For production deployments, you need to deploy and configure dedicated VMware Cloud Director Availability Replicator appliance or appliances, it exposes the low-level data replication engine primitives as REST APIs.

A single appliance that contains the following services:
- VMware Cloud Director Availability Replicator Manager – a management service that operates on the vCenter Server level and understands its concepts for starting the replication workflow of the virtual machines. It must have TCP access to the Lookup Service and all the Replicator appliances.
- VMware Cloud Director Availability Replicator – Replication Manager with embedded VMware Cloud Director Availability Portal - provides the primary interface for the cloud and on-prem replication operations. It understands the VMware Cloud Director service (VMware Cloud Director) level concepts and communicates with its API through VMware Cloud Director LB.

Simplifies provider networking setup by channeling all incoming and outgoing traffic for a site through a single point - the VMware Cloud Director Availability Tunnel appliance. The traffic is both management and monitoring for the replication data (LWD traffic).

You must set an IP and port in the local site that is reachable for remote sites and forward it to the private address of the VMware Cloud Director Availability Tunnel appliance, port 8048 by using destination network address translation (DNAT). By using a public IP on the tunnel, you can migrate into the environment with any Internet connectivity. VMware Cloud Director Availability Appliance for Persons (On-premises Sites), which contains the binaries for the VMware Cloud Director Availability appliance.

Firewall rules should be configured to allow the VMware Cloud Director Availability appliances to communicate with the Management components.

For Cloud Services Providers, an existing vCloud Usage Meter agent hosted at an on-premises cloud can be used. There are two options for collecting the VMware Cloud Director Availability usage data:
- Use the VMware Cloud Director Availability Endpoint (Tunnel public IP address), root credentials and the Allow admin access from anywhere option set.
- Use another public address for directly accessing the VMware Cloud Director Availability Cloud Replication Management appliance, root credentials and the Do not allow admin sessions from the Internet option set.

The vSphere network interface (vmk) of your ESXi hosts needs to have vSphere Replication and vSphere Replication NIC options enabled so it can handle the replication traffic.

---

©2022 VMware, Inc. – Designed by the Cloud Provider Software Technical Product Management team.
VMware Cloud Director Availability is a powerful solution for Cloud Services Providers that offers migration capabilities from on-premises data centers or others clouds to Cloud Director service with Azure VMware Solution SDDC.

For production deployments, you need to deploy and configure dedicated VMware Cloud Director Availability Replicator appliance or appliances, it exposes the low-level data replication engine primitives as REST APIs.

A single appliance that contains the following services:
- VMware Cloud Director Availability Replication Manager – a management service that operates on the vCenter Server level and understands its concepts for starting the replication workflow of the virtual machines. It must have TCP access to the Lookup Service and all the Replicator appliances.
- VMware Cloud Director Availability vApp Replication Manager - provides the primary interface for the cloud and on-prem replication operations. It understands the VMware Cloud Director service (vSphere Cloud Director) level concepts and communicates with its API through VMware Cloud Director LB.

VMware Cloud Director Availability simplifies provider networking setup by channelling all incoming and outgoing traffic for a site through a single point – the VMware Cloud Director Availability Tunnel appliance. The traffic is both management and monitoring for the replication data (LWD traffic).

You must set an IP and port in the local site that is reachable for remote sites and forward to it the private address of the VMware Cloud Director Availability Tunnel appliance, port 8048 by using destination network address translation (DNAT). By using a public IP on the tunnel, you can migrate into the environment with any internet connectivity.

Firewall rules should be configured to allow the VMware Cloud Director Availability appliances to communicate with the Management components.

For Cloud Services Providers, an existing vCloud Usage Meter agent hosted at an on-premises cloud can be used. There are two options for collecting the VMware Cloud Director Availability usage data:
- Use the VMware Cloud Director Availability Endpoint (Tunnel public IP address), root credentials and the Allow admin access from any option set.
- Use another public address for directly accessing the VMware Cloud Director Availability Cloud Replication Management appliance, root credentials and the Do not allow admin sessions from the Internet option set.

Key

- Logical placement showing existing VMware Cloud Director service multi-tenant cloud environments.

©2022 VMware, Inc. – Designed by the Cloud Provider Software Technical Product Management team.