Introduction to VMware Cloud Director Availability

The ever-growing data-centric world is fueling the latest gold rush. Nevertheless, it is ephemeral, difficult to protect, and risk-prone. Similarly, the adoption of the cloud and the Internet of Things (IoT) has grown exponentially in recent years; since the pandemic, cloud computing marketing has been on a rapid upward trajectory regarding cloud adoption, infrastructure, and spending. Many businesses have been compelled to rethink and shift their strategy to accommodate a new wave of working, communicating, and operating business functions. Therefore, most companies are now hybrid; some are still thinking about shifting gears and moving their on-premises environment to the cloud. If cross-collaboration is critical for businesses, they will ultimately need access and control over workloads accommodated on commercial, public, and private clouds or across hybrid infrastructures. The ‘as a service’ segments of cloud spending, combining shared cloud as a service and dedicated cloud as a service, will account for the majority of all cloud spending. Both PaaS and software-as-a-service (SaaS) segments are expected to experience highest end-user spending growth, with Gartner forecasting 23.3% growth for PaaS and 16.8% for SaaS in 2023 (Gartner, 2022).

Whether the business is transiting partially or entirely from on-premises to a cloud environment, VMware Cloud Director Availability offers disaster recovery and migration capabilities that can be implemented across several scenarios and use cases. VMware Cloud Director Availability has inspired cloud transformation and modernization for many businesses, with over 300 partners in production managing thousands of monthly migrations. Between multi-tenant clouds and on-premises, with replications and protections, VMware Cloud Director Availability migrates, protects, fails over, and reverses failover of customer vApps and virtual machines. VMware Cloud Director Availability is available through the VMware Cloud Provider Program. It is designed with cloud providers and tenants in mind with competitively managed and self-service capabilities.

It introduces a unified architecture for disaster recovery and migration of VMware vSphere® workloads. With VMware Cloud Director Availability, cloud providers and their tenants can migrate and protect vApps and virtual machines:
Introducing VMware Cloud Director Availability

VMware Cloud Director Availability introduced a cavalcade of ground-breaking features in early 2022, which expanded the disaster recovery and migration use case for clouds based on VMware Cloud Director and vSphere. With this release, disaster recovery and migration is not limited to Cloud Director as the only endpoint. In addition, with competitive features such as 1-Minute RPO, One-Click Migration, Tunnel Appliance High Availability, Advanced Retention Policy, Recovery Plans Execution and Monitoring, VMware Cloud Director Availability is leading the way to offer cloud providers a fully holistic cloud disaster recovery and migration solution that meets the growing demands of a multi-dimensional cloud infrastructure.

The latest release champions a wide range of features that have been enhanced to cater for multi-cloud and multi-tenanted cloud architecture.

Key Features

vSphere DR and migration enhancement

Version 4.4 of VMware Cloud Director Availability changed the paradigm for VMware’s DR and migration service offering landscape by supporting on-premises to cloud vCenter Replication using the existing underlying technology and ensured support for vCenter Replication Management Appliance. The latest release has enhanced the scalability, availability, and security of vSphere DR and migration capability to make it highly compatible with multi-tenanted environments.
Recovery Plans
VMware Cloud Director Availability 4.6 offers the ability to create and run recovery plans for vSphere DR and Migration between vCenter Server sites. Cloud Providers can orchestrate DR and migration operations on a set of VM replications, and recovery plans can be managed and monitored asynchronously.

Furthermore, recovery plans can have failover, migrate, test failover and test cleanup executed and Cloud Provider.

DR & Migration Public API
Similar to Cloud-to-Cloud deployment, Cloud Providers can independently configure a deployed appliance with the help of the API programming guide. The open AI client is exposed through vSphere DR & Migration portal UI.

To access the API programming Guide and OpenAPI specification, please visit https://developer.vmware.com

Recovery Setting Enhancements
In terms of vSphere DR and Migration recovery setting, Cloud Providers currently can preconfigure the destination virtual machine location, compute resource and the network mapping that’s applied when recovering the workload in the destination site.

With 4.6, Cloud Providers can validate the recovery settings (data center, VM folder, compute and other) based on replication settings (datastore). In addition, the source and destination network mappings allow per-virtual machine network mapping.

This feature now has a unified look and feel therefore, it’s seamless across all use cases. In context of On-premises to Cloud replication (Cloud Director destination clouds), users can map the source and the destination networks per selected replication, exactly as the Cloud to Cloud replication scenario.

For more details, please visit Configure recovery settings for vSphere DR & Migration.

Bandwidth Throttling
Bandwidth throttling is a new feature that allows Cloud Providers to set a global traffic cap per site, which is identical to what is available for VMware Cloud Director Clouds. In other words, traffic limitations can be enforced on a specific Tunnel network interface.
NSX-T vApp Edges Support
Starting from this release, Cloud Provider product management experience will be enriched with extended replication support for DHCP service on vApp isolated network, Routed vApp networks and vApp network services. This feature overcomes layers of complexities which was previously experienced due the unavailability of routed vApp networks and the isolated vApps networks did not support DHCP. This feature is available when the destination cloud is running VMware Cloud Director 10.3 or later. For more information, see Configuring the network settings of replications to the cloud and Configure the network settings for cloud to cloud replications.

Tunnel Appliance High Availability
Multiple tunnels ensure higher resiliency and availability during the incoming and outgoing replication process. Before version 4.6, all the data traffic travelled through one single tunnel appliance for a cloud site, which was prone to failure, disruption, and outages. This feature offers reassurance of a second tunnel appliance that operates in active mode for high availability for the tunnel services, both for new deployments and for upgraded ones. To learn more, please visit Add a second Tunnel Appliance for HA in the Cloud Director site.

Additional improvements and operational features
vApp Template Replication
With VMware Cloud Director Availability 4.3.1, vApp templates could be migrated from one catalog to another in the same or a remote VMware Cloud Director cloud. Version 4.6 introduces a plethora of sub-features which will allow Cloud Providers to fully manage vApp template overwrites with options to automatically configure a new replication with the updated source, delete older and unnecessary replication, specify whether to overwrite the destination template or create a new one, automate migration of the new replication (on and off setting available), set up template tracking and plenty other features.

Improved Event Notification
Several event notification capabilities have been improved in version 4.6 to ensure better visibility and transparency around process and activities undertaken within the system. The main enhancement is focused on replication management, where Cloud Providers and tenants can now send replication management events by using email delivery channel. In addition, Cloud Providers and Tenants can also subscribe to a weekly summary email, users can stay informed about the activities without logging into the VMware Cloud Director portal. For more details please visit Subscribe for weekly summary email.

Guest customization Global Setting
Cloud Providers can exercise this feature on all replications. The purpose of this feature is to control default duplication of customization settings by simply choosing to activate or deactivate guest customization in source site versus recovery site. The parameters can be overwritten through Recovery settings of each replication.

Simple, capable disaster recovery as a service
From the installation in the provider cloud to implementation on-premises, VMware Cloud Director Availability is a simplified, skillful architecture making it easy for customers and providers to implement. Customers can now find and set up DRaaS with a partner with our new vSphere plugin for DRaaS and migration. Qualified DRaaS-validated and Cloud Verified partners are listed in distance priority to the customer vSphere console; with integrated lead generation, a customer can click on the partner and, through the form, fill out a request to learn more about their service.

Once a customer has an agreement with the partner and the destination details, they can self-serve deploy a replication appliance into their vCenter and connect to the provider’s virtual data center via an encrypted tunnel, then start protecting their workloads directly from vCenter or the provider UI using the symmetric nature of the solution. VMware Cloud Director Availability allows customers to configure and manage incoming and outgoing replication from the source and recovery site.
Introducing VMware Cloud Director Availability

Notably, there are no agents to deploy on ESXi hosts, and starting replication is a quick activity; the networking is simplified to make it straightforward to deploy and use. Providers who enable VMware Cloud Director Availability for customers would allow customers to understand their protected status and run DR workflows directly in VMware Cloud Director UI, thereby driving more consumption and better user experience for customers.

VMware Cloud Director Availability provides coverage for two prominent use cases: on-premises to cloud disaster recovery and migration, and cloud to cloud disaster recovery and migration.

Migration capability is cold and warm and quickly scheduled into maintenance windows to suit your customers. Cold migration is the complete sync of an offline workload before cutover, and warm migration just syncs the differential at the time of cutover and is faster to implement. Many providers use VMware Cloud Director Availability for migration as it is simple, at no charge to VMware, but significantly can be driven by customers and allows a customer to self-migrate when it suits them—which is a great experience and selling point.

This release introduces a wide range of features that ensures enterprise data protection with robust security, reliability and high availability and agile data management services. On top of the newly added features in version 4.6, the intuitive user interface with VMware Cloud Director Availability portal is a catalyst for higher solution adoption and feature consumption. The ‘Tunnel Appliance High Availability’ ensures resiliency and consistent availability of the second tunnel during the incoming and outgoing replication process. Similarly, the ‘Recovery Setting Enhancements’ has made it possible to deliver and manage consistent recovery settings features across Cloud to Cloud, On-premises to Cloud and vSphere to vSphere use case. Overall, operational features such as Guest customization been designed with Cloud Providers and Tenants in mind to support visibility, monitoring, and transparency over how the infrastructure is being handled.

VMware Cloud Director Availability is helping customers drive better protection and testing. In case of any issues and to simplify troubleshooting, cloud providers can access cloud support bundles. This allows the provider to easily obtain new on-premises support bundles for VMware Global Support Services troubleshooting if necessary. One big aspect of the solution is the ability to test the bandwidth and capability to ensure that you have limited any uncertainty in your capability to recover in the event of a disaster.
Testing frequently is the key to decreasing risk and protecting against a disaster. Unfortunately, it is perhaps the least-used feature in DRaaS. Typically, this is because disaster recovery is provided by products that do not suit self-service or because the provider needs to ensure resource availability at the target is managed between multiple customers. VMware Cloud Director Availability offers highly competitive failover testing capabilities and the tools to evaluate your existing cloud infrastructure’s DR and migration readiness.

Since 4.5 the recovery settings have been improved for guest customization, and all the properties available in VMware Cloud Director can also be customized for each replication, including the option to add a script to be executed. Moreover, additional features to manage, clone, and control replication policies will offer extra support for cloud providers to accelerate and streamline their replication processes.

VMware Cloud Director Availability is self-service and can also be a managed service or self-service. This means a customer can test their failover, non-impacting, at any time on any frequency. Managed service would mean a provider does this testing for the customer, which could be complemented with additional application testing services. As a self-service capability, it is essential that there are adequate resources at the target end to manage all customers’ compute requirements, as potentially, all could choose to failover or test failover simultaneously. The recommendation is to promote testing as a feature to decrease the risk of recovery uncertainty.

**Workload distribution**

It is essential to realize that not all workloads are equal in requirements. Some may require much higher replication frequency and granular recovery due to the nature of the speed and criticality of the changing data, while others may be non-critical and have longer cycles with less granularity. When considering disaster recovery, you need to have functionality allocated correctly to cost. The higher the importance of a workload, the more expensive it is likely to be, as it will consume more data and replicate more frequently.

Mission-critical workloads affect the entire business; business will stop quickly due to an outage. These applications severely impact a broad part of the business and can be deemed mission critical. For example, financial systems that transact millions of transactions per minute are essential to the business’s success. Customers for DRaaS need to consider what applications are in their business that they cannot survive without for even the shortest duration.

Business-critical characteristics are different and affect the Line of Business (LOB), but overall, a business can operate and survive. These LOB applications can be viewed as business critical. For example, an unavailable HR payroll system will interrupt payroll, but the business will carry on.

Lastly, some non-critical workloads and applications affect people personally. They may delay deliverables, but ultimately, they are not affecting the business or teams in the industry for a short duration. Items such as personal file systems and possibly email could be viewed as non-critical; it all depends on how you run your business.

It is easy to see how the recovery characteristics can be composed for different workload types. The following graphic indicates how customers look at recovery point and time objectives by workload type. Although this data is from 2019, it is unlikely to have changed much, if at all:

**Mission-critical** example: Finance / Billing
RPO Average 1 min
RTO Average <15min
Suggested method – Synchronous Replication

**Business-critical** example: eMail / SharePoint
RPO Average 15 min
RTO Average <2hrs
Suggested method – Async Replication

**Non-critical** example: Personal File Folders
RPO Average >24hrs
RTO Average <48hrs
Suggested method - Backup

It’s essential for a customer to be able to match a workload to a tier of service for disaster recovery as it will be more cost effective to have the appropriate resource capacity aligned to the workload. Having a single-tier DRaaS portfolio does not provide the flexibility to cover mission-critical workloads vs non-critical. There will be underused functionality/capacity, which may cost the customer more overall. From a partner perspective, consumption will be much higher and better aligned with a tiered customer offering.

VMware Cloud Director Availability SLA profiles offer out-of-the-box service classes; the defaults are detailed below and can be added/modified or changed to meet your overall or per-customer DRaaS cost-to-performance needs. With a simple nomenclature, customers understand what they are getting, from a Gold service with a low RPO and long retention time to a Bronze service with a longer RPO for less critical workloads and a short, limited retention time.

As already noted, the retention time in these SLA profiles is the ‘span’ of the Multiple Points in Time (MPIT) instances. With 4.6, these are flexible and in 4.5x, these are extended with Advanced Retention Policies, permitting even more granularity over the MPIT cycle.

Resources are not unlimited, so having suitable options and taking advantage of the Advanced Retention Policies will mean better overall coverage and more revenue. SLA profiles are an essential feature that allows providers to start tiering services in this way to tenants, making the decisions for them on the DR capability and functionality at each tier and, if required, allowing customers to have their custom profiles.

**Market opportunity**

As more customers move to cloud or find themselves in cloud provider VMware clouds, the need to protect their workloads becomes more and more critical, not only from disasters but also from malicious intent as more and more hackers threaten the company’s intellectual property.

For these reasons, the global disaster recovery as a service market generated $6.5 billion in 2021 and is projected to reach $60.4 billion by 2031, growing at a CAGR of 23.9% from 2022 to 2031 (Allied Market Research, 2022). Furthermore, the global cloud migration services market touched a valuation of $92.4 billion in 2021 and is projected to generate revenue of $340.7 billion by 2028 at a CAGR of 24.30% during the forecast period, 2022–2028 (Vantage Market Research, 2022).

Migration, security, and backup and disaster recovery are also some of the highest-in-demand hosted and cloud-managed services organizations are planning to introduce in 2021/2022.
Repatriation is real

In the last 12 months, 54% of companies have moved workloads or data away from the hyperscale public cloud to some other venue 36% moving both applications and data, versus 10% moving only applications and 8% moving only data.

1. Of this 36% state information security concerns as a primary motivator
2. Of this 23% data locality/sovereignty issues and performance issues and the need for better regulatory compliance
3. Of this 16% cost, complexity and lack of transparency issues

Companies in the $10 million-$99.99 million range were most likely to migrate away from the hyperscale public cloud to on-premises (73%) and colocation (27%)

With the migration to the private cloud being a primary use case customers are looking for, VMware Cloud Director Availability provides inclusive cold and warm migration at no additional cost. With a simple vSphere plugin or via the VMware Cloud Director user interface, customers can self-manage their migration or providers can deliver migration as a managed service.

Considering security and malware attacks are prevalent, the ability to restore quickly is key to business recovery. With Cloud Director Availability 4.6 and 4.5, a 1-Minute RPO, One-Click Migration, Tunnel Appliance High Availability, and Advanced Recovery Plans are the front lines to delivering the granularity of restore points and the fastest time to recover (RTO), ensuring businesses can get back working as quickly as possible.

Similarly, with competitive features such as replicating encrypted VMs, One-Click Migration, RPO Compliance, and Advanced Reporting Capability, Cloud providers can offer highly efficient DR and migration services with insights that can influence their customers to make informed decisions and mitigate numerous threats and challenges.

The market is neither fragmented nor, at this time, consolidated from a provider selling DRaaS perspective, so there is plenty of opportunity for all VMware Cloud Providers. Hybrid (on-premises and cloud-based) configurations account for much of the current market share and represent an opportunity provided by several global and regional providers and hyper-scale providers like AWS and Microsoft Azure. However, solutions to Hyperscale or different target hypervisors are viewed as migration solutions and not accurate disaster recovery solutions due to disk conversions making failing back very complex and manual. VMware Cloud Providers, therefore, have an excellent opportunity to sell DRaaS from a hybrid on-premises customer to their cloud solution with the benefit that it is not a migration (although it could easily be used for this); it is a proper self-service disaster recovery as a service capability.

Additional Information

Upgrade

VMware Cloud Director Availability 4.6 supports direct upgrades from 4.4.x or 4.5.x. For vSphere DR and Migrations site, first upgrade to version 4.5.x from 4.4.x before attempting 4.6 upgrade. Please refer to the upgrade process, Upgrade in the Cloud Director site and Upgrade on-premises and provider site. For more, please read the Release Notes.

For more information on cloud computing and VMware Cloud Powered services, please visit https://cloud.vmware.com/providers or contact your VMware representative.

For more information about VMware Cloud Director Availability 4.x please see https://www.vmware.com/products/cloud-director-availability.html

If you would like to understand what your opportunity could look like using VMware Cloud Director Availability, please use our online calculators https://cpscalculator.vmware.com/

Access the VMware Learning Zone for Cloud Providers to learn more about cloud technology you as a provider can use http://bit.ly/VCPPSolutionEnablementLearningPath

If you would like to connect with the VMware Cloud Director Availability team, please use Slack, Facebook, Twitter, Linkedin.