



VMware Cloud Director Availability 4.0

General Availability June 2020

Overview questions

Q. What has been announced?

A. VMware has announced General Availability of VMware Cloud Director Availability 4.0. To align with latest branding of VMware Cloud Director, we are renaming VMware vCloud Availability to VMware Cloud Director Availability. This announcement includes the new product name and then the latest version, 4.0, that includes a set of new features and capabilities.

Q. What is VMware Cloud Director Availability?

A. VMware Cloud Director Availability is a powerful solution used by VMware Cloud Providers to offer simple, secure, and cost-effective onboarding, migration, and disaster recovery as a service to or between multi-tenant VMware clouds. The product was previously named VMware vCloud Availability.

Q. What are the core capabilities of VMware Cloud Director Availability?

A. Intuitive, Disaster Recovery as a service protection and wizard driven workflows to protect virtual machines (VM) or vApps. Replication and Recovery of VMs and vApps between VMware Cloud Director sites or on-premise to VMware Cloud Director and visa versa.

A. Single on-premise appliance installation for ease of deployment and simplicity for customers replicating to provider clouds. Supports a migration path and DR functionality from vSphere 6.5+ U3

A. The capability of each deployment to serve as both source and recovery instances (sites). There are no dedicated source and destination sites with symmetrical replication flow that can be started and managed from either the source or the recovery site means the UI can be accessed from anywhere with correct context.

A. Maximum replicated VMs and retained replications (stored instances) as well as minimum 5min RPO Policy controls for providers to apply to one to-many VDC or replications via SLA policies. This helps to control storage costs and provide tiered services to customers.

A. Secure tunneling through TCP proxy between sites with built-in encryption and optional compression availability

A. Multi-tenant support native within the VMware Cloud Director hierarchy and now in-context DRaaS providing customers a very simple view and action capability directly in VMware Cloud Director.

Q. What use cases does VMware Cloud Director Availability support?

A. On-Premises to Cloud migration, On-Premises to Cloud DR, Cloud-to-Cloud DR, Cross version vCD migration.

Q. What are the main new capabilities for VMware Cloud Director Availability 4.0?

A. Enhanced operation controls include:

- **Bandwidth control** is now available to be able to throttle replication bandwidth. This means providers and customers can choose to limit replication bandwidth at the source, ideal for areas where bandwidth is a premium and to minimize impact on overall bandwidth. Equally providers can opt to limit bandwidth globally to minimize over-saturation of TCP ports on a link
- **Failover Control** enhancements allow machines to be imported into VMware Cloud Director with the option now of disabling Guest Customization to keep the OS name the same and not re-IP the VM, or, all the user to set the computer name at the destination and re-IP the VM.
- VMware Cloud Availability has new **storage reporting capabilities** available in the UI and API that can be viewed by tenant as a whole or by individual VM/vAPP and storage policy. This helps providers and tenants understand their storage utilization over time, what VM/vAPP or org Virtual Data Centers are consuming the largest volumes of storage so they can manage capacity appropriately.
- **Disk Resizing** is a common task as disks in VM fill up with data and need to be extended. Now customers can resize disks in vSphere 7 as they would normally but critically now, they do not need to unconfigure and reconfigure the protection (there was no mechanism to extend the target disk when redo-log chains are used in encoding points in time).

- **Multi-NIC traffic conditioning** enables advanced network setups with higher security requirements and optimization of the replication data traffic. Providers can configure on-premise tunnel environments to send replication traffic from on-premise to cloud via nic1 (connected to public network) and go out from a tunnel or a cloud replicator via nic2 (connected to private network). Replicator traffic can be similarly conditioned to tunnel to replicator over nic1 (internal provider network) and replicator to esxi over nic2 (high-throughput replication data network).

A. Enhanced service consumption controls:

- **Failover resource requirements** are now available for tenants to be able to plan and purchase resources to meet their capacity needs at the target site or prioritize important workloads first. Resources that can be viewed in the UI include replicated source VM, CPU and memory and included disks (for replications that do not have tests and have not yet been failed over). For target org VDC the number of currently deployed VMs, target org VDC configured VM quota, and the number of not yet failed over replications which do not have tests to a given target org VDC can be viewed.
- **Stored instances** are a new feature introduced for customers who wish to keep a replicant instance as persistent instead of having them cycled, in previous versions all replication instances were subject to retention policies and their deletion cycle. Now customers can mark an instance as persistent, essentially taking it out of the cycle and storing it for however long they like. This will naturally hold the storage for that instance for the duration, incurring cost, but this does mean a customer can very quickly restore to a previous instance longer than that or the retention policy.
- **SLA Profiles** have made protection easy for customers. Previously many decisions needed to be made and terminology used implied knowledge of how DR worked. Now customers can select an SLA Profile that the cloud provider has created for them which can be as simple as Gold, Silver and Bronze nomenclature – essentially hiding complex wizard driven choices from the customers. For more advanced customers these profiles can be overridden and modified at the point of usage, but this is optional for each customer. Protection now is enforceable, faster and easier with SLA profiles.
- **Improved workflow and UI screens.** There has been a lot of work to make VMware Cloud Director Availability simpler and easier for customers to use,

including (but not limited to); reduced steps in wizards, page re-arrangements, extended button functionality and new instance and resources views and UI perspectives

- **In Context protection and status from VMware Cloud Director UI.** Now customers have an easier method to ascertaining their protection status and running protective actions right from the vAPP and/or VM in VMware Cloud Director, rather than the VMware Cloud Director Availability plugin.

A: Improved service integration:

- **In Context protection and status from VMware Cloud Director UI.** Now customers have an easier method to ascertaining their protection status and running protective actions right from the vAPP and/or VM in VMware Cloud Director, rather than the VMware Cloud Director Availability plugin.
- **Syslog event-based monitoring** now allows administrators to condition certain event types to be sent to syslog where they can be forwarded to a syslog manager. This is particularly useful for service providers who need to centralize their monitoring of systems into a single view of all services across the business. Now provider operations do not need to have Cloud Availability open all the time to understand the status of the service, if there are issues, they can easily see them in their console. With the Flex core bundle for VMware cloud providers, everyone has access to vRealize Log Insight for log management (it is included whether they use it or not). Hence this can be used to filter and enrich syslog events if the cloud provider does not use syslog today.
- **Support for NSX-T 2.5 & 2.5.1** is key for cloud providers who are evolving their VMware Cloud Director platform in line with VMware's strategy. VMware Cloud Director has supported NSX-T since 9.7, but in 10.0 of VMware Cloud Director on-demand creation of NSX-T networks and service is now available supporting VMware Cloud Director Availability interoperability both on-premise (with customers who have NSX-T standalone) and in cloud (providers with NSX-T and VMware Cloud Director)

Pricing and Packaging

Q. For cloud providers: How is VMware Cloud Director Availability packaged and how may it be purchased?

A. VMware Cloud Director Availability is available as a Pay-As-You-Go service to Service Providers in the VMware Cloud Provider Program. The service is metered monthly based on number of VMs protected, migrations are free. Detailed information is available in the VMware Cloud Provider Program Guide at <http://www.vmware.com/partners/service-provider.html>.

Q. I am a Cloud Provider and am not currently enrolled in the VMware Cloud Provider Program. Can I purchase this product directly from VMware?

A: You must be enrolled in the VMware Cloud Provider Program in order to purchase VMware Cloud Director Availability. To learn more about the VMware Cloud Provider Program, please visit <http://www.vmware.com/partners/service-provider.html>.

Q. For Enterprise Customers: How is VMware Cloud Director Availability packaged and how may it be purchased?

A: Enterprise customers must consume this offering through a VMware Cloud Provider Partner that is offering this service in their VMware Cloud Director VMware clouds. All prices for these services will be quoted by the VMware Cloud Provider Partner. To find a VMware Cloud Provider Partner offering DRaaS please use the assisted search here: <https://cloud.vmware.com/providers/guided-search>.

Migration features

Q. What is the VM/vAPP migration feature?

A. VMware Cloud Director Availability allows end users to protect and migrate virtual machines and vApps from on-premises to VMware Cloud and between different VMware Cloud environments. End users can select an organization virtual data center (oVDC) as a destination and migrate virtual machines from source data center in a few simple steps including assigning destination networks. This provides for a predictable way to migrate workloads in a self-service manner.

Q. How is failover (migration) performed?

A. To perform a migration the virtual machine or virtual app must be protected (replicated) between the source and target location. Once replicated, an optional resync can be initiated prior to failover (migration) to get real-time data migrated before failover to the destination site. This ensures that the latest changes of the source vApp/VM are present in the

recovered instance. If you are migrating a vAPP, it is important to manage the state of all VMs in the vAPP for a stable state; this can be validated simply in the UI and corrective actions can be taken. Migration jobs have additional conditioning to allow for customization post failover of IP and other characteristics such as networks to join.

Q. How are VMs initially replicated between clouds?

A. During the configuration or replication workflow, you can choose to configure replication from seed or to perform full initial synch. Once the workflow is configured to start VM or vAPP replication the VMware Cloud Director Availability vApp Replication Manager ensures that only delta information is sent from one ESXi host to another ESXi host. Management and Monitoring information for the replication is available from the vApp Replication Manager portal and APIs.

Q. What is a test failover?

A. Test failovers allow you to verify whether the source data is replicated correctly on the destination. You can test network connectivity and application (VM) behavior. vAPP can also be powered on to test.

Q. What is the maximum Recovery Point Objective (RPO) supported by VMware Cloud Director Availability?

A. As of today, the minimum RPO is 5 minutes. Therefore, the changes in the protected virtual machine can be replicated every five minutes to a selected destination.

Q. What actions can be taken by users?

- A. By using the Actions pane in the DR Workloads page, you can perform the following tasks:
- Failover workloads among to-destination sites
 - Failback workloads among from-destination sites
 - Reverse Failover workloads to synchronize data between source and destination sites
 - Reverse Failback workloads to synchronize data between source and destination sites
 - Test replication tasks and Cleanup test data

Q. What functionality is available to monitor DR operations?

A. You can monitor the overall VMware Cloud Director Availability status by using the VMware Cloud Director Availability Portal home page in VMware Cloud Director or in the native VMware Cloud Director event window. 4.0 introduces a syslog feature to be able to send syslog event

data about replications and status to a central syslog server. All this information is also available from the API.

Q. How are vApp configurations transferred from source to destination?

A. VMware Cloud Director Availability supports vApp aware migration and DR. Automated transfer of vApp settings and configurations such as vApp networks, guest OS customization and properties etc. happens from source to destination.

Q. Does VMware Cloud Director Availability support VM grouping for accelerated recovery?

A. VMware Cloud Director Availability provides intelligent recovery of the entire VM group accelerating recovery. You

can also prioritize boot order of critical machines over less critical VMs

Policy Control Features

Q. What policies can be used to control / limit functionality?

A. A Cloud Provider can assign replication policies to local one to-many VDC organizations:

- Policy to assign an vCD organization as a replication source and/or destination
- Minimum Recovery Point Objective (RPO)
- Maximum number of VM replications
- Maximum number of point-in-time instances per VM replication
- Maximum number of stored instances per VM replication

Out of the box VMware Cloud Director Availability 4.0 installs 3 default SLA policies. Cloud Administrators and Users who have permissions can option to modify these policies:

Gold: RPO 30m, retention 14 instances over 2 weeks, Quiescing off, Compression enabled, initial sync no delay.

Silver: RPO 2h, retention 7 instances over 1 weeks, Quiescing off, Compression enabled, initial sync no delay.

Bronze: RPO 4h, retention Disabled, Quiescing off, Compression enabled, initial sync no delay.

All policies can control:

- **Outgoing and incoming replications**
- **Maximum incoming replications**
- **Maximum stored instances**
- **Maximum throughput**
- **All custom SLA setting** (this allows a user to modify the setting for a replication job).

Q: Can a provider understand a tenant compute resources and storage usage and limit it?

A. A cloud provider can monitor a tenant's storage consumption reporting by organization and individual workloads. Equally they can see the tenant org compute requirements and disk

capacity to ensure they have enough to start workloads at the target site.

A tenant can view their own disk usage over time and for every replication from within VMware Cloud Director Availability.

Architecture

Q. What services are included in the installation; do I need to configure vSphere Replication somehow?

A. This is where a lot of improvements have been made. The architecture of the solution uses a VMware Cloud Director Availability Replicator appliance, a Replication Manager and a vApp Replication Service/Manager together to support replication, secure communication, and storage of the replicated data.

Each service provider can support recovery for multiple customer Org Virtual Data Center environments that can scale to handle increasing loads for each tenant, and for multiple tenants.

All replication matters are handled within the VMware Cloud Director Availability user interface (or API) and are simple workflow configuration driven tasks for one-to-many VMs and vAPP.

Q. I am a cloud provider using a single VMware Cloud Director across multi data centers. Does VMware Cloud Director Availability support this architecture?

A. Yes. The centralized topology provides simpler management to control replication across multiple data centers. Please refer to the technical documentation for more information.

Q. Does VMware Cloud Director Availability support multiple provider connection options?

A. Yes, VMware Cloud Director Availability offers flexible connection options for providers to support multiple northbound connection types (MPLS, VPN, etc.) with discrete controls of replication traffic and bandwidth. New controls in 4.0 offer Multi-NIC traffic conditioning enabling advanced network setups and bandwidth throttling on-premise to cloud egress traffic.

Minimum Requirements

Q. What are the minimum requirements for VMware Cloud Director Availability?

A. For system requirements and interoperability, see VMware Cloud Director Availability documentation.

<https://docs.vmware.com/en/VMware-Cloud-Director-Availability/index.html>

Service Deployment

Q. Does VMware Cloud Director Availability require any agents to be deployed at the customer site?

A. No, the solution is agentless and uses host-based replication, inherent in the VMware vSphere hypervisor. All that is required at the client site is the deployment of a replicator and tunnel appliance and configuration to connect to the provider cloud.

Q. How is the product installed in the provider data center?

A. VMware Cloud Director Availability can be deployed using the VMware OVF Tool. Alternatively, you can use the vSphere Web Client to install the VMware Cloud Director Availability service; all DR services are deployed via a single installation VMware-Cloud-Director-Availability-OnPrem-release.number-xxxx-build_number_OVF10.ova package.

Q. Why would a provider need multiple vCAv replicators?

A. Replication in terms of volume will impact the capacity and performance of the appliance. When each VM is compressed and encrypted there is an overhead on CPU. Whilst encryption is mandatory, compression can be optional, and both tax system resources.

Multiple replicators can be added to your DR environment to suite processing needs while scaling out supported workloads to protect or migrate.

Q. What are the tested scale limits for a deployment?

A. Please check the configuration maximums for the latest guidelines.

Q. Does VMware Cloud Director Availability work with NSX-T?

A. As of version 4.0 of VMware Cloud Director Availability NSX-T 2.5.0 and 2.5.1 is supported, later versions of NSX-T will be supported in future releases and patches for VMware Cloud Director Availability.

Management

Q. Does VMware Cloud Director Availability support bandwidth monitoring?

A. VMware Cloud Director Availability has natively integrated bandwidth monitoring and reporting on historical bandwidth

consumption, allowing providers to analyze the volume of transferred data per org for provider, and for own data as a tenant.

Q. Does VMware Cloud Director Availability support Usage Meter for automatic metering?

A. Yes, VMware Cloud Director Availability has supported automatic metering from [Usage Meter 3.6.1. Hot Patch 3.](#)

There is an indication in the management interface that vCloud Usage Meter is configured to meter the Cloud service instance. When vCloud Usage Meter has not requested metering information for more than three days, you now see a warning message in the management interface. To collect product consumption data and generate reports for the VMware Cloud Provider Program, see [Add vCloud Availability](#) in the vCloud Usage Meter documentation.

Q. Does VMware Cloud Director Availability support event forwarding?

A. As of 4.0 you can configure syslog event forwarding regarding the following notifications: RPO violations and certificate expiry, Events are also supported in VMware Cloud Director portal, where a system admin can monitor all events if required. Events are either on-demand system events or user-initiated events. Please check the [documentation](#) for a complete list of possible event notifications.

Resources

Q. Where can I find more about VMware Cloud Director Availability 4.0?

A. For more information visit:
<https://www.vmware.com/products/>

