Protecting Workloads to Cloud Director service with Google Cloud VMware Engine

Using VMware Cloud Director Availability

vmware®

Table of contents

Supported Product Versions

The following versions of VMware Cloud Director Availability, VMware Cloud Director, VMware Cloud Director service and more were tested.

Product	Version
VMware Cloud Director Availability	4.3.1
VMware Cloud Director Availability On-Premises	4.3.1
VMware Cloud Director (On-Premises)	10.3.x
VMware Cloud Director (Cloud Director service)	10.3.2
vCloud Usage Meter	4.5
VMware vSphere	7.0U2-U3

User Permissions for Google Cloud VMware Engine

The default vSphere administrative user that comes with Google Cloud VMware Engine is *CloudOwner@gve.local*. Despite its administrative rights, the CloudOwner user misses some privileges (like Host.Config.Connection, for example) for the VMware Cloud Director Availability Classic data engine to operate properly.

Even the temporary elevation of the CloudOwner privileges (*link*) does not help to perform a successful replication.

However, out-of-the-box Google Cloud VMware Engine creates 5 vSphere solution users with full administrative privileges. They are intended to be used by products like VMware Cloud Director, VMware SRM and also other VMware and non-VMware tools.

By using one of the solution users during the VMware Cloud Director Availability configuration, the product can successfully create and maintain a healthy replication. A description of the solution user accounts and steps how to enable them is available *here*.

NOTE: The password of the solution user expires 365 days after it was changed last. This means resetting it needs to be considered every year not to disrupt the service.

Google Cloud VMware Engine Network Configuration

In terms of internal networking and communication, Google Cloud VMware Engine is not as restrictive as VMC on AWS, for example. There is no need to define firewall rules for enabling the VMware Cloud Director Availability appliances to access the ESXi hosts, for example.

Still these requirements need to be met:

1. Have a network segment for the VMware Cloud Director Availability appliances to connect to. It can be an existing one or specially created for VMware Cloud Director Availability. Managing network segments is done directly through the VMware NSX-T Data Center UI deployed in Google Cloud VMware Engine. For further instructions, please refer to the VMware NSX-T Data Center *user documentation*.
2. Request a new public IP and forward it to the VMware Cloud Director Availability Cloud Tunnel appliance internal IP address.

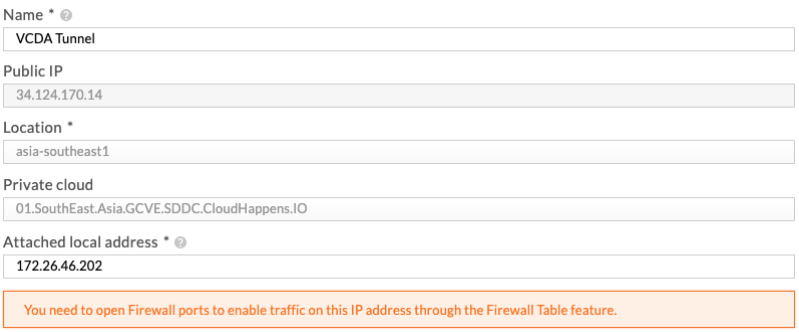

Figure 1: Google Cloud VMware Engine Public IP Request Form

3. Define a firewall table that will allow incoming traffic to the Cloud Tunnel.

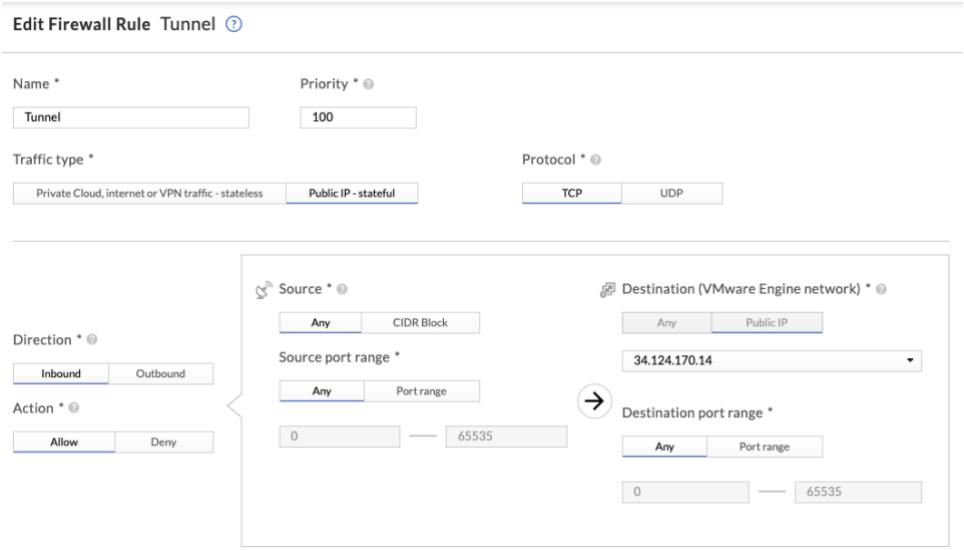

Figure 2: Google Cloud VMware Engine Firewall Table Configuration

VMware Cloud Director Availability Deployment

The VMware Cloud Director Availability appliances deployment is following the typical sequence of deployment steps that can be found in the *documentation*.

The only consideration to be made is during the Initial Setup Wizard when specifying the data engine (**Classic** or **VMC**). When the Classic data engine is selected, the **solution user** credentials need to be provided when connecting to the Lookup service. And when the VMC engine is selected, both **CloudOwner** and **solution user** can be used for connecting to the Lookup service.

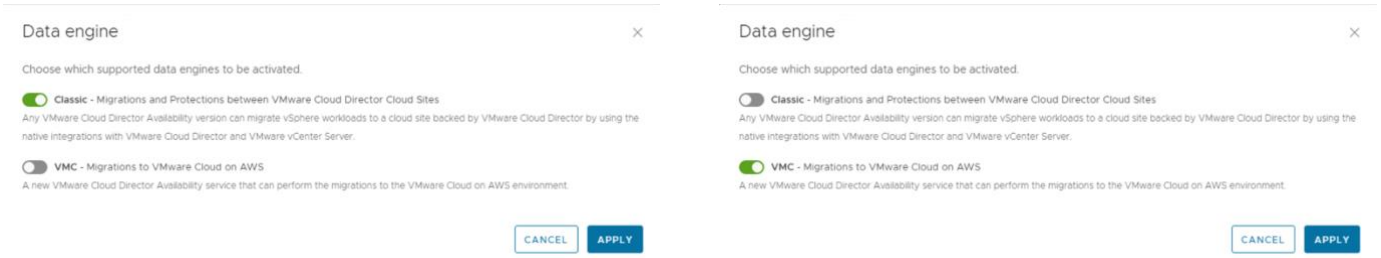

Figure 3: Data Engine Selection

Tested Scenarios

VMware Cloud Director Availability supports several different scenarios for protecting workloads to VMware Cloud Director service with a Google Cloud VMware Engine SDDC:

- On-Premises vSphere to VMware Cloud Director service with Google Cloud VMware Engine
- On-Premises VMware Cloud Director to VMware Cloud Director service with Google Cloud VMware Engine
- VMware Cloud Director service with VMC on AWS to VMware Cloud Director service with Google Cloud VMware Engine
- VMware Cloud Director service with Google Cloud VMware Engine to VMware Cloud Director service with Google Cloud VMware Engine

On-Premises vSphere to VMware Cloud Director service with Google Cloud VMware Engine

High-Level Architecture

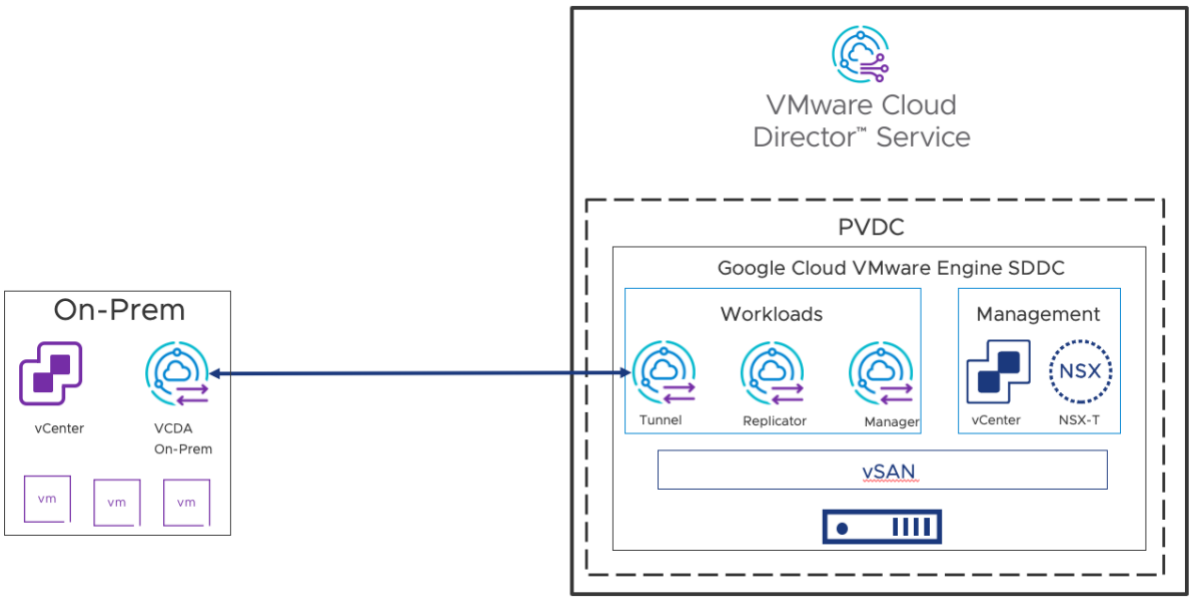

Figure 4: On-Premises to Cloud architecture

Possible Operations

Depending on the user account used during the VMware Cloud Director Availability configuration when deployed at the destination Google Cloud VMware Engine SDDC, there are two possible options for this scenario.

Data Engine	User	Migration	Protection	Reverse
VMC	CloudOwner@gve.local	Yes	N/A	N/A
Classic	Solution user	Yes	Yes	Yes

On-Premises VMware Cloud Director to VMware Cloud Director service with Google Cloud VMware Engine

High-Level Architecture

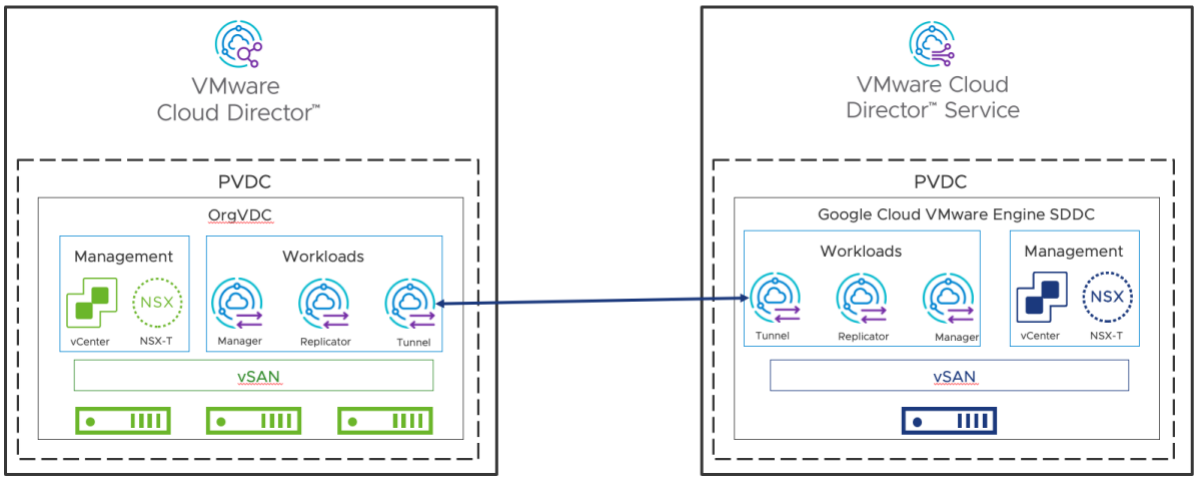

Figure 5: Cloud to Cloud architecture

Possible Operations

Depending on the user account used during the VMware Cloud Director Availability configuration when deployed at the destination Google Cloud VMware Engine SDDC, there are two possible options for this scenario.

Data Engine	User	Migration	Protection	Reverse
VMC	CloudOwner@gve.local	Yes	N/A	N/A
Classic	Solution user	Yes	Yes	Yes

VMware Cloud Director service with VMC on AWS to VMware Cloud Director service with Google Cloud VMware Engine

High-Level Architecture

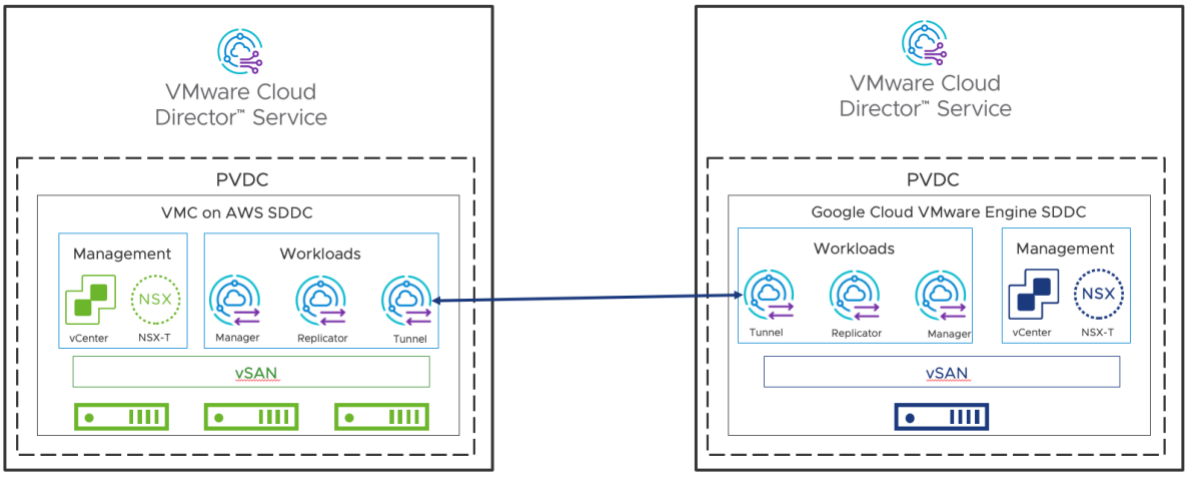

Figure 6: Cloud to Cloud architecture

Possible Operations

Due to the access specifics when VMware Cloud Director Availability is deployed at a VMC on AWS SDDC, only VMC data engine can be used for this scenario.

Data Engine	User	Migration	Protection	Reverse
VMC	CloudOwner@gve.local	Yes	N/A	N/A

VMware Cloud Director service with Google Cloud VMware Engine to VMware Cloud Director service with Google Cloud VMware Engine

High-Level Architecture

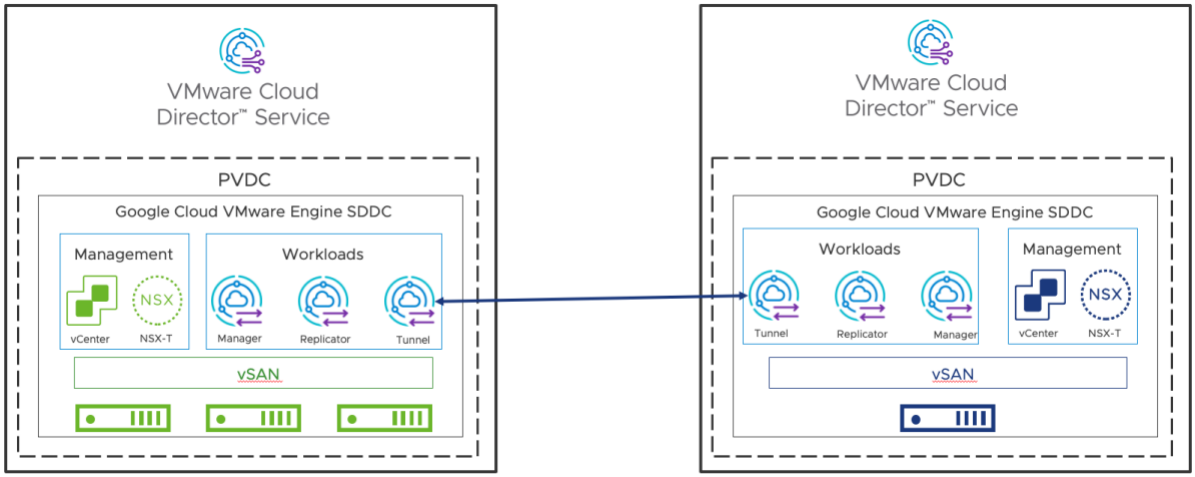

Figure 7: Cloud to Cloud architecture

Possible Operations

Depending on the user account used during the VMware Cloud Director Availability configuration when deployed at the destination Google Cloud VMware Engine SDDC, there are two possible options for this scenario.

Data Engine	User	Migration	Protection	Reverse
VMC	CloudOwner@gve.local	Yes	N/A	N/A
Classic	Solution user	Yes	Yes	Yes

Usage Meter Reporting

To meter the product consumption data of VMware Cloud Director Availability, you must add the product instance to vCloud Usage Meter.

When using a remotely deployed Usage Meter, you don't need any additional network configuration or firewall tables. You only need to specify the VMware Cloud Director Availability Endpoint URL in the vCloud Usage Meter UI to connect to the instance. However, this will require the **Allow admin access from anywhere** option to be set.

If you do not want to allow the admin access, then you will need to create an additional public endpoint for the VMware Cloud Director Availability Management appliance UI.

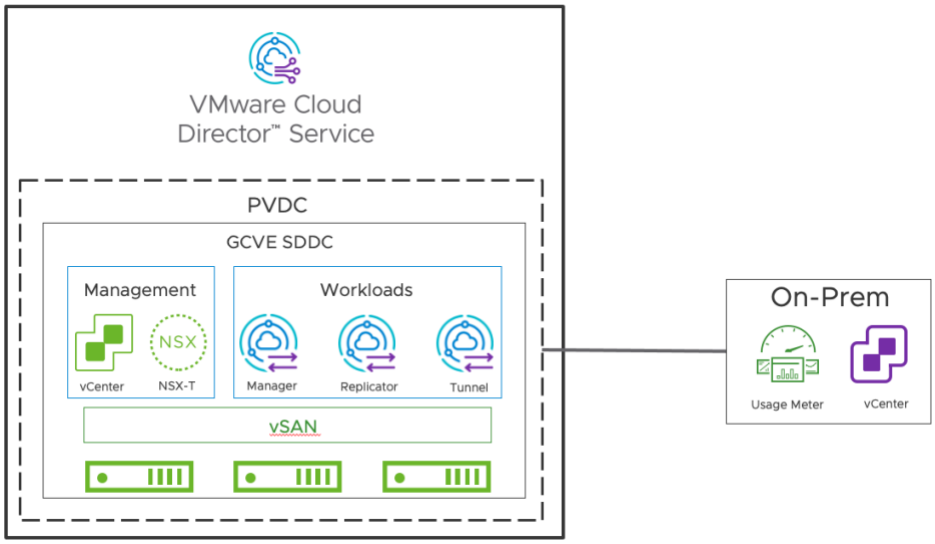

Figure 8: Architecture with a remotely deployed Usage Meter

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com