ZNETLIVE®

THE HOSTING ARCHITECT

SINCE 2001

Disaster Recovery Solution Architecture

ZNETLIVE®

THE HOSTING ARCHITECT

SINCE 2001

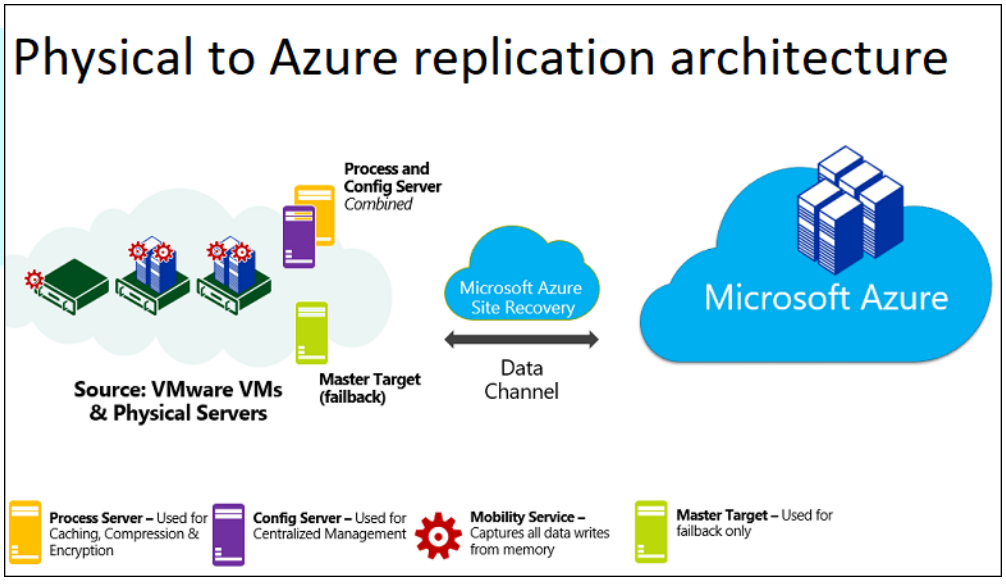
Table of Contents

Physical Server to Azure Replication Architecture

The architecture and processes used when you replicate, fail over, and recover physical Windows and Linux servers between an on-premises site and Azure, using the Azure Site Recovery service.

Architectural components

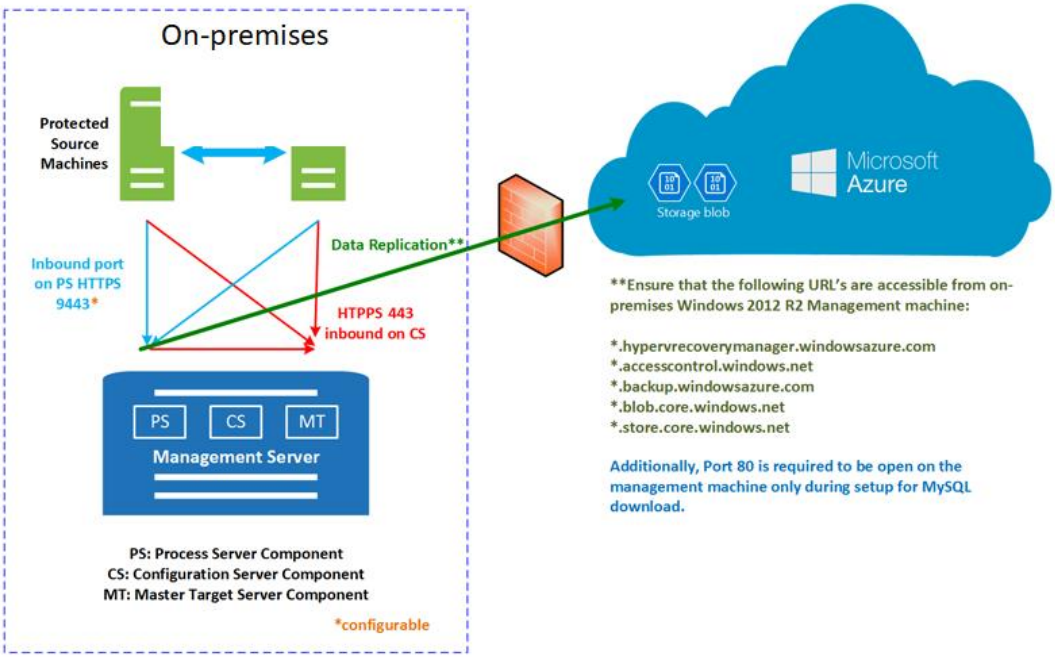
Component	Services	Requirement
Azure	Azure Storage Account Azure Virtual Network	An Azure subscription, Azure storage account, and Azure network.
Configuration server	The configuration server coordinates communications between on-premises and Azure and manages data replication.	A single on-premises physical machine or VMware VM is deployed to run all the on-premises Site Recovery components. The VM runs the configuration server, process server, and master target server.
Process server	Acts as a replication gateway. Receives replication data, optimizes it with caching, compression, and encryption, and sends it to Azure storage.	Installed by default together with the configuration server.
Master target server	Handles replication data during failback from Azure.	Installed by default together with the configuration server
Replicated servers	We recommend you allow automatic installation from the process server.	The Mobility service is installed on each server you replicate.



Prerequisites for Deploying the On-Premises Configuration Server Machine.

Component	Requirement
CPU Cores	8
RAM	16 GB
Number of disks	3, including the OS disk, process server cache disk, and retention drive for failback
Disk free space (process server cache)	600 GB
Disk free space (retention disk)	600 GB
Operating system	Windows Server 2012 R2 & Windows Server 2016
VMware vSphere PowerCLI version	PowerCLI 6.0
Windows Server roles	**Don't enable these roles:** Active Directory Domain Services; Internet Information Services; Hyper-V
Group policies	**Don't enable these group policies:** Prevent access to the command prompt; Prevent access to registry editing tools; Trust logic for file attachments; Turn on Script Execution
IIS	No pre-existing default website; Enable Anonymous Authentication ; Enable FastCGI setting; No pre-existing website/application listening on port 443
NIC type	VMXNET3 (when deployed as a VMware VM)
IP address type	Static
Internet access	The server needs access to these URLs: - *.accesscontrol.windows.net - *.backup.windowsazure.com - *.store.core.windows.net - *.blob.core.windows.net - *.hypervrecoverymanager.windowsazure.com - https://management.azure.com - *.services.visualstudio.com - https://dev.mysql.com/get/Downloads/MySQLInstaller/mysql-installer-community-5.7.20.0.msi (not required for Scale-out Process Servers) - time.nist.gov - time.windows.com
Ports	443 (Control channel orchestration) 9443 (Data transport)

Physical to Azure Replication Process



1. You set up the deployment, including on-premises and Azure components. In the Recovery Services vault, you specify the replication source and target, set up the configuration server, create a replication policy, and enable replication.
2. Machines replicate in accordance with the replication policy, and an initial copy of the server data is replicated to Azure storage.
3. After initial replication finishes, replication of delta changes to Azure begins. Tracked changes for a machine are held in a. hrl file.
    - Machines communicate with the configuration server on port HTTPS 443 inbound, for replication management.
    - Machines send replication data to the process server on port HTTPS 9443 inbound (can be modified).
    - The configuration server orchestrates replication management with Azure over port HTTPS 443 outbound.
    - The process server receives data from source machines, optimizes and encrypts it, and sends it to Azure storage over port 443 outbound.
    - If you enable multi-VM consistency, machines in the replication group communicate with each other over port 20004. Multi-VM is used if you group multiple machines into replication groups that share crash-consistent and app-consistent recovery points when they fail over. This is useful if machines are running the same workload and need to be consistent.

4. Traffic is replicated to Azure storage public endpoints, over the internet. Alternately, you can use Azure ExpressRoute public peering. Replicating traffic over a site-to-site VPN from an on-premises site to Azure isn't supported.

ZNetLive Support Services

Creating support ticket at ZNetLive - Support ticket allows users to report problems or ask for help/action on certain issues to experience seamless services.

- It is a system of records which helps you in keeping track of your issue from your member panel at any given time. As details and responses related to the issue are recorded in the ticket system, you do not need to repeat your problem or explain it repeatedly to different customer support personnel. Request is automatically allocated to the relevant department which ensures speedy resolution of the issues.

- Ticket system is easy to access as you can raise ticket directly using your registered mail id as well as from within your support panel anytime, as per your convenience.

- Since it is registered on the system, you are always well informed throughout the process.

- The entire process of ticket raising at ZNetLive is client friendly and easy to use.

- It gives visibility and clarity to your issue as you can include screen shots or multiple attachments with ticket to provide a more apparent description of the issue.

SERVICE LEVEL AGREEMENT

ZNetLive guarantees 99.9% availability of its monitoring services and infrastructure for Managed Windows service along with the commitment to maintain services in proper operational condition.

However, this assurance excludes infrastructure components that are not in High Availability deployment and unavailability of infrastructure due to hardware/software issues related to OEM.

Severity 1 (S1) -> System down impacting customer significantly

Severity 2 (S2) -> System functioning despite degraded performance

Severity 3 (S3) -> Error not impacting the end customer

We adhere to the service response time commitments as mentioned in the table below.

Severity	Log Time	Respond Time	Target time to update customer
S1	20 minutes	15 minutes	Every 1 hour
S2	40 minutes	30minutes	Every 4 hours
S3	60 minutes	60 minutes	Every 8 hours
Change Request	30 minutes	2 hours	4hrs or up on completion of the CR

We will keep you updated throughout the entire troubleshooting process, in-case of Severity or if there is any request regarding it. You will also receive alerts and notifications via mail, by default. If customers wish to get details, they can login to ZNetLive Member panel.

About ZNetLive

ZNetLive provides managed services to large enterprises and SMBs on latest technologies and enterprise grade hardware with value added benefits. ZNetLive specializes in infrastructure analysis to provide dynamic managed solutions tailored to specific industry processes.

ZNetLive, owned by ZNet Technologies Pvt. Ltd., was founded in 2001 and has been providing managed services to customers in over 141+ countries worldwide.

In addition to industry's best accreditations such as the Host Review Readers' Choice Award; The Deloitte Technology Fast 500 Asia and Fast 50 India Awards for 2010 & 2011; ISO 27001 and D&B certifications, ZNetLive has several Microsoft certifications.

For more information, please visit: https://www.znetLive.com

Get in touch with us: msp@ZNetLive.com

India and from other countries: (91) 141 4070666

India Toll Free: 1-800-102-9638