Designlet: VMware Cloud on AWS SDDC Connectivity With VMware HCX Over Direct Connect

VMware Cloud Migration

Table of contents

Designlet: VMware Cloud on AWS SDDC Connectivity With VMware HCX Over Direct Connect

Introduction

This document provides you with recommendations and guidelines on how to establish HCX data plane over a Direct Connect (DX) Private VIF, or with VMware Transit Connect using Direct Connect Gateway (DXGW).

There are several prerequisites and considerations that you must be aware of before you can start configuring the network.

Refer to the table below for a summary of the use case, considerations, and other details to see if it meets your requirements.

Summary and Considerations

Use Case	When a customer has a DX and is planning migrations with HCX, the migration traffic, L2 Extension traffic, and even management traffic can all leverage the DX instead of going over the Internet.
Pre-requisites	Customers require one or more DX connections to the AWS region where their SDDC is deployed that meets their redundancy requirements, or a transit VIF from their DX connected to a DXGW that is attached to the SDDC Group the SDDC is part of, or to a native TGW that is attached to the SDDC Group. They will require an IP subnet dedicated to the on-prem HCX appliances that has reachability to the SDDC over the DX as well as a corresponding subnet for the SDDC side HCX appliances.
General Considerations/When to use	When a DX is available and has sufficient capacity for replication and L2 extension traffic, in addition to any management and routed production traffic, DX will provide an optimal path for HCX. HCX also provides an encrypted path over DX, as HCX uses the same encrypted traffic path regardless of the nature of the connection. If DX supports jumbo frames and is configured with a jumbo frame MTU in the SDDC, then HCX will be able to take advantage of that increased traffic path for more efficient performance (and better throughput) that is not possible over the Internet path.
Performance Considerations	Migration performance should not be significantly different assuming neither the DX nor Internet connection used is a bottleneck. Latency can be reduced, however, which will be of much more benefit to the L2 extension traffic. In addition, there is likely to be much less jitter & packet loss on a DX circuit vs. over the Internet. Replication traffic will generally use at most 1-1.5Gbps per IX pair, however L2 Extension traffic can use up to 4Gbps per L2C appliance pair.
Incompatibilities	Same limitations as DX connectivity to the SDDC. The IP subnets used for HCX must be unique and distinct on the global network. They cannot overlap the management subnet, AWS VPC or any other on-prem networks
Cost Implications	Traffic over DX is lower cost than traffic over Internet. Neither charges for traffic being sent into the SDDC however, which is what most migration traffic is. Using vTGW + DXGW will have additional costs for the transfer based on the region of the DX being used, as well as TGW charges of $0.02 per GB (in all directions, and region-dependent).
Documentation reference	HCX user guide DNS Settings
Last Updated	Feb 2021

Planning and Implementation

There are many best practices and recommendations to keep in mind when you are planning to use AWS Direct Connect (DX) Private VIF.

Planning

- Determine the number of IPs required for HCX appliances:
  - 1 IP per IX (max. 1 per cluster, min. 1 per site pair)
  - 1 IP per L2C (max. 1 per VLAN, min. 8 VLANs per L2C)
  - Round up to the nearest subnet size, ensure to leave some additional capacity for expansion.
- Define 2 subnets of the determined size, one for use with on-prem, one for use in the SDDC. It is possible to use existing subnets for the on-prem size if IPs that have reachability to the on-prem HCX Manager, ESXi management, and vCenter as well as outbound IP protocol 50 (ESP) / UDP 4500.
- Determine whether HCX Manager site pairing will use private or public IPs, and configure the DNS setting for the HCX Manager appropriately (default is public). The HCX Manager on-prem will require access to the SDDC HCX manager's IP over port TCP/443.
- A web proxy is supported for the HCX Manager. If it is configured, it will become the default path for all port 443 traffic, so ensure that exceptions are configured for the DNS/IPs of local resources that you don't want to go through the proxy (for example, vCenter).
- The on-prem HCX manager also requires outbound HTTPS access to the following URLs:
  - connect.hcx.vmware.com
  - hybridity-depot.hcx.vmware.com.

These URLs will go through the proxy if configured, otherwise the firewall will need to allow outbound access from the HCX Manager to all IPs on port 443, as these URLs can dynamically change IPs.

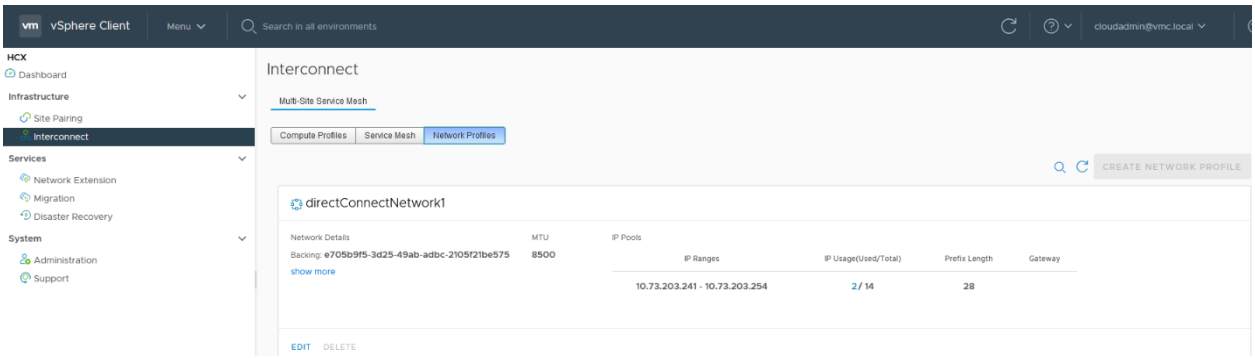
Implementation

To add the private IP subnet to the SDDC's HCX Manager, follow the steps below:

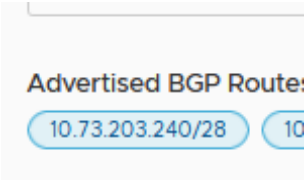
1. In your AWS SDDC console, go to **HCX -> Interconnect -> Network Profiles** page.
2. Edit the **directConnectNetwork1** panel and add the range of IPs to use and the subnet size.

Note the following points when adding the IPs and subnet size:

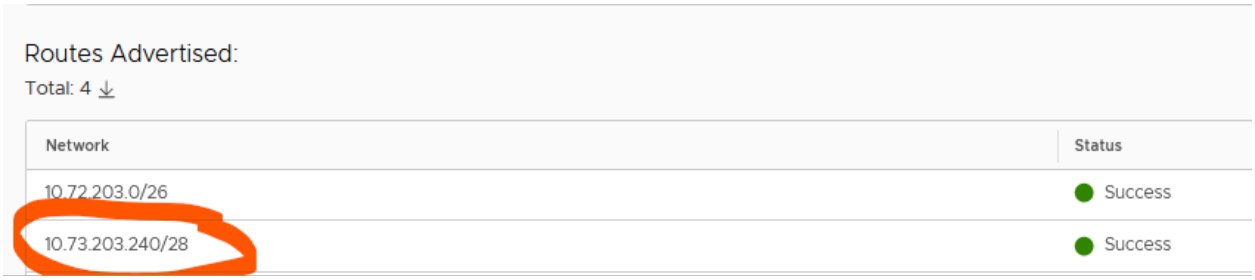
- The BGP route advertisement will be calculated automatically.
- Ensure that all the IPs in the range specified are contained within the selected subnet size.
- No gateway or DNS settings are required (leave them blank).
  - Set the MTU to the maximum supported by the DX If you are using HCX over vTGW, specify 8500. If using DX, use the largest size your DX/VIF supports, up to 8900.



After the subnet is configured, the subnet is advertised on the DX and displayed under **Networking & Security -> Direct Connect**.



It is also displayed on the **Transit Connect**, under **Networking & Security -> Transit Connect**.



The next step is to create a firewall rule on the SDDC's Management gateway firewall to allow access from the on-prem HCX manager to the SDDC's HCX Manager. Firewall rules for the HCX appliances are automatically defined as the appliances are deployed, and are not displayed in the UI, so there is no need to configure the SDDC's firewall for these appliances.

Once the firewall rule is created, the site pairing can be set up from the On-Prem HCX manager to the SDDC's HCX Manager. The remaining configuration is done through the HCX interface either through the vCenter plug-in or directly in the HCX Manager web interface.

Note - It is recommended that the site pairing and all additional HCX configurations are done from the on-prem side HCX Manager or vCenter plug-in rather than the cloud-side (SDDC) HCX Manager. In the case of a cloud-to-cloud HCX pairing, configuration should be made from the SDDC that will be acting as the source side.

Author and Contributors

Michael Kolos, Product Solution Architect, VMware