VMware HCX on IBM Cloud
Solution Architecture

Date: 1/29/2018
Version 1.1
Table of Contents

1 Introduction ........................................................................................................................................... 7
  1.1 VMware HCX on IBM Cloud ........................................................................................................... 7

2 VMware HCX on IBM Cloud Overview .................................................................................................. 9
  2.1 Layer 2 Network Extension ............................................................................................................. 9
  2.2 Virtual Machine Migration ............................................................................................................. 9
    2.2.1 Low-Downtime Migration ........................................................................................................... 9
    2.2.2 vMotion Migration .................................................................................................................. 9
    2.2.3 Cold Migration ......................................................................................................................... 9
    2.2.4 Common Migration Features ..................................................................................................... 10
  2.3 Networking ...................................................................................................................................... 10
    2.3.1 Intelligent Flow Routing .......................................................................................................... 10
    2.3.2 Proximity Routing .................................................................................................................... 10
    2.3.3 Security ..................................................................................................................................... 10
  2.4 Components of HCX ....................................................................................................................... 11
    2.4.1 HCX Manager .......................................................................................................................... 11
    2.4.2 Hybrid Cloud Gateway ........................................................................................................... 11
    2.4.3 WAN Optimization .................................................................................................................. 11
    2.4.4 Layer 2 Concentrators ............................................................................................................ 11
  2.5 Deployment Architecture: Connect to IBM Cloud via Public Internet ............................................. 11
    2.5.1 Usage overview ....................................................................................................................... 13
    2.5.2 Base Design Dependencies ...................................................................................................... 13

3 Source Side Architecture ....................................................................................................................... 14
  3.1 Introducing HCX ............................................................................................................................... 14
    3.1.1 Layer 2 Network Extension ...................................................................................................... 14
    3.1.2 Virtual Machine Migration Methods ...................................................................................... 14
    3.1.3 Networking Features ............................................................................................................... 15
    3.1.4 Understanding HCX ................................................................................................................ 15
  3.2 Deployment Overview ...................................................................................................................... 15
    3.2.1 Deployment Component Performance Considerations .......................................................... 16
    3.2.2 Maximum Number of Migration and Network Extension ......................................................... 16
    3.2.3 HCX Management Enterprise ................................................................................................. 16
    3.2.4 HCX Virtual Appliances ......................................................................................................... 17
    3.2.5 HCX Manager .......................................................................................................................... 17
    3.2.6 HCX Cloud Gateway ................................................................................................................. 17
    3.2.7 WAN Optimizer ........................................................................................................................ 18
    3.2.8 Layer 2 Concentrator ................................................................................................................ 19
# Component level Architecture, Target

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.2.9</td>
<td>Migration Only</td>
</tr>
<tr>
<td>3.2.10</td>
<td>IP Address Requirements</td>
</tr>
<tr>
<td>3.2.11</td>
<td>Proximity Routing</td>
</tr>
<tr>
<td>3.2.12</td>
<td>Asymmetric Routing with Proximity Routing Solution</td>
</tr>
<tr>
<td>3.2.13</td>
<td>MAC Address Retention</td>
</tr>
<tr>
<td>3.2.14</td>
<td>Security Policy Migration</td>
</tr>
<tr>
<td>4.1.1</td>
<td>NSX Edge</td>
</tr>
<tr>
<td>4.1.2</td>
<td>HCX Manager</td>
</tr>
<tr>
<td>4.1.3</td>
<td>Cloud Gateway</td>
</tr>
<tr>
<td>4.1.4</td>
<td>WAN Optimizer</td>
</tr>
<tr>
<td>4.1.5</td>
<td>Layer 2 Concentrator</td>
</tr>
</tbody>
</table>

## Appendix A - Port Access Requirements

## Appendix B - Preparing Installation Environment

<table>
<thead>
<tr>
<th>Sub-section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.1</td>
<td>Configure Network Connectivity</td>
</tr>
<tr>
<td>7.2</td>
<td>On Premises</td>
</tr>
<tr>
<td>7.3</td>
<td>Verify Layer 2 Installation Environment</td>
</tr>
</tbody>
</table>

## Appendix C - Installing and Configuring HCX on Source

<table>
<thead>
<tr>
<th>Sub-section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1</td>
<td>Install the HCX Manager Appliance</td>
</tr>
<tr>
<td>8.2</td>
<td>Procedure</td>
</tr>
</tbody>
</table>

## Appendix D - Register HCX Manager with the vCenter

<table>
<thead>
<tr>
<th>Sub-section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.1</td>
<td>Prerequisites</td>
</tr>
<tr>
<td>9.2</td>
<td>Procedure</td>
</tr>
</tbody>
</table>

## Appendix F - Installing and Configuring Hybrid Services

<table>
<thead>
<tr>
<th>Sub-section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1</td>
<td>Installing and Configuring Hybrid Services</td>
</tr>
<tr>
<td>10.2</td>
<td>Configuration Overview</td>
</tr>
<tr>
<td>10.3</td>
<td>Start Hybrid Service Virtual Appliance Installation and Configuration</td>
</tr>
<tr>
<td>10.4</td>
<td>Configure the Hybrid Cloud Gateway</td>
</tr>
<tr>
<td>10.5</td>
<td>Configure the Network Extension Service</td>
</tr>
<tr>
<td>10.6</td>
<td>Monitor Service Appliance Deployment</td>
</tr>
<tr>
<td>10.7</td>
<td>View Tunnel Status</td>
</tr>
<tr>
<td>10.8</td>
<td>Stretching a Layer 2 Network to IBM Cloud</td>
</tr>
</tbody>
</table>

## Appendix G - Migrating a Virtual Machine

<table>
<thead>
<tr>
<th>Sub-section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1</td>
<td>Migrating a Virtual Machine (VM)</td>
</tr>
<tr>
<td>11.2</td>
<td>Low Down-Time Migration</td>
</tr>
<tr>
<td>11.3</td>
<td>No downtime vMotion</td>
</tr>
</tbody>
</table>
11.4 Cold Migration .......................................................... 46
11.5 Migrate Virtual Machine using bi-directional Wizard .................................. 47
11.6 Checking Your Virtual Machine before Migration .................................. 47
11.7 Monitor a Migration .................................................................................. 47
11.8 View Migrated Virtual Machine ................................................................ 48
12 Appendix H - Modifying or Uninstalling HCX .............................................. 49
12.1 Modifying or Uninstalling HCX ................................................................. 49
12.2 Unstretch a Layer 2 Network .................................................................. 49
12.3 Uninstall HCX Virtual Appliances ............................................................ 49
12.4 Uninstall HCX Manger ............................................................................ 50
12.5 Login to the HCX Management Portal ..................................................... 50
13 Appendix I - Troubleshooting .................................................................. 51
13.1 Troubleshooting ....................................................................................... 51
13.2 Cloud Registration Fails .......................................................................... 51
13.3 Duplicate MAC Address ......................................................................... 51
13.4 High Host Resource Consumption ......................................................... 51

Table of Figures

Figure 1 VMware Cloud Foundation – Hybrid Cloud Services ....................... Error! Bookmark not defined.
Figure 2 Hybrid Cloud Services with single source ......................................... 12
Figure 3 Hybrid Cloud Services with multiple sources .................................... 12
Figure 4 Source Hybrid Cloud Services ............................................................ 17
Figure 5 Source Cloud Gateway ..................................................................... 18
Figure 6 Source WAN Optimizer ................................................................... 19
Figure 7 Source L2 Concentrator ................................................................... 20
Figure 8 VIP Configuration for NSX Edge ....................................................... 25
Figure 9 Pool Configuration for NSX Edge ....................................................... 25
Figure 10 Target - Hybrid Cloud Services Appliance ....................................... 26
Figure 11 Cloud Gateway Deployment ............................................................ 27
Figure 12 WAN Optimizer Deployment .......................................................... 28
Figure 13 L2 Concentrator Deployment .......................................................... 29

List of Tables

Table 1 NSX Edge Deployment ........................................................................ 24
Table 2 NSX Edge Anti-Affinity Rules ............................................................... 24
Table 3 Cloud Gateway Deployment ................................................................. 26
Table 4 WAN Optimization Appliance Sizing .................................................... 27
Table 5 HT L2C Appliance Sizing .................................................................... 29
### Summary of Changes

This section records the history of significant changes to this document.

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Authors</th>
<th>Description of Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>9/11/2017</td>
<td>IBM Cloud VMware Architecture Team</td>
<td>Initial Draft</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Daniel de Araujo</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Frank Chodacki</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Bob Kellenberger</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Simon Kofkin-Hansen</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Jack Benney</td>
<td></td>
</tr>
<tr>
<td>1.1</td>
<td>1/29/2018</td>
<td>IBM Cloud VMware Architecture Team</td>
<td>Updated to reflect GA delivery</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Daniel de Araujo, Frank Chodacki, Bob</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Kellenberger, Simon Kofkin-Hansen, Jack</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Benney, Joseph Brown, Scott Moonen, Rob</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Warren</td>
<td></td>
</tr>
</tbody>
</table>
1 Introduction

1.1 VMware HCX on IBM Cloud

The VMware HCX on IBM Cloud service enables creating a seamless connection between IBM Cloud for VMware Solutions instances and an on-premises VMware® virtualized datacenter.

The IBM Cloud for VMware Solutions include fully automated, rapid deployments of either VMware vCenter Server on IBM Cloud (VCS) or VMware Cloud Foundation on IBM Cloud (VCF) configurations in the IBM Cloud. These offerings complement the on-premises infrastructure and allows existing and future workloads to run in the IBM Cloud without conversion using the same tooling, skills, and processes they use on premise. Please visit IBM Architecture Center for the architecture for these offerings.

The VMware HCX on IBM Cloud service takes this hybridity to the next step, blending instances of either VCS or VCF with existing on-premises virtualized datacenters by enabling the creation of seamless network extensions and bi-directional migration of workloads.

The VMware HCX on IBM Cloud components which are deployed as virtual machines in the IBM Cloud VMware target site enable the establishment of a connection with the VMware HCX on IBM Cloud components installed in the peer on-premises source site.

Figure 1 VMware Cloud Foundation – Hybrid Cloud Services

This creates a loosely coupled interconnectivity between on-premises and IBM Cloud and enables capabilities such as:

- Simple interconnectivity – logical network connections are established easily over any physical connection including public internet, private VPN, or direct link
- Layer 2 extension – on-premises networks are extended into the cloud including on-premises subnets and IP addressing
- Encryption – network traffic is securely encrypted between the two sides
- Optimized network – selects the best connection and efficiently floods the connection so that network traffic is moved as fast as possible
- Data deduplication – as much as 50% reduction in network traffic can be achieved
- Intelligent routing – when a workload is moved, proximity routing can change the network path (i.e. gateway) so that network traffic uses the target site gateway and does not “hairpin” back to the originating site
- Zero down time migration – a running system can be moved to (or back from) the cloud using vMotion
- Scheduled migration – any number of virtual machines can be replicated to the destination site and then activated on that site at a designated time replacing the systems running on the originating site
- Migration of security policies – if NSX is used on-premises any security policies, firewalls, etc. are moved along with the workload

This document details the design of the HCX on IBM Cloud service implementation including both the components on the target side IBM Cloud for VMware Solutions instance and as well as the components deployed on the source, on-premises side.
2 VMware HCX on IBM Cloud Overview

VMware HCX on IBM Cloud seamlessly integrates on-premises vSphere® vCenter™ networks into IBM Cloud for VMware Solutions deployments. Hybrid networking extends on-premises vSphere vCenter networks into the IBM Cloud, supporting bidirectional virtual machine (VM) mobility.

HCX owns the source and destination encryption and decryption processes, ensuring consistent security and providing admission for hybrid workflows such as virtual machine migration and network extension. This offering creates an optimized, software-defined WAN to increase stretched network performance, enabling performance approaching LAN speed. HCX also enables bidirectional workload and VMware NSX® security policy migration to the IBM Cloud. HCX integrates with vSphere vCenter and is managed from the vSphere Web Client.

2.1 Layer 2 Network Extension

HCX allows an existing on-premises vSphere estate to securely stretch a network from its on-premises vCenter to an IBM Cloud datacenter running VMware Cloud Foundation or vCenter Server. This feature is enabled by the following:

- HCX provides an appliance called a Layer 2 Concentrator (L2C).
- Extended networks link to IBM Cloud NSX edge appliances deployed on VMware Cloud Foundation or vCenter Server.
- One can deploy multiple standard Layer 2 concentrators to achieve scalability and increase throughput from the on-premises vCenter.
- Virtual machines migrated through the Cloud Gateway and over stretched Layer 2 can retain their IP and MAC addresses.

2.2 Virtual Machine Migration

HCX provides three methods of virtual machines movement: low-downtime migration, vSphere vMotion migration, and cold migration.

2.2.1 Low-Downtime Migration

Low-downtime migration relies on vSphere Replication, which is a distributed technology implemented in the VMware ESX®/ESXi® hypervisor. The on-premises HCX deployment creates a replica of a live virtual machine in the IBM Cloud, and performs a switchover to power off the source virtual machine and power on the migrated virtual machine.

The migration path is always through the Cloud Gateway. The transport can be the Internet, a Layer 2 stretched network, or a Direct Connect line.

A virtual machine can be migrated multiple times in either direction.

2.2.2 vMotion Migration

Live virtual machines can be transferred using vMotion Migration across a network stretched to the IBM Cloud. vMotion migration is also called zero-downtime migration, or cross-cloud vMotion.

2.2.3 Cold Migration

Cold migration provides the ability to transfer a powered-off virtual machine to the IBM Cloud over a stretched network created via the Layer 2 Concentrator.
2.2.4 Common Migration Features

Additional features available across all three types of migration include software-defined WAN optimization which increases migration throughput and speed. Additionally, migration can be scheduled to occur at a specified time and keep its hostname, virtual machine name, or both.

2.3 Networking

The following networking features are built into the Cloud Gateway and the Layer 2 Concentrators.

2.3.1 Intelligent Flow Routing

This feature automatically selects the best connection based on the Internet path, efficiently flooding the entire connection so that workloads are moved as fast as possible. When larger flows, such as backup or replication, cause CPU contention, smaller flows are routed to less busy CPUs, improving performance of interactive traffic.

2.3.2 Proximity Routing

Proximity routing ensures that forwarding between virtual machines connected to stretched and routed networks, both on-premises and in the cloud, is symmetrical. This feature requires Advanced Networks Services with Dynamic Routing configured between the customer premises and the cloud.

When users extend their networks to the cloud, Layer 2 connectivity is stretched onto IBM Cloud networks. However, without route optimization, Layer 3 communication requests must return to the on-premises network origin to be routed. This return trip is called "tromboning" or "hairpinning." Tromboning is inefficient because packets must travel back and forth between the network origin and the Cloud, even when both source and destination virtual machines reside in the Cloud.

In addition to inefficiency, if the forwarding path includes stateful firewalls, or other inline equipment that must see both sides of the connection, communication might fail. Virtual machine communication (without route optimization) failure occurs when the egress path exiting the cloud can be either the stretched Layer 2 network or the Org Routed Network. The on-premises network does not know about the stretched network "shortcut." This problem is called asymmetric routing. The solution is to enable proximity routing so the on-premises network can learn the routes from the IBM Cloud.

The Cloud Gateway maintains an inventory of virtual machines in the cloud. It also understands the virtual machine state, which can be:

- Transferred to the IBM Cloud with vMotion (zero-downtime migration)
- Migrated to the cloud using host-based replication (low-downtime migration).
- Created in the cloud (on a stretched network).

2.3.3 Security

The Cloud Gateway offers Suite B-compliant AES-GCM with IKEv2, AES-NI offload, and flow-based admission control. HCX also owns the source and destination encryption and decryption process, ensuring consistent security and administration for hybrid workflows such as virtual machine migration and network extension. Security policies defined and assigned to a virtual machine on-premises can be migrated with the virtual machine into the IBM Cloud.

Note that policy migration is only available under the following conditions:

- The on-premises data center must be running NSX 6.2.2 or greater.
- In vSphere, the security policy is a single NSX Section which can contain many rules.
- One can name a Set of IP addresses or MAC addresses to participate in the policy. The name of the MAC Set or IP Set cannot exceed 218 characters.
• Supported rules specify Layer 3 IP addresses or IP Sets, or Layer 2 MAC addresses or MAC Sets as the source or destination.

2.4 Components of HCX

The VMware HCX on IBM Cloud service deploys four virtual appliances installed and configured on both the on-premises datacenter as well as the IBM Cloud target. This section describes each of the four required virtual appliances. Optionally, edge devices may be required depending upon the implementation design.

2.4.1 HCX Manager

The HCX Manager virtual appliance is an extension to the on-premises vCenter. It is deployed as a virtual machine and its file structure contains the other hybrid service virtual appliances. The HCX Manager oversees the deployment and configuration of the Cloud Gateway, the Layer 2 Concentrators, and WAN Optimization virtual appliance both on-premises and within the IBM Cloud.

2.4.2 Hybrid Cloud Gateway

The Hybrid Cloud Gateway (CGW) maintains a secure channel between the on-premises vSphere estate and the IBM Cloud. HCX uses strong encryption to bootstrap a site-to-site connection to the IBM Cloud. The secure channel between vSphere and IBM Cloud prevents networking “middle mile” security problems. The Cloud Gateway also incorporates vSphere replication technology to perform bidirectional migration.

2.4.3 WAN Optimization

The WAN Optimization appliance is the component that performs WAN conditioning to reduce effects of latency. It also incorporates Forward Error Correction to negate packet loss scenarios, and deduplication of redundant traffic patterns. Altogether, these reduce bandwidth use and ensure the best use of available network capacity to expedite data transfer to and from the IBM Cloud.

It is important to note that virtual machine migration relies on the combination of Cloud Gateway and WAN Optimization appliance to achieve unparalleled mobility between vSphere on-premises and the IBM Cloud. Additionally, Layer 2 extension benefits from WAN optimization when the data path is routed through the Cloud Gateway.

2.4.4 Layer 2 Concentrators

The Layer 2 concentrators (L2C) appliances allow the extension of a Layer 2 network from the on-premises vSphere data center to the IBM Cloud. The Layer 2 Concentrators have two interfaces:

1. Internal trunk interface: Handles virtual machine traffic on-premises for the extended networks using a translational bridge mapping to a corresponding stretched network in IBM Cloud
2. Uplink interface: HCX uses this interface to send encapsulated overlay traffic to and from IBM Cloud. Application data travels through this interface

2.5 Deployment Architecture: Connect to IBM Cloud via Public Internet

This section describes the layout of the HCX components within the IBM Cloud as well as client on-premises. In this design, the architecture specifies a hub-and-spoke model exists between the source environment and the IBM Cloud. Thus, the source estate serves as the hub with connections to different IBM Cloud environments as shown in Figure 2 HCX with single source.
Note that the source can be placed within the IBM Cloud environment as well; spokes are always cloud deployments within this design as shown in Figure 3 HCX with multiple sources.

---

**Figure 2 HCX with single source**

**Figure 3 HCX with multiple sources**
2.5.1 Usage overview
The following tasks are completed from the vSphere Web Client:
- Deploy the HCX virtual appliances, and configure software-defined WAN components.
- Extend on-premises VLAN and VXLAN networks from on-premises vCenter to Cloud (IBM Cloud).
- Migrate workloads to the cloud and back.

2.5.2 Base Design Dependencies
Before the components are described in more detail, it is imperative to understand the base deployment required as part of this design:

- The source environment must contain a vSphere implementation managed by a vCenter Server. Supported vCenter of 5.5U3 or vCenter 6.0U2 and higher, with ESXi 5.5 or higher is required for Hybrid Cloud Services.
- If NSX is used, version 6.2.2 or higher. NSX is required for policy migration.
- If cross-cloud vMotion is intended, the same affinity restrictions apply across clouds as they do on-premises.
- The source environment must have a method to connect to cloud environments. This includes public Internet access or private connections via IBM Cloud Direct link. Note that connections—other than public Internet—to other cloud vendors will not be discussed.
- The source environment VM’s and networks to be migrated or stretched must be on portgroups within a Virtual Distributed Switch or Cisco Nexus 1000v Virtual Distributed Switch.
- The IBM Cloud must contain at least one instance of either a VMware Cloud Foundation or vCenter Server deployment.
- Sufficient resources for the virtual appliances.
- The networks must permit the appliances to communicate with both local and remote virtual appliances, and other virtual machines.
- Port Access Requirements (Appendix A) lists ports that must be opened so that Hybrid Cloud Services virtual appliances can install successfully.
- A vSphere service account with the Administrator vCenter Server system role assigned to it.
- Enough disk space for installing Hybrid Cloud Services and the associated service appliances.
- Sufficient IP addresses for the on-premises VMs provisioned during the installation.
- If the SSO server is remote, the URL of the vCenter, external SSO Server, or Platform Services Controller (PSC) that runs the external lookup service must be identified. When the HCX service is registered with the vCenter, this URL must be supplied.
3  **Source Side Architecture**

This section describes the architecture of each HCX component deployed in the source environment.

3.1  **Introducing HCX**

HCX technology seamlessly integrates vSphere vCenter networks into IBM Cloud VCF or VCS platforms. Hybrid networking extends on-premises vSphere vCenter networks into IBM Cloud, supporting bidirectional virtual machine (VM) mobility.

This introduction summarizes the tasks which can be accomplished and the features that support and enhance migration and network extension.

- HCX owns the source and destination encryption and decryption processes, ensuring consistent security and providing admission for hybrid workflows such as virtual machine migration and network extension.
- HCX creates an optimized, software-defined WAN to increase stretched network performance, enabling performance approaching LAN speed.
- HCX also enables bidirectional workload and VMware NSX security policy migration to IBM Cloud Networking services.
- HCX integrates with vSphere vCenter and is managed from the vSphere Web Client.

3.1.1  **Layer 2 Network Extension**

- Securely stretch a network from a vCenter to IBM Cloud.
- HCX provides the High Throughput Layer 2 Concentrator (HT L2C).
- Extended networks link to IBM Cloud NSX edge appliances.
- Multiple standard Layer 2 concentrators can be deployed to achieve scalability and increase throughput.
- Virtual machines migrated through the Cloud Gateway and over stretched Layer 2 can retain their IP and MAC addresses.

3.1.2  **Virtual Machine Migration Methods**

- **Low-Downtime Migration**
  - Low-downtime migration relies on vSphere Replication, which is a distributed technology implemented in the VMware ESX/ESXi hypervisor. HCX creates a replica of a live virtual machine, moves it to IBM Cloud, and performs a switchover to power off the source virtual machine and power on the migrated virtual machine.
  - The migration path is always through the Cloud Gateway. The transport can be the Internet, a Layer 2 stretched network, or a Direct Connect line.
  - A virtual machine can be migrated multiple times in either direction.

- **vMotion Migration**
  - Uses vMotion to transfer a live virtual machine across a network stretched to IBM Cloud. vMotion migration is also called zero-downtime migration, or cross-cloud vMotion.

- **Cold Migration**
  - Transfer a powered-off virtual machine to IBM Cloud over a stretched network.
• Common Features
  o Optional software-defined WAN optimization, if installed, increases migration, throughput, and speed.
  o Migration can be scheduled to occur at a specified time.
  o A migrated virtual machine can keep its host name, virtual machine name, or both.

3.1.3 Networking Features

The following networking features are built into the Cloud Gateway and the Layer 2 Concentrators.

Intelligent Flow Routing

Automatically selects the best connection based on the Internet path, efficiently flooding the entire connection so that workloads are moved as fast as possible. When larger flows, such as backup or replication, cause CPU contention, smaller flows are routed to less busy CPUs, improving performance of interactive traffic.

Proximity Routing

Ensures that forwarding between virtual machines connected to stretched and routed networks both on-premises and in the cloud is symmetrical.

Security

The Cloud Gateway offers Suite B-compliant AES-GCM with IKEv2, AES-NI offload, and flow-based admission control.

HCX owns the source and destination encryption and decryption processes, ensuring consistent security and providing admission for hybrid workflows such as virtual machine migration and network extension.

A security policy defined in the on-premises vCenter and assigned to a virtual machine can be migrated with the virtual machine.

3.1.4 Understanding HCX

HCX supports a many-to-many relationship between on-premises vCenters and IBM Cloud. vCenter Server in Linked Mode is supported. This topic provides a high-level overview of how the installer interacts with both the on-premises data center and the IBM Cloud IBM Cloud.

During the installation, the HCX Manager virtual appliance is imported and configured as a plug-in for the on-premises vCenter. This plug-in is then used to configure the Software-Defined WAN service deployment. The automated configuration provisions each hybrid service appliance as a virtual machine in the on-premises vCenter, and deploys a corresponding virtual machine in IBM Cloud IBM Cloud.

A successful deployment requires:
  o Sufficient resources for the virtual appliances.
  o The network must permit the appliances to communicate with both local and remote virtual appliances, and other virtual machines.

3.2 Deployment Overview

The HCX Manager virtual machine is installed first, and it manages the installation of any other service virtual machine appliances on premises and in the cloud.

The following is a summary of the basic installation tasks.
• Obtain Hybrid Cloud Enterprise virtual appliance OVA file
• From the vSphere Web Client, install the HCX Manager service virtual appliance in the on-premises vCenter that connects to IBM Cloud
• From the vSphere Web Client, register an IBM Cloud endpoint with the HCX plug-in. Registration establishes the one-to-one relationship between the on-premises HCX and the HCX instance on IBM Cloud.
• Install and configure the service virtual appliances.
• For each appliance installed on premises, the installer provisions a corresponding service virtual appliance in the target IBM Cloud.
• After the installation, HCX Manager controls both local and remote service virtual appliances. In the IBM Cloud, HCX manages the provisioned Software-Defined WAN components as a service.

3.2.1 Deployment Component Performance Considerations

Architecture planning includes the VMs to be migrated, the networks used for virtual machine traffic, and the networks to be extended. This topic summarizes some maximum and minimum values for the deployment components.

• vSphere vCenter
  • The HCX manager appliance must be installed on the vCenter that requires hybrid services. There can be only one HCX deployment per vCenter. This restriction applies to linked mode: the HCX management appliance is only installed in the primary vCenter. HCX supports up to five registered vCenters (in linked mode).
• Cloud Registrations
  • The maximum number of cloud endpoints is ten. To find the number of endpoints, Hybrid Cloud Services tracks vCenter connections to the cloud.

3.2.2 Maximum Number of Migration and Network Extension

• Max concurrent low downtime migration tasks - 15
• Max concurrent L2C stretching tasks - 1
• Max concurrent vMotion migration tasks - 1

3.2.3 HCX Management Enterprise

The HCX Management Enterprise OVA is deployed on the source environment and registered as a plugin for the vCenter Server managing the source vSphere infrastructure. This plugin is then used to configure the migration and network services required to enable cross cloud migration and L2 network stretching. Note that there can be only one HCX deployment per vCenter. This restriction applies to linked mode: the HCX Manager appliance is only installed in the primary vCenter. The HCX Manager supports up to five registered vCenters (in linked mode).
3.2.4 HCX Virtual Appliances

The installation package is an OVA file containing the Hybrid Cloud Services plug-in. This Hybrid Cloud Services management appliance is installed and configured and then used to configure the service appliance virtual machines.

- HCX Manager
- Hybrid Cloud Gateway
- Layer 2 Concentrators
- WAN Optimizers

3.2.5 HCX Manager

The HCX Manager plug-in is deployed on-premises only. It manages the service virtual appliances for the SD-WAN. The HCX Manager virtual appliance is an extension to the source vCenter and is deployed as a virtual machine. This appliance’s file structure contains all the hybrid service virtual appliances. The HCX Manager oversees the deployment and configuration of the Cloud Gateway, the Layer 2 Concentrators, and WAN Optimization virtual appliance both on-premises and in the cloud.

The virtual appliance can be installed with either thin or thick provisioning for the hard drive. By default, hard drives for the service virtual appliances are thinly provisioned.

After the service, virtual appliance configuration and deployment is done, log in to this virtual machine to use the Hybrid Cloud Services Management Portal.

3.2.6 HCX Cloud Gateway

The HCX Cloud Gateway establishes and maintains a secure channel between vSphere and the IBM Cloud.
HCX uses strong encryption to bootstrap a site-to-site connection to IBM Cloud. The secure channel between vSphere and IBM Cloud achieves multi-tenancy for vSphere protocols that are not tenant-aware, and to prevent networking "middle mile" security problems.

The Cloud Gateway also incorporates vSphere replication technology to perform bidirectional migration.

**Figure 5 Source Cloud Gateway**

3.2.7 WAN Optimizer

HCX also provides software-defined WAN Optimization.

The WAN Optimization appliance is a highly recommended component that performs WAN conditioning to reduce effects of latency. It also incorporates Forward Error Correction to negate packet loss scenarios, and deduplication of redundant traffic patterns. Altogether, these reduce bandwidth use and ensure the best use of available network capacity to expedite data transfer to and from IBM Cloud.

Virtual machine migration relies on the combination of Cloud Gateway and WAN Optimization appliance to achieve unparalleled mobility between vSphere on-premises and IBM Cloud.
3.2.8 Layer 2 Concentrator

The Network Extension Service is provided by the Layer 2 Concentrator (L2C). It extends a Layer 2 network from the on-premises vSphere data center to IBM Cloud and enables seamless migration between the data center and the cloud.

The Layer 2 concentrator is required to stretch the on-premises network to IBM. The Layer 2 Concentrator appliance have two interfaces:

- **Internal trunk interface:** Handles virtual machine traffic on-premises for the extended networks using a translational bridge mapping to a corresponding stretched network in IBM Cloud.
- **Uplink interface:** HCX uses this interface to send encapsulated overlay traffic to and from IBM Cloud. Application data travels through this interface.
The Layer 2 Concentrators create encrypted tunnels to extend networks into the cloud. Data traffic between virtual machines uses the data paths established by the Layer 2 concentrators.

The Cloud Gateway handles all migration and any network traffic for appliances in the fleet, while the independent Layer 2 Concentrators handle communication among virtual machines. Separating the migration path from the data path minimizes the chance of migration workloads interfering with communication between VMs.

Network extension with a concentrator requires a virtual distributed switch.

- To configure a Layer 2 network extension, certain prerequisites must be set, as explained in the “Verify Layer 2 Installation Requirements” section of the appendices.

### 3.2.9 Migration Only

The minimal configuration to perform migration only requires the HCX manager and the Cloud Gateway appliances. It is possible to migrate virtual machines without network extension. In this case, the virtual machine obtains a new IP address using the Guest Customization service after it is migrated.

To stretch a network and maintain the original IP address, a distributed virtual switch must be configured in the on-premises vSphere vCenter.

WAN Optimization can improve speed in the situations described; configuring the Cloud Gateway to use a high-speed line (such as a Direct Connect) improves speed by providing a higher bandwidth link for WAN optimized traffic.

Migrating virtual machines on extended networks into IBM Cloud is advantageous because it reduces downtime and the configuration does not change on the virtual machine. The virtual machine can retain the IP addresses, MAC addresses, computer names, and virtual machine names. Retaining these properties greatly simplifies the migration to IBM Cloud and enables easy return trips to the on-premises data center. The Network Extension feature requires a vSphere Distributed Switch, which is available with vSphere Enterprise Plus Edition.
3.2.10 IP Address Requirements

To deploy the HCX, the proper number of IP addresses must be available both on-premises and in the target IBM Cloud. This section addresses how to calculate the addresses required.

- **vMotion Address**
  - Maintaining a separate network for vMotion is a common practice in the on-premises data center. The Cloud Gateway must have access to the vMotion network. If it does not, an extra IP address is needed to communicate with the vMotion network.

- **On Premises**
  - One IP address for the HCX Manager appliance.
  - One for each Cloud Gateway, add one if there is a separate vMotion network.
  - One for each standard Layer 2 Concentrator

- **IBM Cloud**
  - Two IP addresses per HCX Manager appliance connected to IBM Cloud. The addresses can be used to connect to the Internet or one or more Direct Connect lines.
  - Add one if there is a separate vMotion network connection.

3.2.11 Proximity Routing

Proximity Routing is a networking feature which can be enabled when the Cloud Gateway is configured.

Proximity routing ensures forwarding between virtual machines connected to stretched and routed networks, both on-premises and in the cloud, is symmetrical. This feature requires Dynamic Routing configured between the customer premises and the cloud.

When users extend their networks to the cloud, Layer 2 connectivity is stretched onto IBM Cloud. However, without route optimization, Layer 3 communication requests must return to the on-premises network origin to be routed. This return trip is called "tromboning" or "hairpinning." Tromboning is inefficient because packets must travel back and forth between the network origin and the Cloud, even when both source and destination virtual machines reside in the Cloud. In addition to inefficiency, if the forwarding path includes stateful firewalls, or other inline equipment that must see both sides of the connection, communication might fail. Virtual machine communication (without route optimization) failure occurs when the egress path exiting the cloud can be either the stretched Layer 2 network or through the VCS/VCF NSX Edge Gateway. The on-premises network does not know about the stretched network "shortcut." This problem is called asymmetric routing. The solution is to enable proximity routing so the on-premises network can learn the routes from IBM Cloud.

To prevent tromboning, HCX uses intelligent route management to choose routes appropriate to the virtual machine state. The Cloud Gateway maintains an inventory of virtual machines in the cloud. It also understands the virtual machine state, which can be:

- Transferred to the cloud with vMotion (zero-downtime migration).
- Migrated to the cloud using host-based replication (low-downtime migration).
- Created in the cloud (on a stretched network).

3.2.12 Asymmetric Routing with Proximity Routing Solution

In the diagram, the N*a components on the left reside in the on-premises data center, and the N*b component on the right reside in the cloud.
R1 is the default gateway for N1-b, therefore, N1-b must return to R1 to route traffic through R2. To prevent asymmetric routing, HCX injects host routes into within the NSX overlay of the IBM Cloud VCS/VCF deployment.

If the virtual machine was newly created in the cloud, or it was moved with low-downtime migration, the host route is injected immediately.

If the virtual machine was transferred using vMotion, the route is not injected until the virtual machine reboots. Waiting until after the reboot ensures that the on-premises stateful devices continue to service the existing session until the virtual machine reboots. After the reboot, the routing information is consistent both on-premises and in the cloud.

That is, R1 can use routing to reach a specific virtual machine through R2, rather than using the locally connected extended Network. R2 fully owns the path for other networks to reach virtual machines with Proximity Routing enabled.

3.2.13 MAC Address Retention

- The option to retain the MAC address is a check box in the migration wizard. It is only visible for replication-based migration.
- By default, “Retain MAC” is enabled if the source virtual machine is in a stretched network, and disabled when the network is not stretched. If the MAC address is not retained the virtual machine obtains a new address when the migration is done. The decision to retain a MAC address or acquire a new one can impact the migration process and the post-migration network traffic flow.
- Retaining the MAC address is required for the following reasons:
  - Licenses based on the MAC address: Some software pairs the license to the MAC address of the VM. Changing the MAC address of a virtual machine invalidates the license.
  - Linux NIC order: In Linux, if the MAC address is changed on a virtual machine, the NIC Ethernet device number might change after a reboot. A device number change can alter
the NIC presentation order within the operating system, breaking applications or scripts that depend on NIC order.

- Less downtime if the network is stretched: If the virtual machine is migrated over a stretched network, enabling “Retain MAC” minimizes downtime because the network does not have to learn a new MAC address.
- The check box is on the “Select destination network” page during migration operation.

3.2.14 Security Policy Migration

The Policy Migration feature enables NSX distributed firewall rules to be moved from an on-premises vCenter to a VCF/VCS HCX enabled Cloud.

Policy Migration is possible when using low-downtime migration or vMotion to move a virtual machine over a network stretched with the High Throughput Layer 2 Concentrator.

The on-premises data center must be running NSX 6.2.2 or greater.

In vSphere, the security policy is a single NSX Section, which can contain many rules. There can be only one Section (policy) per Org vDC.

A Set of IP addresses or MAC addresses can be identified to participate in the policy. The name of the MAC Set or IP Set cannot exceed 218 characters.

All rules in a Section must have a unique name. Do not leave a rule name blank.

Supported rules specify Layer 3 IP addresses or IP Sets, or Layer 2 MAC addresses or MAC Sets as the source or destination.

Note: Rules that specify security groups or application groups for the source or destination are not migrated.

Any change to the migrated policy is propagated to all VMs that use the policy.
4 Component level Architecture, Target

This section describes the architecture of each HCX component deployed within the IBM Cloud environment. Note that the spoke (i.e., target) deployment model within the IBM Cloud is discussed.

4.1.1 NSX Edge

The first component configured within the IBM Cloud is a pair of NSX Edge virtual machines. It is important to note that all IBM Cloud for VMware Solutions deployments already install and configure an edge device for clouddriver outbound communication. While this ESG could be re-used for Hybrid Cloud Services communication, however it is advised that a new pair are deployed.

The NSX Edge virtual machines are configured as an Active/Passive pair of X-Large NSX Edge devices. These devices are used to connect into the IBM Cloud VMware environment via a public internet connection. The X-Large NSX Edge was chosen for the internal environment since it is suited for environments which have load balancer with millions of concurrent sessions that do not necessarily require high-throughput. As part of the configuration process, the NSX Edge is connected to the IBM Cloud public VLAN as well as the IBM Cloud private VLAN designated for management infrastructure.

<table>
<thead>
<tr>
<th>Component</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>6 vCPU</td>
</tr>
<tr>
<td>RAM</td>
<td>8 GB</td>
</tr>
<tr>
<td>Disk</td>
<td>4.5 GB VMDK resident on shared storage with 4 GB swap</td>
</tr>
</tbody>
</table>

*Table 1 NSX Edge Deployment*

Since the set of NSX Edges are configured as active/passive in either the internal or dedicated deployment, vSphere Distributed Resource Scheduler (DRS) anti-affinity rules must be created by the user to ensure that NSX Edges do not execute on the same host as their respective peer appliance.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>NSX Edge External Gateway</td>
</tr>
<tr>
<td>Type</td>
<td>Separate Virtual Machines</td>
</tr>
<tr>
<td>Members</td>
<td>NSX Edge 1</td>
</tr>
<tr>
<td></td>
<td>NSX Edge 2</td>
</tr>
</tbody>
</table>

*Table 2 NSX Edge Anti-Affinity Rules*

In addition to the NSX Edge appliances deployed within the IBM Cloud, the HCX Manager virtual appliance is deployed if the VMware HCX on IBM Cloud service is ordered. After the deployment of this appliance the aforementioned NSX Edge is enabled to utilize load balancing and configured with application profiles that utilize a certificate for inbound connection from the source. The NSX Edge is also configured with load balancing pools to point to the HCX Manager, vCenter, and PSC appliances. Additionally, a virtual server is created with a virtual IP address (VIP) on the public interface with rules that connect the pools with VIP. A sample of the virtual server configuration and pool configuration on the NSX Edge is shown in Figure 8 VIP Configuration for NSX Edge and
Once the load balancing configuration is complete, the firewall rules on the NSX are updated to accept inbound connections to the HCX Manager for port 443 (HTTPS) from the source HCX.

4.1.2 HCX Manager

The HCX Manager component is the first appliance deployed after the NSX Edge appliances are configured on the target. This appliance is used as the main interface into the cloud environment for the previously discussed source components, and provides an abstracted networking user interface that can be used to add, edit, and delete networks as well as design and configure routing without direct use of NSX. As a result of the vCenter and NSX integration, the HCX Manager appliance is assigned a private portable IP address on the management VLAN. Additionally, it is configured to access vCenter and NSX with a specific user. It is important to note the HCX Manager’s IP address is the same IP address used in the NSX edge for load balancing.

After the HCX Manager cloud component is deployed and configured, the source components create a connection to the HCX Manager via the VIP addresses configured in the NSX ESG. Once this connection is made, the cloud gateway and WAN optimizer appliances are deployed within the IBM Cloud.
4.1.3 Cloud Gateway

As previously mentioned, a virtual appliance is deployed after a connection is established from the source to the target cloud. This appliance is the Cloud Gateway (CGW) and is used to maintain a secure channel between vSphere environment designated as the source and the IBM Cloud. The sizing specification of the CGW appliance deployed within the IBM Cloud is listed in Table 3 Cloud Gateway Deployment.

<table>
<thead>
<tr>
<th>Component</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>8 vCPU</td>
</tr>
<tr>
<td>RAM</td>
<td>3 GB</td>
</tr>
<tr>
<td>Disk</td>
<td>2.0 GB VMDK resident on shared storage</td>
</tr>
</tbody>
</table>

This Cloud Gateway is deployed configured to reside on the management VLAN (Private Portable Subnet) as well as the vMotion VLAN (Private Portable Subnet) of the IBM Cloud for VMware Solutions deployment. Additionally, another interface is configured on the Public VLAN (Public Portable) for connections made over the public internet. Note that public access is not required if there is a direct connection (i.e., private connection in place). The last connection associated with the Cloud Gateway is a logical switch that is created and configured upon site pairing. This logical switch is a private, non-routable network that is used as a communication channel between the Cloud Gateway and WAN Optimizer discussed in 4.1.4 WAN. Figure 11 Cloud Gateway Deployment depicts a high-level component diagram of the cloud gateway appliance and assigned connections.

---

**Figure 10 Target - Hybrid Cloud Services Appliance**

**Table 3 Cloud Gateway Deployment**
The second component deployed is the WAN Optimization appliance. While the WAN Optimization appliance is optional, it performs WAN conditioning to reduce effects of latency. It also incorporates Forward Error Correction to negate packet loss scenarios, and deduplication of redundant traffic patterns. Altogether, these reduce bandwidth use and ensure the best use of available network capacity to expedite data transfer to and from the IBM Cloud. Note that the WAN Optimizer is disk intensive and requires sufficient amount of IOPS to function properly. As a result, the WAN optimizer resides on vSAN storage within the VCF environment and Endurance storage supporting over 2000 IOPS within a VCS deployment. The sizing specification for the WAN Optimization appliance is specified in Table 4 WAN Optimization Appliance Sizing.

<table>
<thead>
<tr>
<th>Component</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>8 vCPU</td>
</tr>
<tr>
<td>RAM</td>
<td>14 GB</td>
</tr>
<tr>
<td>Disk</td>
<td>30 GB VMDK + 70 GB VMDK resident on shared storage</td>
</tr>
</tbody>
</table>

*Table 4 WAN Optimization Appliance Sizing*
Unlike the Cloud Gateway, the WAN Optimization appliance is only attached to a logical switch to enable communication between itself and the Cloud Gateway. Note that the appliance is required if WAN optimization is in use within the source environment. See Figure 12 WAN Optimizer Deployment for a view of the network layout.

![Figure 12 WAN Optimizer Deployment](image)

4.1.5 Layer 2 Concentrator

The third component is known as the Layer 2 Concentrator (L2C) and is part of the Network Extension Services. The L2C is the virtual machine that allows the extension of on-premises datacenter networks to the IBM Cloud. The L2C stretches on-premises VLANs and/or VXLANs. Each L2C can stretch up to 4096 VLANs. Each L2C, when paired with its on-premises partner can provide up to 1Gbps per “flow” and up to an aggregate of 4Gbps per VLAN (or VXLAN). Deployment of more L2C appliances is supported if additional network throughputs are required.

As part of this design, the L2C appliance is deployed such that a customer can stretch multiple VLANs and VXLANs into the IBM Cloud over the public internet or via the private network via Direct Link. The sizing specification of the L2C appliance on the IBM Cloud is listed in Table 5 HT L2C Appliance Sizing.
<table>
<thead>
<tr>
<th>Component</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>8 vCPU</td>
</tr>
<tr>
<td>RAM</td>
<td>38 GB</td>
</tr>
<tr>
<td>Disk</td>
<td>2 GB VMDK on shared storage</td>
</tr>
</tbody>
</table>

*Table 5 HT L2C Appliance Sizing*

The L2C appliance is deployed on the management VLAN as well as the public VLAN. The public interface is used for application traffic that bound for the source of the extended network. Additional connections, i.e., the extended networks, are created and attached to the L2C appliance once the source administrator initiates the network extension into the IBM Cloud. Example of these networks and connections are denoted depicted in Figure 13 L2 Concentrator Deployment.

*Figure 13 L2 Concentrator Deployment*
5 Summary

The architecture discussed in this document explains the configuration details of the VMware HCX on IBM Cloud offering within an IBM Cloud for VMware Solution deployment in addition to an on-premises vSphere estate.

For more information on IBM Cloud for VMware Solutions, please visit:


For more information on the IBM Cloud for VMware Solutions architecture, please visit:

https://www.ibm.com/devops/method/content/architecture/virtCloudFoundationPlatform
## Appendix A - Port Access Requirements

HCX must traverse the public Internet and private lines, and connect to data center components, such as networks, switches, and port groups.

The following Port Access Requirements table lists ports that must be opened so that Hybrid Cloud Services virtual appliances can install successfully.

Both the vSphere environment and the IBM Cloud environment must permit Network Time Protocol (NTP) clock synchronization among vSphere on-premises devices and the IBM Cloud devices. UDP port 123 must be accessible to Hybrid Cloud Services virtual appliances and networks. Installed NTP Servers can be specified when the Hybrid Cloud Services Appliance is installed.

<table>
<thead>
<tr>
<th>Source</th>
<th>Target</th>
<th>Port</th>
<th>Protocol</th>
<th>Purpose</th>
<th>Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>HCX</td>
<td>Customer DNS</td>
<td>53</td>
<td>TCP/UDP</td>
<td>Name Resolution</td>
<td>DNS</td>
</tr>
<tr>
<td>HCX</td>
<td>NSX LB in IBM Cloud</td>
<td>443</td>
<td>TCP</td>
<td>Registration service</td>
<td>HTTPS</td>
</tr>
<tr>
<td>HCX</td>
<td>vCenter in IBM Cloud</td>
<td>443</td>
<td>TCP</td>
<td>HCX REST service</td>
<td>HTTPS</td>
</tr>
<tr>
<td>HCX</td>
<td>PSC in IBM Cloud</td>
<td>443</td>
<td>TCP</td>
<td>HCX REST service</td>
<td>HTTPS</td>
</tr>
<tr>
<td>HCX</td>
<td>connect.hcx.vmware.com</td>
<td>443</td>
<td>TCP</td>
<td>Registration service</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Web Browser</td>
<td>HCX</td>
<td>9443</td>
<td>TCP</td>
<td>HCX Virtual Appliance Management Interface for HCXsystem configuration.</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Admin Network</td>
<td>HCX</td>
<td>22</td>
<td>SSH</td>
<td>Administrator SSH access to Hybrid Cloud Services.</td>
<td>SSH</td>
</tr>
<tr>
<td>HCX</td>
<td>ESXi Hosts</td>
<td>902</td>
<td>TCP</td>
<td>Send management and provisioning instructions from HCXto ESXi Hosts in IBM Cloud</td>
<td>Internal</td>
</tr>
<tr>
<td>HCX</td>
<td>vCenter SSO Server</td>
<td>7444</td>
<td>TCP</td>
<td>vSphere Lookup Service</td>
<td></td>
</tr>
<tr>
<td>HCX</td>
<td>NTP Servers</td>
<td>123</td>
<td>UDP</td>
<td>Time Synchronization</td>
<td></td>
</tr>
<tr>
<td>HCX</td>
<td>Syslog</td>
<td>User Configured</td>
<td>Connection between HCX(the client)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>HCX</td>
<td>Cloud Gateway</td>
<td>8123</td>
<td>TCP</td>
<td>Send host-based replication service instructions to the Hybrid Cloud Gateway.</td>
<td>HTTP</td>
</tr>
<tr>
<td>-----------</td>
<td>---------------</td>
<td>------</td>
<td>-----</td>
<td>--------------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>HCX</td>
<td>Cloud Gateway</td>
<td>9443</td>
<td>TCP</td>
<td>Send management instructions to the local Hybrid Cloud Gateway using the REST API.</td>
<td>HTTP HTTPS</td>
</tr>
<tr>
<td>Cloud Gateway</td>
<td>L2C</td>
<td>443</td>
<td>TCP</td>
<td>Send management instructions from Cloud Gateway to L2C when L2C uses the same path as the Hybrid Cloud Gateway.</td>
<td>HTTP HTTPS</td>
</tr>
<tr>
<td>Cloud Gateway</td>
<td>L2C</td>
<td>8443</td>
<td>TCP</td>
<td>Bidirectional management instructions from Cloud Gateway to L2C, when L2C uses an alternate data path.</td>
<td>HTTP HTTPS</td>
</tr>
<tr>
<td>L2C</td>
<td>L2C (remote)</td>
<td>443</td>
<td>TCP</td>
<td>Bidirectional management instructions from Cloud Gateway to L2C, when L2C uses an alternate data path.</td>
<td>HTTP HTTPS</td>
</tr>
<tr>
<td>Source</td>
<td>Destination</td>
<td>Port</td>
<td>Protocol</td>
<td>Description</td>
<td>Path</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------------------------</td>
<td>---------------</td>
<td>----------</td>
<td>------------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Cloud Gateway</td>
<td>ESXi Hosts</td>
<td>80, 902</td>
<td>TCP</td>
<td>Management and OVF deployment</td>
<td>Internal</td>
</tr>
<tr>
<td>ESXi Hosts</td>
<td>Cloud Gateway</td>
<td>31031, 44046</td>
<td>TCP</td>
<td>Internal host-based replication traffic.</td>
<td>Internal</td>
</tr>
<tr>
<td>Cloud Gateway</td>
<td>ESXi Hosts</td>
<td>8000</td>
<td>TCP</td>
<td>vMotion (zero-downtime migration)</td>
<td></td>
</tr>
<tr>
<td>Cloud Gateway (local)</td>
<td>Cloud Gateway (remote)</td>
<td>4500</td>
<td>UDP</td>
<td>Internet key exchange (IKEv2) to encapsulate workloads for the bidirectional tunnel.</td>
<td>IPSEC</td>
</tr>
<tr>
<td>Cloud Gateway (local)</td>
<td>Cloud Gateway (remote)</td>
<td>500</td>
<td>UDP</td>
<td>Internet key exchange (ISAKMP) for the bidirectional tunnel.</td>
<td>IPSEC</td>
</tr>
</tbody>
</table>
Appendix B - Preparing Installation Environment

The installation of VMware HCX on IBM Cloud has the following software requirements:

- vSphere 5.5 U3, or vSphere 6.0u2 or higher.
- If NSX is used, version 6.2.2 or higher. NSX is required for policy migration.
- To use cross-cloud vMotion, the same affinity restrictions apply across clouds as they do on-premises. See the VMware EVC and CPU Compatibility FAQ located at: http://bit.ly/2vK6Sp5.

7.1 Configure Network Connectivity

HCX must traverse the public Internet and private lines, and connect to data center components, such as networks, switches, and port groups.

- Port Access Requirements (Appendix A) lists ports that must be opened so that HCX virtual appliances can install successfully.
- Both the on-premises vSphere environment and the VCF/VCS HCX Cloud environment must permit Network Time Protocol (NTP) clock synchronization among vSphere on-premises devices and the VCF/VCS HCX devices. UDP port 123 must be accessible to HCX virtual appliances and networks.

7.2 On Premises

Before installing HCX, verify that your environment can support the tasks you want to accomplish. The on-premises environment must support the following tasks before HCX can be installed.

- Virtual Center with vSphere 5.5 Update 3 or 6.0 Update 2.
- vMotion and policy migration features require NSX version 6.2.2 or higher.
- In the vCenter, enough disk space for the HCX appliances to be installed.
- Sufficient IP addresses for the on-premises VMs provisioned during the installation. See IP Address Requirements for the minimum requirements for each configuration.
- Ports and firewalls opened as required as documented in Port Access Requirements.
- If the single sign-on (SSO) server is remote, the URL of the vCenter, external SSO Server, or Platform Services Controller (PSC) that runs the external lookup service must be identified. When the HCX Manager is registered with the vCenter, this URL must be supplied.
- If a vCenter does not have its own internal instance of the lookup service, it might be for one of the following reasons:
  - vCenter 6.0u2 is running an external Platform Services Controller.
  - The vCenter is in linked mode (where the secondary vCenter uses the SSO service from the primary vCenter or an external SSO service).

7.3 Verify Layer 2 Installation Environment

Layer 2 network stretching requires the following

- A vSphere Enterprise Plus edition.
  - The vSphere vCenter must meet the following requirements to support Layer 2 extension.
    - vSphere Enterprise Plus license
    - Must have a vSphere Distributed Switch (vDS). The distributed switch is available with vSphere Enterprise Plus Edition.
- When installed, the on-premises Layer 2 concentrator service appliance must have access to a vNIC port and any VLANs to be stretched.
- If the network is to be stretched over the public Internet or a VPN (on an alternate path) the L2C virtual machine in VCF/VCS requires an IP address. The remote IP address is required to configure the Layer 2 concentrator.
- If multiple Layer 2 concentrators are desired, each must have an IP address on-premises and in the cloud.
8 Appendix C - Installing and Configuring HCX on Source

The on-premises installation entails deploying the HCX management appliance and registering it with the vCenter and one or more VCF/VCS HCX enabled cloud endpoints.

- Install the HCX Manager Appliance
  - Install the HCX Manager appliance in the on-premises vCenter.
- Register the HCX Manager with the vCenter
  - Register the HCX plug-in in the vSphere® Web Client and start the HCX management service.
- Configure the Proxy Settings
  - HCX can be configured to work with a proxy server.
- Register the source HCX with a VCF/VCS HCX enabled cloud
  - Associate the HCX (on premises) with a VCF/VCS HCX enabled cloud endpoint.

8.1 Install the HCX Manager Appliance

Install the HCX Manager appliance in the on-premises vCenter.

8.2 Procedure

1. Log in to My VMware and download the Hybrid Cloud Services OVA file from the product download page.
2. Open a browser and log in to the vSphere® Web Client. (This task cannot be performed from the vSphere Client.) View the Home tab.
3. In the Inventories Trees list, click Host and Clusters.
4. Expand the hierarchy to show the data centers.
5. Right-click the target data center and select Deploy OVF Template from the context menu (it might take a few seconds for the Deploy OVF Template menu item to appear). The Deploy OVF template wizard opens.

6. Choose Deploy OVF template
Select “Local file” and click Browse to find the OVA file downloaded to the computer. Click Next.

On the “Review details” page, click the “Accept extra configuration options” check box and click Next.

On the "Accept EULAs" page, scroll down to review the VMware end-user license agreement. Click Accept and Next.

On the “Select name and folder” page, edit the name (if necessary) and select the location for the Hybrid Cloud Services. Click Next.

On the “Select a resource” page, select the installation location.

On the “Select storage” page, select the storage for the Hybrid Cloud Services and click Next. From the “Select virtual disk format” drop-down menu, either thin or thick provisioning can be selected.

On the “Setup networks” page, map the Hybrid Cloud Services adapter to a host network chosen from the Destination drop-down menu.

7. On the “Customized template” page, enter the values specific to the environment.
   - **Passwords.**
     - The default user name for both the command-line interface (CLI) and the Web user interface is: admin. The “admin” user and password to log in to the Web user interface (see “Log in to the Hybrid Cloud Services Management Portal”) is required as is also a root user account that has a password that can be set.
     - Enter and reenter the CLI “admin” user password.
     - Enter and reenter the root user password. In the future, if help is needed from VMware Global Support Services (GSS), this password might have to be shared so they can troubleshoot the system.
   - **Network Properties.**
     - Enter the hostname for the HCX Manager VM. Enter the network IPv4 address, the IPv4 prefix (the CIDR), and the default gateway. The following values are samples:

   ![Customized template](image)

   - **DNS.**
     - Click DNS, and enter the IP addresses for DNS servers (separated by spaces) and the domain search list. The values in the following screenshot are samples:
   - **DS configuration**
8. Review the vService bindings page. Click Next to continue, or to change previous screens, click Back.

9. On the “Ready to complete” page:
   - Check the “Power on after deployment” check box.
   - Review the Hybrid Cloud Services settings, and click Finish. It might take several minutes for the Hybrid Cloud Services appliance to power on.
   - To check the status, go to the vSphere Web Client home page, and in the Home tab, go to Inventories and click Hosts and Clusters. Expand the data center hierarchy, and click the Hybrid Cloud Services service virtual machine to display a summary in the center pane.
   - The Summary tab, the console reads “Powered On” and the Play button is green.

10. The HCX Manager is powered on and ready to be registered with the vCenter.
9 Appendix D - Register HCX Manager with the vCenter

Register the Hybrid Cloud Services plug-in in the vSphere® Web Client and start the Hybrid Cloud Services management service.

9.1 Prerequisites

The Hybrid Cloud Services virtual appliance must be powered on before it can be registered.

9.2 Procedure

1. Log in to Hybrid Cloud Services service virtual appliance.
2. Click the Manage Settings tile.
   a. In the left pane, under Configure Systems, select vCenter.
   b. Click the Add vCenter button on the upper right.
   c. Enter the IP address of the vCenter Server in the form https:\\<vCenter-host-name> or https:\\<vCenter-IP-address>.
   d. For example, https:\\My-vCenter or https:\\10.108.26.211.
   e. Enter the vCenter Server user name and password. The account used must have the vCenter Administrator role.
   f. Click OK. Do not restart when the “You need to restart the app” message is displayed. Proceed to next step.

3. Configure the lookup service.
   a. Click the Manage tab.
   b. Click the Edit button on the far right of the Lookup Service URL text box.
   c. Enter the lookup service endpoint in the following form:
      i. vCenter Server 5.5u3: https://ssoip:/7444/lookupservice/sdk
      ii. vCenter Server 6.0u2: https://ssoip/lookupservice/sdk
   d. Click OK. Do not restart when a message to restart the Web Engine is displayed. Proceed to next step.

4. Click the Summary tab, and find the Hybridity Management Components section.
a. Stop and start both the application engine and the Web engine.

5. To finalize the registration, log out of the vSphere® Web Client. Log back in to verify that the screen update has occurred.

Notice the existing Hybrid Cloud icon and the Hybrid Cloud Services menu item on the left, as indicated in red the following screenshot. The Hybrid Cloud Services registration updates these labels as shown in the following screenshot. In the inventory, Hybrid Cloud Services becomes Hybrid Cloud Services, and the icon label also becomes Hybrid Cloud Services.
10 Appendix F - Installing and Configuring Hybrid Services

10.1 Installing and Configuring Hybrid Services

- The installer provisions and configures a virtual machine for each service virtual appliance. The service virtual machines are deployed both on-premises and in the cloud.
- Prerequisites
  - The HCX Manager must be installed on premises, and registered with a VCF/VCS HCX enabled cloud endpoint.
  - The target virtual data center must have sufficient resources. See IP Address Requirements and Verify the Minimum Installation Environment.
- Configuration Overview
  - The configuration procedure assumes the configuration of all service virtual appliances; however, they are not all required.
- Start Hybrid Service Virtual Appliance Installation and Configuration
  - The virtual appliances can be installed and configured using a simple Web interface.
- Configure the Hybrid Cloud Gateway
  - This topic describes how to configure the Hybrid Cloud Gateway service virtual appliance.
- Configure the Network Extension Service
  - This topic describes how to configure a Network Extension service. You can perform this task for a single path deployment, or for a standalone network extension on an alternate path.
- Stretching a Layer 2 Network to IBM Cloud
  - This procedure extends a Layer 2 network from the on-premises data center to IBM Cloud.

10.2 Configuration Overview

- The configuration procedure assumes all service virtual appliances will be configured, however, they are not all required.
- The Hybrid Cloud Gateway is required.
- Installing WAN optimization is accomplished by checking the WAN Optimization Service box during the installation. No further configuration is required.
- To configure the Network Extension service, see Configure the Network Extension Service. The deployment of the optional appliance and can be deferred by returning to the Hybrid Services page and install the appliance later.

10.3 Start Hybrid Service Virtual Appliance Installation and Configuration

- The simple web interface is used to install the service virtual appliances and to configure additional Layer 2 Concentrators.
- Prerequisites
  - The HCX Manager must be installed and registered with the VCF/VCS HCX enabled cloud endpoint.
- Procedure
  - Log in to the vSphere Web Client. On the Home tab, click the Hybrid Cloud Services icon.
○ Click the Hybrid Services tab.
○ Click Install Service.
○ The "Choose Hybrid Services" page opens.
○ Select the Services to be installed
○ Click Next.

- What to do next
  ○ The next step is to configure the Hybrid Cloud Gateway if required.
  ○ A Layer 2 concentrator can be added to an existing installation at any time provided there are sufficient resources to support the extension.

10.4 Configure the Hybrid Cloud Gateway

This topic describes how to configure the Hybrid Cloud Gateway service virtual appliance.

Prerequisites

○ Follow the steps in "Start the Hybrid Service Virtual Appliance" and check Hybrid Cloud Gateway. On the Hybrid Cloud Gateway page, provide the following values:

Procedure

○ Network: The switch that connects the Hybrid Cloud Gateway management interface. In use cases 1 and 2, it can be a standard virtual switch or a virtual distributed switch. For any configuration using Layer 2 extension, it must be a virtual distributed switch.
○ Cluster/Host: Select the Cluster or Host in which the Cloud Gateway is to be deployed.
○ Datastore: Select the datastore where to deploy the Cloud Gateway.
○ VM/Hostname: This value is optional.
○ Provide the IP address/CIDR, Default Gateway, and DNS server to use for the Cloud Gateway management interface.
○ To enter multiple addresses for the DNS server, separate them with commas.
○ Under Extended (optional), choose the vMotion network (if applicable), and set the admin and root passwords. These passwords are specifically for the Hybrid Cloud Gateway appliance. The user name and password do not have to match the ones configured for the Hybrid Cloud Services appliance.
○ Click Next.

10.5 Configure the Network Extension Service

This topic describes the configuration of a Network Extension service either for single path deployment, or for a standalone network extension on an alternate path.

Prerequisites

Select the Network Extension service. (If the Single Path configuration is installed, Network Extension is your only choice).

Procedure

○ On the Network Extension Service page, select a virtual distributed switch from the Distributed Switch drop-down menu.
○ When installing a standard Layer 2 Concentrator, the "Route stretched networks via Hybrid Cloud Gateway" check box will be available. It is not there for the high throughput L2C.
○ If “Route stretched networks via Hybrid Cloud Gateway” is selected the installer determines a reasonable placement for the Layer 2 Concentrator (based on the switch) and populates the placement information accordingly.
○ Otherwise the placement information must be manually entered in the next step.
• Set the route for the L2 Concentrator placement. (If “Route stretched networks via Hybrid Cloud Gateway” was selected these values cannot be edited.)
  o Network: The deployment network for the Layer 2 Concentrator’s management interface.
  o Compute: The deployment cluster or host for the Layer 2 Concentrator.
  o Datastore: Deployment datastore for the Layer 2 Concentrator.
  o VM/Hostname: This value is optional.
• Specify the Network Parameters for the local Layer 2 Concentrator.
  o If this option is disabled, use the default parameters provided by the installer.
  o If the port group selected in the Hybrid Cloud Gateway page Network drop-down menu is not part of the distributed switch, check “Specify the Network Parameters for the local Layer 2 Concentrator” and edit the “Extended Configurations” text boxes.
• (Optional) Extended Configurations: Set the admin and root passwords for this specific Layer 2 Concentrator.
  • Click Next.
  • On the “Ready to complete” page, review the information, and click Finish.

10.6 Monitor Service Appliance Deployment

The task console can be used to monitor deployment progress for a service virtual machine.

• Procedure
  o Log in to the vSphere Web Client. On the Home tab, click the Hybrid Cloud Services icon.
  o The Hybrid Cloud Services pane opens.
  o Click the Hybrid Services tab.
  o The virtual appliance deployment can be monitored from the Task console.
  o Go to the Recent Tasks panel and view the All Users’ Tasks
  o Click More Tasks to open the Task Console.
  o In the Task Console, watch the deployment tasks.
  o When all tasks are completed, go to the inventory list and click Hybrid Cloud Services.
  o In the central panel, click the Hybrid Services tab.
  • Review the configuration summary for the hybrid service virtual appliances

10.7 View Tunnel Status

• This procedure describes how to view the Cloud Gateway tunnel status.
• Prerequisites
  o The network extension service must be up before stretching a network.
• Procedure
  o To check the tunnel status from the Web client, select Hybrid Cloud Services in the inventory, and click the Hybrid Services tab.
  o The following screenshot shows a successful Hybrid Cloud Gateway tunnel. CGW is the acronym for the Hybrid Cloud Gateway. The status is "Active," and on the far right, the tunnel is color-coded green.
10.8 Stretching a Layer 2 Network to IBM Cloud

- This procedure extends a Layer 2 network from the on-premises data center to VCF/VCS HCX enabled cloud.
- Prerequisites
  - Only VLAN tagged port groups (other than VLAN type None, or VLAN ID 0) can be stretched. VXLANs are considered VLANs.
  - This process uses the "Extend Network" wizard. This wizard must be run from the vSphere® Web Client networking inventory view. Although the wizard is visible from other views, it must be run from the inventory context to get the correct information.
- Procedure
  - Log in to the vSphere® Web Client. On the Home tab in the central pane, click the Networking icon in the Inventories list.
  - In the Networking hierarchy, identify the port group for the network to be extended.
  - Right-click the port group, and from the context menu, select Hybridity Actions and select “Extend Network.”
  - The “Extend network to Cloud” wizard opens.
  - On the “Select source port groups” page, confirm the port group information and enter the Gateway IP address and prefix for the network. Click Next.
  - On the “Select destination gateway” page:
    - Select the VCF/VCS Hybrid Cloud Services Cloud Organization from the Organization menu.
    - Select the VCF/VCS Hybrid Cloud Services Cloud virtual data center from the menu.
    - Leave Proximity Routing disabled to force a VM within VCF/VCS Hybrid Cloud Services enabled cloud to always use the on-premises gateway to access the Internet. By default, traffic originating from a VM in VCF/VCS Hybrid Cloud Services enabled cloud traverses the Layer 2 data path back to the on-premises data center and out to the default gateway. If Proximity Routing is checked, a VM within VCF/VCS Hybrid Cloud Services enabled cloud can access the Internet without traversing the Layer 2 data path to vSphere.
    - Select the remote destination gateway from the list of gateways (click the row). Click Next.
    - On the “Ready to complete” page, review all values provided. Click Finish.
• To track the progress of the network extension, go to the Recent Tasks window, click the All tab, and view All Users’ Tasks. To open the Task Console, click More Tasks.
• The network extension is done when the “Extend Network” task status is “Completed.”
11 Appendix G - Migrating a Virtual Machine

11.1 Migrating a Virtual Machine (VM)

- HCX enables bidirectional migration: from on-premises to the cloud, or from the cloud to the on-premises data center. HCX uses replication technology during the migration process.
- Replication technology is integrated in the Hybrid Cloud Gateway virtual appliance. No additional replication software needs to be installed.

11.2 Low Down-Time Migration

- Low-downtime migration uses host-based replication to move a live virtual machine from a vCenter to a virtual data center (or the opposite direction). To reduce downtime, the source VM remains online during the replication and is bootstrapped on the destination ESX host after replication completes.
- A migration request triggers the following actions:
  - Replication begins a full synchronization transfer into a VCF/VCS HCX virtual data center. The time it takes to replicate is a function of the size of the VM and available bandwidth.
  - Replication bandwidth consumption varies depending on how the workload changes blocks on the disk.
- When full synchronization finishes, a delta synchronization occurs.
- When the delta synchronization finishes, HCX triggers a switchover. The switchover can start immediately or scheduled until a specific time.
- Following the switchover, the source VM is powered-off, and the migrated replica is powered-on. If for some reason the VM cannot power on, the new VM is powered off (or remains powered off) and the original is powered on.
- HCX renames the powered-off original VM to avoid a naming conflict with the migrated VM and appends a binary timestamp to the original VM name.
- If enable “Retain MAC” was not specified the migrated VM obtains a new MAC address.
- The migration is done. Hybrid Cloud Services copies the original VM to the “Migrated VMs” folder in the vSphere Templates view.

11.3 No downtime vMotion

- vMotion transfers a live virtual machine from a vSphere vCenter to a VCF/VCS Cloud. This vMotion requires a stretched network. The vMotion transfer captures the virtual machine’s active memory, its execution state, its IP address, and its MAC address.
- Note
  - The virtual machine hardware version must be at least version 9, or cross-cloud vMotion might fail.

11.4 Cold Migration

- Cold migration uses the same data plane as cross-cloud vMotion to transfer a powered-off virtual machine over an extended network. Its IP address and MAC address are preserved. The virtual machine requirements and restrictions are the same as for vMotion.
- Migrate Virtual Machines Using the Bidirectional Wizard
  - Using the vSphere Web Client, the bidirectional migration wizard is accessible from the Hybrid Cloud Services Getting Started tab. This wizard handles all migration details, including multiple virtual machines.
- Check The Virtual Machine Before Migration
To migrate a virtual machine, a secure connection maintained by the Hybrid Cloud Gateway is required, and the VM must meet the requirements in this topic.

- Monitor a Migration
  - The progress of a replication-based migration can be monitored from the user interface, or from the command line.

- View Migrated Virtual Machines
  - When Hybrid Cloud Services powers on a successfully migrated virtual machine, it powers off the original virtual machine and stores it in a folder in the vCenter. The stored virtual machines remain until it is manually deleted.

11.5 Migrate Virtual Machine using bi-directional Wizard

- From the vSphere Web Client, the bidirectional migration wizard can be accessed from the Hybrid Cloud Services Getting Started tab. This wizard handles all migration details, including multiple virtual machines.

- From vSphere to VCF/VCS Hybrid Cloud Services
- From VCF/VCS HCX Cloud to vSphere

11.6 Checking Your Virtual Machine before Migration

- To migrate a virtual machine, a secure connection maintained by the Hybrid Cloud Gateway is required, and the VM must meet the requirements in this topic.
- Migration Requirements
  - Before migrating a virtual machine, be sure that it meets these conditions.
    - The virtual machine must be powered on.
    - The underlying architecture, regardless of OS, must be x86.
    - To use vMotion migration, the hardware version must be greater than 9.
    - The hardware version must be less than 10.
    - VMs with Raw Disk Mapping in compatibility mode can be migrated.

- Unsupported
  - Virtual machines with the following attributes are not supported for migration.
    - Exceed 2 TB.
    - Share VMDK files.
    - Have virtual media or ISOs attached.
    - Hardware version less than 9.

11.7 Monitor a Migration

- The progress of a replication-based migration can be monitored from the user interface, or from the command line.

- View the Task Console, as described in Monitor Service Appliance Deployment, and look for the “Migrate VM” task. When the status is “Completed,” the VM has been migrated and powered on VCF/VCS Hybrid Cloud Services Cloud.

- This procedure uses an unrelated VM in the same vCenter to track the progress of a migrating VM.

- Procedure
  - Identify the VM to migrate, and choose an observer VM that can ping the migrating VM.
  - From the user interface, start migrating the VM, and monitor it from the task console.
  - Using SSH, log in to the ESXi host running the observer VM.
  - Run the following command to obtain the virtual machine ID (the vmid).
- # vim-cmd vmsvc/getallvms | grep -i vmname 5
  - Run the following commands to monitor the replication state, where the vmid is the value obtained in the previous step.
    - # vim-cmd hbrsvc/vmreplica.getState vmid # vim-cmd hbrsvc/vmreplica.queryReplicationState vmid 6
  - ICMP Ping: Monitor the continuous ping started earlier.
  - There will be an interruption in the continuous ping during the switchover. However, the test ping quickly resumes after the “Migrate VM” task completes (as reflected in the task console).

11.8 View Migrated Virtual Machine

- When Hybrid Cloud Services powers on a successfully migrated virtual machine, it powers off the original virtual machine and stores it in a folder in the vCenter. The stored virtual machines remain until they are manually deleted.

- Prerequisites
  - Migrated virtual machines.

- Procedure
  - After the migration, view the vCenter and note the folders labeled “VMs migrated from the cloud,” and “VMs migrated to the cloud.”
  - As replicas, the powered-off VMs have the original name, with a binary timestamp appended.
  - Migrated VMs can be treated like any other VMs. For example, it can be moved a VM to a different location and powered on.
  - Unwanted VMs within these folders can be deleted
  - Deletion is final, unless a backup solution is in place.
12 Appendix H - Modifying or Uninstalling HCX

12.1 Modifying or Uninstalling HCX

- Existing installations can be upgraded, or some or all of a Hybrid Cloud Services deployment can be removed.
- Unstretch a Layer 2 Network
  - Unstretching a Layer 2 network is necessary before removing the associated Layer 2 concentrator service virtual appliance, or uninstalling Hybrid Cloud Services.
- Uninstall Hybrid Virtual Service Appliances
  - A service appliance may be uninstalled in preparation for uninstalling Hybrid Cloud Services or due to a change in the installation architecture.
- Uninstall Hybrid Cloud Services
  - The Hybrid Cloud Services appliance should be uninstalled before removing Hybrid Cloud Services solution from the on-premises data center.
- Log in to the Hybrid Cloud Services Management Portal
  - The Hybrid Cloud Services deployment can be administered from the Management Portal via a browser-based user interface.
- Upgrade Hybrid Cloud Services
  - Existing Hybrid Cloud Services installations can be upgraded. The upgrade occurs while the service virtual machines are running. Previous networking capabilities remain the same.

12.2 Unstretch a Layer 2 Network

Unstretching a Layer 2 network is necessary before removing the associated Layer 2 concentrator service virtual appliance, or before uninstalling Hybrid Cloud Services.

- Procedure
  - Check the stretched networks.
  - From the Hybrid Cloud Services plug-in page, view the Hybrid Services tab and check the Network Extension Service section. If there are active or scheduled jobs, wait until they are complete (or stop them) before continuing.
  - To remove the network, click the red X (on the right).
  - Click OK to confirm.

12.3 Uninstall HCX Virtual Appliances

- A service appliance may be uninstalled in preparation for uninstalling Hybrid Cloud Services or due to a change in the installation architecture. Use the Hybrid Cloud Services to administer appliances, as outlined in the following procedure.
- Prerequisites
  - Note - Never delete virtual appliances from the vSphere inventory. Always use the management portal to interact with service virtual appliances.
  - Cancel or reset the execution time for any migrations that might occur during the uninstallation task.
  - Check the vSphere Web Client task console for any running migrations, and wait until they are complete.
Ensure that there are no active Hybrid Cloud Services tasks of any type.

Procedure
- In the vSphere Web Client interface, select the Hybrid Cloud Services plug-in from the left panel.
- In the center pane, click the Hybrid Services tab. The center pane displays a list of the installed appliances.
- Locate the Hybrid Cloud Gateway appliance and click the entry to display the details.
- On the lower right, click the red X to remove the appliance.
- If a stretched network does not share an IP address with the Hybrid Cloud Gateway, you must remove it separately. Expand the Network Extensions Service details, and click the red X icon to remove the Layer 2 Concentrator.
- The Hybrid Cloud Gateway and any hybrid service virtual appliances that use the Hybrid Cloud Gateway are removed from both the vCenter and the VCF/VCS Hybrid Cloud Services Cloud.

12.4 Uninstall HCX Manager

- The HCX Manager appliance should be uninstalled before removing the HCX solution from the on-premises data center. Follow these steps to uninstall the Hybrid Cloud Services virtual machine.
- Procedure
  - Unstretch all Layer 2 networks.
  - Remove the hybrid service virtual appliances.
  - In the on-premises vCenter, power off the Hybrid Cloud Services virtual machine.
  - Delete the Hybrid Cloud Services virtual machine.
  - At this point, all virtual service appliances are removed. The following elements might remain behind:
    - Logs
    - Migrated VMs
- What to do next
  - The migrated virtual machines and logs can be manually backed-up or deleted.

12.5 Login to the HCX Management Portal

- The Hybrid Cloud Services deployment can be administered from the Management Portal via a browser-based user interface.
- Procedure
  - In a Web browser, enter the IP address assigned to the Hybrid Cloud Services, and specify port 9443.
  - For example: https://HCXip:9443.
  - The Hybrid Cloud Services user interface opens in a Web browser window using SSL. If necessary, accept the security certificate. The VMware Hybridity and Networking login screen opens.
  - Enter the user name and password.
  - By default, the user name is Admin. The password is the value supplied when the Hybrid Cloud Services virtual appliance was installed.
  - The Hybridity & Networking Appliance Management page opens.
13 Appendix I - Troubleshooting

13.1 Troubleshooting

- Cloud Registration Fails
  o Hybrid Cloud Services does not retry if credentials are incorrect. The credentials must authenticate before Hybrid Cloud Services attempts to log in and start the cloud registration.
- Duplicate MAC Address
  o When the MAC address is retained during a migration, this might inadvertently create a duplicate MAC address. The MAC address for the migrated virtual machine can be changed to resolve this problem.
- High Host Resource Consumption
  o If all service virtual appliances reside on the same host, certain situations might exhaust the host’s resources.

13.2 Cloud Registration Fails

- Hybrid Cloud Services does not retry if credentials are incorrect. The credentials must authenticate before Hybrid Cloud Services attempts to log in and start the cloud registration.
- Cloud Registration can fail if the credentials are mistyped or if the VCF/VCS Hybrid Cloud Services Cloud credentials are changed after Hybrid Cloud Services registers with VCF/VCS Hybrid Cloud Services Cloud, causing a mismatch.
- To update the credentials in the Web client, go to the Hybrid Cloud Services Getting Started tab, and under "Basic tasks," choose, "Register new Cloud."

13.3 Duplicate MAC Address

- When the MAC address is retained during a migration, this might inadvertently create a duplicate MAC address. The MAC address for the migrated virtual machine can be changed to resolve this problem.
- Problem
  o After migration, there are communication problems among your virtual machines.
- Cause
  o A duplicate MAC address was created during the migration process.
- Solution
  o In the vSphere client, power off the virtual machine.
  o In the inventory, right-click the virtual machine and choose Edit Settings... from the context menu.
  o The Edit Settings window opens.
  o On the Virtual Hardware tab, expand the Network adapter.
  o Next to the MAC Address text box, choose "Manual" from the drop-down menu.
  o The MAC Address text box is editable.
  o Specify a unique MAC address.
  o Click OK.
  o Check to see whether the unique MAC address solves the communication problem.

13.4 High Host Resource Consumption

- If all service virtual appliances reside on the same host, certain situations might exhaust the host’s resources.
- Problem
In rare cases, the Hybrid Cloud Services service virtual machines can exhaust a host's CPU and disk resources.

- **Cause**
  - Some users have seen this issue when all virtual appliances were installed on one physical host. Given this configuration, performance degrades when the following things happen concurrently:
    - The network has high latency, or packet loss, or both. Migration or data transport is slow when using the public Internet or a busy network.
    - The WAN Optimizer is consuming bandwidth to encrypt and compress (or decrypt and uncompress) large workloads.
    - There is high application traffic between on-premises VMs and migrated VMs.

- **Solution**
  - Contact steady state support if resources are being exhausted.
  - Before changing the data center configuration, review the requirements to steady state support. They can advise how to reconfigure the environment with a minimum amount of downtime.