cloud VMware Engine (GCVE).



Assumptions

This document assumes you have either Google Cloud VPN or Cloud Interconnect or other networking option in place to establish network connectivity from existing vSphere servers to Google Cloud VMware Engine.



There are multiple options for connecting on-premises datacenters to Google Cloud, which prevents us from outlining a specific workflow in this document. Refer to the [Google Cloud documentation](#) for the appropriate on-premises-to-Google connectivity method.

Deploying the Migration Solution

Solution Deployment Overview

1. Make sure NFS datastore from NetApp Cloud Volume Service is mounted on GCVE vCenter.
2. Ensure Veeam Backup Recovery is deployed on existing VMware vSphere environment
3. Create Replication Job to start replicating virtual machines to Google Cloud VMware Engine instance.
4. Perform Failover of Veeam Replication Job.
5. Perform Permanent Failover on Veeam.

Deployment Details

Make sure NFS datastore from NetApp Cloud Volume Service is mounted on GCVE vCenter

Login to GCVE vCenter and ensure NFS datastore with sufficient space is available. If not, Please refer [Mount NetApp CVS as NFS datastore on GCVE](#)

Ensure Veeam Backup Recovery is deployed on existing VMware vSphere environment

Please refer [Veeam Replication Components](#) documentation to install required components.

Create Replication Job to start replicating virtual machines to Google Cloud VMware Engine instance.

Both on-premises vCenter and GCVE vCenter needs to be registered with Veeam. [Setup vSphere VM Replication Job](#)

Here is a video explaining how to [Configure Replication Job](#).



Replica VM can have different IP from the source VM and can also be connected to different port group. For more details, check the video above.

Perform Failover of Veeam Replication Job

To Migrate VMs, perform [Perform Failover](#)

Perform Permanent Failover on Veeam.

To treat GCVE as your new source environment, perform [Permanent Failover](#)

Benefits of this solution

- Existing Veeam backup infrastructure can be utilized for migration.
- Veeam Replication allows changing VM IP addresses on target site.
- Has ability to remap existing data replicated outside of Veeam (like replicated data from BlueXP)
- Has ability to specify different network portgroup on target site.
- Can specify the order of VMs to power on.
- Utilizes VMware Change Block Tracking to minimize the amount of data to send across WAN.
- Capability to execute pre and post scripts for replication.
- Capability to execute pre and post scripts for snapshots.

Copyright information

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.