VMware Cloud Director Availability™

4.3 Datasheet update

AT A GLANCE

VMware Cloud Director Availability offers simple, secure, and cost-effective onboarding, migration, and disaster recovery as a service (DRaaS) to or between multitenant VMware Cloud Director clouds.

KEY BENEFITS NEW IN 4.3

1 MIN RPO

New in 4.3 is 1 min RPO, now you can really address customers with mission critical workloads with the granularity needed for fast changing workloads that need a 1 minute delta record.

ADVANCED RETENTION POLICIES

New Advanced Retention Policies extend the existing 'Retention Policy' SLA Profile allowing more control over the maximum of 24 instance retention Multiple Point in Time replication deltas. Previously they were spread evenly across the duration with no flexibility.

DISASTER RECOVERY AND MIGRATION PLANS

Customizable recovery sequencing and grouping. Now you can offer more control over the execution of recovery with steps, timings, and grouping of VM and vApps for DR or migration.

EASIER MIGRATION WINDOWS WITH SCHEDULED INITIAL SYNC

Migration within a change window is hard if you have to also run an initial sync in that window, you will likely run out of time. Now you can schedule these in advance, so you are ready for migration when the change window starts.

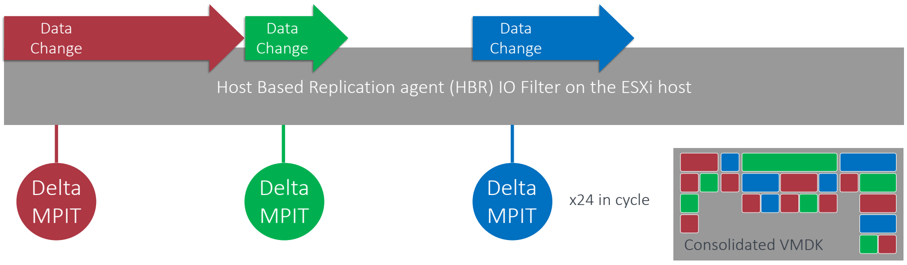
TUNNEL HEALTH MONITORING

Lots of customer tunnels connected? Now you can monitor them all via UI and API to monitor their health and assist in troubleshooting network issues.

4.3 Key updates

1 minute Recovery Point Objective (RPO)

If granularity is important to your customers and you have critical VMs in which data changes regularly, then you want the smallest distance between changes, i.e., a more granular recovery. Now providers can enable a 1-minute RPO using replication policies and SLA policies, if chosen, this is cycled every 24 minutes with the Multiple Point In Time (MPIT) rotation, with the last MPIT being consolidated (full consolidated vmdk created) before starting the next cycle.



As the process above shows, at each given RPO timeslot, of which the fastest is a maximum of 1 minute, a Delta VMDK MPIT image written, only the data changed from the previous Delta MPIT point will be written and a maximum of 24 MPIT is permitted. The 24th MPIT is consolidated into a VMDK and then the cycle repeats.

Of course, this is a desirable feature for critical workloads, but it comes at a price – network, storage and compute must be able to handle the additional read and write tasks, which will be intensive. For a 1 min RPO to be available VMware recommends the use of all flash storage with a low current storage utilization, and cache to capacity ratio for disk groups. Please check the official documentation to ensure your infrastructure is suitable before offering this option to tenants.

What is the actual use case for a 1 min RPO? As already explained such a capability will require significant resource, and this will in turn mean cost, that is why a 1 min RPO should be used for mission-critical applications, those the business cannot live without and/or have significant financial impact with downtime. It should be noted that modern applications including database systems, clustering technologies and other solutions can help protect these applications with active-active and standby setups when zero downtime is required and disaster recovery, really means disaster recovery.

Advanced Retention Policies

MPIT from the retention policy setting and RPO were, prior 4.3, spread evenly across the chosen duration and there was no way to change this. Now retention policies allow a maximum of 5 rules to be defined to keep an instance of an MPIT (a change delta) in each schedule to the maximum of 24.

This can be applied as apart of an SLA profile and inherits that flexibility for assignment per tenant, also as a nice feature, the system will calculate automatically the number of MPIT to not exceed 24 and warn you if this does. Simular to the normal policy for MPIT, once the cycle point is reached the system will overwrite the cycle in rotation.

Note that even with advanced retention, the source disk will still be required for recovery consolidation and the higher the delta change rate between MPIT, the longer the consolidation will take.

LOOKING AT A 1 MIN RPO?

PRE-REQUISITES

- All-flash storage with vSAN
- 50% utilisation of the storage
- Ensure all management components and Cloud Director Availability components run on hosts where enough compute resources are available, ie there is no resource over-provisioning
- Ensure configuration consistency across all hosts (in source and destination)
- Design Cloud Director Availability in a way that as less as possible layer 3 hops exist between components
- If replicators are hosted in resource clusters, set reservations for the resource pool

LIMITATIONS

- Quiescing is NOT ENABLED
- VSAN: datastore should not be utilized more than 70%, including VMs and replication independent disks
- VSAN: cache-to-capacity ratio per disk group should be no less than 25%
- Total network throughput must be at least 2 GBit/s

RECOMMENDATIONS

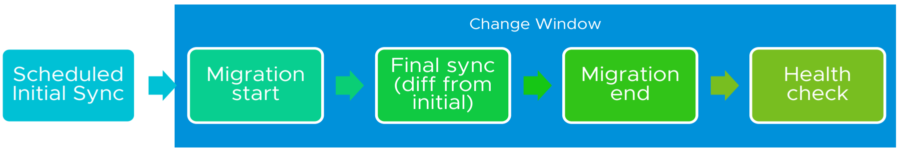
- All management components and Cloud Director Availability components in a single site communicate with latency less than 1ms
- VSAN: avoid long disk groups, ie one caching drive and 5+ capacity drives
- VSAN: monitor for disk congestion
- Know the workload (delta+rw profile) you intend to protect
- Know destination VSAN performance capabilities at utilization close to 70%

Recovery and Migration plans

Recovery and Migration plans are a new feature in 4.3 that delivers stepped sequencing between tasks required to get an application stack up and running, whether after a disaster, a test or a migration. Recovery of an application can be a complex task; it is rarely as simple as just starting up a VM. Cloud Director Availability has always recovered the VM and allowed some networking changes on recover to assist with customized recovery. In 4.3 we have taken this one step further with the ability to group VMs and vApps according to their recovery sequence priority with options for error handling.

The sequencing is very flexible to allow for as many steps as necessary in between tasks and can utilize wait timers and automated UI prompts to permit move to the next sequence step. Steps are logged in the replication tasks for plan execution or test and for all manual prompts. The plans can easily be tested (non-production impacting) also to ensure that they will work, just like a normal test failover.

When looking at migrations, a new scheduled initial sync feature will help ensure that no time is wasted in a change window to complete a migration.

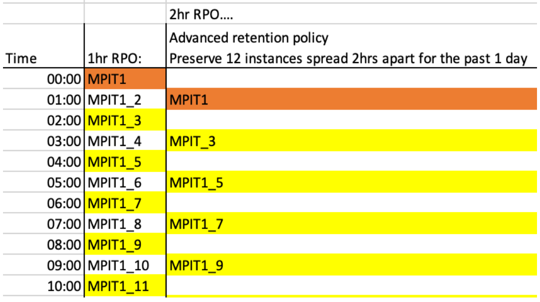


Before 4.3 without the ability to schedule the initial full sync, there would have been a delay whilst this was done in the change window, rather than scheduling it to execute prior. Now operations can save time and manage the migration of multi-tier applications with recovery plans and starting a migration change window with an up to date full sync of the VMs and vApps already complete.

Advanced Retention Policies

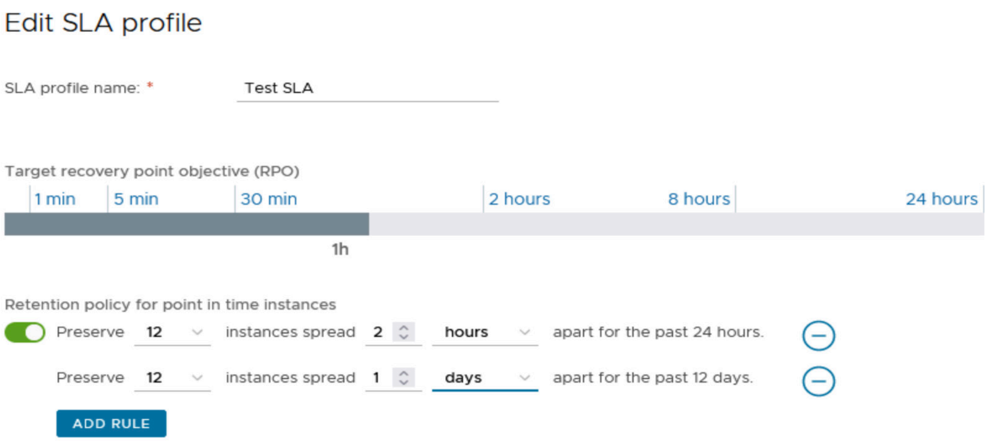
Replication with VMware Cloud Director Availability works using vSphere Replication and a maximum of 24 MPIT over a retention period, the MPIT used to be spanned evenly across this period automatically without choice, so a 1hr RPO would span 1hr even MPIT across a 24hr period, before cycling, there would be no choice in this. Now retention policies allow a maximum of 5 tiers to be managed, this means you can create up to 5 rules to define an instance schedule of an MPIT (a change delta) in each tier.

Whilst retention policies provide you further granularity over the MPIT cycles you effectively get more RPO tiers with this. For example, if you have a 1hr RPO, AND you define a Advanced Retention Policy rile to keep 12 instances over 2hrs for the past 1 day, this means that each day you would have your 1hr MPIT AND a 2hr MPIT from the advanced retention policy, you can think of this like so in the following table:



		2hr RPO....
Time	1hr RPO:	Advanced retention policy Preserve 12 instances spread 2hrs apart for the past 1 day
00:00	MPIT1	
01:00	MPIT1_2	MPIT1
02:00	MPIT1_3	
03:00	MPIT1_4	MPIT_3
04:00	MPIT1_5	
05:00	MPIT1_6	MPIT1_5
06:00	MPIT1_7	
07:00	MPIT1_8	MPIT1_7
08:00	MPIT1_9	
09:00	MPIT1_10	MPIT1_9
10:00	MPIT1_11	

However, as already stated, you can have up to 5 rules, each rule must get progressively larger than the last in terms of timespan and the system will work out whether the policy is valid or violates the 24 MPIT rule. In the following SLA we have detailed an additional rule that will ALSO set a daily retention:



Edit SLA profile

SLA profile name: * Test SLA

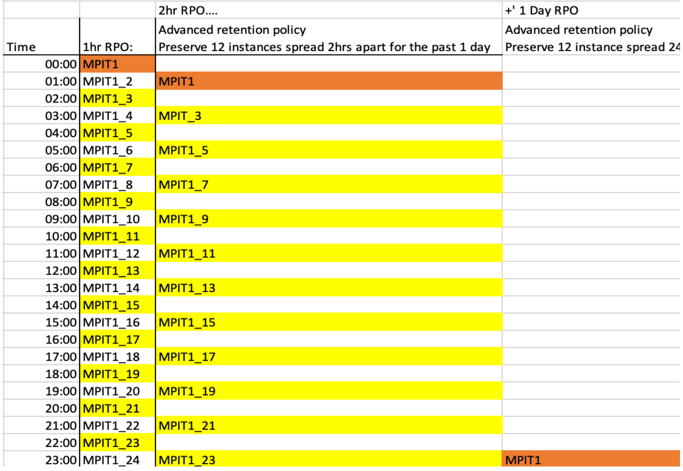
Target recovery point objective (RPO)

Retention policy for point in time instances

Preserve 12 instances spread 2 hours apart for the past 24 hours.

Preserve 12 instances spread 1 days apart for the past 12 days.

This affectively sets an additional 1-day RPO across 12 days, increasing the granularity of resource over an additional 12 day RPO. Note that the system permits this as there is still only 24 MPITs created, one way to think about these is as copies of a re-scheduled MPIT in a cycle, there are many ways of looking at this, as long as the golden rule of 24 is not broken! Another important point is that although there may be some distance between MPITs as retention policies always get a step larger in timeframe, you will still need the source disk for recovery, these are not isolated images, they are still deltas.



		2hr RPO....	+' 1 Day RPO
Time	1hr RPO:	Advanced retention policy Preserve 12 instances spread 2hrs apart for the past 1 day	Advanced retention policy Preserve 12 instance spread 24
00:00	MPIT1		
01:00	MPIT1_2	MPIT1	
02:00	MPIT1_3		
03:00	MPIT1_4	MPIT_3	
04:00	MPIT1_5		
05:00	MPIT1_6	MPIT1_5	
06:00	MPIT1_7		
07:00	MPIT1_8	MPIT1_7	
08:00	MPIT1_9		
09:00	MPIT1_10	MPIT1_9	
10:00	MPIT1_11		
11:00	MPIT1_12	MPIT1_11	
12:00	MPIT1_13		
13:00	MPIT1_14	MPIT1_13	
14:00	MPIT1_15		
15:00	MPIT1_16	MPIT1_15	
16:00	MPIT1_17		
17:00	MPIT1_18	MPIT1_17	
18:00	MPIT1_19		
19:00	MPIT1_20	MPIT1_19	
20:00	MPIT1_21		
21:00	MPIT1_22	MPIT1_21	
22:00	MPIT1_23		
23:00	MPIT1_24	MPIT1_23	MPIT1

4.3 Service Operation &Administration improvements

UI option to select appliance NIC for communication with other local components

Many appliances have multiple Network Interface Cards (NIC) that are multi-homed to other networks for many different reasons. Providers frequently want to route replication traffic over a different network, perhaps a dedicated link or one with a different Quality of Service set. Cloud Director Availability previously expected the first NIC to be only usable interface and hence with some appliances where different networking was required, this caused configuration issues and needed to be corrected by using CLI.

Now in 4.3 we are deliver this capability into the user interface to support configuring traffic control multi NIC support, including user-defined static routes for:

- Tunnel for communication with other local components
- Replicator for communication with other local components

Change cloud service certificate without impact on premises

Cloud providers have many customers replicating from on-premises. Changing the Cloud Director Availability certificate forced all the attached peers to re-pair. In 4.3 certificate details are now stored on-premises using the default java CA trust store and uses the associated verification procedure to ascertain whether the central site certificate is valid or not, this provides a full certificate chain verification without manual intervention needed in a certificate change.

Tunnel endpoint health

In an environment with many customers replicating to cloud, there are many tunnel connections. These tunnels will typically traverse firewalls and other network components, which can make troubleshooting hard. In 4.3 we have introduced a tunnel API to query the health of all local endpoints (components) and all remote tunnel endpoints (customer side or other cloud site). The API will query DNS resolution, connection status, route to host, and endpoint availability.

Backup and Restore

In previous releases we have provided the capability to back up the configuration and services of an appliance and restore in situ to a 'vanilla' appliance that was required to be deployed before the restore could be done. In this release we are removing the need for an existing appliance to be deployed to restore the back up to, and also encrypting backups for additional security.

Assessable provider Virtual Data Centers

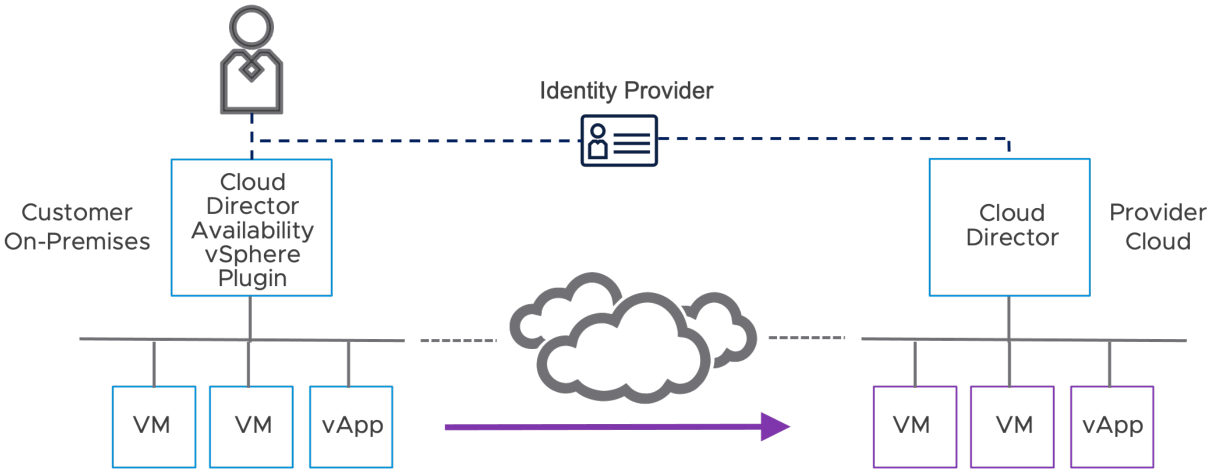
Many providers configure their environment with a single SSO Domain with multiple vCenters. Some of them are workload vCenter and provide Provider VDC (PVDC) resources and some are management vCenters which host all management components for the cloud.

In the case where each PVDC has its own VMWare Cloud Director instance there maybe network connectivity limitations to management vCenters or other workload vCenters (perhaps in other geos and would not be replication targets). These are now configured in a 'permit' list meaning that "Accessible Provider VDCs" can be configured so the UI will return only the vCenters that are backing the corresponding PVDCs and not the other vCenters in the SSO domain.

4.3 Product Maturity, Troubleshooting & Supportability enhancements

On-premises to cloud plugin authentication for tenant identity provider

Cloud Director Availability has improved on premise customers using the Cloud Director Availability vSphere plugin capability to do replication management operations without having to login to the provider Cloud Director instance using local Cloud Director credentials. Previously credentials for on premises and at Cloud Director were both local, and would only work if they matched, or the tenant would be re-challenged to authenticate with Cloud Director credentials, also, critically, there was no option to use the tenants own identity provider for both. Now tenants are able to authenticate with their own identity provider on premise and also using an API token instead of a local username and password, the authentication can be relayed to their identity provider and reused for accessing VMware Cloud Director Availability at the provider site, eliminating the need to have local users matching.



Add VMs to existing vApp groups

Creating replications to protect applications from on-premises to cloud is a day to day activity, but when applications change, editing an existing replication to add in additional resources wasn't previously possible. If you are creating a replication, you can select multiple machines which can be grouped in a vApp, now in 4.3 you can also edit existing replications and add or remove VMs to a group. You can also specify the virtual machines boot order, boot delays, and protect or migrate them as a single vApp replication in the destination cloud site.

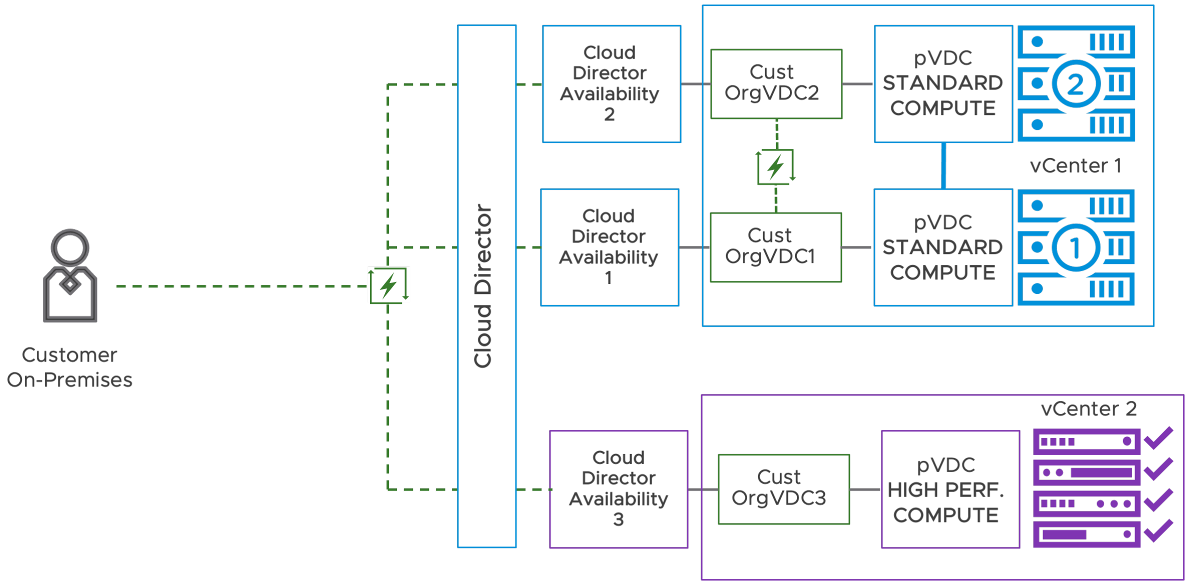
Optimized re-protect of only delta changes when reversing replication

If you have migrated to cloud and wish to perform a migrate back (reversed) the replication before 4.3 always resulted in a full sync despite that there might not be any actual changes of the VM disks in between the migration and reverse. 4.3 tracks the changes on a migrated VM and only transfers the delta changes from the original source, making failback much quicker and effective. To accomplish this Cloud Director Availability keeps stored additional data per replicated disk and implements dormant replication management, these replications are used to track changes of the migrated VM upon reverse.

Multisite SAML authentication

When tenants replicating between org VDC or multiple Cloud Director Availability instances use the same Cloud Director instance.

Many cloud providers have differing hardware platforms to offer tenants, from high performance compute to standard as example. To manage these Provider Virtual Data Center (VDC) resources and to manage traffic control more optimally they deploy Cloud Director Availability in each site on each differing platform and corresponding pVDC under management. In this way they can have multiple pVDC connected to a single VMware Cloud Director instance spanning the sites, as in the diagram below:



Tenants may wish to replicate between OrgVDC (i.e. between instances that Cloud Director Availability manages) and wish to extend their session (without having to login again with a local username and password) to Cloud Director Availability to create the replication.The problem is that those tenants could not extend their session to a remote Cloud Director Availability instance to create a replication, they would need to login using a local username and password, which presents a security issue for some providers.

In 4.3, now when opening the "extend session" dialog in the UI to create a task on a remote Cloud Director Availability instance, json web tokens (or SAML) are used and using a new API these sessions are extended using the same token, supporting VMware Cloud Director Availability multisite capabilities. Essentially 4.3 enables the 'challenging' destination Cloud Director Availability to check the login of the origin Cloud Director Availability, and allow access to the same token, thus extending the login session to two or more Cloud Director Availability instances simultaneously.

LEARN MORE

For more information visit:

https://www.vmware.com/products/cloud-director-availability.html

4.3 Release Notes:
https://www.vmware.com/en/VMware-Cloud-Director-Availability/4.3/rn/VMware-Cloud-Director-Availability-43-Release-Notes.html

Provider download:
https://my.vmware.com/en/web/vmware/downloads/info/slug/datacenter_cloud_infrastructure/vmware_cloud_director_availability/4_3#product_downloads

Tenant download:
https://my.vmware.com/en/web/vmware/downloads/info/slug/datacenter_cloud_infrastructure/vmware_cloud_director_availability/4_3#drivers_tools

GET INVOLVED.

Join our VMware Cloud Director Availability *SLACK channel*

FOR MORE INFORMATION OR TO PURCHASE VMWARE PRODUCTS

Call 877-4-VMWARE (outside North America, +1-650-427-5000), visit *vmware.com/products*, or search online for an authorized reseller. For detailed product specifications and system requirements, alwasy refer to the online documentation.

Cleanup ‘stale’ replications

Typically, after a redeployment of Cloud Director Availability without stopping existing replications, the system will lose track of the replication as the information will not be in the newly deployed database and the replication can remain configured on the source side. This is a problem for the user as the system believes the replication is still configured and prevents the user from initiating start again until the source is unconfigured. Currently the user would have to log into ESXi host and run a few commands in order to unconfigure the source replication, such a use case is unusual and often the result of administration error. Such a replication is referred to as a stale replication. To avoid this happening 4.3 forcefully unconfigures the VM and configures it anew on start, and, shows a warning in the Replication Tasks view.

There are many more enhancements and improvements in VMware Cloud Director Availability 4.3, please check out the *release notes* for a complete update on all changes.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com