10TH MAGNITUDE

Azure Site Recovery (ASR) Planning Guide

10th Magnitude, LLC
20 North Wacker Drive #530
Chicago, IL 60606

TABLE OF CONTENTS

SUMMARY

This document is intended to serve as a high-level guide for planning deployment of Azure Site Recovery (ASR) components both on-prem and in the cloud for the purpose of migration. The information and checklists in this document are not exhaustive, they only contain common scenario information. We strongly urge you to explore the following ASR documentation.

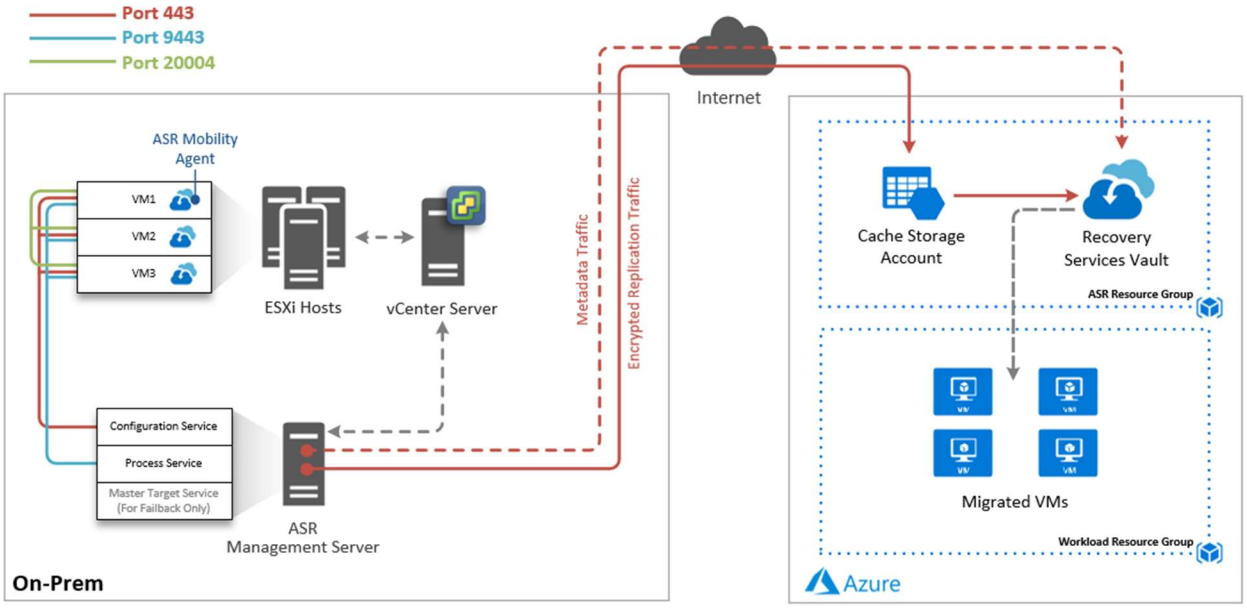
General ASR documentation and support matrix:
https://docs.microsoft.com/en-us/azure/site-recovery/
https://docs.microsoft.com/en-us/azure/site-recovery/vmware-physical-azure-support-matrix
https://docs.microsoft.com/en-us/azure/site-recovery/hyper-v-azure-support-matrix

ASR supported workloads:
https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-workload

ASR capacity planning guide:
https://docs.microsoft.com/en-us/azure/cloud-solution-provider/migration/on-premises-to-azure-csp/asr-capacity-planning

ASR setup guides:
https://docs.microsoft.com/en-us/azure/cloud-solution-provider/migration/on-premises-to-azure-csp/asr-setup-guide

VMWARE ASR ARCHITECTURE OVERVIEW



In most environments, the ASR Components are typically hosted on a single management server in the source environment. A preconfigured virtual appliance is available for quick deployment. The process server can be scaled out to allow for additional concurrent migration capacity.

Core ASR Components

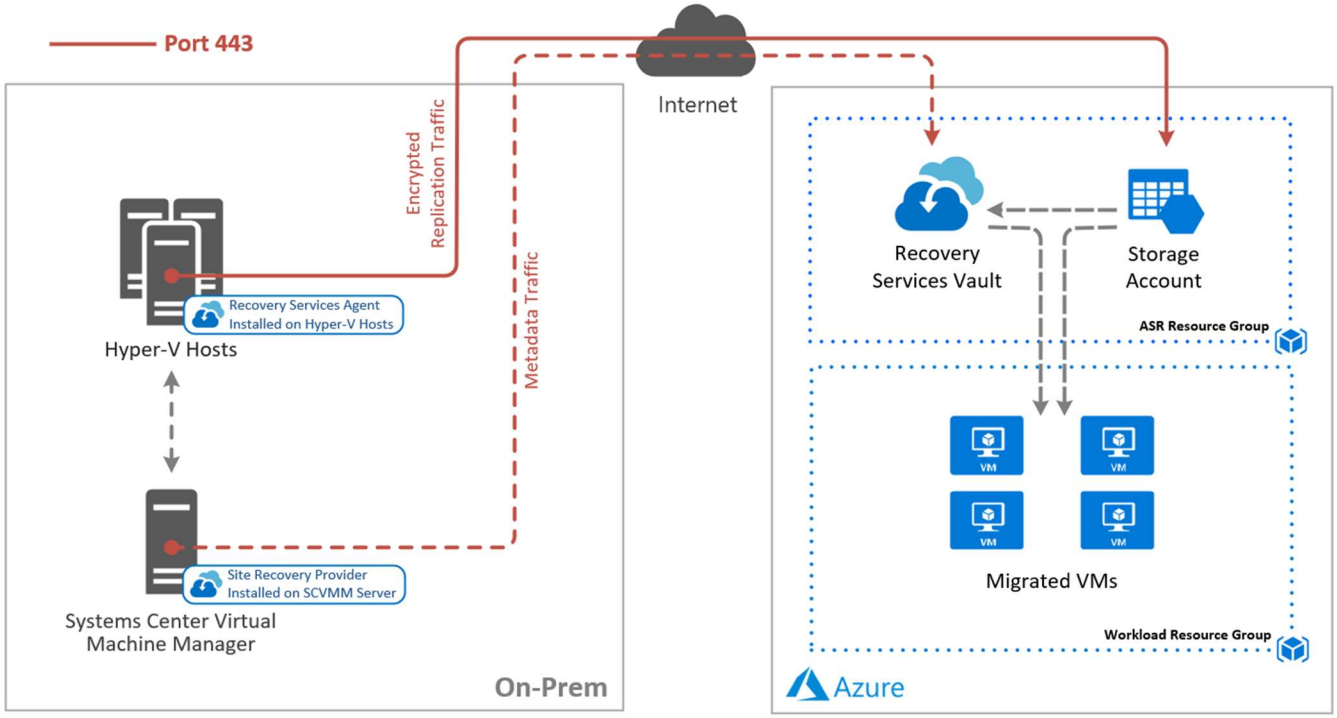
Configuration Server – Used for centralized migration management.
Process Server – Used for caching, compression, and encryption. *The process server can also be scaled out to allow for additional replication capacity per ASR instance.*
Master Target Server – Used only during failback to route replication data to the on-prem configuration and process service. This component is not needed for a migration only project.
Mobility Agent – Light-weight agent installed on the source machines that sends the configuration and replication data to the configuration and process services.
Recovery Services Vault – The Azure cloud target storage entity that houses the source replication data to be used to create the new Azure VMs.
Cache Storage Account – An Azure storage account used to cache incoming ASR replication data before being written to the Recovery Services Vault.

Network Communication

HTTPS Port 443 – Used for replication management from the mobility agent on the source VMs to the configuration server. Also used by the configuration and process servers to communicate outbound to Azure to facilitate replication.
HTTPS Port 9443 – Used by the mobility agent on the VMs to send replication data to the process server.
Port 20004 – Used for communicate between VMs to facilitate application consistency.

This communication must be allowed on the network for successful operation of ASR components and replication.

HYPER-V ASR ARCHITECTURE OVERVIEW



Core ASR Components

Site Recovery Provider – Software installed on the Systems Center Virtualization Manger server. The provider connects to Azure Site Recovery and sends VM metadata as well orchestrates migration with the Hyper-V hosts and Azure.
Site Recovery Agent – Software installed on each Hyper-V host. The agent communicates with the Hyper-V service and sends replicated data to Azure storage.
Recovery Services Vault – The Azure cloud target storage entity that houses the source replication metadata to be used to create the new Azure VMs.
Target Storage Account – An Azure storage account used to store ASR replicated disk data. Azure virtual machines are created using the replicated virtual disk data in the storage account, or if configured, the data is used to create new managed disks when the Azure VMs are created during failover.

Network Communication

HTTPS Port 443 – Used for replication management from the Site Recovery Proivder on the SCVMM server Azure Site Recovery. Also used by the Hyper-V hosts to communicate outbound to Azure storage to replicate disk data.

ASR PREREQUISITES

The following table outlines common prerequisites and considerations when deploying Azure Site Recovery and enabling replication of on-prem machines to the Azure cloud. We recommend in addition to reviewing this guide, also reviewing the Microsoft documentation specific to your migration goals.

Component	Requirement
Azure	☐ Microsoft Azure account ☐ Grant 10M access to the appropriate subscriptions ☐ A resource group for ASR resources – 10M will configure. ☐ A storage account in the target region(s) to be used for the ASR cache – 10M will configure ☐ A Log Analytics Workspace to be used to collect ASR logs. – 10M will configure ☐ A virtual network in the target region(s) to test failover – 10M will configure ☐ Resource groups and virtual networks to land the migrated resources – 10M will configure ☐ Optionally an Automation Account to create detailed failover runbooks and automation tasks to be performed during failover.
Failback from Azure	Note: This is usually not applicable in a migration scenario. ☐ A VPN or ExpressRoute connection from the Azure network to the on-prem site. ☐ If you only have a S2S VPN connection back to the on-prem site, a temporary process server should be deployed in Azure. This can be created when you're ready to fail back and can be deleted after failback Is complete. This is not required if you have an Azure ExpressRoute connection. A list of all requirements can be found at https://docs.microsoft.com/en-us/azure/site-recovery/vmware-azure-reprotect##before-you-begin.
VMware vSphere	☐ Deploy vCenter Server to manage your ESXi hosts (if not existing). ☐ Deploy the ASR Process Server(s) in the same physical location and network as your vCenter Server or ESXi hosts. ☐ Configure a service account to use for automatic discovery. This account should have a non-expiring password and at least read-only rights on the vCenter server. ☐ Grant the automatic discovery service account local administrator rights on the servers to be protected. This will be used by ASR to push install the mobility agent on the source machines. **Optionally, an additional service account can be created and configured for this purpose.** Supprted versions of VMware components can be found on the Microsoft VMware/Physical to Azure Support Matrix page.

Component	Requirement
Hyper-V	☐ Deploy Systems Center Virtual Machine Manager (SCVMM) to centrally manage your Hyper-V hosts (if not existing). ☐ Systems Center Virtual Machine Manager (SCVMM) and the Hyper-V hosts must have internet access over port 443 to Azure public endpoints. ☐ You must install the Azure Site Recovery provider on the SCVMM server and the Azure Recovery Services Agent on the Hyper-V hosts and register them to a Recovery Services Vault in each target Azure region. ☐ The virtual machines targeted for migration must be added to a cloud in SCVMM that is configured to sync with Azure Site Recovery.
ASR Configuration Server	In order to configure the on-prem ASR components, the following is required: ☐ A virtual machine to host the ASR Component Services – Process Server, Configuration Server, Master Target Server. (Can be physical, but VM is preferred) The server should have the following configuration: • Windows Server 2012 R2 or later • If using a VM, it should use a VMXNET3 network adapter • The server should have a static IP address • The server should not be a domain controller • The host name of the server should contain 15 or less characters • The Operating System should be in English only • vSphere PowerCLI 6.0 or later should be installed on the server • UAC should be disabled • Print and File services and WMI should be allowed through the Windows Firewall, regardless of if the firewall is enabled or not. ☐ The Configuration Server will require following network communication to be allowed: • Temporary outbound access on HTTP port 80 during the setup of the ASR components to download MySQL • Ongoing outbound access on HTTPS 443 for replication management • Ongoing outbound access on HTTPS 9443 for replication traffic (this port can be changed) • Allow IP address ranges for the Azure region of your resources. You need to allow the Azure Datacenter IP Ranges, and the HTTPS 443 protocol. • The server will require access to the following URLs: ○ *.hypervrecoverymanager.windowsazure.com ○ *.accesscontrol.windows.net ○ *.backup.windowsazure.com ○ *.blob.core.windows.net ○ *.store.core.windows.net ○ http://cdn.mysql.com/archives/mysql-5.5/mysql-5.5.37-win32.msi Note: Depending on number of migrating servers and churn rate, additional servers may be required to scale the deployment.

Component	Requirement
ASR Configuration Server Capacity Planning	The following should be considered: ☐ Maximum daily change rate - A protected machine can only use one process server and a single process server can handle a daily change rate of up to 2 TB. As a result, 2 TB is the maximum daily data change rate supported for a protected machine. ☐ The configuration server should be able to handle the daily change rate capacity across all workloads running on protected machines and needs sufficient bandwidth to continuously replicate data to Azure storage. As a best practice, we recommend the configuration server be located on the same network and LAN segment as the protected machines. In the event this is not possible, the configuration server can be located on a different VLAN but all protected servers should have L3 network visibility.

All On-Prem Replicated VMs	☐ The following common requirements should be met for on-prem virtual machines that are to be replicated to Azure:
	
	• VMware Tools should be installed and running on VMware machines
	• The OS disks should not exceed 2TB for VMware and 300GB for Hyper-V
	• Individual data disks should not exceed 8TB in size when replicating to managed disks (recommended for VMware and physical machines, not supported for Hyper-V), and 4TB when replicating to a storage account (Hyper-V).
	• Minimum of 2GB available disk space for component installation on VMware and physical machines
	• If application consistent snapshots are required across VMs, port 20004 should be opened on the VM's local Windows Firewall (VMware or physical machines only)
	• Machine names should contain between 1 and 63 characters (letters, numbers, and hyphens). The name must start with a letter or number and end with a letter or number. After you've enabled replication for a machine, you can modify the Azure name.
	• Note: If protected virtual machines have an iSCSI disk, then Site Recovery converts the protected VM iSCSI disk into a VHD file when the VM fails over to Azure. If the iSCSI target can be reached by the Azure VM, then it will connect to it and essentially see two disks – the VHD disk on the Azure VM, and the source iSCSI disk. In this case, you'll need to disconnect the iSCSI target that appears on the Azure VM.
	• Note: If the source VM has NIC teaming, it will be converted to a single NIC after failover to Azure.
	• Common Limitations:
	  ○ Protection of VMs with encrypted disks is not supported. The VM must be decrypted first.
	  ○ Shared disk guest configurations are not supported
	
	For a full list of requirements and limitations, please visit the Azure VM Requirements page. For a full list of supported Operating Systems, please visit the Supported Operating Systems page.

Component	Requirement
Windows Protected VMs	☐ The following common requirements should be met for on-prem Windows virtual machines that are to be replicated to Azure: • The VM must be running a 64-bit operating system, Windows Server 2008 R2 or newer. • The Operating System should be installed on the C:\ drive. The OS disk should be a Windows basic disk and NOT dynamic. Data disk(s) can be dynamic. • Site Recovery supports VMs with an RDM disk. During failback, Site Recovery reuses the RDM disk if the original source VM and RDM disk is available. If they aren't available, during failback Site Recovery creates a new VMDK file for each disk. • By default all the disks on a machine are replicated. To exclude a disk from replication, the Mobility service must be installed manually on the machine before you enable replication. For a full list of requirements and limitations, please visit the Azure VM Requirements page. For a full list of supported Operating Systems, please visit the Supported Operating Systems page.
Linux Protected VMs	☐ The following common requirements should be met for on-prem Linux virtual machines that are to be replicated to Azure: • /etc/hosts files on protected machines should contain entries that map the local host name to IP addresses associated with all network adapters • If you want to connect to an Azure virtual machine running Linux after failover using a Secure Shell client (ssh), ensure that the Secure Shell service on the protected machine is set to start automatically on system boot, and that firewall rules allow an ssh connection to it. • The host name, mount points, device names, and Linux system paths and file names (eg /etc/; /usr) should be in English only. • Protection can only be enabled for Linux machines with the following storage: File system (EXT3, ETX4, ReiserFS, XFS); Multipath software-Device Mapper (multipath)); Volume manager: (LVM2). Physical servers with HP CCISS controller storage are not supported. The ReiserFS filesystem is supported only on SUSE Linux Enterprise Server 11 SP3. • Site Recovery supports VMs with an RDM disk. During failback for Linux, Site Recovery doesn't reuse the RDM disk. Instead it creates a new VMDK file for each corresponding RDM disk. • Ensure that you set the disk.enableUUID=true setting in the configuration parameters of the VM in VMware. Create the entry if it doesn't exist. It's needed to provide a consistent UUID to the VMDK so that it mounts correctly. Adding this setting also ensures that only delta changes are transferred back to on-premises during failback, and not a full replication. For a full list of requirements and limitations, please visit the Azure VM Requirements page. For a full list of supported Operating Systems, please visit the Supported Operating Systems page.