VMware Cloud Director Availability 4.0

A Natural Partnership

"Atea has been using VMware Cloud Director Availability to provide Disaster Recovery as a Service to many customers in Sweden. We are excited about the 4.0 release increased solution capabilities and building these into our offerings to existing customers and new."

JONAS EMILLSON
DIRECTOR PRODUCT MARKETING
ATEA

NEW FEATURES

- Remote site bandwidth throttling
- Customer bandwidth monitoring
- Customer storage monitoring
- Customer failover enhancements
- Customer failover assessment
- Persistent Stored Instances
- Disk Resizing auto protection
- SLA Profile service customization
- In-context VM/vAPP protection
- Multi-NIC traffic conditioning
- Global traffic limiting
- Syslog event management
- NSX-T 2.5 support

Introduction to VMware Cloud Director Availability

Every business in every sector needs to protect their investment in their digital estate. Typically, companies employ backup to be able to restore in case of a disaster. However, with exponential growth in data, backups are rarely tested and do not meet the recovery point needed for data that changes frequently. VMware Cloud Director Availability whilst able to cover frequency for replication, goes much further in granularity to low recovery point objectives and high frequency of point in time instances - helping businesses keep recovery as close to real time as possible.

Lots of companies have an expectation of either a managed service or a self-service depending on this size and budget. Self-service Disaster Recovery has become a simple expectation that has been popular in Hyperscale clouds, but most of these clouds require disk conversion to the target hypervisor, making testing difficult if not impossible and Disaster Recovery becomes a migration. Having a vSphere source and vSphere target cloud means there is no disk conversion, no different architecture or security to worry about and makes true Disaster Recovery as a (self-)service possible. Indeed, VMware Cloud Director Availability is the only Disaster Recovery solution integrated to VMware Cloud Director that supports self-service Disaster Recovery and migration at a click of a button.

Of course, recovery is only as good as the testing to ensure recovery will work, and whilst many solutions cannot provide self-service or simplistic testing, none-impacting testing is out of the box for VMware Cloud Director Availability. Ensuring that customers can test when they wish to reduce risk of issues in a real failover Disaster Recovery event.

Whilst Disaster Recovery solutions are targeting applications, not all requirements are equal; some applications are mission critical and some are business critical, others are non-critical. It is important that a customer understands their application portfolio and has the option to choose the appropriate coverage for the application. Like insurance policies, it is not one size fits all, but the ability to differentiate is key to aligning cost to capability and criticality. VMware Cloud Director Availability features capabilities to tier offerings in repeatable, sustainable way – meeting all workload types and criticality.

Using a Disaster Recovery solution can also be a great way of onboarding into a cloud environment as many companies wish to move out of their data centers to a Cloud Provider, replicating workloads and cutting over from on-premise to cloud is exactly the same for Disaster Recovery as it is for migration. VMware Cloud Director Availability supports both Disaster Recovery and Migration allowing for complex networking and security and self-service failover use cases.

vmware®

Service Operation

Monitoring, Reporting, Control

Helping Providers and customers operationalize their DRaaS services with enhancements for monitoring, reporting on capacity and controls for restoring logic and workflows.

Service Consumption

Service Tiering, Optional Upsell Functions

Improving features designed to drive increased ease of use to help drive consumption of DRaaS services. Helping customers and providers plan and assess capacity and failover requirements to increase confidence and service reliability.

Platform Integration

In-context DR In VCD, NSX-T support

Further enhanced integration to keep aligned to VMware Cloud Director and make the solution more intuitive for customers.

Main themes for 4.0 release

Service Operation

Cloud Providers need to be able to operate the solution in amongst their other systems, this can provide difficult if there are many systems, each providing different services. To meet this challenge 4.0 introduces syslog support, enabling providers to centralize their event management of the DRaaS, rather than having a VMware Cloud Director console open 24/7.

Consumers of the DRaaS service have increased visibility with storage reporting available in the UI. Since DR only uses storage until a failover operation when compute (RAM & CPU) is needed, understanding your storage requirement as a whole or by individual VM/vAPP is key. VMware Cloud Availability can now also handle customer vSphere 7 disks that are re-sized without having to reconfigure replication, this is a nice feature that means customers do not need to link any resize operations to DRaaS, it happens automatically.

Customers also benefit from enhanced failover controls and bandwidth controls. Failover is a complex task and DRaaS now can handle/correct Operating System behavior regarding IP and hostnames/DNS updates that can leave a VM unreachable post cutover. Bandwidth in areas that are bandwidth sensitive or for customers who may take too much provider bandwidth can now be limited at source to help providers optimize their services.

Service Consumption

Consuming a service will impact cost and as all workloads have different criticality there is a need to align a different service tier to them and also provide the ability to store replications for longer periods (take them out of the DR cycle). Cost for DR is not storage alone, customers must be able to start workloads at the target, so understanding the storage capacity and the compute capacity required to start all workloads enables providers to judge what compute should be provisioned for each customer as a minimum. VMware Cloud Availability now provides destination resource calculations based on source configuration to assist providers understand the target resources.

Providers can now tier their DRaaS service much easier than before using 'SLA profiles' that contain key data regarding DRaaS choices to meet the criticality of a protected workload. These can be applied tenant wide and could easily be mapped to a service tier, i.e. 'Gold' SLA profile could have a fast RPO, granular retention time and compression turned on. Providers can event give tenants' rights to modify and make custom profiles for individual protection if required. This is known as personalization, the ability to provide on-mass tuning of a service personalized to the customer requirement, but critically still supportable for a provider. Providers can also now allow customers to take a replication out of circulation and 'farm' this away for any amount of time, basically akin to a long-term backup done from within DRaaS.

Service Integration

Given the need to drive better consumption of the service, what if customers don't have to go into VMware Cloud Availability tab to drive DRaaS protection and failover operations? Now they can, directly in their VCD console they can see the status of VM and vAPP protection and launch in-context operations, this should drive much more consumption of the service for providers.

Lastly VMware Cloud Director Availability as a key service for VMware Cloud Director tenants, now supports NSX-T version 2.5 & 2.5.1 and will support future releases in patch releases in the future. This aligns with the direction that cloud providers are taking as NSX-T starts to supersede NSX-V in deployments.

Simple, Capable Disaster Recovery as a Service

From the installation in the provider cloud to implementation on premise, VMware Cloud Director Availability is a simplified very capable architecture making it easy for customers and providers to implement. Customers can self-serve deploy a replication appliance into their vCenter and connect to a provider Virtual Data Center via an encrypted tunnel, then start protecting their workloads directly from vCenter or from the Provider UI using the symmetric nature of the product. VMware Cloud Director Availability allows customers to configure and manage both incoming and outgoing replication from the source and recovery site.

Importantly there are no agents to deploy on ESXi hosts and starting replication is a quick activity, equally the networking is vastly simplified to make it straightforward to deploy and use. In version 4.0 providers who enable VMware Cloud Director Availability for customers, enable 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 2 main use cases; on-premise to cloud Disaster Recovery and / or migration and Cloud to Cloud Disaster Recovery and / or migration.
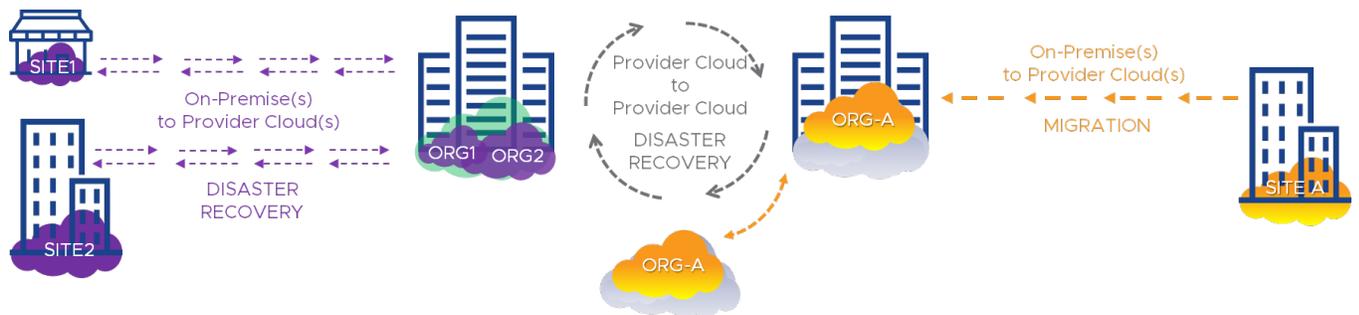
Migration capability is cold and warm and easily scheduled into maintenance windows to suit your customers. Cold Migration is the complete sync of an offline workload before cutover and warm migration just syncs the differential at the time of cutover and is faster to implement. Many providers use VMware Cloud Director Availability for migration as it is simple, at no charge to VMware, but importantly can be driven by customers and allowing a customer to self-migrate when it suits them is a great experience and selling point.

Usability in this release has been significantly improved and many UI improvements make the solution far more intuitive for customers to enjoy Disaster Recovery as a Service. Having intuitive usage is preferential for customers to be able simply use the solution and drives better consumption. Around the themes explained in the previous section, VMware Cloud Director Availability is really helping customers drive better protection and testing. In fact, one big aspect of the solution is the ability to test, i.e. the ability to ensure that you have limited any uncertainly in your capability to recovery in the event or a disaster.
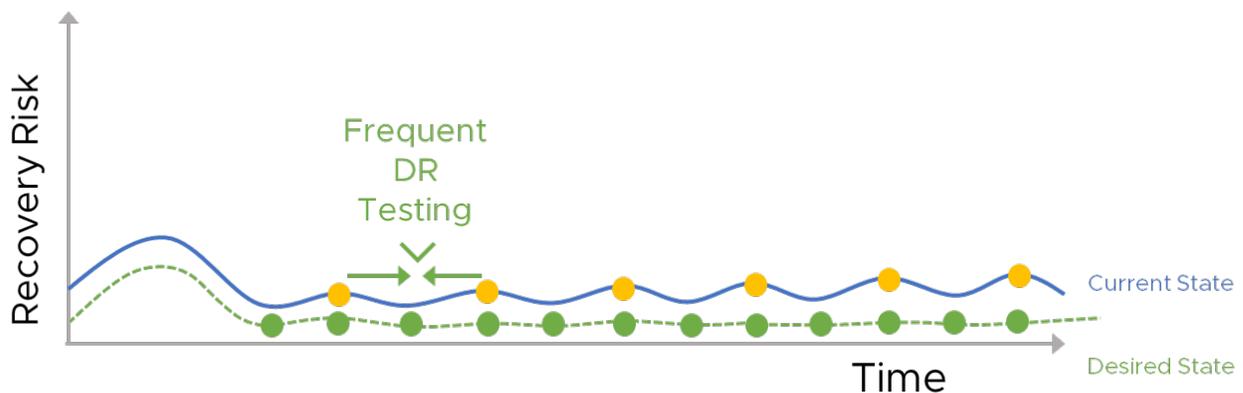
Testing frequently is the key to decreasing risk and protecting against a disaster, unfortunately it is perhaps the least used feature in DRaaS. Typically, this is because Disaster Recovery is provided by products that do not suit self-service or because the provider needs to ensure resource availability at the target is managed between multiple customers.

VMware Cloud Director Availability is self-service and can also be a managed service; self-service, and 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 and this could be complimented with additional application testing services. As a self-service capability it is important 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 at the same time. The recommendation is to promote testing as feature to decrease risk of recovery uncertainty.

Workload distribution

It is important 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, others may be non-critical and have longer cycles with less granularity. When considering Disaster Recovery, you need to have cost and functionality allocated correctly to cost, i.e. the higher the importance of a workload the more cost it is likely to take to cover it as it will consume more data, more replicants more frequently.

Mission Critical characteristics are defined as affecting the entire business, business will stop quickly in the result of outage. These are applications that have serious impacts on a broad part of the business can be deemed mission critical. E.g. financial systems which transact millions of transactions per minute are critical to the business success. Customers for DRaaS need to think about what applications are in their business that the business cannot survive without for even the shortest duration?

Business Critical characteristics are different and affect Line of Business, but overall business can operate and survive. These Line of Business applications can be viewed as business critical. E.g. HR payroll system, although without it payroll will be interrupted, the business will carry on.

Lastly there are non-critical workloads and applications, they affect people personally and may delay deliverables, but ultimately, they are not affecting the business, nor teams in the business 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:
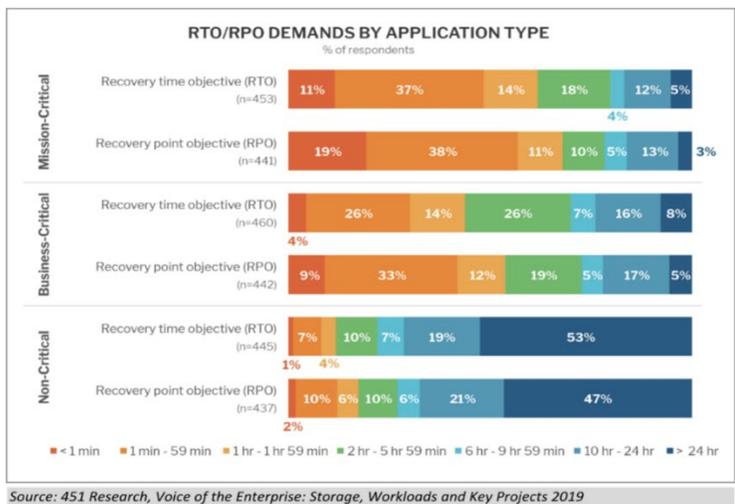
For a customer to be able to match a workload to a tier of service for Disaster Recovery is important as it will be more cost effective to have the appropriate resource capacity aligned to the workload. Having a single tier DRaaS portfolio does not provide the flexibility to cover mission critical workloads vs noncritical – there will be underused functionality/ capacity which
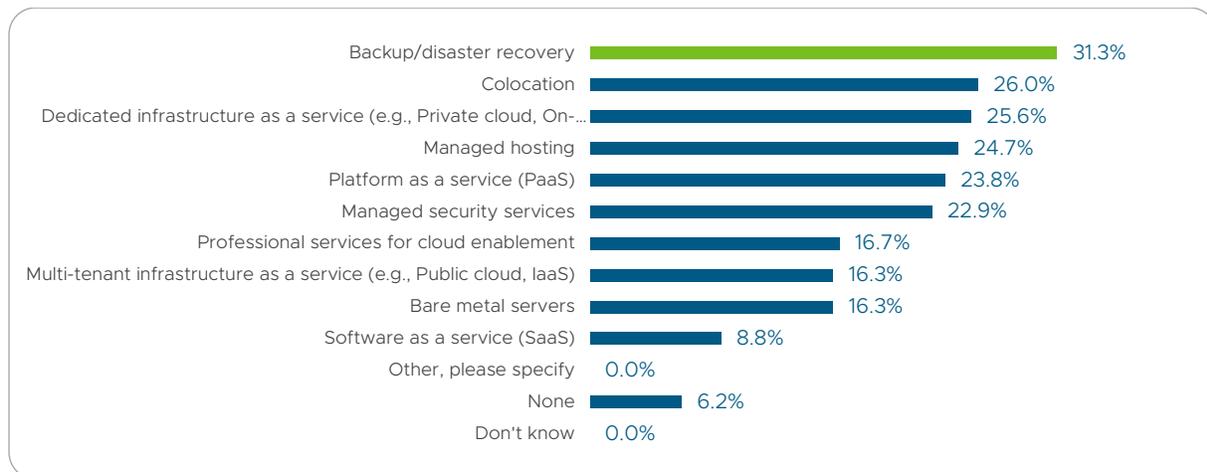
may cost the customer more overall. From a partner perspective, consumption will be much higher and better aligned with a tiered offering to customers.

Resources are not unlimited so having the right option choices available will mean better coverage overall and more revenue ultimately. SLA profiles in version 4.0 is an important 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 own 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 important, not only from disasters, but also from malicious intent as more and more hackers threaten company's intellectual property.

For these reasons, the growth in the Disaster Recovery market continues to grow at a *CAGR of 36% from 2018-2022* and expected to increase to *41.8% from 2022 to 2025*. Backup and Disaster Recovery are also the highest in demand hosted and cloud service organizations are planning to introduce in 2020:

Category	Percentage
Backup/disaster recovery	31.3%
Colocation	26.0%
Dedicated infrastructure as a service (e.g., Private cloud, On-…	25.6%
Managed hosting	24.7%
Platform as a service (PaaS)	23.8%
Managed security services	22.9%
Professional services for cloud enablement	16.7%
Multi-tenant infrastructure as a service (e.g., Public cloud, IaaS)	16.3%
Bare metal servers	16.3%
Software as a service (SaaS)	8.8%
Other, please specify	0.0%
None	6.2%
Don't know	0.0%

451 Voice of the Service Provider, Workloads and Key Projects 2020

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-premise and cloud based) configurations account for much of the current market share and represents an opportunity this today is provided by several global and regional providers as well as hyperscale providers like AWS and Microsoft Azure. However, solutions to Hyperscale or different target hypervisors are really viewed as migration solutions and not true Disaster Recovery solutions due to disk conversions making failing back very complex and manual. VMware cloud providers therefore have a great opportunity to sell DRaaS in a hybrid on-premise to their cloud solution with the benefit that it is not a migration (although it could easily be used for this), it is a true self service Disaster Recovery capability.

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

For more information about VMware Cloud Director Availability 4.0 please see *https://www.vmware.com/products/vcloud-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*