Technical White Paper: **August 2023**

Architecting VMware Cloud Director Availability Solution in a Multi-Cloud Environment

Shady Ali ElMalatawey
Sr. Staff Multi-Cloud Solutions Architect, VCDX #249
August 2023

Version 1.2

vmware®

Table of contents

Version History

Version Log		
Version	Date	Description
1.0	March 2023	• Initial Release • VCDA version 4.5
1.2	August 2023	• Update Release • VCDA version 4.6 • VCDA Cloud Tunnel Appliance High-availability added • Minor typos corrections

Introduction

VMware Cloud Director Availability (VCDA) is a Disaster-Recovery-as-a-Service (DRaaS) solution. It provides protection and migration for vApps, vApp templates and VMs. VMware Cloud Director Availability is available for the Cloud Service Providers in VMware Partner Connect Program and allows them to protect and migrate vApps, vApp templates and VMs:

- From on-premises vCenter Server site(s) to a VMware Cloud Director (VCD) or Cloud Director Service (CDS) cloud site(s).
- From a VCD or CDS cloud site(s) to an on-premises vCenter Server site(s).
- Between VCD and/or CDS clouds.

The goal of this document is to provide information how to architect a DRaaS solution for Cloud Director based clouds on VCDA 4.6.

Note: VMware Cloud Director Availability supports replicating vApp templates between VCD/CDS clouds only. Replicating vCenter vApp templates from on-premises vCenter Server sites to the cloud is not supported.

Note: VMware Cloud Director Availability and vSphere Replication are two different and independent products and there is no interoperability between them. Both products can coexist in a single vSphere infrastructure but it's not possible to replicate and migrate virtual machines between them.

VMware Cloud Director Availability Components

VCDA can protect and migrate vApps, vApp templates and VMs between on-premises sites and cloud sites.

In each cloud site, one or more VCDA instances must be deployed. Each VCDA instance consists of the following components:

- One or two Cloud Tunnel Appliances
- One Cloud Replication Manager Appliance
- One or more Cloud Replicator Appliances

Each VCDA instance in any cloud site can be associated only with one vSphere Single Sign-on (SSO) domain used in the resources vSphere infrastructure where workloads are hosted. Hence, if multiple vSphere SSO domains exist in the resources vSphere infrastructure, multiple VCDA instances must be deployed and configured. For other concurrency and scale limit factors which may affect the number of deployed VCDA instances per each cloud site, refer to VMware Configuration Maximums.

Note: VCDA Combined appliance is not supported for production environments. It's supported only for labs and small Proof-of-Concept (POC) installations. Hence, it is not in the scope of this document.

In each on-premises site, one or more VCDA On-premises Appliance must be deployed to replicate or migrate VMs running in the tenant-managed vCenter Server environment.

Note: vSphere DR & Migration capabilities are not in the scope of this document.

Cloud Tunnel Appliance

Cloud Tunnel Appliance is a dedicated appliance for the Tunnel Service, which will be the single point which channels all the site traffic (management and replication data traffic). This simplifies networking and security setup by channelling all types of traffic through a single tunnelled/encrypted endpoint. With VCDA 4.6, one or two Cloud Tunnel Appliances are deployed within each VCDA instance to provide high availability for the Tunnel Service. For more information, refer to Cloud Tunnel Appliance High Availability section in this document.

Cloud Replication Manager Appliance

Cloud Replication Management Appliance is a dedicated cloud appliance that runs the Manager Service. This is a management service operating with vCenter Server-level concepts for managing the replication workflow, and it must have TCP access to the vCenter Server, Lookup Service and all the Replicator appliances. The appliance also runs the Cloud Service with embedded VCDA Portal, which provides the main interface for replication operations and operates with Cloud Director-level concepts and works with vApps, vApp templates and VMs. Only one Cloud Replication Manager Appliance is deployed within each VCDA instance.

Cloud Replicator Appliance

Cloud Replicator Appliances are dedicated cloud appliances for the Replicator Service that handle the replication traffic for a site and expose the low-level Host-Based Replication (HBR) primitives as REST API calls.

The number of the Cloud Replicator Appliances is determined by the number of active protections per each appliance. We recommend deploying at least two Cloud Replicator Appliances per each VCDA instance. This will distribute the replicators utilization between different hosts and allow maintenance of an appliance while moving live replications to the other appliances. Scaling the number of the Cloud Replicator Appliances enables scaling the number of active replications. For tested concurrency and scale limits, refer to VMware Configuration Maximums.

Note: Scaling the number of Cloud Replicator Appliances does not increase the total replication speed. It increases the maximum of active simultaneous replications. Use the vSphere Replication Calculator to calculate the replication bandwidth required or the minimum achievable RPO in your environment.

On-Premises Appliance

On-Premises Appliance internally contains a Replicator Service and a Tunnel Service. Each appliance will be responsible for the migration of a group of tenant's VMs to a certain cloud site. A VM can be migrated by a single VCDA On-Premises Appliance only.

Each On-Premises Appliance in any on-premises site can be associated only with one vSphere SSO domain used in the resources vSphere infrastructure where workloads are hosted. Hence, if multiple vSphere SSO domains exist in the resources vSphere infrastructure, multiple On-Premises Appliances must be deployed and configured. In addition, each On-Premises Appliance can replicate workloads to a single destination. If different workloads are being migrated to different destinations, multiple appliances are required. For other concurrency and scale limit factors which may affect the number of deployed On-Premises Appliances, refer to VMware Configuration Maximums.

VMware Cloud Director Availability Deployment Models

VCDA deployment differs according to the site type, whether it is a cloud site or an on-premises site.

Provider-hosted Cloud Director Site

Provider-hosted Cloud Director site is a cloud site completely hosted and managed by the provider. The provider has an on-premises VMware Cloud Director installation and the underlying VMware (vSphere/NSX) infrastructure. One or more VCDA instances must be deployed and configured by the provider to establish VCDA Cloud Site.

Simplified Deployment Model

In the simplified deployment model, all VCDA instance components are deployed to a single network. This network can be the same management network where all other management components are connected. This simplifies networking and security configurations, and it is usually used in small to medium environments.

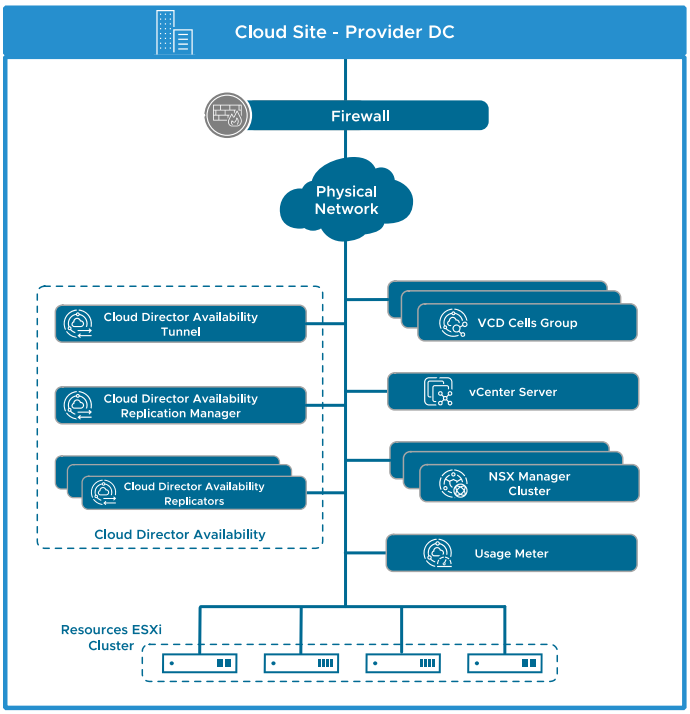

Figure 1: VCDA Simplified Deployment Model in a Provider-hosted Cloud Director Site

Advanced Deployment Model

In the advanced deployment model, each VCDA component is deployed to a certain network and certain vSphere cluster according to its purpose. This deployment model is usually used in large environments or security-strict environments.

Table 1 - Recommended VCDA Components Deployment Locations

VCDA Component	Location
Cloud Tunnel Appliance	• DMZ network for external accessibility. • DMZ vSphere cluster or Edge vSphere cluster (if either exists) or resources vSphere cluster.
Cloud Replication Manager Appliance	• Management network for accessibility to other management components, like vCenter Server and VCD. • Management vSphere cluster.

Cloud Replicator Appliances	• Replication network where replication enabled VMKernel ports of resources ESXi hosts are connected. This will prevent replication traffic hopping across different networks. Each appliance must have two network interfaces, one interface would be connected to a routed network to reach other VCDA appliances and the external components, and the other interface would be connected to the replication network of ESXi hosts for replication traffic. • Resources vSphere cluster for simplified networking configuration.

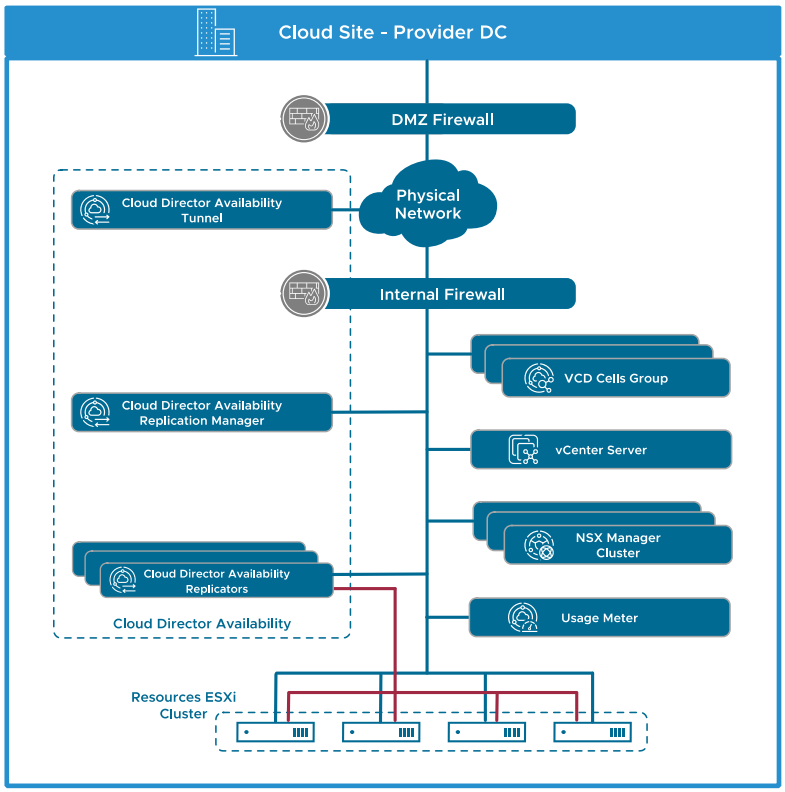

Figure 2: VCDA Advanced Deployment Model in a Provider-hosted Cloud Director Site

Cloud-hosted VMware Solution with Cloud Director Service

This is a cloud site which is hosted completely outside the provider data center(s). The provider is using CDS instance to manage a VMware Solution on one of the hyperscale clouds, like VMware Cloud on AWS (VMC on AWS or VMC for short), Azure VMware Solutions (AVS), Google Cloud VMware Engine (GCVE) or Oracle Cloud VMware Solution (OCVS).

In this scenario, one or more VCDA instances are deployed directly on the VMware Solution and connected to a single network behind the T1 gateway (Compute Gateway in case of VMC) as shown in the following figures

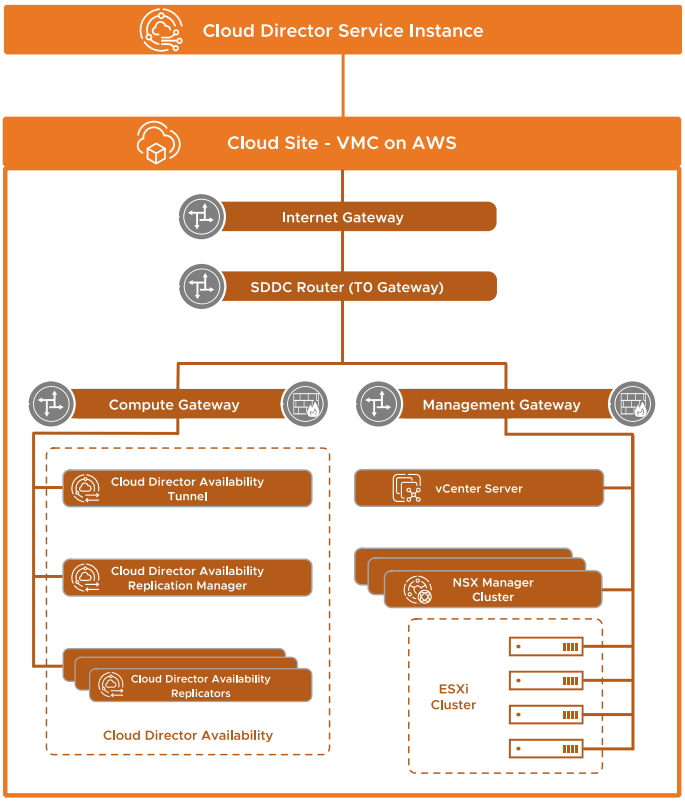

Figure 3: VCDA Deployment Model in a CDS-managed VMC Cloud Site

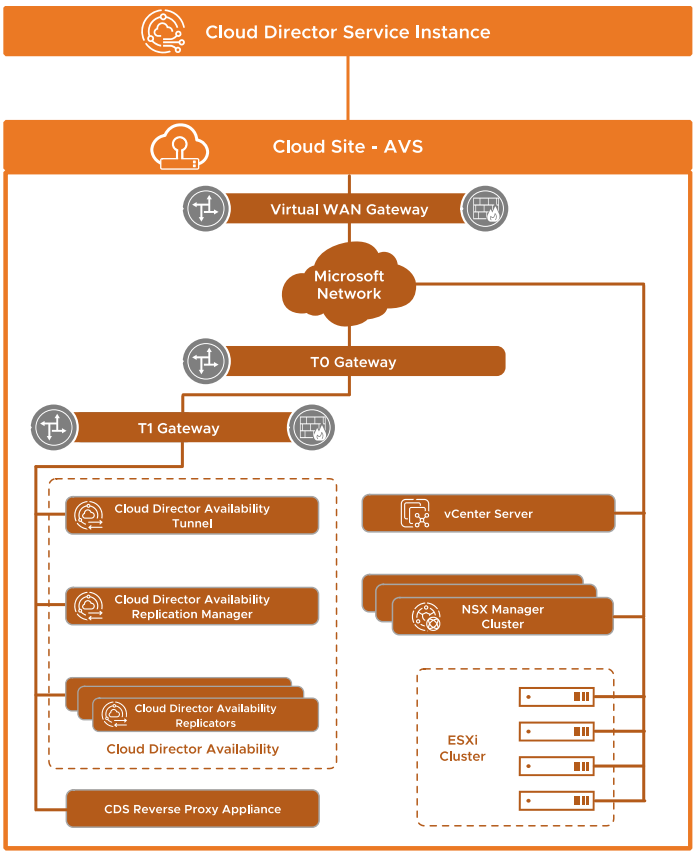

Figure 4: VCDA Deployment Model in a CDS-managed AVS Cloud Site

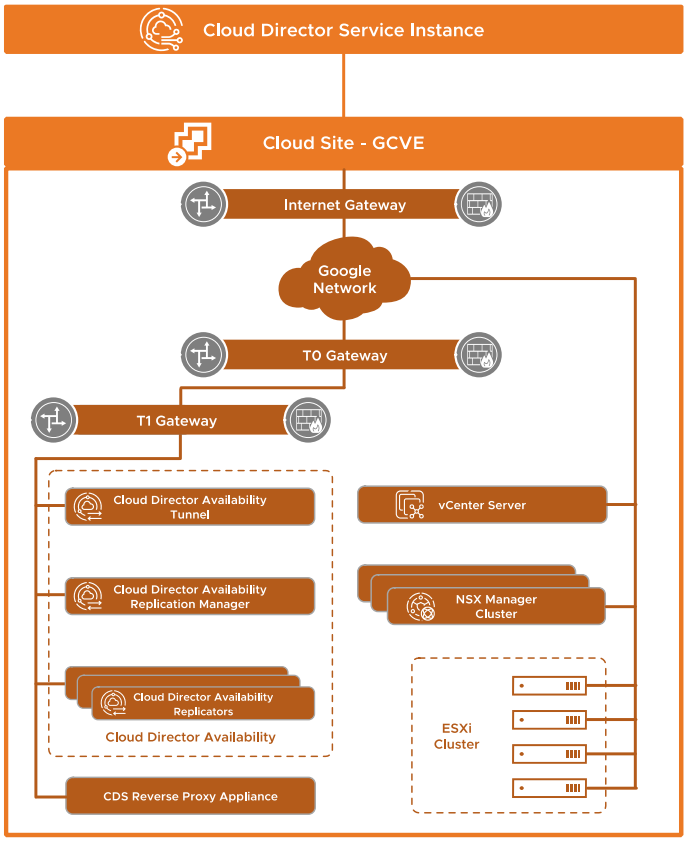

Figure 5: VCDA Deployment Model in a CDS-managed GCVE Cloud Site

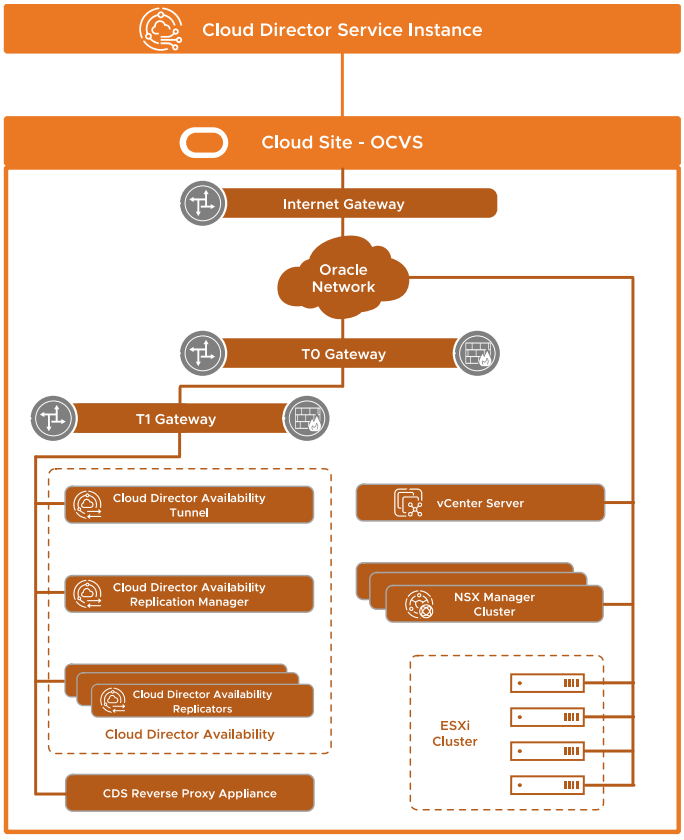

Figure 6: VCDA Deployment Model in a CDS-managed OCVS Cloud Site

Provider-hosted VMware Infrastructure with Cloud Director Service

This is a hybrid cloud site, where the provider hosts and manages VMware (vSphere/NSX) infrastructure for the cloud resources while using CDS instance to manage the infrastructure. In this model, one or more VCDA instances are deployed on the provider infrastructure and connected to CDS to establish the cloud site. The VCDA deployment models, mentioned in Provider-hosted Cloud Director Site section, are applicable.

Tenant On-Premises Site

This is an on-premises data center hosted and managed by the tenant. Usually, it is considered as the source location of tenant VMs/workloads. The tenant deploys one or more VCDA On-Premises Appliances to protect or onboard/migrate VMs to one or more cloud sites.

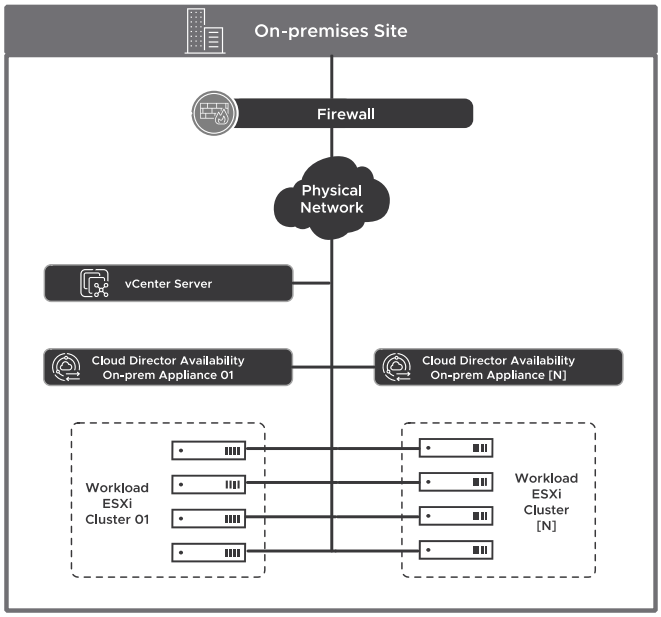

Figure 7: VCDA On-Premises Appliance Deployment Model in a Tenant-managed On-premises Site

Cloud Tunnel Appliance High Availability

With VCDA 4.6, the provider can now deploy one or two Cloud Tunnel Appliances to achieve high availability for the Tunnel Service. After deploying the VCDA instance with the initial Cloud Tunnel Appliance, the provider can add a second Cloud Tunnel Appliance to the instance. The two Cloud Tunnel Appliances can operate in Active/Active mode. This might also positively impact the performance of the appliances as the traffic will be balanced between them.

This new setup is only available for the cloud sites and requires an external load balancer to distribute traffic between the two appliances. It is recommended to use NSX Advanced Load Balancer with a dedicated Service Engine Group (SEG) for the Tunnel Service load balancing. However, any other third-party load balancer or native hyperscale cloud load balancer service is supported.

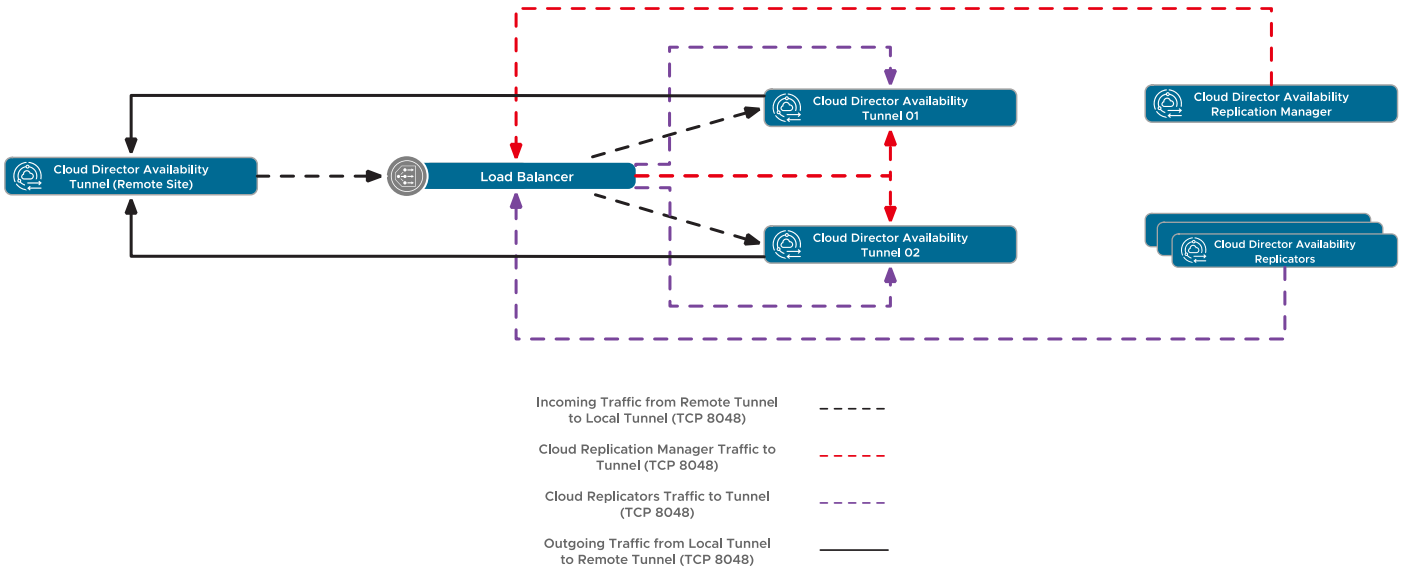

Figure 8: Cloud Tunnel Appliance High Availability High-level Traffic Flow

Note: Although any third-party load balancer is supported, VMware carried only testing on NSX Advanced Load Balancer configuration at the time of writing this document.

Design Considerations

There are few design considerations for the Cloud Tunnel Appliance HA:

- The high availability configuration can only be applied to the cloud site and not to the on-premises site.
- Any load balancer used must support TCP Layer 4 (L4) load balancing.
- TLS/HTTPS termination and TLS/HTTPS inspection are not supported and, if present, will result in service failure.
- In case of using NSX Advanced Load Balancer and due to the high volume of replication traffic, it is highly recommended to use a dedicated VMware NSX Advanced Load Balancer Service Engine Group for load balancing the VMware Cloud Director Availability Tunnels.
- To correctly scale the Service Engines, please refer to the VMware NSX Advanced Load Balancer Sizing Compute and Storage Resources. Alternatively, refer to the third-party load balancer sizing guide for the correct sizing.
- The load-balanced Public Service Endpoint address should be reachable and properly resolvable from the internal network for the other appliances to operate as well as externally for the tenant and remote sites access.

Greenfield Deployment Workflow

The provider needs to complete the following steps at each cloud site to enable the high availability of the Cloud Tunnel Appliance:

- Deploy the initial VCDA instance appliances with one Cloud Tunnel Appliance.
- Run the initial configuration wizard to configure the VCDA instance.
- Deploy and configure the second Cloud Tunnel Appliance.
- Configure the load balancer virtual service.

  Note: The load balancer virtual service IP address must be reachable and properly resolvable from the internal network for the other appliances to operate as well as externally for the tenant and remote sites access.
- Configure the VCDA instance with the details of the load balancer virtual service and the second Cloud Tunnel Appliance.

For more information, refer to VMware Cloud Director Availability Official Documentation.

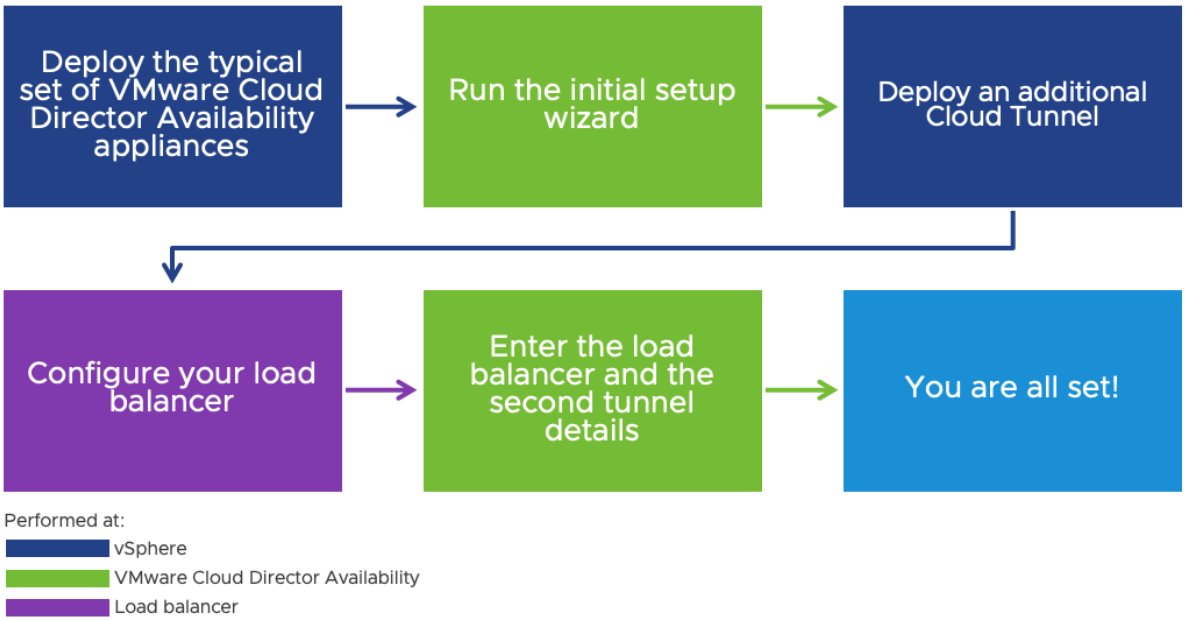

Figure 9: Greenfield Deployment Workflow for the Cloud Tunnel Appliance High Availability

Brownfield Deployment Workflow

The provider needs to complete the following steps at each cloud site to upgrade the VCDA instance version to a version where the Cloud Tunnel Appliances High Availability is available (4.6 or later) and then, enable it:

- Upgrade the VCDA instance to the latest version.
- Deploy and configure the second Cloud Tunnel Appliance.
- Configure the load balancer virtual service.

  Note: The load balancer virtual service IP address must be reachable and properly resolvable from the internal network for the other appliances to operate as well as externally for the tenant and remote sites access.
- Configure the upgraded VCDA instance with the details of the load balancer virtual service and the second Cloud Tunnel Appliance.

For more information, refer to VMware Cloud Director Availability Official Documentation.

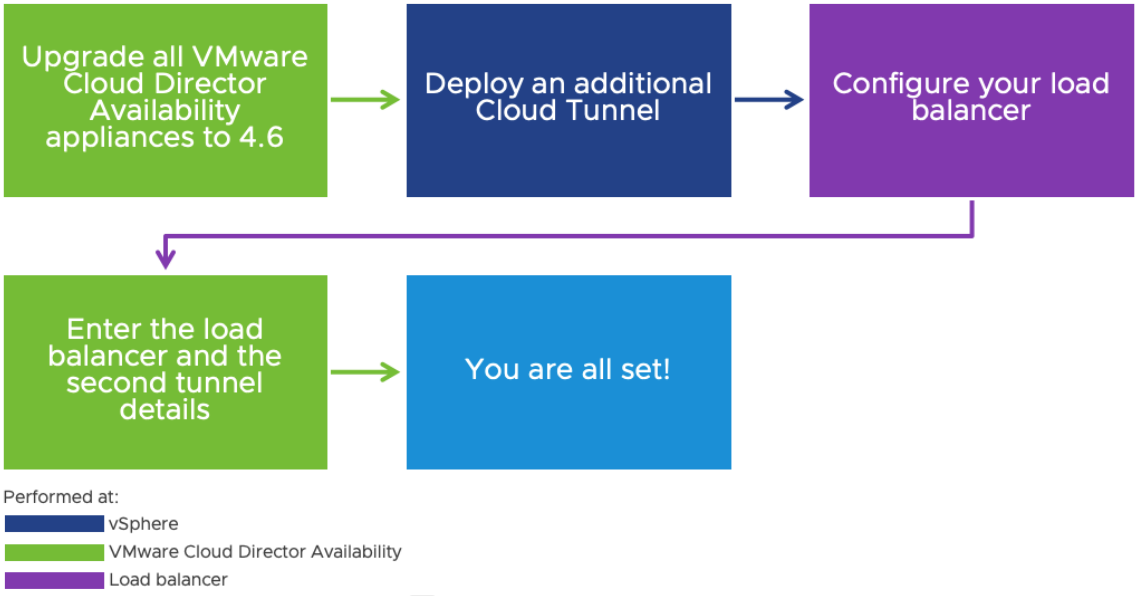

Figure 10: Brownfield Deployment Workflow for the Cloud Tunnel Appliance High Availability

Load Balancer Configuration

The following tables detail the load balancer configuration required

Table 2 - Recommended Configuration for Cloud Tunnel Appliance Load Balancer Virtual Service	
Attribute	Specifications
Type	L4 TCP Profile
Port	8048

Table 3 - Recommended Configuration for Cloud Tunnel Appliance Load Balancer Service Monitoring	
Attribute	Specifications
Type	Active Monitoring
Protocol	TCP
Port	8048
Send Interval	10 seconds
Receive Timeout	4 seconds
Successful Checks	3
Failed Checks	3

Table 4 - Recommended Configuration for Cloud Tunnel Appliance Load Balancer Pool Settings	
Attribute	Specifications

Default Port	8048
Load Balancing Algorithm	Round Robin
Connection Ramp	10 seconds
Connections per Server	15,000
Connection Used Times	0
Cached Connections per Server	0
Default Server Timeout	60 seconds
Idle Timeout	60 seconds
Life Timeout	600 seconds
Enable TLS SNI	Enabled
Pool Health Monitor	Service Monitoring detailed in the previous table

Operational Considerations

There are few operational considerations for the Cloud Tunnel Appliance High Availability

- The Cloud Tunnel Appliances behind the load balancer operate in Active/Active mode. Neither of the Tunnel Appliances are primary or secondary as both appliances are considered equal for data routing purposes and do not perform flexible data routing.
- Incoming data bandwidth throttling operates differently with dual Cloud Tunnel Appliances configured. The throughput value limit applies to each appliance independently, and since the traffic is balanced between both, the aggregate incoming traffic may reach up to twice the configured individual limit. If one of the appliances reaches its cap while the other does not, the busy appliance can't borrow from the quota of the other appliance.
- In case only one of the cloud sites is running VCDA version 4.6 or newer:
    - Paired cloud sites running earlier versions, where the Cloud Tunnel Appliances High Availability is not yet available, will operate normally when paired with a cloud site running dual Cloud Tunnel Appliances, while both instances are operational. If one instance is down, these sites might experience management traffic issues. However, the data channel automatically recovers and the replication traffic continues without any intervention.
    - Paired on-premises sites running older VCDA versions where the Cloud Tunnel Appliances High Availability is not yet available, may in some cases experience connectivity issues when one of the Cloud Tunnel Appliances in the cloud site is not operational.

VMware Cloud Director Availability Use Cases and Supported Topologies

VCDA is a Disaster Recovery-as-a-Service (DRaaS) tool which supports different use cases:

- Cloud-to-Cloud (C2C) Disaster Recovery (DR)
- Ground-to-Cloud (G2C) Disaster Recovery (DR)
- Onboarding/Migration

For each of these use cases, VCDA can be deployed to a different combination of cloud and on-premises sites. According to the source and destination sites, certain VCDA Data Engine must be used. VCDA has two Data Engines:

- Classic Data Engine: The original HBR replication engine which supports migration and DR protection, failover, and reverse failover operations to the destination cloud site. This data engine can't be used if the source or the destination cloud site is CDS-managed VMC or AVS.
- VMC Data Engine: A new replication engine which supports only migration operation. This data engine must be used if the source or the destination cloud site is CDS-managed VMC or AVS.

VCDA Data Engines can co-exist on the same VCDA instance. During initial configuration, only one of the data engines can be selected. After the VCDA instance is installed and configured, both data engines can be enabled. For more information, refer to VCDA Official Documentation.

The following table summarizes the supported deployment topologies for different cloud or on-premises sites combinations

Table 5 - VCDA Supported Topologies for Different Use Cases

Source Site	Destination Site						
	Provider-hosted VCD	CDS with VMC	CDS with AVS	CDS with GCVE	CDS with OCVS	CDS with Provider-hosted infra	VCDA On-Premises Appliance
Provider-hosted VCD	DR and Migration (Classic Data Engine)	Migration Only (VMC Data Engine)	Migration Only (VMC Data Engine)	DR and Migration (Classic Data Engine)	DR and Migration (Classic Data Engine)	DR and Migration (Classic Data Engine)	DR and Migration (Classic Data Engine)
CDS with VMC	Migration Only (VMC Data Engine)	Migration Only (VMC Data Engine)	Migration Only (VMC Data Engine)	Migration Only (VMC Data Engine)	Migration Only (VMC Data Engine)	Migration Only (VMC Data Engine)	Migration Only (VMC Data Engine)
CDS with AVS	Migration Only (VMC Data Engine)	Migration Only (VMC Data Engine)	Migration Only (VMC Data Engine)	Migration Only (VMC Data Engine)	Migration Only (VMC Data Engine)	Migration Only (VMC Data Engine)	Migration Only (VMC Data Engine)
CDS with GCVE	DR and Migration (Classic Data Engine)	Migration Only (VMC Data Engine)	Migration Only (VMC Data Engine)	DR and Migration (Classic Data Engine)	DR and Migration (Classic Data Engine)	DR and Migration (Classic Data Engine)	DR and Migration (Classic Data Engine)
CDS with OCVS	DR and Migration (Classic Data Engine)	Migration Only (VMC Data Engine)	Migration Only (VMC Data Engine)	DR and Migration (Classic Data Engine)	DR and Migration (Classic Data Engine)	DR and Migration (Classic Data Engine)	DR and Migration (Classic Data Engine)
CDS with Provider-hosted infra	DR and Migration (Classic Data Engine)	Migration Only (VMC Data Engine)	Migration Only (VMC Data Engine)	DR and Migration (Classic Data Engine)	DR and Migration (Classic Data Engine)	DR and Migration (Classic Data Engine)	DR and Migration (Classic Data Engine)
VCDA On-Premises Appliance	DR and Migration (Classic Data Engine)	Migration Only (VMC Data Engine)	Migration Only (VMC Data Engine)	DR and Migration (Classic Data Engine)	DR and Migration (Classic Data Engine)	DR and Migration (Classic Data Engine)	N/A

Cloud-to-Cloud (C2C) Disaster Recovery

In this use case, the provider uses VCDA to protect, failover and reverse failover tenant VMs between different cloud sites. The provider deploys one or more VCDA instances in each cloud site, then configures site pairing between each two VCDA instances to establish full mesh as needed. All VCDA instances must be configured to use Classic Data Engine.

Any VM can be protected by a single VCDA instance which is configured with the vSphere SSO domain of the parent vCenter Server and the VM can be replicated to a single destination.

The following table and figure show the supported combination of cloud sites for VCDA C2C disaster recovery

Table 6 - VCDA Supported Topologies for Cloud-to-Cloud Disaster Recovery (C2C DR) Use Case

Source Site	Destination Site			
	Provider-hosted VCD	CDS with GCVE	CDS with OCVS	CDS with Provider-hosted infra
Provider-hosted VCD	☑	☑	☑	☑
CDS with GCVE	☑	☑	☑	☑
CDS with OCVS	☑	☑	☑	☑
CDS with Provider-hosted infra	☑	☑	☑	☑

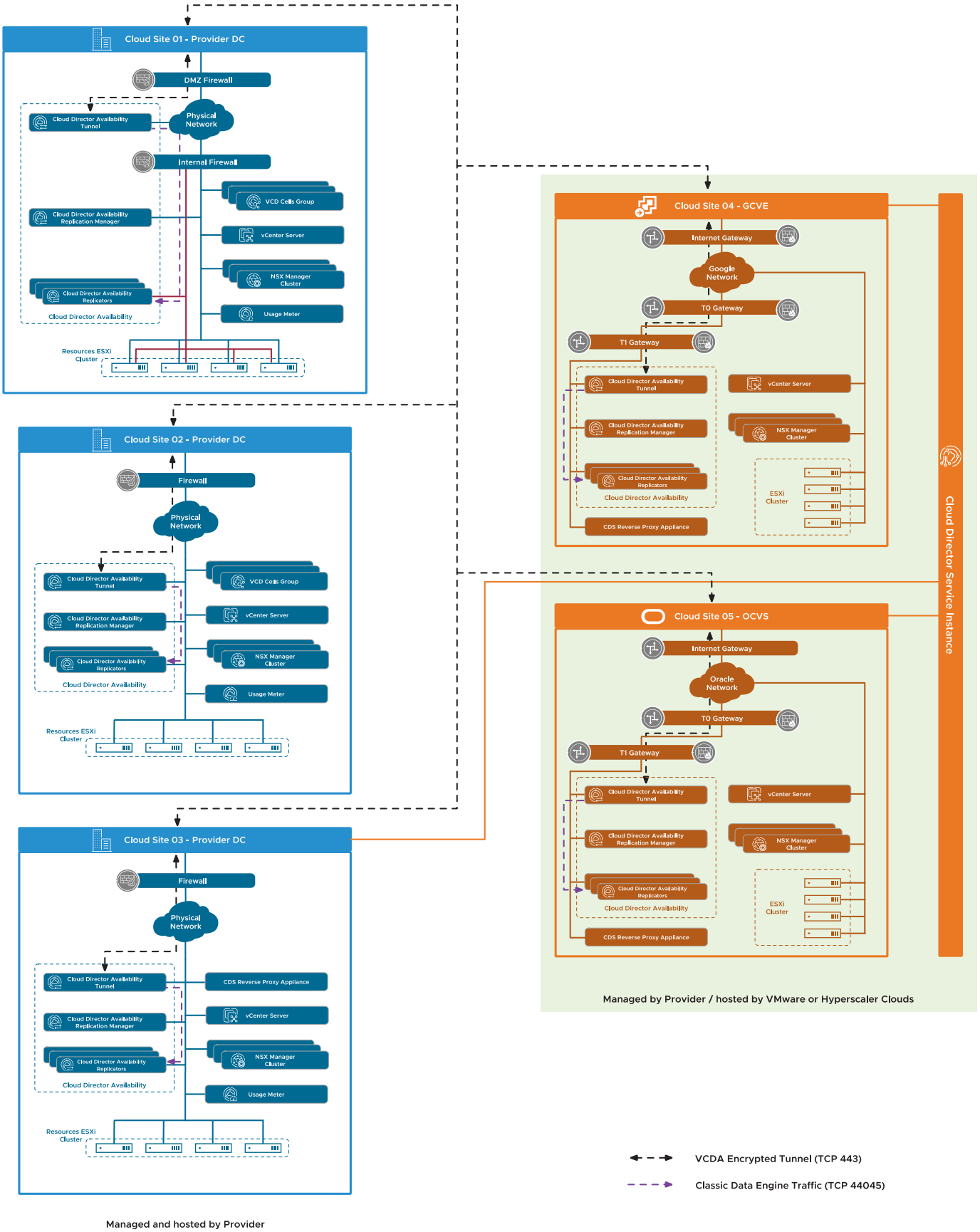

Figure 11: VCDA Supported Topology for C2C DR Use Case

Ground-to-Cloud (G2C) Disaster Recovery

In this use case, the provider uses VCDA to protect, fail over and reverse fail over tenant VMs between on-premises tenant's data center(s) and cloud site(s). The provider must configure the VCDA instance(s) in the cloud sites to use the Classic Data Engine.

One or more VCDA On-Premises Appliances must be deployed and configured in the tenant's data center(s). Each VCDA On-Premises Appliance can be paired to a single cloud site. Any VM can be protected by a single VCDA On-Premises Appliance which is configured with the same vSphere SSO domain of the parent vCenter Server and the VM can be replicated to a single destination cloud site. If multiple vCenter Servers exist in the same vSphere SSO domain and the requirement is to do replications from the cloud site to the on-premises site, then each vCenter Server needs a dedicated appliance due to the way how placement works.

The following table and figure show the supported combination of on-premises and cloud sites for G2C disaster recovery

Table 7 - VCDA Supported Topologies for Ground-to-Cloud Disaster Recovery (G2C DR) Use Case

Source Site	Destination Site			
	Provider-hosted VCD	CDS with GCVE	CDS with OCVS	CDS with Provider-hosted infra
VCDA On-Premises Appliance	☑	☑	☑	☑

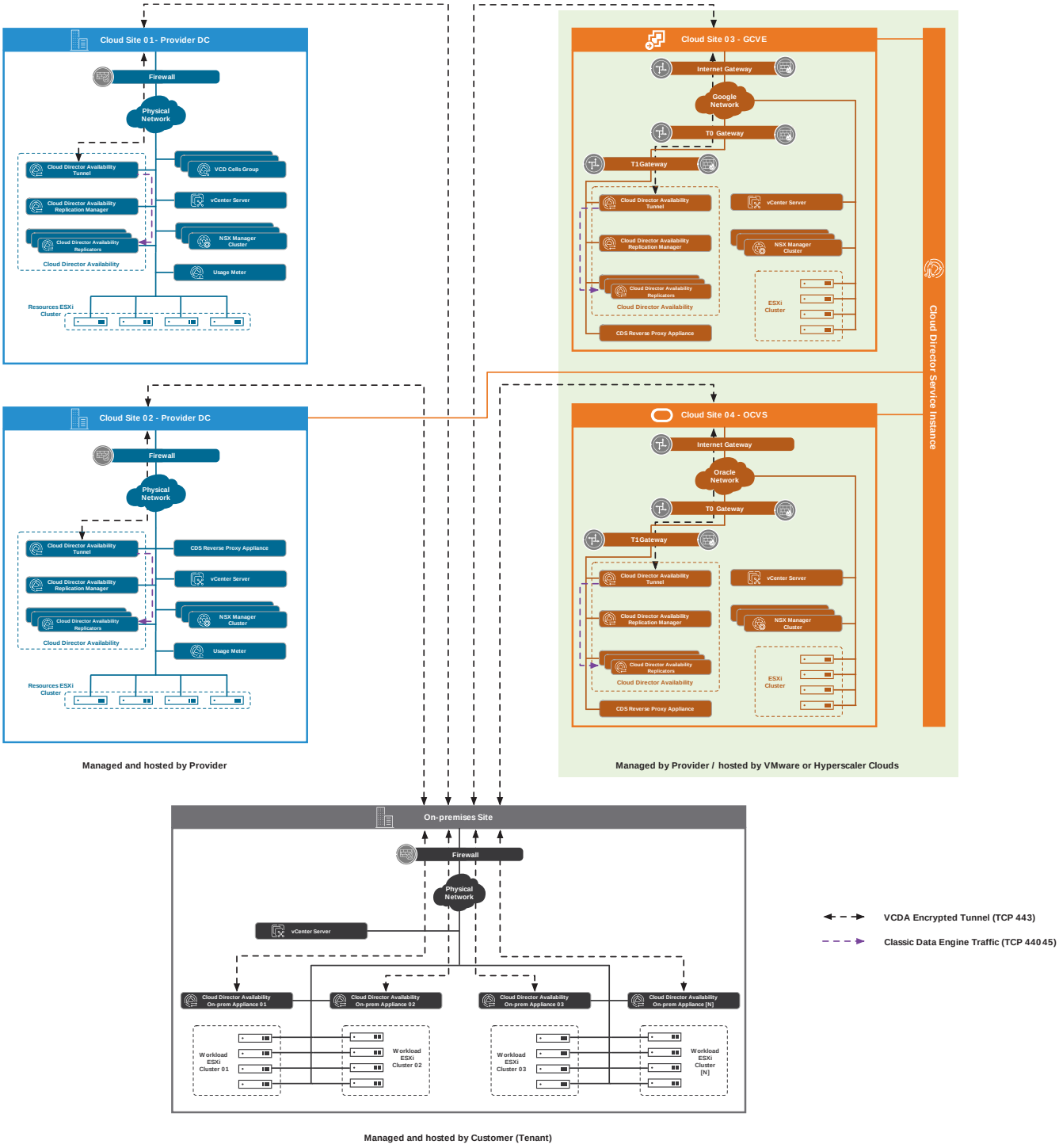

Figure 12: VCDA Supported Topology for G2C DR Use Case

Onboarding/Migration

In this use case, the provider uses VCDA to onboard/migrate tenant VMs from the on-premises data center(s) to the cloud, to migrate tenant VMs between different cloud sites and/or to evacuate tenant VMs from a cloud site to an on-premises data center(s).

In the cloud site(s), the provider deploys one or more VCDA instances in each cloud site, then configures site pairing between each two VCDA instances to establish full mesh as needed.

In the tenant's data center(s), one or more VCDA On-Premises Appliances must be deployed and configured, then each appliance must be paired with a single cloud site.

Both VCDA Data Engines can be used according to the source and the destination and both engines can co-exist on the same VCDA instance. The Cloud service on the destination VCDA Cloud Replication Manager Appliance negotiates with the Cloud service on the source appliance which data engine to be used for migration configuration. If a common data engine is enabled on both sites, this data engine will be used. If both data engines are enabled on both sites, Classic Data Engine takes precedence. If no common data engine is found between both sites, migration configuration fails. In case of migrations from/to VCDA On-Premises Appliance, the Cloud service in the cloud site determines which data engine to be used.

The following table and figure show the supported combination of on-premises and cloud sites for the onboarding/migration use case.

Table 8 - VCDA Supported Topologies for Onboarding/Migration Use Case

Source Site	Destination Site						
	Provider-hosted VCD	CDS with VMC	CDS with AVS	CDS with GCVE	CDS with OCVS	CDS with Provider-hosted infra	VCDA On-Premises Appliance
Provider-hosted VCD	Migration (Both Data Engines)	Migration (VMC Data Engine)	Migration (VMC Data Engine)	Migration (Both Data Engines)	Migration (Both Data Engines)	Migration (Both Data Engines)	Migration (Both Data Engines)
CDS with VMC	Migration (VMC Data Engine)	Migration (VMC Data Engine)	Migration (VMC Data Engine)	Migration (VMC Data Engine)	Migration (VMC Data Engine)	Migration (VMC Data Engine)	Migration (VMC Data Engine)
CDS with AVS	Migration (VMC Data Engine)	Migration (VMC Data Engine)	Migration (VMC Data Engine)	Migration (VMC Data Engine)	Migration (VMC Data Engine)	Migration (VMC Data Engine)	Migration (VMC Data Engine)
CDS with GCVE	Migration (Both Data Engines)	Migration (VMC Data Engine)	Migration (VMC Data Engine)	Migration (Both Data Engines)	Migration (Both Data Engines)	Migration (Both Data Engines)	Migration (Both Data Engines)
CDS with OCVS	Migration (Both Data Engines)	Migration (VMC Data Engine)	Migration (VMC Data Engine)	Migration (Both Data Engines)	Migration (Both Data Engines)	Migration (Both Data Engines)	Migration (Both Data Engines)
CDS with Provider-hosted infra	Migration (Both Data Engines)	Migration (VMC Data Engine)	Migration (VMC Data Engine)	Migration (Both Data Engines)	Migration (Both Data Engines)	Migration (Both Data Engines)	Migration (Both Data Engines)
VCDA On-Premises Appliance	Migration (Both Data Engines)	Migration (VMC Data Engine)	Migration (VMC Data Engine)	Migration (Both Data Engines)	Migration (Both Data Engines)	Migration (Both Data Engines)	N/A

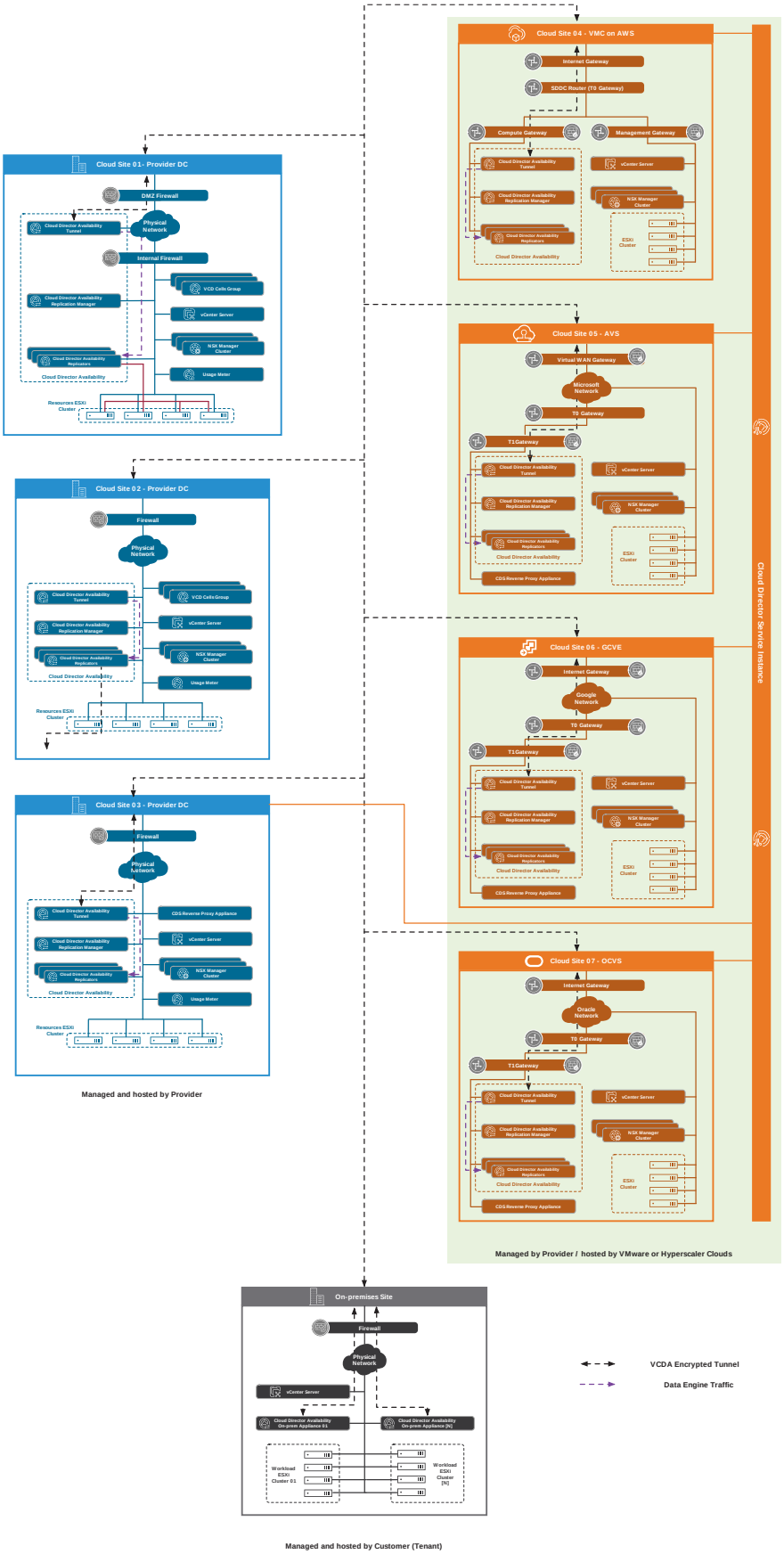

Figure 13: VCDA Supported Topology for Onboarding/Migration Use Case

VMware Cloud Director Availability Traffic Flow and Communication Matrix

There are several types of traffic flows within VCDA deployment:

- Management / Control traffic: which is related to administration, protection, and replication operations, monitoring and statistics.
- Replication / Data traffic

In any cloud site, the Tunnel service on VCDA Cloud Tunnel Appliance is the entry point for all traffic flows through the encrypted TLS tunnel. Only the VCDA Cloud Tunnel Appliance needs to have a dedicate externally accessible endpoint (VCDA Tunnel Endpoint) because it receives requests to establish encrypted TLS tunnels to other cloud or on-premises sites. The Tunnel service forwards the traffic to VCDA Cloud Replication Manager or Cloud Replicator Appliances.

In any tenant's on-premises site, the Tunnel service on VCDA On-Premises Appliance is the entry point for all traffic flows. Although VCDA On-Premises Appliance needs to have access externally, it only initiates the encrypted TLS tunnel to the paired cloud site. Hence, VCDA On-Premises Appliance does not need to have a dedicated externally accessible endpoint (VCDA Tunnel Endpoint). The Tunnel service on VCDA On-Premises Appliance forwards the traffic internally to the Replicator service.

Provider-hosted Cloud Director Site

The following diagram and tables show the traffic flow in a provider-hosted Cloud Director site as well as the required NAT rules for external accessibility

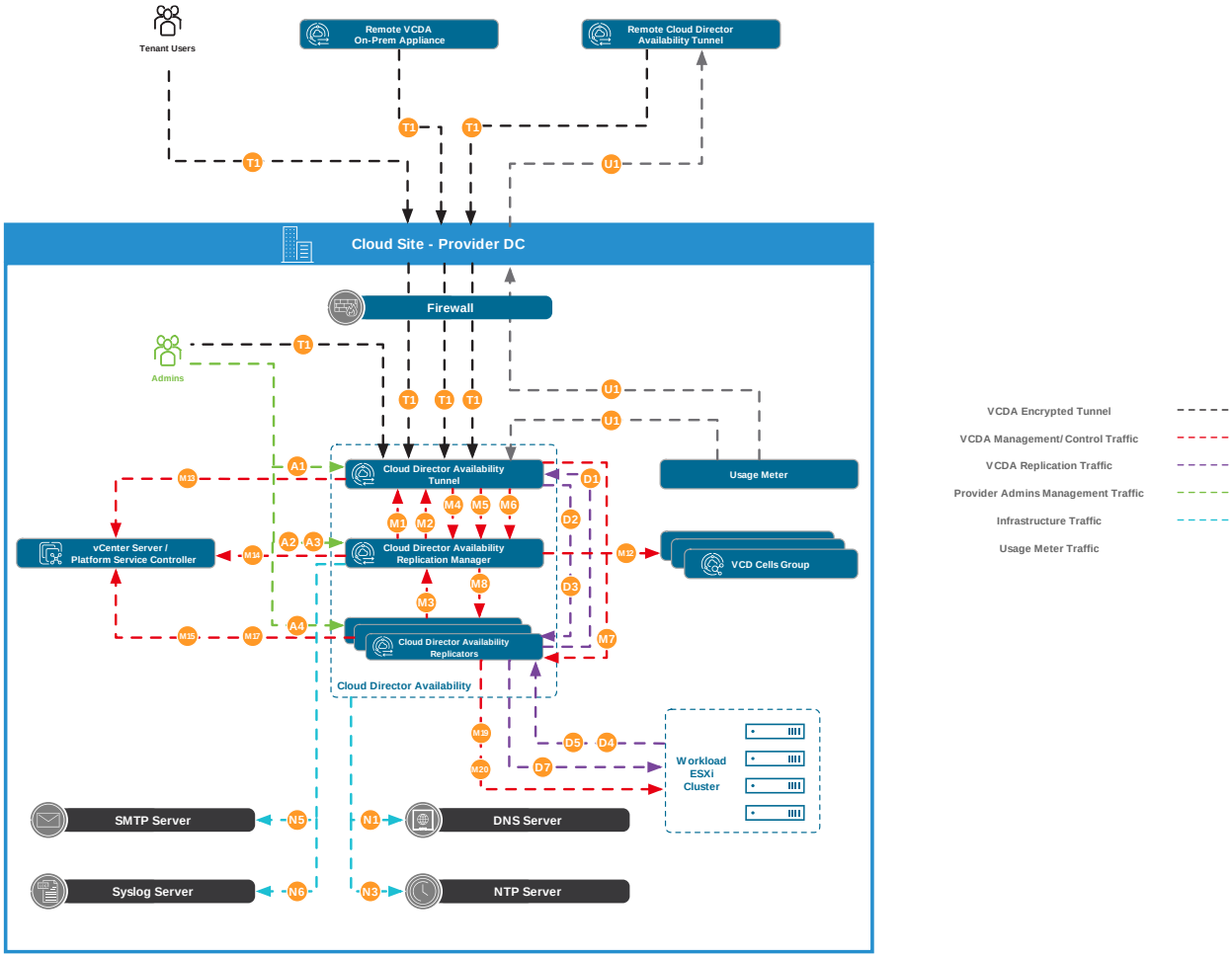

Figure 14: VCDA Traffic Flows in a Provider-hosted Cloud Director Cloud Site

Table 9 - VCDA Traffic Flows in a Provider-hosted Cloud Director Cloud Site				
Legend	Source	Destination	Protocol / Port	Description
T1	- Remote Cloud Tunnel Appliance(s) Public IPs - Remote VCDA On-prem Appliance(s) Public IPs - VCD Plugin Users	Cloud Tunnel Appliance or Tunnel Load Balancer VIP	TCP 8048	Used to access to the local VCDA Tunnel Endpoint
U1	vCloud Usage Meter Appliance	- Cloud Tunnel Appliance or Tunnel Load Balancer VIP - Remote Cloud Tunnel Appliance(s) Public IPs or Tunnel Load Balancer VIP Public IP	TCP 8048	Used to access to the local VCDA Tunnel Endpoint for metering / reporting purposes
A1	Admins	Cloud Tunnel Appliance	TCP 443 / 8442	Used for administrative login to the Tunnel Service to perform administrative operations
A2	Admins	Cloud Replication Manager Appliance	TCP 443	Used for administrative login to the Cloud Service to perform administrative operations
A3	Admins	Cloud Replication Manager Appliance	TCP 8441	Used for administrative login to the Manager Service to perform administrative operations
A4	Admins	Cloud Replicator Appliance(s)	TCP 443 / 8440	Used for administrative login to the Replicator Service to perform administrative operations
M1	Cloud Replication Manager Appliance	Cloud Tunnel Appliance or Tunnel Load Balancer VIP	TCP 8048	Used by the Cloud Replication Management Appliance for management traffic to the remote Replicator Appliances through the Tunnel Service
M2	Cloud Replication Manager Appliance	Cloud Tunnel Appliance	TCP 8047	Used by the Cloud Replication Management Appliance for management traffic to the Tunnel Service related to local site operations
M3	Cloud Replicator Appliance(s)	Cloud Replication Manager Appliance	TCP 8044	Used by the Replicator Service for management traffic to the Cloud Replication Management Appliance
M4	Cloud Tunnel Appliance	Cloud Replication Manager Appliance	TCP 8443	Used by the Tunnel Service for communication with the cloud service in Cloud Replication Management Appliance for serving VCDA portal
M5	Cloud Tunnel Appliance	Cloud Replication Manager Appliance	TCP 8046	Used by the Tunnel Service for management communication with the cloud service in Cloud Replication Management Appliance
M6	Cloud Tunnel Appliance	Cloud Replication Manager Appliance	TCP 8044	Used by the Tunnel Service for general communication with the manager service in Cloud Replication Management Appliance.
M7	Cloud Tunnel Appliance	Cloud Replicator Appliance(s)	TCP 8043	Used by the Tunnel Service for management traffic to the Replicator Service

M8	Cloud Replication Manager Appliance	Cloud Replicator Appliance(s)	TCP 8043	Used by the Cloud Replication Management Appliance for management traffic to the Replicator Service
M12	Cloud Replication Manager Appliance	VMware Cloud Director	TCP 443	Used by the Cloud Replication Management Appliance for interaction with the VMware Cloud Director API
M13	Cloud Tunnel Appliance	Platform Services Controller	TCP 443	Optionally used for single sign-on login to the Tunnel Service
M14	Cloud Replication Manager Appliance	Platform Services Controller	TCP 443	Used by the Cloud Replication Management Appliance to communicate with the vCenter Server Lookup service located on the Platform Services Controller
M15	Cloud Replicator Appliance(s)	Platform Services Controller	TCP 443	Used by the Replicator Service to communicate with the vCenter Server Lookup service located on the Platform Services Controller
M17	Cloud Replicator Appliance(s)	vCenter Server	TCP 443	Used by the Replicator Service for interaction with the vSphere API on the vCenter Server
M19	Cloud Replicator Appliance(s)	ESXi Hosts	TCP 80	Used by the Replicator Service to initiate the flows of replication traffic to the destination ESXi hosts. This port carries no replication traffic. This port is used only when Classic Data Engine is used.
M20	Cloud Replicator Appliance(s)	ESXi Hosts	TCP 443	Used by the Replicator Service to initiate the flows of replication traffic to the destination ESXi hosts. This port carries no replication traffic. This port is used only when VMC Data Engine is used.
D1	Cloud Replicator Appliance(s)	Cloud Tunnel Appliance or Tunnel Load Balancer VIP	TCP 8048	Used by the Replicator Service for replication traffic to the Tunnel Service
D2	Cloud Tunnel Appliance	Cloud Replicator Appliance(s)	TCP 44045	Used by the Tunnel Service for replication data traffic to the Replicator Service when Classic Data Engine is used
D3	Cloud Tunnel Appliance	Cloud Replicator Appliance(s)	TCP 3030	Used by the Tunnel Service for replication data traffic to the Replicator Service when VMC Data Engine is used
D4	ESXi Hosts	Cloud Replicator Appliance(s)	TCP 44046	Used by the source ESXi Hosts for replication data traffic to the Replicator Service
D5	ESXi Hosts	Cloud Replicator Appliance(s)	TCP 32032	Used by the source ESXi hosts for encrypted virtual machines replication traffic to the Replicator Service
D7	Cloud Replicator Appliance(s)	ESXi Hosts	TCP 902	Used by the Replicator Service to send replication data traffic to the destination ESXi hosts
N1	All VCDA Appliances	DNS Server	TCP/UDP 53	Used for name resolution
N3	All VCDA Appliances	NTP Server	UDP 123	Used for time synchronisation using NTPv4 as per RFC 5905
N5	Cloud Replication Manager Appliance	Syslog Server	UDP 514	Used by the Cloud Service for sending events to the syslog server
N6	Cloud Replication Manager Appliance	SMTP Server	TCP 25	Used by the Cloud Service to send events notifications emails to the SMTP server, as configured in VMware Cloud Director

Table 10 – Required NAT Rules in a Provider-hosted Cloud Director Cloud Site					
Legend	Type	Internal IP	Internal Port	External IP	External port
T1	DNAT	Cloud Tunnel Appliance or Tunnel Load Balancer VIP	TCP 8048	Public IP	User-Selected
U1	SNAT	vCloud Usage Meter Appliance	Any	Public IP	Any

Cloud-hosted VMware Solution with Cloud Director Service

The following sections detail the traffic flow and the required NAT rules in the different CDS-managed VMware solutions in the different hyperscale clouds

VMware Cloud on AWS (VMConAWS)

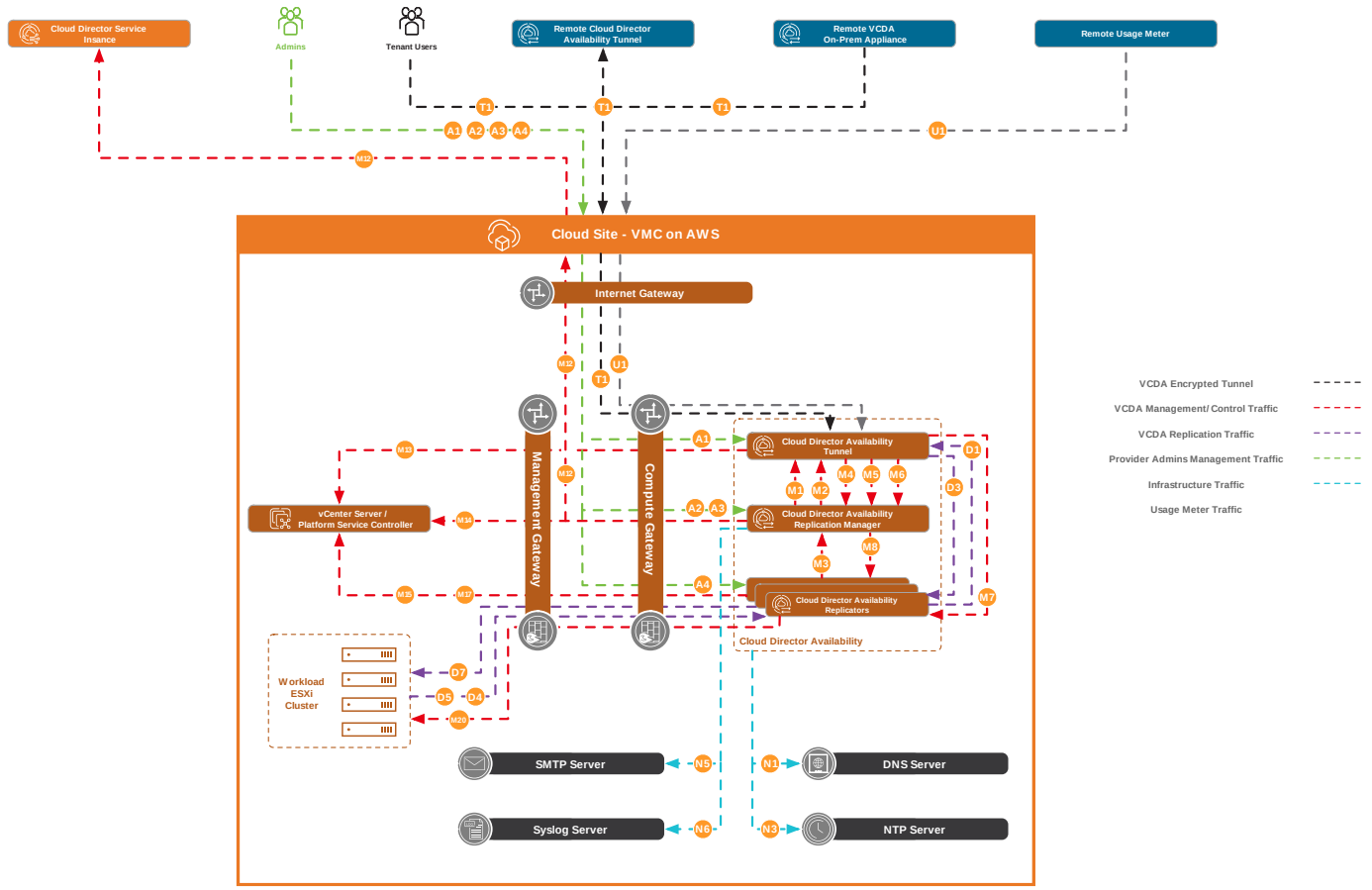

Figure 15: VCDA Traffic Flows in a CDS-managed VMC Cloud Site

Table 11 - VCDA Traffic Flows in a CDS-managed VMC Cloud Site				
Legend	Source	Destination	Protocol / Port	Description
T1	- Remote Cloud Tunnel Appliance(s) Public IPs - Remote VCDA On-prem Appliance(s) Public IPs - CDS Plugin Users	Cloud Tunnel Appliance or Tunnel Load Balancer VIP	TCP 8048	Used to access to the local VCDA Tunnel Endpoint
U1	Remote vCloud Usage Meter Appliance	Cloud Tunnel Appliance or Tunnel Load Balancer VIP	TCP 8048	Used to access to the local VCDA Tunnel Endpoint for metering / reporting purposes
A1	Admins	Cloud Tunnel Appliance	TCP 443 / 8442	Used for administrative login to the Tunnel Service to perform administrative operations
A2	Admins	Cloud Replication Manager Appliance	TCP 443	Used for administrative login to the Cloud Service to perform administrative operations

A3	Admins	Cloud Replication Manager Appliance	TCP 8441	Used for administrative login to the Manager Service to perform administrative operations
A4	Admins	Cloud Replicator Appliance(s)	TCP 443 / 8440	Used for administrative login to the Replicator Service to perform administrative operations
M1	Cloud Replication Manager Appliance	Cloud Tunnel Appliance or Tunnel Load Balancer VIP	TCP 8048	Used by the Cloud Replication Management Appliance for management traffic to the remote Replicator Appliances through the Tunnel Service
M2	Cloud Replication Manager Appliance	Cloud Tunnel Appliance	TCP 8047	Used by the Cloud Replication Management Appliance for management traffic to the Tunnel Service related to local site operations
M3	Cloud Replicator Appliance(s)	Cloud Replication Manager Appliance	TCP 8044	Used by the Replicator Service for management traffic to the Cloud Replication Management Appliance
M4	Cloud Tunnel Appliance	Cloud Replication Manager Appliance	TCP 8443	Used by the Tunnel Service for communication with the cloud service in Cloud Replication Management Appliance for serving VCDA portal
M5	Cloud Tunnel Appliance	Cloud Replication Manager Appliance	TCP 8046	Used by the Tunnel Service for management communication with the cloud service in Cloud Replication Management Appliance
M6	Cloud Tunnel Appliance	Cloud Replication Manager Appliance	TCP 8044	Used by the Tunnel Service for general communication with the manager service in Cloud Replication Management Appliance.
M7	Cloud Tunnel Appliance	Cloud Replicator Appliance(s)	TCP 8043	Used by the Tunnel Service for management traffic to the Replicator Service
M8	Cloud Replication Manager Appliance	Cloud Replicator Appliance(s)	TCP 8043	Used by the Cloud Replication Management Appliance for management traffic to the Replicator Service
M12	Cloud Replication Manager Appliance	CDS Instance Public URL	TCP 443	Used by the Cloud Replication Management Appliance for interaction with the Cloud Director API
M13	Cloud Tunnel Appliance	Platform Services Controller	TCP 443	Optionally used for single sign-on login to the Tunnel Service
M14	Cloud Replication Manager Appliance	Platform Services Controller	TCP 443	Used by the Cloud Replication Management Appliance to communicate with the vCenter Server Lookup service located on the Platform Services Controller
M15	Cloud Replicator Appliance(s)	Platform Services Controller	TCP 443	Used by the Replicator Service to communicate with the vCenter Server Lookup service located on the Platform Services Controller
M17	Cloud Replicator Appliance(s)	vCenter Server	TCP 443	Used by the Replicator Service for interaction with the vSphere API on the vCenter Server
M20	Cloud Replicator Appliance(s)	ESXi Hosts	TCP 443	Used by the Replicator Service to initiate the flows of replication traffic to the destination ESXi hosts in VMC on AWS and AVS. This port carries no replication traffic
D1	Cloud Replicator Appliance(s)	Cloud Tunnel Appliance or Tunnel Load Balancer VIP	TCP 8048	Used by the Replicator Service for replication traffic to the Tunnel Service
D3	Cloud Tunnel Appliance	Cloud Replicator Appliance(s)	TCP 3030	Used for transferring replication data, only when the VMC Data Engine is used
D4	ESXi Hosts	Cloud Replicator Appliance(s)	TCP 44046	Used by the source ESXi Hosts for replication data traffic to the Replicator Service
D5	ESXi Hosts	Cloud Replicator Appliance(s)	TCP 32032	Used by the source ESXi hosts for encrypted virtual machines replication traffic to the Replicator Service

D7	Cloud Replicator Appliance(s)	ESXi Hosts	TCP 902	Used by the Replicator Service to send replication data traffic to the destination ESXi hosts
N1	All VCDA Appliances	DNS Server	TCP/UDP 53	Used for name resolution
N3	All VCDA Appliances	NTP Server	UDP 123	Used for time synchronisation using NTPv4 as per RFC 5905
N5	Cloud Replication Manager Appliance	Syslog Server	UDP 514	Used by the Cloud Service for sending events to the syslog server
N6	Cloud Replication Manager Appliance	SMTP Server	TCP 25	Used by the Cloud Service to send events notifications emails to the SMTP server, as configured in VMware Cloud Director

Table 12 – Required NAT Rules in a CDS-managed VMC Cloud Site

Legend	Type	Internal IP	Internal Port	External IP	External port
T1 / U1	DNAT	Cloud Tunnel Appliance or Tunnel Load Balancer VIP	TCP 8048	Public IP	User-Selected
A1*	DNAT	Cloud Tunnel Appliance	TCP 443 / 8442	Public IP	User-Selected
A2*	DNAT	Cloud Replication Manager Appliance	TCP 443	Public IP	User-Selected
A3*	DNAT	Cloud Replication Manager Appliance	TCP 8441	Public IP	User-Selected
A4*	DNAT	Cloud Replicator Appliance(s)	TCP 443 / 8440	Public IP	User-Selected
T1	SNAT	Cloud Tunnel Appliance	Any	Public IP	Any
M12	SNAT	Cloud Replication Manager Appliance	Any	Public IP	Any

*Note: VMware doesn't recommend allowing access to VCDA components management portals from the internet through NAT rules for security reasons. A more secure approach would be to use a jump host inside VMC cluster to access these management portals.

Azure VMware Solution (AVS)

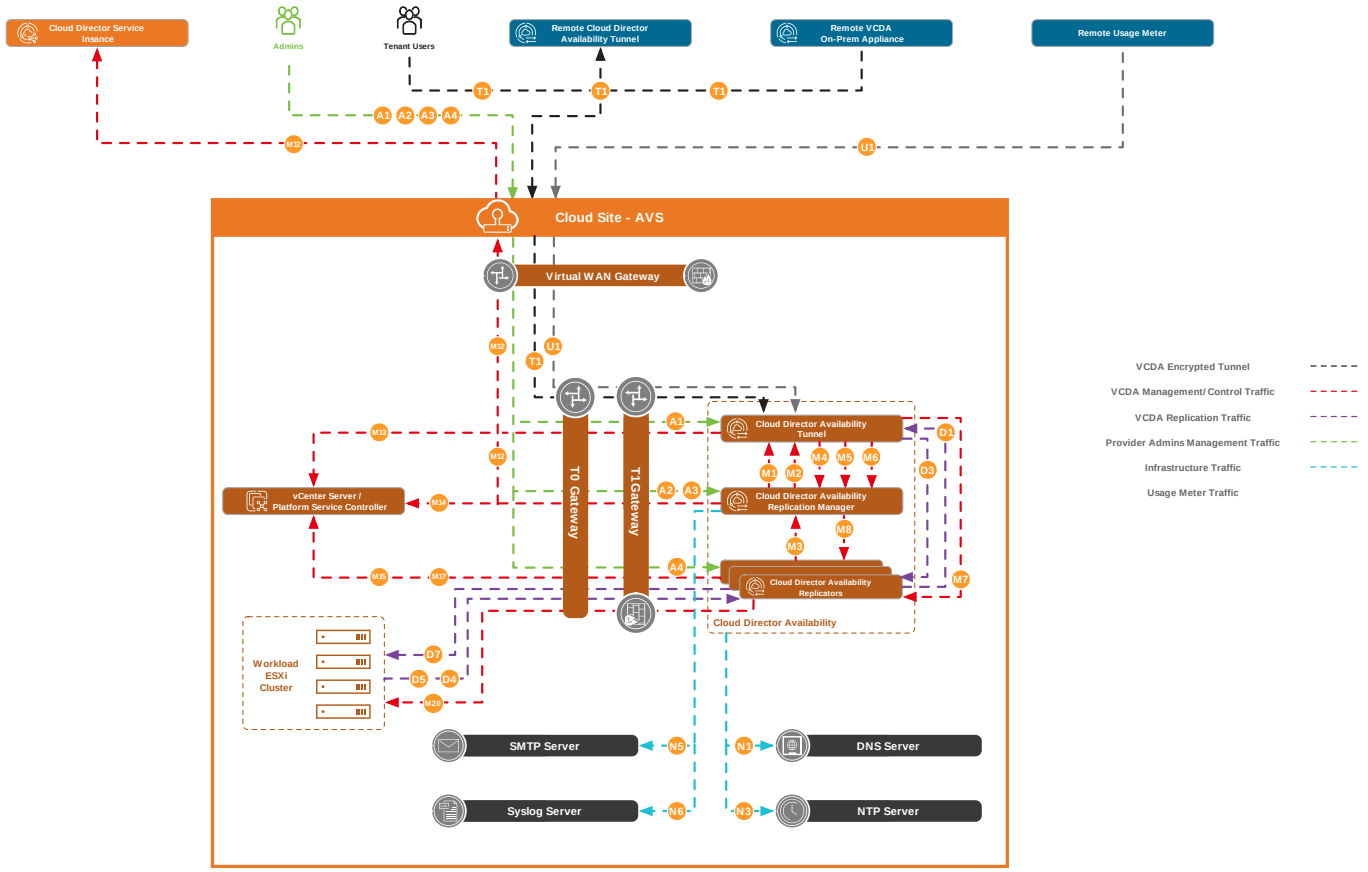

Figure 16: VCDA Traffic Flows in a CDS-managed AVS Cloud Site

Table 13 - VCDA Traffic Flows in a CDS-managed AVS Cloud Site				
Legend	Source	Destination	Protocol / Port	Description
T1	- Remote Cloud Tunnel Appliance(s) Public IPs - Remote VCDA On-prem Appliance(s) Public IPs - CDS Plugin Users	Cloud Tunnel Appliance or Tunnel Load Balancer VIP	TCP 8048	Used to access to the local VCDA Tunnel Endpoint
U1	Remote vCloud Usage Meter Appliance	Cloud Tunnel Appliance or Tunnel Load Balancer VIP	TCP 8048	Used to access to the local VCDA Tunnel Endpoint for metering / reporting purposes
A1	Admins	Cloud Tunnel Appliance	TCP 443 / 8442	Used for administrative login to the Tunnel Service to perform administrative operations
A2	Admins	Cloud Replication Manager Appliance	TCP 443	Used for administrative login to the Cloud Service to perform administrative operations
A3	Admins	Cloud Replication Manager Appliance	TCP 8441	Used for administrative login to the Manager Service to perform administrative operations
A4	Admins	Cloud Replicator Appliance(s)	TCP 443 / 8440	Used for administrative login to the Replicator Service to perform administrative operations

M1	Cloud Replication Manager Appliance	Cloud Tunnel Appliance or Tunnel Load Balancer VIP	TCP 8048	Used by the Cloud Replication Management Appliance for management traffic to the remote Replicator Appliances through the Tunnel Service
M2	Cloud Replication Manager Appliance	Cloud Tunnel Appliance	TCP 8047	Used by the Cloud Replication Management Appliance for management traffic to the Tunnel Service related to local site operations
M3	Cloud Replicator Appliance(s)	Cloud Replication Manager Appliance	TCP 8044	Used by the Replicator Service for management traffic to the Cloud Replication Management Appliance
M4	Cloud Tunnel Appliance	Cloud Replication Manager Appliance	TCP 8443	Used by the Tunnel Service for communication with the cloud service in Cloud Replication Management Appliance for serving VCDA portal
M5	Cloud Tunnel Appliance	Cloud Replication Manager Appliance	TCP 8046	Used by the Tunnel Service for management communication with the cloud service in Cloud Replication Management Appliance
M6	Cloud Tunnel Appliance	Cloud Replication Manager Appliance	TCP 8044	Used by the Tunnel Service for general communication with the manager service in Cloud Replication Management Appliance.
M7	Cloud Tunnel Appliance	Cloud Replicator Appliance(s)	TCP 8043	Used by the Tunnel Service for management traffic to the Replicator Service
M8	Cloud Replication Manager Appliance	Cloud Replicator Appliance(s)	TCP 8043	Used by the Cloud Replication Management Appliance for management traffic to the Replicator Service
M12	Cloud Replication Manager Appliance	CDS Instance Public URL	TCP 443	Used by the Cloud Replication Management Appliance for interaction with the Cloud Director API
M13	Cloud Tunnel Appliance	Platform Services Controller	TCP 443	Optionally used for single sign-on login to the Tunnel Service
M14	Cloud Replication Manager Appliance	Platform Services Controller	TCP 443	Used by the Cloud Replication Management Appliance to communicate with the vCenter Server Lookup service located on the Platform Services Controller
M15	Cloud Replicator Appliance(s)	Platform Services Controller	TCP 443	Used by the Replicator Service to communicate with the vCenter Server Lookup service located on the Platform Services Controller
M17	Cloud Replicator Appliance(s)	vCenter Server	TCP 443	Used by the Replicator Service for interaction with the vSphere API on the vCenter Server
M20	Cloud Replicator Appliance(s)	ESXi Hosts	TCP 443	Used by the Replicator Service to initiate the flows of replication traffic to the destination ESXi hosts in VMC on AWS and AVS. This port carries no replication traffic
D1	Cloud Replicator Appliance(s)	Cloud Tunnel Appliance or Tunnel Load Balancer VIP	TCP 8048	Used by the Replicator Service for replication traffic to the Tunnel Service
D3	Cloud Tunnel Appliance	Cloud Replicator Appliance(s)	TCP 3030	Used for transferring replication data, only when the VMC Data Engine is activated
D4	ESXi Hosts	Cloud Replicator Appliance(s)	TCP 44046	Used by the source ESXi Hosts for replication data traffic to the Replicator Service
D5	ESXi Hosts	Cloud Replicator Appliance(s)	TCP 32032	Used by the source ESXi hosts for encrypted virtual machines replication traffic to the Replicator Service
D7	Cloud Replicator Appliance(s)	ESXi Hosts	TCP 902	Used by the Replicator Service to send replication data traffic to the destination ESXi hosts
N1	All VCDA Appliances	DNS Server	TCP/UDP 53	Used for name resolution

N3	All VCDA Appliances	NTP Server	UDP 123	Used for time synchronisation using NTPv4 as per RFC 5905
N5	Cloud Replication Manager Appliance	Syslog Server	UDP 514	Used by the Cloud Service for sending events to the syslog server
N6	Cloud Replication Manager Appliance	SMTP Server	TCP 25	Used by the Cloud Service to send events notifications emails to the SMTP server, as configured in VMware Cloud Director

Table 14 – Required NAT Rules in a CDS-managed AVS Cloud Site

Legend	Type	Internal IP	Internal Port	External IP	External port
T1 / U1	DNAT	Cloud Tunnel Appliance or Tunnel Load Balancer VIP	TCP 8048	Public IP	User-Selected
A1*	DNAT	Cloud Tunnel Appliance	TCP 443 / 8442	Public IP	User-Selected
A2*	DNAT	Cloud Replication Manager Appliance	TCP 443	Public IP	User-Selected
A3*	DNAT	Cloud Replication Manager Appliance	TCP 8441	Public IP	User-Selected
A4*	DNAT	Cloud Replicator Appliance(s)	TCP 443 / 8440	Public IP	User-Selected
T1	SNAT	Cloud Tunnel Appliance	Any	Public IP	Any
M12	SNAT	Cloud Replication Manager Appliance	Any	Public IP	Any

***Note:** VMware doesn't recommend allowing access to VCDA components management portals from the internet through NAT rules for security reasons. A more secure approach would be to use a jump host inside AVS cluster to access these management portals.

Google Cloud VMware Engine (GCVE)

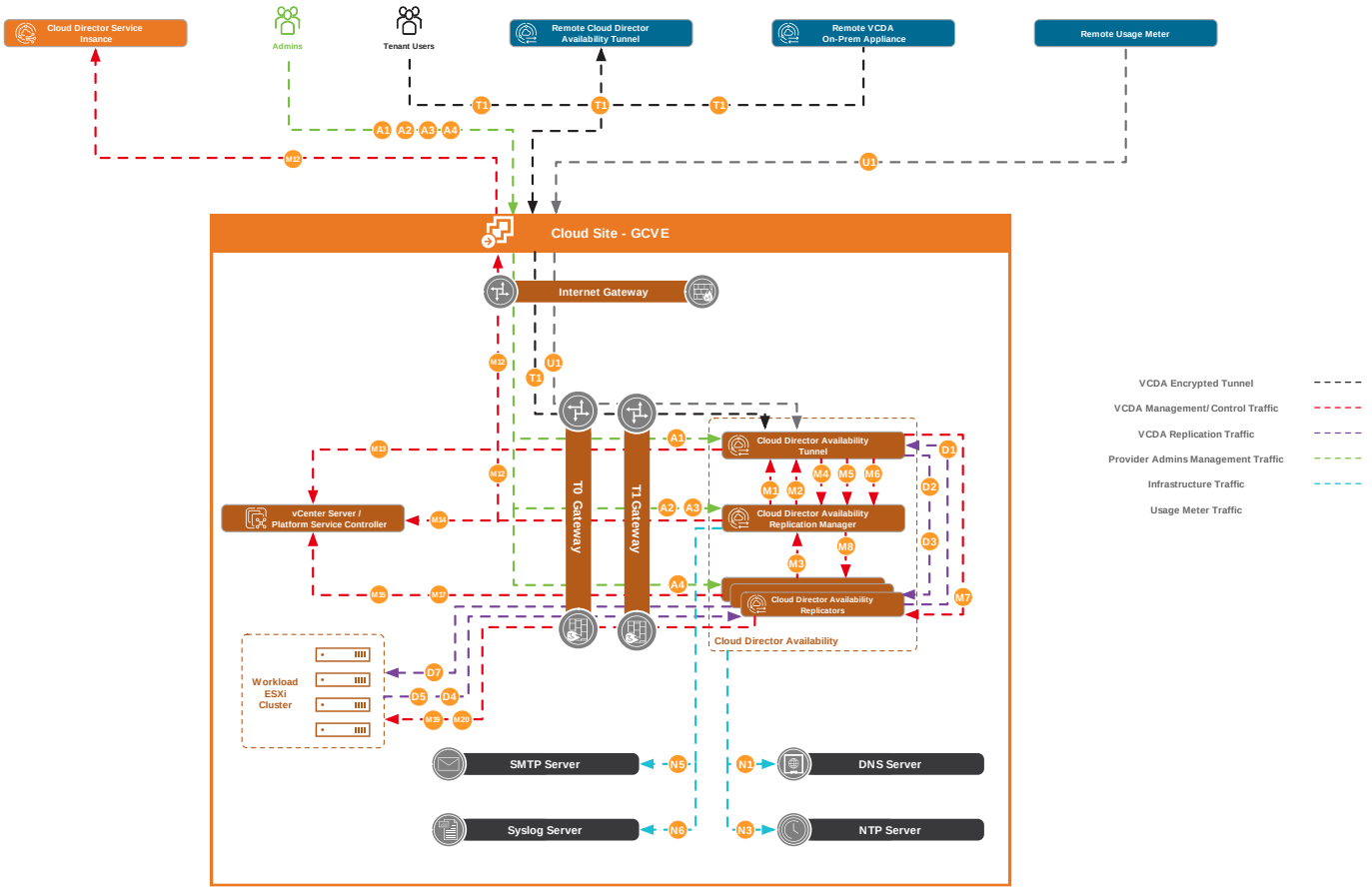

Figure 17: VCDA Traffic Flows in a CDS-managed GCVE Cloud Site

Table 15 - VCDA Traffic Flows in a CDS-managed GCVE Cloud Site				
Legend	Source	Destination	Protocol / Port	Description
T1	- Remote Cloud Tunnel Appliance(s) Public IPs - Remote VCDA On-prem Appliance(s) Public IPs - CDS Plugin Users	Cloud Tunnel Appliance or Tunnel Load Balancer VIP	TCP 8048	Used to access to the local VCDA Tunnel Endpoint
U1	Remote vCloud Usage Meter Appliance	Cloud Tunnel Appliance or Tunnel Load Balancer VIP	TCP 8048	Used to access to the local VCDA Tunnel Endpoint for metering / reporting purposes
A1	Admins	Cloud Tunnel Appliance	TCP 443 / 8442	Used for administrative login to the Tunnel Service to perform administrative operations
A2	Admins	Cloud Replication Manager Appliance	TCP 443	Used for administrative login to the Cloud Service to perform administrative operations
A3	Admins	Cloud Replication Manager Appliance	TCP 8441	Used for administrative login to the Manager Service to perform administrative operations
A4	Admins	Cloud Replicator Appliance(s)	TCP 443 / 8440	Used for administrative login to the Replicator Service to perform administrative operations

M1	Cloud Replication Manager Appliance	Cloud Tunnel Appliance or Tunnel Load Balancer VIP	TCP 8048	Used by the Cloud Replication Management Appliance for management traffic to the remote Replicator Appliances through the Tunnel Service
M2	Cloud Replication Manager Appliance	Cloud Tunnel Appliance	TCP 8047	Used by the Cloud Replication Management Appliance for management traffic to the Tunnel Service related to local site operations
M3	Cloud Replicator Appliance(s)	Cloud Replication Manager Appliance	TCP 8044	Used by the Replicator Service for management traffic to the Cloud Replication Management Appliance
M4	Cloud Tunnel Appliance	Cloud Replication Manager Appliance	TCP 8443	Used by the Tunnel Service for communication with the cloud service in Cloud Replication Management Appliance for serving VCDA portal
M5	Cloud Tunnel Appliance	Cloud Replication Manager Appliance	TCP 8046	Used by the Tunnel Service for management communication with the cloud service in Cloud Replication Management Appliance
M6	Cloud Tunnel Appliance	Cloud Replication Manager Appliance	TCP 8044	Used by the Tunnel Service for general communication with the manager service in Cloud Replication Management Appliance.
M7	Cloud Tunnel Appliance	Cloud Replicator Appliance(s)	TCP 8043	Used by the Tunnel Service for management traffic to the Replicator Service
M8	Cloud Replication Manager Appliance	Cloud Replicator Appliance(s)	TCP 8043	Used by the Cloud Replication Management Appliance for management traffic to the Replicator Service
M12	Cloud Replication Manager Appliance	CDS Instance Public URL	TCP 443	Used by the Cloud Replication Management Appliance for interaction with the Cloud Director API
M13	Cloud Tunnel Appliance	Platform Services Controller	TCP 443	Optionally used for single sign-on login to the Tunnel Service
M14	Cloud Replication Manager Appliance	Platform Services Controller	TCP 443	Used by the Cloud Replication Management Appliance to communicate with the vCenter Server Lookup service located on the Platform Services Controller
M15	Cloud Replicator Appliance(s)	Platform Services Controller	TCP 443	Used by the Replicator Service to communicate with the vCenter Server Lookup service located on the Platform Services Controller
M17	Cloud Replicator Appliance(s)	vCenter Server	TCP 443	Used by the Replicator Service for interaction with the vSphere API on the vCenter Server
M19	Cloud Replicator Appliance(s)	ESXi Hosts	TCP 80	Used by the Replicator Service to initiate the flows of replication traffic to the destination ESXi hosts. This port carries no replication traffic. This port is used only when Classic Data Engine is used.
M20	Cloud Replicator Appliance(s)	ESXi Hosts	TCP 443	Used by the Replicator Service to initiate the flows of replication traffic to the destination ESXi hosts. This port carries no replication traffic. This port is used only when VMC Data Engine is used.
D1	Cloud Replicator Appliance(s)	Cloud Tunnel Appliance or Tunnel Load Balancer VIP	TCP 8048	Used by the Replicator Service for replication traffic to the Tunnel Service
D2	Cloud Tunnel Appliance	Cloud Replicator Appliance(s)	TCP 44045	Used by the Tunnel Service for replication data traffic to the Replicator Service when Classic Data Engine is used
D3	Cloud Tunnel Appliance	Cloud Replicator Appliance(s)	TCP 3030	Used by the Tunnel Service for replication data traffic to the Replicator Service when VMC Data Engine is used
D4	ESXi Hosts	Cloud Replicator Appliance(s)	TCP 44046	Used by the source ESXi Hosts for replication data traffic to the Replicator Service

D5	ESXi Hosts	Cloud Replicator Appliance(s)	TCP 32032	Used by the source ESXi hosts for encrypted virtual machines replication traffic to the Replicator Service
D7	Cloud Replicator Appliance(s)	ESXi Hosts	TCP 902	Used by the Replicator Service to send replication data traffic to the destination ESXi hosts
N1	All VCDA Appliances	DNS Server	TCP/UDP 53	Used for name resolution
N3	All VCDA Appliances	NTP Server	UDP 123	Used for time synchronisation using NTPv4 as per RFC 5905
N5	Cloud Replication Manager Appliance	Syslog Server	UDP 514	Used by the Cloud Service for sending events to the syslog server
N6	Cloud Replication Manager Appliance	SMTP Server	TCP 25	Used by the Cloud Service to send events notifications emails to the SMTP server, as configured in VMware Cloud Director

Table 16 – Required NAT Rules in a CDS-managed GCVE Cloud Site

Legend	Type	Internal IP	Internal Port	External IP	External port
T1 / U1	DNAT	Cloud Tunnel Appliance or Tunnel Load Balancer VIP	TCP 8048	Public IP	User-Selected
A1*	DNAT	Cloud Tunnel Appliance	TCP 443 / 8442	Public IP	User-Selected
A2*	DNAT	Cloud Replication Manager Appliance	TCP 443	Public IP	User-Selected
A3*	DNAT	Cloud Replication Manager Appliance	TCP 8441	Public IP	User-Selected
A4*	DNAT	Cloud Replicator Appliance(s)	TCP 443 / 8440	Public IP	User-Selected
T1	SNAT	Cloud Tunnel Appliance	Any	Public IP	Any
M12	SNAT	Cloud Replication Manager Appliance	Any	Public IP	Any

***Note:** VMware doesn't recommend allowing access to VCDA components management portals from the internet through NAT rules for security reasons. A more secure approach would be to use a jump host inside GCVE cluster to access these management portals.

Oracle Cloud VMware Solution (OCVS)

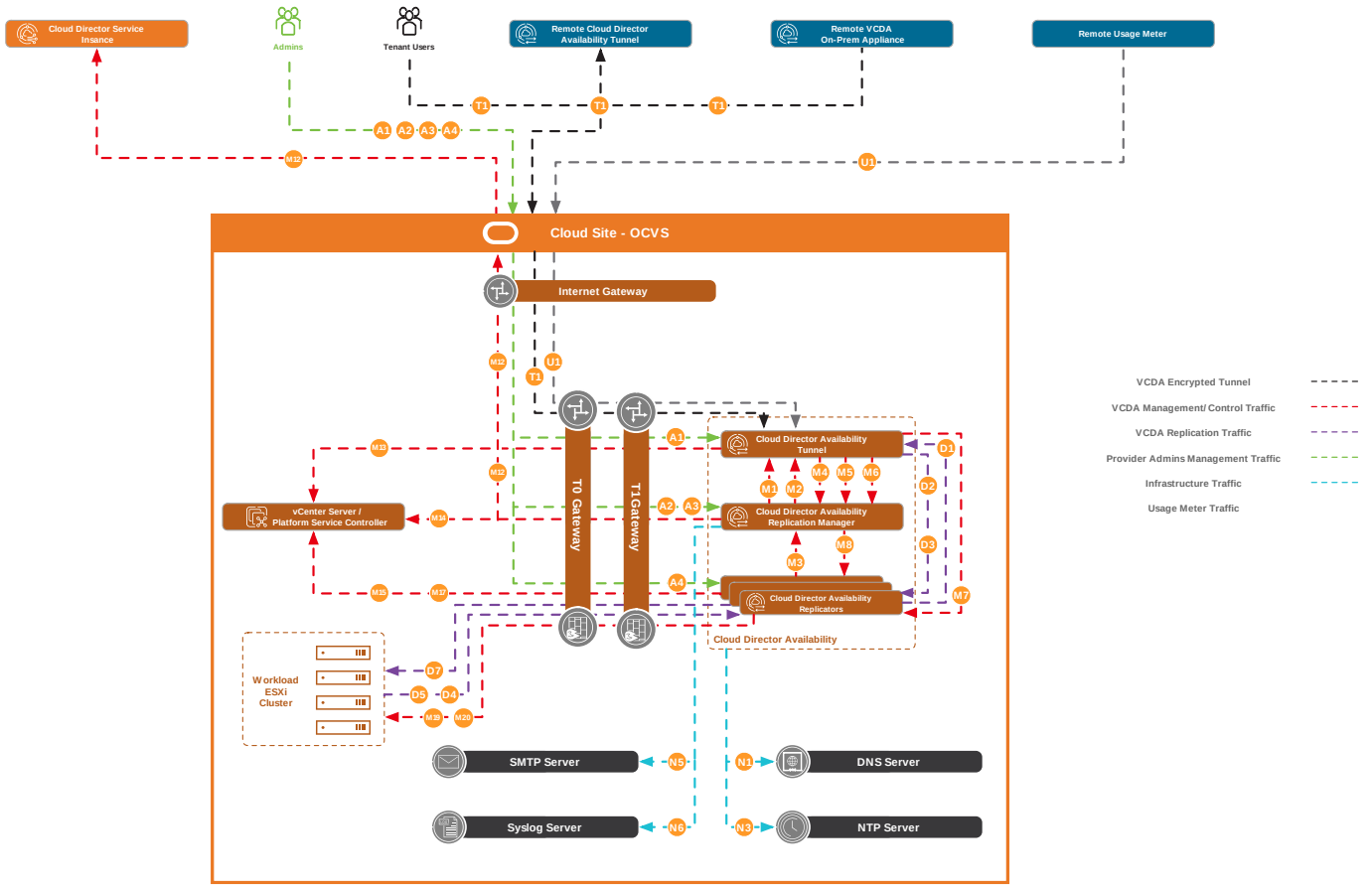

Figure 18: VCDA Traffic Flows in a CDS-managed OCVS Cloud Site

Table 17 - VCDA Traffic Flows in a CDS-managed OCVS Cloud Site				
Legend	Source	Destination	Protocol / Port	Description
T1	- Remote Cloud Tunnel Appliance(s) Public IPs - Remote VCDA On-prem Appliance(s) Public IPs - CDS Plugin Users	Cloud Tunnel Appliance or Tunnel Load Balancer VIP	TCP 8048	Used to access to the local VCDA Tunnel Endpoint
U1	Remote vCloud Usage Meter Appliance	Cloud Tunnel Appliance or Tunnel Load Balancer VIP	TCP 8048	Used to access to the local VCDA Tunnel Endpoint for metering / reporting purposes
A1	Admins	Cloud Tunnel Appliance	TCP 443 / 8442	Used for administrative login to the Tunnel Service to perform administrative operations
A2	Admins	Cloud Replication Manager Appliance	TCP 443	Used for administrative login to the Cloud Service to perform administrative operations
A3	Admins	Cloud Replication Manager Appliance	TCP 8441	Used for administrative login to the Manager Service to perform administrative operations
A4	Admins	Cloud Replicator Appliance(s)	TCP 443 / 8440	Used for administrative login to the Replicator Service to perform administrative operations

M1	Cloud Replication Manager Appliance	Cloud Tunnel Appliance or Tunnel Load Balancer VIP	TCP 8048	Used by the Cloud Replication Management Appliance for management traffic to the remote Replicator Appliances through the Tunnel Service
M2	Cloud Replication Manager Appliance	Cloud Tunnel Appliance	TCP 8047	Used by the Cloud Replication Management Appliance for management traffic to the Tunnel Service related to local site operations
M3	Cloud Replicator Appliance(s)	Cloud Replication Manager Appliance	TCP 8044	Used by the Replicator Service for management traffic to the Cloud Replication Management Appliance
M4	Cloud Tunnel Appliance	Cloud Replication Manager Appliance	TCP 8443	Used by the Tunnel Service for communication with the cloud service in Cloud Replication Management Appliance for serving VCDA portal
M5	Cloud Tunnel Appliance	Cloud Replication Manager Appliance	TCP 8046	Used by the Tunnel Service for management communication with the cloud service in Cloud Replication Management Appliance
M6	Cloud Tunnel Appliance	Cloud Replication Manager Appliance	TCP 8044	Used by the Tunnel Service for general communication with the manager service in Cloud Replication Management Appliance.
M7	Cloud Tunnel Appliance	Cloud Replicator Appliance(s)	TCP 8043	Used by the Tunnel Service for management traffic to the Replicator Service
M8	Cloud Replication Manager Appliance	Cloud Replicator Appliance(s)	TCP 8043	Used by the Cloud Replication Management Appliance for management traffic to the Replicator Service
M12	Cloud Replication Manager Appliance	CDS Instance Public URL	TCP 443	Used by the Cloud Replication Management Appliance for interaction with the Cloud Director API
M13	Cloud Tunnel Appliance	Platform Services Controller	TCP 443	Optionally used for single sign-on login to the Tunnel Service
M14	Cloud Replication Manager Appliance	Platform Services Controller	TCP 443	Used by the Cloud Replication Management Appliance to communicate with the vCenter Server Lookup service located on the Platform Services Controller
M15	Cloud Replicator Appliance(s)	Platform Services Controller	TCP 443	Used by the Replicator Service to communicate with the vCenter Server Lookup service located on the Platform Services Controller
M17	Cloud Replicator Appliance(s)	vCenter Server	TCP 443	Used by the Replicator Service for interaction with the vSphere API on the vCenter Server
M19	Cloud Replicator Appliance(s)	ESXi Hosts	TCP 80	Used by the Replicator Service to initiate the flows of replication traffic to the destination ESXi hosts. This port carries no replication traffic. This port is used only when Classic Data Engine is used.
M20	Cloud Replicator Appliance(s)	ESXi Hosts	TCP 443	Used by the Replicator Service to initiate the flows of replication traffic to the destination ESXi hosts. This port carries no replication traffic. This port is used only when VMC Data Engine is used.
D1	Cloud Replicator Appliance(s)	Cloud Tunnel Appliance or Tunnel Load Balancer VIP	TCP 8048	Used by the Replicator Service for replication traffic to the Tunnel Service
D2	Cloud Tunnel Appliance	Cloud Replicator Appliance(s)	TCP 44045	Used by the Tunnel Service for replication data traffic to the Replicator Service when Classic Data Engine is used
D3	Cloud Tunnel Appliance	Cloud Replicator Appliance(s)	TCP 3030	Used by the Tunnel Service for replication data traffic to the Replicator Service when VMC Data Engine is used
D4	ESXi Hosts	Cloud Replicator Appliance(s)	TCP 44046	Used by the source ESXi Hosts for replication data traffic to the Replicator Service

D5	ESXi Hosts	Cloud Replicator Appliance(s)	TCP 32032	Used by the source ESXi hosts for encrypted virtual machines replication traffic to the Replicator Service
D7	Cloud Replicator Appliance(s)	ESXi Hosts	TCP 902	Used by the Replicator Service to send replication data traffic to the destination ESXi hosts
N1	All VCDA Appliances	DNS Server	TCP/UDP 53	Used for name resolution
N3	All VCDA Appliances	NTP Server	UDP 123	Used for time synchronisation using NTPv4 as per RFC 5905
N5	Cloud Replication Manager Appliance	Syslog Server	UDP 514	Used by the Cloud Service for sending events to the syslog server
N6	Cloud Replication Manager Appliance	SMTP Server	TCP 25	Used by the Cloud Service to send events notifications emails to the SMTP server, as configured in VMware Cloud Director

Table 18 – Required NAT Rules in a CDS-managed OCVS Cloud Site

Legend	Type	Internal IP	Internal Port	External IP	External port
T1 / U1	DNAT	Cloud Tunnel Appliance or Tunnel Load Balancer VIP	TCP 8048	Public IP	User-Selected
A1*	DNAT	Cloud Tunnel Appliance	TCP 443 / 8442	Public IP	User-Selected
A2*	DNAT	Cloud Replication Manager Appliance	TCP 443	Public IP	User-Selected
A3*	DNAT	Cloud Replication Manager Appliance	TCP 8441	Public IP	User-Selected
A4*	DNAT	Cloud Replicator Appliance(s)	TCP 443 / 8440	Public IP	User-Selected
T1	SNAT	Cloud Tunnel Appliance	Any	Public IP	Any
M12	SNAT	Cloud Replication Manager Appliance	Any	Public IP	Any

***Note:** VMware doesn't recommend allowing access to VCDA components management portals from the internet through NAT rules for security reasons. A more secure approach would be to use a jump host inside OCVS cluster to access these management portals.

Provider-hosted VMware Infrastructure with Cloud Director Service

The following diagram and tables show the traffic flow in a provider-hosted VMware Infrastructure with CDS cloud site as well as the required NAT rules for external accessibility

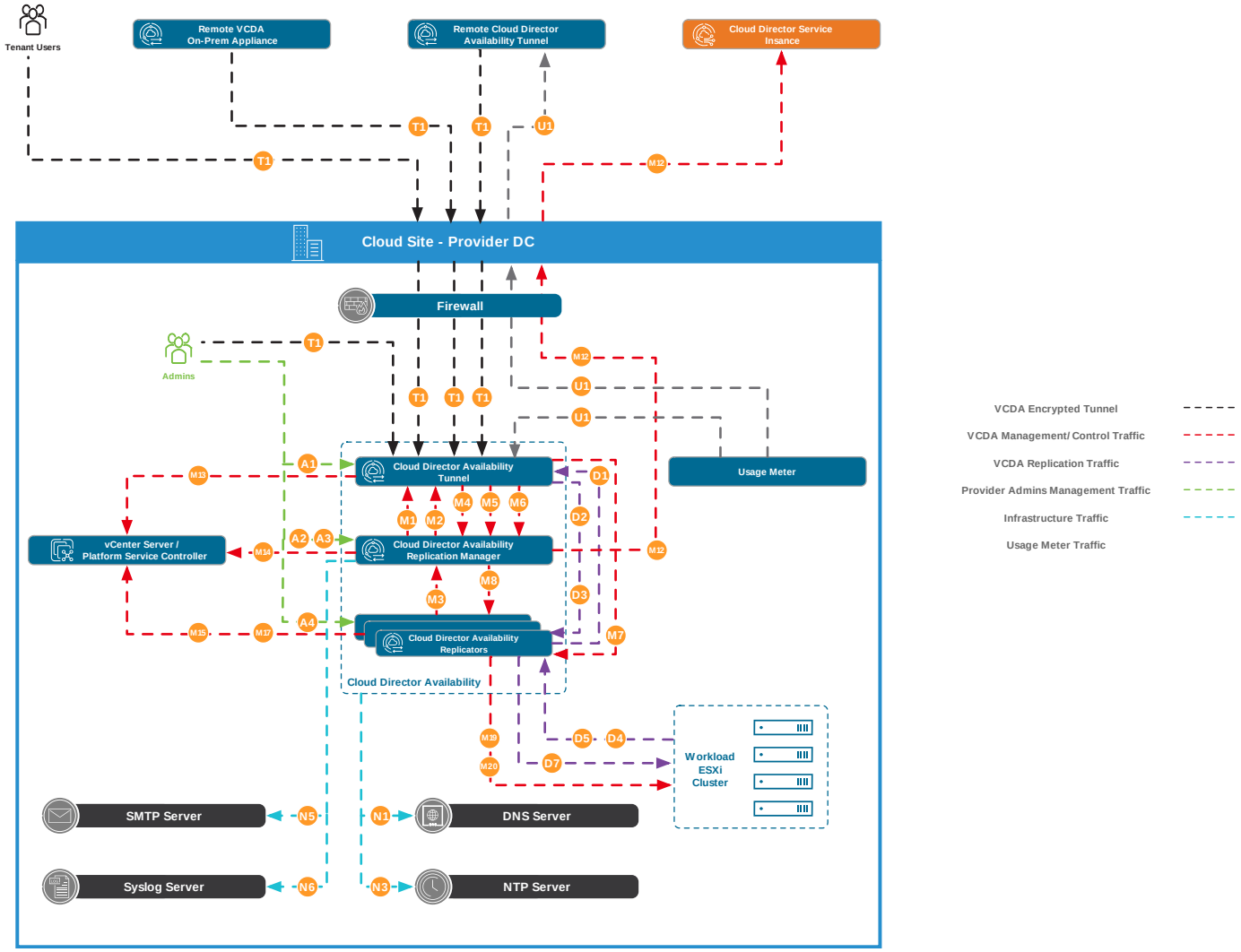

Figure 19: VCDA Traffic Flows in a Provider-hosted VMware Infrastructure with CDS Cloud Site

Table 19 - VCDA Traffic Flows in a Provider-hosted VMware Infrastructure with CDS Cloud Site				
Legend	Source	Destination	Protocol / Port	Description
T1	- Remote Cloud Tunnel Appliance(s) Public IPs - Remote VCDA On-prem Appliance(s) Public IPs - VCD Plugin Users	Cloud Tunnel Appliance or Tunnel Load Balancer VIP	TCP 8048	Used to access to the local VCDA Tunnel Endpoint

U1	vCloud Usage Meter Appliance	- Cloud Tunnel Appliance or Tunnel Load Balancer VIP - Remote Cloud Tunnel Appliance(s) Public IPs or Tunnel Load Balancer VIP Public IP	- TCP 8048 (local Cloud Tunnel Appliance) - Remote Cloud Tunnel Appliance(s) TCP Port	Used to access to the local VCDA Tunnel Endpoint for metering / reporting purposes
A1	Admins	Cloud Tunnel Appliance	TCP 443 / 8442	Used for administrative login to the Tunnel Service to perform administrative operations
A2	Admins	Cloud Replication Manager Appliance	TCP 443	Used for administrative login to the Cloud Service to perform administrative operations
A3	Admins	Cloud Replication Manager Appliance	TCP 8441	Used for administrative login to the Manager Service to perform administrative operations
A4	Admins	Cloud Replicator Appliance(s)	TCP 443 / 8440	Used for administrative login to the Replicator Service to perform administrative operations
M1	Cloud Replication Manager Appliance	Cloud Tunnel Appliance or Tunnel Load Balancer VIP	TCP 8048	Used by the Cloud Replication Management Appliance for management traffic to the remote Replicator Appliances through the Tunnel Service
M2	Cloud Replication Manager Appliance	Cloud Tunnel Appliance	TCP 8047	Used by the Cloud Replication Management Appliance for management traffic to the Tunnel Service related to local site operations
M3	Cloud Replicator Appliance(s)	Cloud Replication Manager Appliance	TCP 8044	Used by the Replicator Service for management traffic to the Cloud Replication Management Appliance
M4	Cloud Tunnel Appliance	Cloud Replication Manager Appliance	TCP 8443	Used by the Tunnel Service for communication with the cloud service in Cloud Replication Management Appliance for serving VCDA portal
M5	Cloud Tunnel Appliance	Cloud Replication Manager Appliance	TCP 8046	Used by the Tunnel Service for management communication with the cloud service in Cloud Replication Management Appliance
M6	Cloud Tunnel Appliance	Cloud Replication Manager Appliance	TCP 8044	Used by the Tunnel Service for general communication with the manager service in Cloud Replication Management Appliance.
M7	Cloud Tunnel Appliance	Cloud Replicator Appliance(s)	TCP 8043	Used by the Tunnel Service for management traffic to the Replicator Service
M8	Cloud Replication Manager Appliance	Cloud Replicator Appliance(s)	TCP 8043	Used by the Cloud Replication Management Appliance for management traffic to the Replicator Service
M12	Cloud Replication Manager Appliance	CDS Instance Public URL	TCP 443	Used by the Cloud Replication Management Appliance for interaction with the VMware Cloud Director API
M13	Cloud Tunnel Appliance	Platform Services Controller	TCP 443	Optionally used for single sign-on login to the Tunnel Service
M14	Cloud Replication Manager Appliance	Platform Services Controller	TCP 443	Used by the Cloud Replication Management Appliance to communicate with the vCenter Server Lookup service located on the Platform Services Controller

M15	Cloud Replicator Appliance(s)	Platform Services Controller	TCP 443	Used by the Replicator Service to communicate with the vCenter Server Lookup service located on the Platform Services Controller
M17	Cloud Replicator Appliance(s)	vCenter Server	TCP 443	Used by the Replicator Service for interaction with the vSphere API on the vCenter Server
M19	Cloud Replicator Appliance(s)	ESXi Hosts	TCP 80	Used by the Replicator Service to initiate the flows of replication traffic to the destination ESXi hosts. This port carries no replication traffic. This port is used only when Classic Data Engine is used.
M20	Cloud Replicator Appliance(s)	ESXi Hosts	TCP 443	Used by the Replicator Service to initiate the flows of replication traffic to the destination ESXi hosts. This port carries no replication traffic. This port is used only when VMC Data Engine is used.
D1	Cloud Replicator Appliance(s)	Cloud Tunnel Appliance or Tunnel Load Balancer VIP	TCP 8048	Used by the Replicator Service for replication traffic to the Tunnel Service
D2	Cloud Tunnel Appliance	Cloud Replicator Appliance(s)	TCP 44045	Used by the Tunnel Service for replication data traffic to the Replicator Service when Classic Data Engine is used
D3	Cloud Tunnel Appliance	Cloud Replicator Appliance(s)	TCP 3030	Used by the Tunnel Service for replication data traffic to the Replicator Service when VMC Data Engine is used
D4	ESXi Hosts	Cloud Replicator Appliance(s)	TCP 44046	Used by the source ESXi Hosts for replication data traffic to the Replicator Service
D5	ESXi Hosts	Cloud Replicator Appliance(s)	TCP 32032	Used by the source ESXi hosts for encrypted virtual machines replication traffic to the Replicator Service
D7	Cloud Replicator Appliance(s)	ESXi Hosts	TCP 902	Used by the Replicator Service to send replication data traffic to the destination ESXi hosts
N1	All VCDA Appliances	DNS Server	TCP/UDP 53	Used for name resolution
N3	All VCDA Appliances	NTP Server	UDP 123	Used for time synchronisation using NTPv4 as per RFC 5905
N5	Cloud Replication Manager Appliance	Syslog Server	UDP 514	Used by the Cloud Service for sending events to the syslog server
N6	Cloud Replication Manager Appliance	SMTP Server	TCP 25	Used by the Cloud Service to send events notifications emails to the SMTP server, as configured in VMware Cloud Director

Table 20 – Required NAT Rules in a Provider-hosted VMware Infrastructure with CDS Cloud Site

Legend	Type	Internal IP	Internal Port	External IP	External port
T1	DNAT	Cloud Tunnel Appliance or Tunnel Load Balancer VIP	8048	Public IP	User-Selected
U1	SNAT	vCloud Usage Meter Appliance	Any	Public IP	Any

M12	SNAT	Cloud Replication Manager Appliance	Any	Public IP	Any

Tenant On-Premises Site

The following diagram and tables show the traffic flow in a tenant on-premises site as well as the required NAT rules for external accessibility

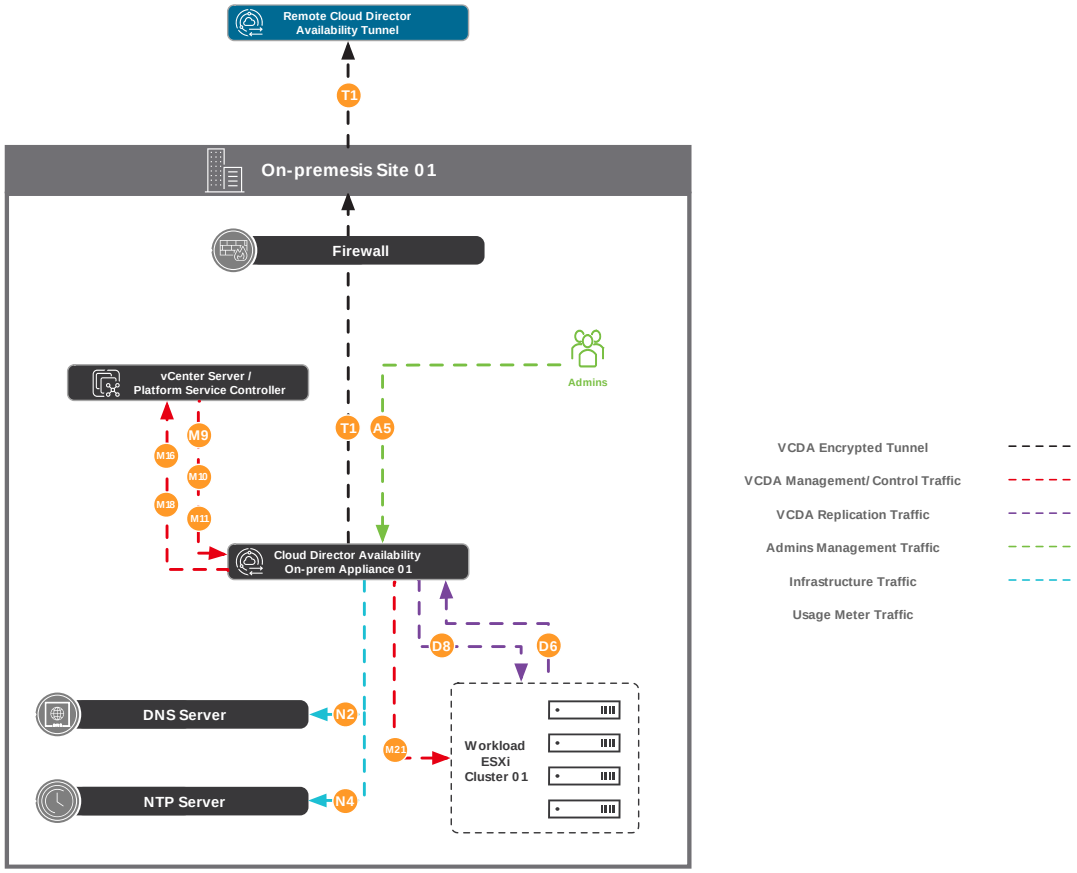

Figure 20: VCDA Traffic Flows in a Tenant On-Premises Site

Table 21 - VCDA Traffic Flows in a Tenant On-Premises Site				
Legend	Source	Destination	Protocol / Port	Description
T1	VCDA On-Premises Appliance	Remote Cloud Tunnel Appliance(s) Public IPs or Tunnel Load Balancer VIP Public IP	Remote Cloud Tunnel Appliance(s) TCP Port	Used to access to the remote VCDA Tunnel Endpoint
A5	Admins	VCDA On-Premises Appliance	TCP 443	Used for browser logins to the VCDA On-Premises Appliance
M9	vCenter Server	VCDA On-Premises Appliance	TCP 443	Used for downloading VCDA vSphere plugin and for plugin management traffic to VCDA On-Premises Appliance in VCDA 4.2 and later
M10	vCenter Server	VCDA On-Premises Appliance	TCP 8043	Used for downloading VCDA vSphere plugin from VCDA On-Premises Appliance in VCDA 4.0 and 4.1
M11	vCenter Server	VCDA On-Premises Appliance	TCP 8048	Used for plugin management traffic to VCDA On-Premises Appliance in VCDA 4.0 and 4.1
M16	VCDA On-Premises Appliance	Platform Services Controller	TCP 443	Used by the VCDA On-Premises Appliance to communicate with the vCenter Server Lookup service located on the Platform Services Controller and for optional single sign-on login

M18	VCDA On-Premises Appliance	vCenter Server	TCP 443	Used by the Replicator Service for interaction with the vSphere API on the vCenter Server
M21	VCDA On-Premises Appliance	ESXi Hosts	TCP 80	Used by the VCDA On-Premises Appliance to initiate the flows of replication data traffic to the destination ESXi hosts. This port carries no replication data traffic
D6	ESXi Hosts	VCDA On-Premises Appliance	TCP 44046	Used for transferring replication data traffic from the ESXi hosts to the VCDA On-Premises Appliance
D8	VCDA On-Premises Appliance	Cloud Replicator Appliance(s)	TCP 902	Used for transferring replication data traffic from the VCDA On-Premises Appliance to the ESXi hosts.
N2	VCDA On-Premises Appliance	DNS Server	TCP/UDP 53	Used for name resolution
N4	VCDA On-Premises Appliance	NTP Server	UDP 123	Used for time synchronisation using NTPv4 as per RFC 5905

Table 22 – Required NAT Rules in a Tenant On-Premises Site					
Legend	Type	Internal IP	Internal Port	External IP	External port
T1	SNAT	VCDA On-Premises Appliance	Any	Public IP	Any

VMware Cloud Director Availability Usage Reporting

Provider Usage Reporting

The provider must deploy vCloud Usage Meter appliance(s) to report and meter DR protections usage data from all VCDA instances in all cloud sites. There are two options for collecting VCDA usage data:

- Use VCDA Tunnel Endpoint (Tunnel public IP address or FQDN), root credentials and ***Allow admin access from anywhere*** option set
- Use another public IP address or FQDN for directly accessing the VCDA Cloud Replication Management appliance, root credentials and the ***Do not allow admin sessions from the Internet*** option set

For migrations, the provider must only report migrations usage data from all VCDA instances, however migrations are free of charge within VCDA license.

For more information about how to add VCDA instance(s) to vCloud Usage Meter Appliance, refer to vCloud Usage Meter Official Documentation. For more information about the latest VCDA pricing within the VMware Cloud Services Provider program, refer to the latest Product Usage Guide. For more information about what attributes are collect by vCloud Usage Meter appliance, refer to the latest Product Detection Guide. Both Product Usage Guide and Product Detection Guide are available through Partner Connect portal.

Tenant Showback / Chargeback

The tenant's users can monitor their VCDA usage by using the native monitoring features of VCDA. Users can view:

- Traffic Usage
- Disk Usage
- Required Resources for replication

The provider can also showback/chargeback tenant's VCDA usage by extracting the previous metrics gathered by VCDA through APIs and feeding these metrics into an external billing system to generates the required bills.

Alternatively, the provider can use VMware Chargeback. VMware Chargeback natively integrates with VCD and VCDA to report tenant's VCDA Usage. In addition, the provider can configure pricing policies for VCDA usage which automatically generates monthly bill to the tenant about their VCDA cost. For more information, refer to VMware Chargeback 8.10 Official Documentation.

Glossary

AVS	Azure VMware Solution
DR	Disaster Recovery
DRaaS	Disaster Recovery as a Service
C2C	Cloud-to-Cloud
CDS	Cloud Director Service
G2C	Ground-to-Cloud
GCVE	Google Cloud VMware Engine
HBR	Host-based Replication
OCVS	Oracle Cloud VMware Solution
POC	Proof of Concept
SEG	Service Engine Group
SSO	Single Sign-On
VCD	VMware Cloud Director
VCDA	VMware Cloud Director Availability
VMC / VMConAWS	VMware Cloud on AWS Solution

About the Authors

Shady Ali ElMalatawey is a Senior Staff Solutions Architect in the global Multi-cloud Architecture team. He has 12 years of experience and has been in distinct roles in VMware since joining in 2018. He is working with VMware Cloud Service Providers to provide architecture best practices and technical guidance on different VMware products under the VMware Partner Connect program. He holds three VMware Certified Design Expert (VCDX) certificates, and his number is 249. In addition, he is a VMware Education SME, an exam contributor and a VCDX Panelist. He has been member of vExpert Program since 2014, vExpert Pro Program since 2020 and vExpert Cloud Providers Program since 2020.

Nikolay Patrikov is a Senior Technical Product Manager at VMware with a primary focus on the VMware DRaaS solutions and VMware NSX Advanced Load Balancer.

Acknowledgments and Reviewers

In alphabetic order:

Adam Bohle - Director, Multi-Cloud Solutions Architecture, EMEA

Atanas Stankov - Senior Solutions Architect, VCPP Engineering

Gerrit Lehr - Principal Multi-Cloud Strategist, EMEA

Joseph Polcar - Staff Multi-Cloud Solutions Architect, AMER

Matt Elliott - Staff Multi-Cloud Solutions Architect, AMER

Tim Gless - Cloud Solutions Architect, Cloud Providers, EMEA

Timo Sugliani - Senior Staff Multi-Cloud Solutions Architect, EMEA

Item No: vmw-wp-tech-temp-a4-word-2021 8/21