Zerto
FAQ

Microsoft Azure and Zerto Virtual Replication

Frequently Asked Questions

What makes ZVR 5.0 for Azure so special?

ZVR 5.0 is the only solution that enables replication and recovery to Microsoft Azure with Recovery Point Objectives (RPOs) in seconds, Recovery Time Objectives (RTOs) in minutes, no snapshots, no impact failover testing and multi-VM consistency groupings for scalable enterprise-class DR. Installable in minutes, for both VMware vSphere and Microsoft Hyper-V, get your free trial of ZVR 5.0 from the Azure marketplace today.

What do I need to configure in Microsoft Azure?

In Azure deploy a Zerto Cloud Appliance (ZCA), on a Windows D3 v2 VM, from the Azure Marketplace by searching for "Zerto Virtual Replication for Azure". The ZCA handles all the replication and recovery orchestration in Azure and should be deployed in the region you want to replicate and recover VMs to.

What do I need to install on-premises?

In your VMware vSphere or Microsoft Hyper-V environment you need to install a Zerto Virtual Manager (ZVM) in a Windows VM which connects to your vCenter or SCVMM server. From the ZVM deploy Virtual Replication Appliances (VRAs) onto each hypervisor host you need to replicate VMs from. No downtime or major configuration changes are required to install ZVR.

What connectivity do I need to replicate to Azure?

A minimum WAN link of 5Mbps is required with at least a VPN to a VM network in Azure. ExpressRoute connectivity is also supported. Routing is required from the on-premises ZVM & VRAs to the ZCA in Azure. The ZVM must be paired to the ZCA to enable replication directly into Azure. WAN sizing tools are available in the supplementary product documentation.

Where is the replica data stored in Azure?

Replica disks are stored as single page blobs and journal volumes are stored in multiple 16MB block blobs, which are cheaper than page blobs, in a dedicated storage account automatically created by the ZCA in the same region. The journal data enables point in time recovery to increments in seconds.

Can I encrypt the replica data?

Encryption can be manually enabled on the storage account automatically created by the ZCA.

How does ZVR protect & recover multi-VM applications?

ZVR 5.0 uses the concept of Virtual Protection Groups (VGPs) to enable consistent protection and recovery of multi-VM applications to the exact same point in time. Write-order fidelity is maintained across all VMs and vDisks to ensure transactional level consistency of the recovered VMs.

Are the protected VMs always running in Azure?

No, the recovery VMs are only created when needed. Performing a failover test, failover or move operation will automatically create the VMs in minutes.

How do I select the correct VM size in Azure?

During VPG creation VM sizing can be configured for each VM. Using simple drop-down selection boxes, sizes are configurable per VM. When selecting the closest matching VM size take note of the protected VM vDisk and VMNIC count. Failure to select a VM size with at least the same number of vDisks and VMNICs will break the recovery of the VM. This can be validated in advance with a failover test.

What do I need to install in the VMs?

Nothing is required to be pre-installed in the protected VMs as Microsoft Azure drivers have been included in all Windows operating systems since 2012 R2 and Microsoft has a list of Linux operating systems supported in Azure. It is recommended to configure the "Default SAN Policy" in Windows VMs to "OnlineAll" to ensure the disks are automatically mounted when recovering the VMs in Azure.

What happens to my D:\ drive when I recover to Azure?

The D:\ is used as a temporary scratch disk by default in Azure VMs. If you recover a VM which already has a D:\ drive then the scratch disk will automatically be mounted on the next available drive letter. As a best practice, it is recommended to change the VM configured to ensure the D:\ drive is not used to avoid mistaking the drive for temporary space and vice versa.

Which resource groups are VMs recovered to?

New Azure Resource Groups are automatically created per VPG for VMs upon recovery.

What about failback?

Failback from Azure is planned for the next version of ZVR due to be released in 2017. With a simple in-place upgrade single click failback will be enabled, with only the changed blocks replicated back to production to minimize the Azure cost of replicating data out. Replication from Azure is planned to deliver sub 20 second RPOs with no performance impact by using Azure CBT APIs.

How do I failback in the meantime?

A manual VM conversion can be performed using VMware Converter to export the VMs back on-premises as an interim solution. Alternatively, the VMs can be left to run in Azure until ZVR enables failback and the production datacentre is rebuilt or recreated. If failover is required for testing purposes the no-impact failover test mechanism should be utilized to prove recovery.

How does ZVR replicate the data?

ZVR replicates an initial copy of the VMs selected to Azure. Subsequently, only the changed blocks are replicated real-time, asynchronously, enabling sub 20 second RPOs with no snapshots in the protected VMs, no agents or performance impact. If nothing changes nothing replicates. Data is also compressed on the fly, saving an average 60% bandwidth on WAN links.

How long does it take to recover my VMs?
ZVR mounts the replica VM disks direct from the storage account to deliver RTOs in minutes. The RTO is subject to the amount of data in the journal that must be applied to the replica disks and the apply process is optimized to only apply the most recently changed blocks.

How do I configure the recovery settings and VM sizes?
When protecting the VMs you pre-configure the VM size and settings required per VM. This includes VM Virtual Network, Subnet, Network Security Group and Private IP address (all configurable per VNIC). All recovery settings available are derived from the Azure region of the recovery ZCA.

Can ZVR automatically change my IP addresses?
Yes, ZVR can automatically change the IP address of VMs upon recovery to simplify the testing and recovery process.

Can I test the failover?
No-impact failover testing can be utilized to validate the recovery of the VMs with no break in the replication and no downtime to production. This can be used to test RTOs and validate VM recovery in minutes during working hours.

How far back in time can I recover?
ZVR Journaling enables recovery from thousands of points in time, every few seconds, from any point in time, configurable up to 30 days in the past.

How much storage space will ZVR use in Azure?
The total space usage equals the total size of the protected VMs, plus an additional 7-10% for the Journal enabling point in time recovery. Journal data is also compressed to minimize usage.

What can I recover?
VMs and groups of VMs can be recovered directly into Azure in minutes with just a few clicks. Individual files and folders can be recovered direct to production, with only the data required pulled from the storage account. The files are compressed on the fly to minimize restore time and cost.

What operating systems can ZVR protect and recover?
ZVR supports protecting and recovering the VMs that are supported by Microsoft Azure. If Azure supports the OS then ZVR supports it too. Windows 2003 VMs can also be recovered, contact Zerto support for more information.

What is the cost of replicating to Azure?
After purchasing ZVR licensing, per VM, the total cost can be calculated by the running cost of the ZCA and storage account usage for the replica VM data. No recovery VMs are created until needed making the solution extremely cost effective, typically 70% cheaper than DIY on-premise.

What are the default limits in Azure I need to configure?
Each Azure region has default settings that need to be increased to enable recovery of VMs at scale. These are altered by raising a support ticket in your Azure account. It is recommended to increase "VMs per Subscription", "VM Cores per Subscription", "VM Cores per Instance Size" which are all 20 by default.

How many recovery VMs are supported per ZCA?
Each ZCA is sized to protect and recover up to 200 VMs and/or 90MB/sec of total protected VM writes during continuous replication. There is also an Azure maximum of 500TB per storage account. Additional ZCAs can be deployed and paired with the same ZVM to scale-out the replication to many hundreds or thousands of VMs.

What is the maximum disk size supported?
Currently there is a limitation of 1TB disks due to the maximum page blob disk size limitation in Azure. Microsoft are planning to increase this to 8TB in Q2 2017 at which point ZVR will support larger disks. As an interim solution, it is possible to use multiple 1TB disks and Windows Storage Spaces or Storage Pools with virtual disks to present the disks as a single volume.

What type of storage can I replicate to?
ZVR 5.0 supports standard storage accounts only and therefore the recovered VMs type are always HDD and not SSD. The recovered VMs will still use the local SSD as a temporary scratch disk. Premium storage may be an option in a future release of ZVR.

Does Zerto support recovering UEFI & Gen 2 VMs?
VMs installed with UEFI rather than BIOS and Gen 2 VMs in Hyper-V environments are not supported by ZVR 5.0 due to Microsoft Azure not supporting either. This may change in the future.

About Zerto

Businesses need to be available to their customers, 24/7/365. Zerto provides Resilience for Evolving IT™ by ensuring enterprises and their customers always have access to business-critical applications without any IT interruption, downtime or delay. Zerto's award-winning Cloud Continuity Platform is the simplest, most reliable BC/DR software solution built to protect applications on any virtualized IT environment — be it public, private or hybrid cloud. Zerto's proactive approach to recovery gives companies the confidence they need to withstand any disaster, easily incorporate new technology, and quickly adapt to accommodate evolving IT and business priorities. **www.zerto.com**

04215