Table of Contents

1. Introduction ................................................................................................................................. 3
2. Executive Summary ..................................................................................................................... 3
3. High Level Product Review Summary ....................................................................................... 4
4. Substantial Feature Comparison Summary ............................................................................... 5
5. Deployment Topology ................................................................................................................ 7
   5.1. Azure Site Recovery .............................................................................................................. 7
   5.2. Zerto Virtual Replication .................................................................................................. 8
6. Installation Prerequisites .......................................................................................................... 9
   6.1. Azure Site Recovery ........................................................................................................... 9
   6.2. Zerto Virtual Replication ................................................................................................11
7. Installation Summary ................................................................................................................. 12
   7.1. Azure Site Recovery ........................................................................................................12
   7.2. Zerto Virtual Replication ................................................................................................12
8. Workload Protection .................................................................................................................. 13
   8.1. Azure Site Recovery ........................................................................................................13
   8.2. Zerto Virtual Replication ................................................................................................14
9. Resource Usage in Practice ...................................................................................................... 14
   9.1. Azure Site Recovery ........................................................................................................14
   9.2. Zerto Virtual Replication ................................................................................................15
10. Failover Testing .................................................................................................................... 15
    10.1. Azure Site Recovery .......................................................................................................16
    10.2. Zerto Virtual Replication ..............................................................................................16
11. Failback ................................................................................................................................... 16
    11.1. Azure Site Recovery .......................................................................................................17
    11.2. Zerto Virtual Replication ..............................................................................................17
12. Migration Use Cases ............................................................................................................... 17
    12.1. Azure Site Recovery .......................................................................................................17
    12.2. Zerto Virtual Replication ..............................................................................................18
13. Multiple Site Protection ........................................................................................................... 18
    13.1. Azure Site Recovery .......................................................................................................18
    13.2. Zerto Virtual Replication ..............................................................................................19
14. References .................................................................................................................................. 20
1. INTRODUCTION

Both Microsoft and Zerto customers and partners often ask us, “What the differences between Azure Site Recovery (ASR) and Zerto Virtual Replication (ZVR)?” The primary reason we get this question is the potential customer or partner is familiar with one of the technologies and not the other and on the surface, they sound similar.

This guide will explain step by step, why ZVR and ASR are very different products and meet different levels of performance and usability. We also provide a relative ease of use guide to add a bit more color to the user experience working with both products.

2. EXECUTIVE SUMMARY

Azure Site Recovery and Zerto Virtual Replication are both great tools that can help any IT organization improve the success rate of their disaster recovery plan. The point of this document is not to be a kill sheet for one product or another, instead it is intended to highlight the pros and cons of each product in relation to VMware virtual machine replication into Microsoft Azure public cloud.

At a high level both products are very capable of accomplishing the previously mentioned task, but as this article will demonstrate, each product does have advantages over the other depending on the workload that needs protected.

For example, Zerto Virtual Replication, while a little more time consuming to initially configure, has more time saving workflows integrated into it not only for disaster recovery, but also for migrations and testing too. Failback is also another area where Zerto shines above ASR, since the required networking is already configured, and reverse replication can be enabled with a single check mark.

One of the major pros for ASR is that it can protect physical workloads into Azure. Zerto does not have physical workload support, and is limited in terms of supported source workloads. Today only VMware vSphere and Microsoft Hyper-V are supported as a source. In theory, any physical or virtual machine could be replicated with ASR if the operating system is supported in Azure. This is because ASR is agent based for both physical workloads and for VMware based workloads.

Installation requirements for each product are unique, and for customers who need to protect only a few virtual machines, or VMs on a single Hyper-V host, ASR is a clear winner in terms of ease and speed of installation. But as the number of protected workload increases, the required ASR infrastructure can become overwhelming and ZVR’s ease of scalability become much more evident.

In terms of costs, ASR and ZVR when compared on a monthly subscription bases are very similar. List price for ASR is $25/month per protected VM, and ZVR is about $21/month per protected VM. Both solutions also require you to pay for the storage that is consumed by your replicated workloads, but there are a few additional costs for Zerto that ASR does not require. One of these costs is the compute instance that runs the Zerto Cloud Appliance, and the other is the cost of a VPN or ExpressRoute connection. So, keep in mind that ZVR may be more feature rich but it can also cost a slightly more than ASR too.

This document will dig deeper into several key areas of tools like ASR and ZVR and compare the two at a
technical level. Remember, the point of this document is only to aid customers in the decision-making process when choosing between ASR and ZVR for disaster recovery or migration purposes when Azure public cloud is the target.

3. HIGH LEVEL PRODUCT REVIEW SUMMARY

Product highlights rated on a scale of 0-10, with 10 being the maximum number of points.

<table>
<thead>
<tr>
<th>ASR</th>
<th>ZVR</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="icons/5.png" alt="Rating" /></td>
<td><img src="icons/8.png" alt="Rating" /></td>
</tr>
<tr>
<td><img src="icons/5.png" alt="Rating" /></td>
<td><img src="icons/8.png" alt="Rating" /></td>
</tr>
<tr>
<td><img src="icons/8.png" alt="Rating" /></td>
<td><img src="icons/5.png" alt="Rating" /></td>
</tr>
<tr>
<td><img src="icons/5.png" alt="Rating" /></td>
<td><img src="icons/8.png" alt="Rating" /></td>
</tr>
<tr>
<td><img src="icons/5.png" alt="Rating" /></td>
<td><img src="icons/8.png" alt="Rating" /></td>
</tr>
<tr>
<td><img src="icons/5.png" alt="Rating" /></td>
<td><img src="icons/8.png" alt="Rating" /></td>
</tr>
<tr>
<td><img src="icons/5.png" alt="Rating" /></td>
<td><img src="icons/8.png" alt="Rating" /></td>
</tr>
<tr>
<td><img src="icons/5.png" alt="Rating" /></td>
<td><img src="icons/8.png" alt="Rating" /></td>
</tr>
</tbody>
</table>

| Overall Score | 4.5 | 8.5 |
## 4. SUBSTANTIAL FEATURE COMPARISON SUMMARY

<table>
<thead>
<tr>
<th>Comparison Point</th>
<th>Zerto Virtual Replication</th>
<th>Azure Site Recovery</th>
</tr>
</thead>
<tbody>
<tr>
<td>Replication Technology: How is data moved between locations?</td>
<td>Continuous Replication. Industry leading continuous data replication engine deployed at 6,000+ locations. Linear scale with each new physical host.</td>
<td>Collected and Shipped Replication: Collection servers consume production resources and difficult to scale, point in time recovery is sporadic because changes are shipped and not streamed.</td>
</tr>
<tr>
<td>Does the solution leverage agents?</td>
<td>Agentless: Zerto connects to Hypervisor at each host and does not examine content of individual VMs. There is no software to be installed into each VM. No reboots of VMs and ESX environment in most cases.</td>
<td>Agents required for vSphere: Agents must be supported on each OS type. Change management and approvals required to install agents on production servers. Possible incompatibility issues and negative impact on performance.</td>
</tr>
<tr>
<td>What is the end user management experience like?</td>
<td>Streamlined experience with single management interface for all operations. Zerto Virtual Manager is consistent across private, public, and ZCSP platforms. Build on HTML5 and compatible with all browsers.</td>
<td>Multiple Management Interfaces. Separate Interfaces for certain actions - Azure Resource Manager for overall control and failover/testing. On-Premises Process Server Configuration Interface for configuring access credentials and journal location, and Guest Agent Interface.</td>
</tr>
<tr>
<td>What workloads are protectable?</td>
<td>All virtual workloads on a supported hypervisor platform. Zerto can move data between platforms and hypervisors if the destination supports that OS.</td>
<td>No cross-hypervisor replication. Can do VMware and Hyper-V to Azure, but not all OS's are supported in Azure.</td>
</tr>
<tr>
<td>Can the solution be used in a multi-tenant environment?</td>
<td>Yes, Used by 350+ cloud service providers</td>
<td>No. ASR is designed for single-tenant use between on-premises to Azure.</td>
</tr>
<tr>
<td>Does the solution support hybrid cloud strategies?</td>
<td>Many options based on workload requirements. Azure, AWS, IBM Cloud, and Zerto Cloud Service Provider Network all supported.</td>
<td>ASR is only capable of replicating between on-premises hypervisors and Azure.</td>
</tr>
<tr>
<td>Is Linux failback supported out of the box?</td>
<td>Yes. Zerto leverages the same components to protect, failover, and failback all workloads.</td>
<td>No. ASR requires a Windows process server for Windows workloads and a Linux based process server for Linux workloads.</td>
</tr>
<tr>
<td>What connectivity requirements are there for replication and failback?</td>
<td>A secure connection between sites is required for all communications. Once in place no other requirements needed for failback.</td>
<td>Replication to Azure is supported over a simple SSL connection. However, reverse protection and failback requires a VPN or ExpressRoute to be configured before failback can start.</td>
</tr>
<tr>
<td>Comparison Point</td>
<td>Zerto Virtual Replication</td>
<td>Azure Site Recovery</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Are there any performance implications on the production workload?</td>
<td>No, resources required for replication are consumed in a dedicated replication appliance. No additional CPU/Memory/Network used in guest OS.</td>
<td>Yes, guest agents consume guest CPU, RAM, network capacity to move change data to the process server.</td>
</tr>
<tr>
<td>What are the journal storage requirements at the source and destination sites?</td>
<td>Zerto only leverages a journal at the recovery site. This journal is compressed and only contains changed blocks.</td>
<td>ASR requires a journal at both the source and destination (Azure or on-premises) sites. The minimum requirements are 600GB per process server, the maximum is 2TB per process server.</td>
</tr>
<tr>
<td>Is there a limit on how much change data per VM can be processed?</td>
<td>Zerto can protect workloads with any data change rate, if the destination storage and WAN connectivity can handle the change rate.</td>
<td>ASR can protect VMs with a maximum daily change rate of 2TB. If a VM has more than 2TB of daily change data, ASR cannot protect it.</td>
</tr>
<tr>
<td>How is the solution priced?</td>
<td>Zerto is priced per VM, replication to Azure is included with Zerto Virtual Replication Enterprise Cloud Edition, or can be purchased separately.</td>
<td>ASR is priced per VM and is added to your monthly Azure bill.</td>
</tr>
</tbody>
</table>
5. DEPLOYMENT TOPOLOGY

This paper is based on Zerto Virtual Replication 5.5 and Azure Site Recovery 9.11.4609.1 (Sept 2017). Running on top of vSphere 6.0 going to the Ohio region of Azure. While we will focus on VMware as a source platform, there is mention of other source hypervisor platforms throughout the document if it is a significant differentiator.

In the following section, the products were compared based on topology requirements and project planning complexities that one would encounter for an example workload.

5.1. Azure Site Recovery

There are four major components needed to replicate from Azure Site Recovery on-premises to the Azure Public Cloud. These components are downloaded from the Azure Vault configuration wizard and installed on a Windows machine in your on-premises datacenter.

The first server you install is a Config Server. A Config Server is a central management server that communicates with the Azure Vault and executes jobs on-premises. A default installation will also install two other components on your main Config Server, a Process Server and a Master Target Server.

The Process Server component is what processes the protected data and transports it to the Azure Vault. Process Servers have CPU, Memory, and disk requirements depending on the size of the workload to be protected. If a single Process Server cannot scale up large enough to protect your workload, a scale out approach can be taken and an additional process servers can be deployed.

Master Target Servers are only needed during failback operations. It is important to note that a Master Target Server can only failback servers that are of the same operating system type, so a Windows Master Target Server cannot failback Linux servers. For Linux servers, a Linux Master Target server must also be installed.
The last component of the ASR topology is a Mobility Services Agent. This agent gets installed on each protected virtual machine and is responsible for sending changed data to the Process Server so that it can be shipped to the Azure Vault.

In summary, ASR installs multiple components on premise that differ based on what workloads you plan on protecting. For small to medium sized deployments the amount of planning and number of components may be acceptable. For larger deployments, a customer may have to invest extensive amount into planning as more than one process server and more than one master target server will be required. This can make deployment more complex and means that you have several machines to maintain.

5.2. Zerto Virtual Replication

Zerto has two main components, a manager – Zerto Virtual Manager (ZVM), and workers – Zerto Virtual Replication Appliances (VRA). Each physical hypervisor host in your environment gets a VRA if it will contain protected VMs or if it will receive data for protected VMs. Normally this means all hosts in a cluster will get VRAs.

For multi-site deployments, each site gets a ZVM and clusters with protected data will get one VRA for each of the physical hypervisor hosts.

For public cloud sites including Azure and AWS, Zerto leverages a combined ZVM/VRA architecture called a ZCA or Zerto Cloud Appliance. For Azure, the ZCA can be deployed from the Azure Marketplace or you can build from scratch with a Windows VM and the Zerto for Azure installation package from MyZerto. Because the ZCA uses an embedded VRA, the only way to scale the replication capacity to Azure is in a scale out fashion. So once a ZCA has reached its maximum (approximately 100MB/s throughput) an additional ZCA will need to be deployed.

In summary, the Zerto architecture contains the same number of components no matter how many VM’s you are protecting on-premises. Planning is also straight forward because it scales along with your environment, meaning if you add an ESXi host or Hyper-V host – you add a VRA as well.

On the cloud side, planning is recommended to ensure enough ZCA capacity is available for the protected workload.
6. INSTALLATION PREREQUISITES

In this section, the products were compared based on resource requirements needed to protect a given workload. We looked at the number of components we would need to deploy, the size of each component, as well as other infrastructure considerations required to make the two solutions work as advertised.

6.1. Azure Site Recovery

To use Azure Site Recovery for replication to Microsoft Azure you will need to have a valid Azure account, a WAN connection to Azure, as well as at least one Windows Server on-premises to act as a Config/Process Server.

Your WAN connection requirements will depend on the amount and rate of change of the data that you will be protecting.

You will also need to have a Resource Group and some Vnets defined in Azure so that failover can take place.
The on-premises Config/Process server requirements will vary based on the dataset you are protecting. The minimum requirements are as follows:

<table>
<thead>
<tr>
<th>Hardware</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of CPU cores</td>
<td>8</td>
</tr>
<tr>
<td>RAM</td>
<td>12 GB</td>
</tr>
<tr>
<td>- OS disk</td>
<td>3</td>
</tr>
<tr>
<td>- Process server cache disk</td>
<td></td>
</tr>
<tr>
<td>- Retention drive (for failback)</td>
<td></td>
</tr>
<tr>
<td>Disk free space (process server cache)</td>
<td>600 GB</td>
</tr>
<tr>
<td>Disk free space (retention disk)</td>
<td>600 GB</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Software</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating system version</td>
<td>Windows Server 2012 R2</td>
</tr>
<tr>
<td>VMware vSphere PowerCLI version</td>
<td>PowerCLI 6.0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Network interface card type</td>
<td>VMXNET3</td>
</tr>
<tr>
<td>IP address type</td>
<td>Static</td>
</tr>
</tbody>
</table>

If you have a dataset larger than what a single process server can handle, you can deploy additional process servers. Each process server will require the following resources based on how much daily change data it will protect:

<table>
<thead>
<tr>
<th>Data Change Rate</th>
<th>CPU</th>
<th>RAM</th>
<th>Boot Disk</th>
<th>Cache Disk Size</th>
<th>Total Disk Throughput Required</th>
<th>NIC Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up to 300 GB/day</td>
<td>4</td>
<td>8</td>
<td>40 GB</td>
<td>Minimum of 400 GB</td>
<td>15 - 20 MB/s</td>
<td>2 x 1 GigE with Static IP</td>
</tr>
<tr>
<td>Up to 700 GB/day</td>
<td>8</td>
<td>16</td>
<td>40 GB</td>
<td>Minimum of 790 GB</td>
<td>34.9 - 46.6 MB/s</td>
<td>2 x 1 GigE with Static IP</td>
</tr>
<tr>
<td>Up to 1 TB/day</td>
<td>8</td>
<td>32</td>
<td>40 GB</td>
<td>Minimum of 790 GB</td>
<td>51.2 - 68.27 MB/s</td>
<td>2 x 1 GigE with Static IP</td>
</tr>
</tbody>
</table>

The last thing that is required to successfully protect VMware VMs with Azure Site Recovery is network access and administrator credentials to the protected virtual machines. An Active Directory service account with administrator access can be used on VMs on a domain, and a root level account on Linux will be required.

In summary, consumption of CPU, Disk Space, and IOPS on the production site are the main things to plan for with ASR. As an ASR deployment scales, you may need dedicated storage spindles for the process servers to keep up with the protected workload. CPU usage should also be monitored on both the Process Server and inside each protected VM, during initial synchronizations as well as times of high IO the Mobility services agent can also consume significant amounts of CPU power which could affect your production services.
6.2. Zerto Virtual Replication

Zerto requires “LAN like” IP connectivity between the sites that you want to replicate between, so most implementations will require a VPN, secure MPLS, or some other sort of “LAN like” WAN connection with routing capabilities. Zerto does not provide network level encryption, and Network Address Translation (NAT) is not supported between Zerto components.

The Zerto Virtual Manager requirements will vary based on the number of VM you are protecting as well as the number of sites. The minimum and maximum requirements for the Zerto Virtual Manager are in the table below, refer to the Zerto Virtual Replication installation guide for guidance on when to use the minimum or maximums.

<table>
<thead>
<tr>
<th>Hardware</th>
<th>Minimum</th>
<th>Maximum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of CPU cores</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>RAM</td>
<td>4 GB</td>
<td>8 GB</td>
</tr>
<tr>
<td>Number of disks</td>
<td>1 – OS Size + 5GB</td>
<td>1 – OS Size + 5GB</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Software</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating system version</td>
<td>Windows Server 2012 R2</td>
<td>Windows Server 2012 R2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address type</td>
<td>Static</td>
<td>Static</td>
</tr>
</tbody>
</table>

Each physical hypervisor node will also require one Zerto Virtual Replication Appliance. Their configuration varies depending on the number of protected workloads and the amount of delta changes.

<table>
<thead>
<tr>
<th>VRA size per host</th>
<th>vCPU</th>
<th>RAM</th>
<th>HDD</th>
<th>NIC Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum</td>
<td>1 vCPU</td>
<td>3 GB</td>
<td>12.5 GB</td>
<td>1 x 1 GigE with Static IP</td>
</tr>
<tr>
<td>Maximum</td>
<td>2 vCPU</td>
<td>16 GB</td>
<td>12.5 GB</td>
<td>1 x 1 GigE with Static IP</td>
</tr>
</tbody>
</table>

One major difference between Azure Site Recovery and Zerto Virtual Replication is that ZVR does not require any journal space at the production site. This means that there are no additional writes IO’s, and therefore no impact on the production storage array during normal replication. During initial synchronizations, bitmap, and delta sync processes there is additional read IOps that are placed on the production storage as Zerto reads change data from the production VMDK files.
7. INSTALLATION SUMMARY

The installation process of a product is the first impression for many users, how well and how quickly an installation goes has a significant impact on how successful the product will be during its lifecycle. For this document, we looked at three major areas while installing the products: ease of installation, the speed of installation, and intuitiveness of the installation.

Both products have pro’s and con’s to their installation process, and there is no clear advantage to either product regarding installation.

7.1. Azure Site Recovery

To install Azure Site Recovery for replication to Microsoft Azure you start by logging in to your Azure portal. From the portal, you will deploy a new Azure Vault from the Azure Marketplace. To do this, you select “Backup and Site Recovery (OMS)” from the marketplace. There will be a confirmation page, as well as some fields where you can name your new Azure Vault. Once you click OK, Azure Resource Manager (ARM) will deploy your Vault.

Once the Vault has been deployed, you can navigate to it in Azure Resource Manager (ARM), and begin the on-premises infrastructure setup. At a high level, you will be going through several wizards to download the Azure Site Recovery software package, generate a pairing key, and finally defining a replication policy (where your RPO and RTO are defined).

Once you have this wizard complete and the ASR software downloaded, you can perform the ASR Config Server (with embedded process server) installation. During this installation, ASR will also pair to your Azure Site Recovery Vault and make sure that communication is working properly between Azure and your datacenter. No special VPN or networking is needed, besides an internet connection with the proper outbound access to Azure.

After installing the Config Server, you will want to log in to it and use the ASR configuration tool to add the user credentials needed to access your protected workloads. These credentials are needed so ASR can try to deploy the Mobility Services agent to each workload that you protect. Proper network access to each of the protected VMs is therefore also needed from the ASR Config and Process Servers.

Once your credentials have been added, you can switch back into the Azure Resource Manager web interface to start configuring replication jobs.

The take away from the installation section is that while networking and pairing to Azure is very simple with ASR, other tasks like installing agents, configuring replication jobs, etc., require you to jump back and forth between several different user interfaces which makes things confusing.

7.2. Zerto Virtual Replication

Zerto requires a private connection before replication can happen. So, before starting your Zerto installation make sure that you have VPN or ExpressRoute connectivity between your on-premises datacenter and your Azure Resource Group. Once you can pass traffic between sites you are ready to start your Zerto installation.

For the on-premises side you will want to deploy a Windows machine to serve as the Zerto Virtual Manager.
Next, download the ZVM installation package from the MyZerto portal and install it on the ZVM Windows server. Once installation is complete, enter your license key information and login.

Once ZVM is installed, you will deploy Zerto Virtual Replication Appliances. The deployment process is automated once the administrator specifies the required parameters for each VRA.

For the Azure side, login to ARM and navigate to the Azure Marketplace. Once there, search for “Zerto Virtual Replication” and deploy the ZCA appliance from the official template. Assign the ZCA an appropriate instance size and wait for it to deploy. Once deployment has completed login and run the ZCA installation/configuration wizard from the desktop.

The wizard will ask you for your Azure login information, this information is what is used for API access to your Azure instance and then configure the ZCA.

Once the configuration is completed you can login to the Zerto Virtual Replication web interface and pair the ZCA (Azure side) with your ZVM (on-premises side). After pairing the sites, you are ready to start protecting workloads.

The only real downside to Zerto during installation is that networking must be configured before replication can start. However, once in place you have no further networking changes to make. With ASR you can start replication without a special connection in place, but before you can failback the same VPN or ExpressRoute type connection must be in place. So it’s more about when you have to setup networking more than if you have to setup networking.

8. WORKLOAD PROTECTION

To compare how workload protection is enabled in each product we focused on a few areas which we thought were critical. These areas were: interface intuitiveness, source workload variety, failover customizations, and success rate of protection tasks.

Protecting workloads with both ASR and Zerto is similar. At a high level, you are simply selecting the workloads to protect, specifying some failover settings, and determining what their RPO and history requirements are. The two solutions implement this workflow differently, but they are similar. The subsections below will highlight only the major differences in each product, please refer to the respective product administration guides for detailed information on the respective product.

8.1. Azure Site Recovery

One major advantage of ASR over Zerto is that ASR can protect physical workloads. While this guide focuses on virtual machines, it is important to note that if you have a significate population of physical workloads and not many virtual machines, ASR will likely be a better fit in your environment.

To start protecting a workload ASR has the administrator create replication policies in the Azure Resource Manager web interface. These policies include things like RPO alert thresholds, recovery point retention length, app-consistency checkpoint interval, among other things. Once these policies are created they can be assigned to protection jobs.
By default, the policies are set to 15 minute RPO alerts, 24-hour recovery point retention, and 60 minutes between app-consistent checkpoints. The smallest RPO alert threshold can be set to 1 minute, while recovery points can be stored for a maximum of 72 hours. Application consistent checkpoints can be setup to run anywhere between 0 and 720 minutes (where 0 is disabled).

Each protected workload can have its own replication policy, unless you are using multi-vm consistency – then the replication group is assigned a policy.

The downside to ASR is that you must navigate through several other interfaces before you are able to protect a workload. These interfaces include the Config Server credential wizard, as well as the replication policy setup wizard. This can be confusing at first, but once your workload credentials are setup and your policies are defined, the protection workflow is straightforward and intuitive.

8.2. Zerto Virtual Replication

ZVR has multi-VM consistency which is implemented by a concept called a Virtual Protection Group. A Virtual Protection Group, or VPG, is a collection of VM’s along with their recovery settings and an automation workflow for recovering those VMs.

To protect one or more virtual machines, you run the Create VPG Wizard. This wizard will allow you to select all the VMs you want, as well as specify a boot order and pick other recovery settings such as IP changes, virtual network attachments, etc.

Once you have specified all the settings in the VPG, Zerto will start replication. Once replication has finished its initial synchronization, recovery points will begin to be created every few seconds.

Zerto however does not automatically take application consistent checkpoints, but the VSS plugin can be scheduled or manually ran when needed.

In conclusion, aside from the VSS plugin, the entire workflow protection process is done in a single interface – the VPG creation wizard. Zerto also does not require network connectivity or credentials for the protected workload which makes protecting a workload much faster and easier. This makes protecting a large number of workloads quick and easy.

9. RESOURCE USAGE IN PRACTICE

In our testing, resource usage and its effect on production workloads and the underlying infrastructure was very different between the two products. These impacts were monitored during initial protection, ongoing replication, and during periods of connectivity issues. However, while the product differ greatly, proper planning can help mitigate most negative effects on production workloads.

9.1. Azure Site Recovery

Azure Site Recovery leverages a Mobility Services Agent in each VM that is protected. This agent is what is responsible for monitoring for change data and sending it to the Process Server.
Because the Mobility Services Agent lives inside of the protected VM it draws CPU, RAM, and Network capacity from the protected (production) virtual machine, and this can affect performance of that workload.

During an initial synchronization of a VM in our tests the CPU, Network, and Disk usage on both the protected machine and the Process Server were greatly affected. We observed the mobility services agent, and its sub processes consuming as much as 75% of our CPU resources, and as much as 500Mbps of our 1Gbps network interface. Therefore, if your protected server is sensitive to network congestion it would be advisable to run the initial sync during a time when it will not affect production.

During period of high IO on the protected virtual machine, CPU usage by the agent can once again become an issue, however under a moderate workload the added overhead is unnoticeable.

In summary, if using ASR for replication you will want to plan for the heavy overhead of the Mobility Services Agent. Make sure there is additional CPU and Network capacity so that production workloads are not affected negatively.

9.2. Zerto Virtual Replication

Zerto monitors for and captures changed data at a different layer of the write stream – at the hypervisor layer--after it has left the guest operating system. This process is performed by the Zerto VRA and its underlying technology.

The Zerto VRA is an independent Linux based VM that consumes CPU and Network capacity just like any other VM, because of this, there is no impact on production workloads that are being protected. Zerto also has throttling in place so that if storage latency were to become an issue, ZVR will automatically slow down replication until the latency has fallen under the threshold. (Note Zerto only adds additional read IO during initial copies, and “Catch-up” replication processes.)

Another advantage of doing replication at the hypervisor level is that there is no need to provide credentials or network access to the protected VM, this is almost always a requirement for multi-tenant environments.

Zerto’s minimal overhead on a virtual environment and zero footprint inside of protected workloads allows it to scale to thousands of virtual machines and also allows it to work great in multi-tenant environments. This explains why most cloud service providers use Zerto technology to replicate and separate client data.

10. FAILOVER TESTING

Failover testing can be considered one of the most critical parts of disaster recovery software, without the ability to test DR software is just an insurance policy that may or may not ever get paid. The ability to do DR testing should provide a customer with the assurance that everything will work if a true disaster is declared.

For this guide ASR and ZVR were compared to see how disaster recovery testing worked in each product. The main comparisons were made in each of the following categories: automation, ease of use, ability to test without impacting production, and compliance reporting.
10.1. Azure Site Recovery

ASR covers most of the categories mentioned in the summary above. In terms of automation, ASR leverages recovery plans which can orchestrate multiple virtual machines into a single recovery operation. This allows you to construct entire datacenter failovers, or multi-tiered applications. However, when doing a failover test, you must manually specify which network subnet (vnet) you would like the VM to attach to at the time of the test. This slows down the automation process and could introduce user error because the user must remember which vnet to attach to each time.

ASR does allow you to do test failovers without taking down the production workload, however keep in mind that you need to pick a vnet that will not allow traffic from your test back to your production servers. In terms of compliance reporting, we could not find any automated compliance reports in ASR.

Overall, ASR allows for the majority of the required features to be a good replication technology. However, reporting during failover as well reporting after tests is minimal and not all in one area. This means that ASR has a bit of a learning curve until you find where all of the information you want is.

10.2. Zerto Virtual Replication

Zerto Virtual Replication has test failover automation built in to the Virtual Protection Group concept. When you create a virtual protection group you can also specify failover test settings, such as which IP address to use, what vnet to use, etc. This allows push button DR testing with no need to specify any settings during the failover test process.

In addition to allowing one or many VMs to be tested without affecting production, Zerto also gathers all the tasks and execution times and formats it into an easy to read report. This report can be used for internal or external compliance reporting with detailed information about how your DR test went, with no additional work from the user.

Zerto’s failover testing process provides a superior user experience and excellent reporting during and after testing. There is a minimal learning curve, and once you learn how the test process works, the live failover process is identical and only requires the flip of a switch in the GUI.

11. FAILBACK

When we think of failback we mean that production workloads can be moved back to the site from which they came from before a DR event. To successfully failback we would expect the production workload to have no data loss, and to have minimal downtime. Automation of the failback process, including IP changes, DNS updates, and minimal reconfiguration are also highly sought after.

ASR and ZVR will both successfully allow you to failback a workload after you have rebuilt your datacenter, but there are differences in how the products go about providing this vital recovery option.
11.1. Azure Site Recovery

Failback for Azure is a little more complex than failover. This is mainly due to the fact that you must have a VPN or ExpressRoute setup in order to do reverse replication. So while there is no VPN or ExpressRoute requirements for replication to Azure, it will have to be configured before you can replicate back.

Also, as mentioned earlier, if you have a mixed workload of Linux and Windows machines you will need to configure a Linux Master Target server before you can replicate Linux machines back to on-premises.

Failback with ASR will failback to a snapshot that has been replicated. This means that there could be data loss during failback to on-premises. Therefore, planning is needed to ensure that critical applications are not damaged during the process.

Note: For physical server replicating to Azure with ASR. Upon failback, the machine will be converted to a virtual machine. Failback to a physical machine is currently not supported.

11.2. Zerto Virtual Replication

Zerto Virtual Replication can automatically configure reverse replication if required. In the process of doing so, it will save all replication settings that are needed to ensure a proper failback. After the failed site has been recovered Zerto will automatically synchronize the two sites so that all changes that were made while the site was offline are not lost while failing back.

Zerto can leverage the “Failover” process to failback, however to ensure zero data loss during failback, the user should initiate a “Move” operation from the “Actions” menu in the bottom ribbon of the ZVR interface. The move operation works just like a failover but with a slightly different workflow. Basically the production workload is shut down before the failover happens, this means that no data loss occurs.

12. MIGRATION USE CASES

IT departments are asked to adapt to all types of corporate change, whether it’s a new plan for reducing costs, or a merger, or an acquisition, IT departments have a need for a product that can migrate their workloads to whatever new platform is needed by the business.

If we step back from the VMware to Azure use case that has been the focus of this paper, we can examine the true flexibility of ASR and ZVR to meet the ever-changing needs of an IT organization.

12.1. Azure Site Recovery

ASR is a conglomerate of several products that have been acquired by Microsoft over the years. Each product was added to the portfolio to address a specific need, and what you end up with is Azure Site Recovery. ASR can protect a much wider variety of workloads that just VMware virtual machines, in fact it fully supports Hyper-V workloads, and physical workloads too.
In some use cases Azure is only involved as the service broker, and a customer may never replicate any data into Azure. This makes ASR very flexible in terms of migration uses cases because it can protect many different types of workloads to different destinations.

The downside is that ASR must support the operating system that needs to be protected (because they need an agent on the machine), so while physical servers are supported... not all operating systems that run on physical servers can be replicated.

Lastly ASR has different components that need to be configured to support this wide variety of workloads, so if you are planning a complex migration you will need to research which components of ASR you need at each site to accomplish your goals.

**12.2. Zerto Virtual Replication**

ZVR's move operation has the same look and feel as the failover operation with a few minor differences. First, during a move operation the source virtual machine is shutdown or powered off BEFORE anything else. Shutting down the source workload allows ZVR to capture shutdown change data so that all volumes are consistent and no data loss is incurred. Once the final change data is moved to the DR site Zerto will start the process of bringing the replica copy online in the same way that it would during a failover.

Once the user has verified that the workload is as expected on the replica VM they can commit the move operation and reverse replication will start if desired.

The downside of Zerto for migrations is that it can only migrate workloads that are on a supported hypervisor. Therefore, workloads running on VMware and Hyper-V, are excellent migration candidates for Zerto. Target destinations for Zerto managed migrations include: Azure, Amazon Web Services, Zerto Cloud Service Providers, VMware to Hyper-V, Hyper-V to VMware, and homogenous migrations between hardware stacks as well.

**13. MULTIPLE SITE PROTECTION**

Multisite replication has many use cases, for some customers that have strict recovery requirements they may need a copy of the data replicated within their datacenter as well as to a different geography. For other customers, it can be as simple as maintaining replication to a current DR site while also starting replication to a new production datacenter (for migration purposes).

**13.1. Azure Site Recovery**

This is one area where ASR falls short, today there is no support for multisite replication.
13.2. Zerto Virtual Replication

Zerto allows customers to take a virtual machine and replicate it to as many as three different targets. You can mix and match the destinations between on-premises hypervisors (VMware and HyperV), as well as public cloud (Azure and AWS), and even to a Zerto Cloud Service provider.

The only requirement is Zerto Virtual Replication – Enterprise Cloud Edition Licensing.

14. INTER-REGION AZURE REPLICATION

Just as multisite replication has a place in today’s hybrid cloud, so does inter-region replication within Azure. For some customers, the idea of not owning a datacenter, and only leveraging public cloud is becoming a reality, and for them, protecting data between regions of Azure or from one public cloud to another is a growing need.

14.1. Azure Site Recovery

As of this document’s writing, AZR is in the public beta stage of inter-region Azure replication. Because of its beta status, it was not tested, however more information can be found here:

https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-azure-to-azure

14.2. Zerto Virtual Replication

As of this document, Zerto Virtual Replication does not provide support for inter-region replication. It is however on the roadmap, and scheduled for an early 2018 release.
15. REFERENCES

Linux Master Target Server Install Guide
https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-how-to-install-linux-master-target

Best Practices for Process Server Deployment when protecting VMware and Physical workloads with ASR

Inter-Region Azure Replication
https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-azure-to-azure