Advanced Architecture Design for Cloud-Based Disaster Recovery

WHITE PAPER
Introduction

Disaster Recovery (DR) is a fundamental tool for mitigating IT and business risks. But because it is perceived as expensive and complicated, only a minority of even Tier 1 and Tier 2 applications are protected by DR. New virtual hybrid cloud services — some purpose-built for DR — have changed the technical and business landscape. The purpose of this report is to update perceptions of DR cost and complexity, and chart a path toward wider adoption.

This paper is part of a project to design and build a full-scale hybrid architecture using VMware vCloud® Air™. Specifically, it shows how organizations can replicate their virtual machines to a disaster-recovery virtual data center in vCloud Air, to protect more of their applications from data loss and downtime without the burdens of building and managing their own tertiary DR sites.

The brief covers both basic and advanced topics related to vCloud Air Disaster Recovery environments:

- The advantages and basics of setting up and migrating to a vCloud Air hybrid cloud Disaster Recovery environment.
- How and where to set up resources to run supporting infrastructure such as Active Directory and DNS.
- Data Seeding, using a live cloned copy of a virtual machine to reduce the time needed to replicate it.
- Configuring multiple machines for vCloud Air Disaster Recovery replication.
- Setting up native failback via reverse replication.

This paper assumes that the reader is familiar with vCloud Air and knows how to access vCloud Air resources.

vCloud Air Disaster Recovery — Overview and Installation

Managed-services approaches to DR services can be expensive, because instead of reducing the complexity of the underlying environment, they often try to overpower it by applying human resources. This causes problems during recovery, because complexity slows down recovery processes and it’s difficult to scale up or re-deploy staff quickly enough to cope with an emergency.

vCloud Air Disaster Recovery was designed for simplicity. This not only holds down costs, it allows planning, maintenance, management, and emergency response to be carried out by an organization’s own teams. For organizations that prefer a managed-services model, VMware’s worldwide network of partners offers services to meet any requirement.

Because vCloud Air Disaster Recovery is based on VMware vSphere®, it supports the industry’s widest range of certified operating systems (90+) and applications (more than 5,000). It requires no tricky virtual machine conversions — vital in a real disaster when you need your applications back right away.

In a disaster, you may run your applications on vCloud Air as long as you need, and then transfer your virtual machines and data back to your own site at your convenience.

Working with vCloud Air Disaster Recovery is simple:

1. Download and install the replication virtual appliance into your supported vSphere environment.
2. Connect the replication appliance to your vCloud Air Disaster Recovery environment.
3. Specify the virtual machines to protect in your vSphere environment with their recovery point objective(s).
4. Start replication.

Alternately, you can also ship VMware a disk containing your virtual machines to seed the initial replication process. After seeding, only the changes (deltas) are replicated to vCloud Air.

More information about the installation and configuration for vCloud Air Disaster Recovery can be found in the VMware vCloud Air – Disaster Recovery User’s Guide.
Setting up Supporting Infrastructure

Most enterprise applications rely on a domain controller or directory service for authentication. Most physical Disaster Recovery environments run these infrastructure services like Active Directory and DNS on machines that are kept hot and always on at the DR site. As a best practice, domain controllers aren’t replicated, because the DR site has a different IP address range. Instead, the DR environment is treated as simply another “site” in Active Directory, and certain applications and resources are kept running there waiting for failed-over machines to use them.

But vCloud Air Disaster Recovery resources are not “always on.” To keep standby costs low, a virtual machine replica is only on storage until a failure or test failover — the machines don’t use any compute and memory resources until then. As a result, infrastructure services like Active Directory or DNS should not be running inside a Disaster Recovery environment.

There are several options for running these “pilot light” services on machines outside your vCloud Air Disaster Recovery subscription:

1. Connect to an existing physical site by VPN.
2. Cross-connect to a cage in a vCloud Air location where those resources may already be running.
3. Purchase a vCloud Air Virtual Private Cloud or vCloud Air Dedicated Cloud subscription to run the services and set up a cloud-to-cloud VPN, or leverage vCloud Air Virtual Private Cloud OnDemand to run the services and setup a cloud-to-cloud VPN.

1. VPN from Physical Site

This option only works if you already have two or more physical sites running these infrastructure services. With just one site, the services you need would be running on the infrastructure you are protecting — so if the site goes down, your services do, too. But if you have two sites and are protecting only one of them into vCloud Air, you can use the other site to run your services as shown in Figure 1:

![Figure 1: Arranging for Active Directory and DNS services by VPN from a physical site.](image-url)
2. Cross-Connect to a Cage

With vCloud Air, you can arrange to stand up your own physical infrastructure in a co-location arrangement at the same data centers as the vCloud Air Disaster Recovery environment. vCloud Air then offers an add-on option of cross-connect — the ability to wire from your vCloud Air resources directly to your cage with a high-speed private connection. The directory services can be running in your cage as a secondary site along with other workloads and the failed over workloads in vCloud Air Disaster Recovery can point to the cage when they are recovered.

Figure 2: Cross-connect option from customer data center cage.

3. Cloud-to-Cloud VPN with Virtual Private Cloud, Dedicated Cloud or Virtual Private Cloud OnDemand

This final option is particularly good if you are planning to add infrastructure-as-a-service resources with vCloud Air, or plan to connect new standard vCloud Air resources back to your on-premises data center with basic services provided from the cloud. Once you have these in place, you are already set up to configure a cloud-to-cloud VPN.

Figure 3: Cloud-to-cloud option.
This is the setup used in the tutorial video series available on the tutorials page. The benefit of this last approach is you can run these resources in any vCloud Air location and connect them together as well as back to your own premises.

**Network Considerations**

Some network considerations apply when configuring VPN connections and Active Directory Sites and Services:

- For VPN, the endpoint networks cannot be the same.
- VPN mappings must use the correct vCloud Air Edge Gateway firewall rules to allow traffic to pass.
- Networks in the vCloud Air Disaster Recovery environment should be defined as a new “Site” with the proper domain controller assigned.

**Support Infrastructure – Conclusions**

As shown, there are multiple ways to provide “always-on” support infrastructure for cloud Disaster Recovery resources. The intent here is not to give step-by-step configuration instructions for every possible setup, but to illustrate concepts you can apply to your own environment.

**Zero-Downtime Seeding for Replication**

Depending on the size of the virtual machine and the available network bandwidth, the initial replication or transfer of data to Disaster Recovery environments can take a long time. Data seeding can reduce it considerably, but there is a trade-off. Data seeding for vCloud Air Disaster Recovery is usually done using the vCloud Connector copy feature, which requires that the machine be powered off before it can be copied.

This section documents an alternative approach: first cloning the machine while running, using VMware vCloud Connector® to copy it, and then configuring the replication seed from the cloned-and-copied version. Three options are compared:

1. **Full replication from the ground up**

2. **“Standard” seeding**: vCloud Connector copy of the powered-off machine with data-seed replication. This option requires copying the machine to a vCloud Air Disaster Recovery catalog, and then deploying it to the cloud.

3. **Live clone of the machine in VMware vCenter™ under a temporary name, then copying it into vCloud Air Disaster Recovery under the original name, followed by data seeding.** This also requires copying it to the catalog, then deploying to the cloud.

**1. Full Replication**

In the test case, initial sync over the Internet transferred about 14GB of data, the usage of the virtual machine on disk. It runs a checksum on the entire disk, configured in this case for 50GB, but only transfers what is actually in use.

Figure 4 shows the full amount of data transferred. The entire process took 68 minutes to transfer 14GB of data.

![Figure 4: Full replication in progress.](image)
2. Seeding by vCloud Connector Copy

Here the machine was shut down, copied to the vCloud Air Catalog, then deployed to the cloud for use as a seed. When using this approach, please note:

- Unlike the unique identifiers assigned when machines are replicated from scratch, vCloud Connector leaves it up to the user to create templates and vApp names in VMware vCloud Director®.
- “From scratch” machines are owned by “System”, but those deployed from templates or vCloud Connector copies are owned by the user specified in vCloud Director.
- Stopping replication does not remove the seeded virtual machine from vCloud Air Disaster Recovery the way it does for a ground-up replication. The seeded virtual machine will remain deployed to the cloud and in the catalog until they are removed.

This approach significantly reduced the amount of data transferred for the seed — only about 7.32MB. The checksum process still takes time to complete on the entire machine, so the total time needed for synchronization, at 71 minutes, was about the same — but with much less data transfer over the wire.

3. Live vSphere Clone With vCloud Connector Data Seed

This final approach is similar to the preceding one, except that it starts with a vSphere live clone of the running machine. Then, as before, vCloud Connector copied the live clone up to vCloud Air Disaster Recovery and deployed it for use as a seed. The expectation is that the initial sync will be comparable to the preceding method, but because live cloning allows export of the copies using Offline Data Transfer, it eliminates downtime.

The approach is straightforward:

1. Take a live clone of the virtual machine in vSphere, with no customization, not even powered-on. Keep the original virtual machine powered on and running.
2. Use vCloud Connector Copy or Offline Data Transfer to offload the cloned data to vCloud Air Disaster Recovery.
3. Deploy the vCloud Connector Copy machine imported into template to the cloud for use as a seed. With ODT, this is done for you.
4. Configure VMware vSphere Replication™ using data seeding for every cloned and imported machine. This will initiate synchronization on the changed data between the live virtual machine and the seeded clone.
5. Repeat the process for every virtual machine that needs a seed.
6. Remove the vSphere clones from disk.

In practice, the data for each machine would usually be sent to the ODT appliance and on to VMware for import to the cloud. If there are on-premises storage limitations, this might need to be done in batches: clone and copy each batch to the appliance, delete the clones, and repeat.
You can see in Figure 6 that the initial sync is similar to the other approaches. The initial sync time took 65 minutes, but it transferred a total of 617 MB of data.

![Figure 6: Seeding by live vSphere clone, in progress.](image)

This workaround lets you seed replications using Offline Data Transfer without the need to power off the source machine. Please note that this works with vCloud Air Disaster Recovery because although vSphere Replication validates disk UUID values when making vCenter-to-vCenter replications, it ignores them for replications to vCloud Air.

## Configuring Multiple Machines for Replication

vCloud Air Disaster Recovery allows you to configure multiple machines for replication. The following example assumes you have set up the correct version of vSphere Replication Appliance for replication to vCloud Air, and you have a vCloud Air Disaster Recovery account. Please also note:

- You must select machines of the same OS type. If you select Windows and Linux, for example, the Linux machines may fail to configure because Windows supports Guest Quesicing under Microsoft Volume Shadow (Copy) Service.
- All machines will begin replicating at about the same time, staggered slightly according to when their configuration steps finish. This can push a lot of data over your networks if there are too many machines in a group.
- Every machine in a group will initially be set up with the same Recovery Point Objective (RPO). You can adjust machines later by changing their individual settings.
- You can use vSphere tags to group machines according to RPO, OS type, or other logical groupings. Once tagged, you can sort them to configure the replication.
Configuration Process

Highlighting the group you want and right-click to select “Configure Replication” as shown in Figure 7:

![Figure 7: Selecting a group of machines for replication.](image)

After a validation check, continue configuration using the normal options for a Cloud Provider. When you finish, the task pane will show all selected machines configuring:

![Figure 8: Multiple machine configuration in progress.](image)

You can also use multi-select to stop replication on multiple machines at once. Only re-configure, stop, and pause options — not failover and test — are available when you multi-select. You may call the failover options on multiple machines through scripts using the vCloud Air API extensions.
Multi-select configuration also works for Data Seeding, producing a side-by-side selection in which you may choose and match sources to destination seeds. This is shown in Figure 9. Note that many of the same limits apply, for example that all selections will initially use the same RPO.

Figure 9: Multiple machine configuration in progress.

**Setting up Failback with Reverse Replication**

Once you have initiated a failover to a vCloud Air Disaster Recovery, you may want to fail-back to your on-premises vSphere environment when that site is operational again. This is easily achieved by using the incoming replication option in the vSphere Replication appliance. The example shown here assumes you have already performed a failover to vCloud Air Disaster Recovery and have a new on-premises vSphere environment without any existing virtual machines:

1. Select the Incoming Replications in vSphere Replication Monitor area of the vSphere Web Client and click the Configure replication from Cloud Provider configure button. This will display the Configure replication from Cloud Provider Wizard.

2. Walk through the same configuration steps as you would to configure replication to a cloud provider. Once you have access to your vCloud Air Disaster Recovery environment, you are prompted with a set of virtual machines that are hosted in your cloud.
3. Select the virtual machines you want to replicate from vCloud Air back to your on-premises environment.
4. Pick a target data store on-premises that is attached to your vSphere hosts.
5. Specify your Recovery Point Objective.

![Configuration settings for cloud-based disaster recovery](image)

6. Confirm your settings, and click Finish.

![Confirmation of replication settings](image)
You will then see a task appear in vCenter confirming that the configuration is being performed.

<table>
<thead>
<tr>
<th>Task Name</th>
<th>Size</th>
<th>Start Time</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure a virtual machine for replication from site A</td>
<td>52 MB</td>
<td>00:00:00</td>
<td>01:00:00</td>
</tr>
</tbody>
</table>

Once the replication has been completed, you will see that the status shows a Green OK, indicating the initial full sync has completed and that replication was successful.

Conclusions

Assuring continuity of applications and data through enterprise-grade Disaster Recovery practices is a prerequisite for any full-scale enterprise hybrid architecture using VMware vCloud Air or any cloud infrastructure-as-a-service solution.

The examples reviewed here extend the vCloud Air use cases to include Disaster Recovery in the cloud, with

2. Multiple options to support the DR environment with Active Directory, DNS, and other infrastructure services.
   - Efficient data seeding alternatives to reduce initial migration time.
3. Multiple-machine configuration protocols to reduce administrative burdens.
4. Easy to deploy failback replication to move workloads back on-premises.

vCloud Air is an enterprise-ready hybrid cloud solution, ready now to meet the most demanding requirements.