White Paper

Azure Site Recovery with SAN Replication to NetApp Private Storage for Microsoft Azure

Solution Configuration and Testing

Pavel Lobanov, Vinith Menon, Nilesh Maheshwari, Mark Beaupre, NetApp
May 2015 | WP-7215

Abstract

This white paper describes disaster recovery solution configuration for highly available virtual machines hosted on Microsoft Hyper-V on Windows Server 2012 R2 using NetApp® Private Storage for Microsoft Azure, Azure Site Recovery, and System Center. It is intended to be a solution-planning guide, providing Hyper-V infrastructure administrators and planners with key architecture components that enable them to successfully design a disaster recovery solution with Azure Site Recovery and a NetApp Private Storage solution. This white paper discusses the use of NetApp SnapMirror® technology for Azure Site Recovery with SAN replication for both clustered and standalone Hyper-V Server configurations.

TABLE OF CONTENTS

LIST OF FIGURES

1 Introduction

Private and public cloud technologies have not only drastically changed the manner in which IT departments offer services, but of IT infrastructure itself. Business applications for different services are taking advantage of virtualization technologies, and servers running such applications are often virtualized. In most cases virtual machines (VMs) don't have hard dependencies on hardware on which they are running and can easily be moved from one physical server to another.

Microsoft has been developing technologies for the private cloud, based on Microsoft® Hyper-V® and System Center Virtual Machine Manager (VMM), and for the public cloud, using the Microsoft® Azure™ cloud platform. Microsoft recognized the need to connect multiple private and public clouds into a single IT infrastructure, and Azure Site Recovery (ASR) plays an important role in this area, specifically for hybrid cloud disaster recovery. It enables virtual machines to move not only between Hyper-V servers within a single site, but also between multiple sites, in both secondary private cloud data centers as well as Azure cloud data centers.

These technologies take disaster recovery to a new level. ASR enables disaster recovery in a simplified, orchestrated, and more automated manner. Rather than the lengthier backup and restore process, business applications and IT services can be restored within minutes, minimizing recovery point objectives (RPO) and recovery time objectives (RTO).

At the same time, many storage companies have been developing technologies to replicate data to remote sites for disaster recovery purposes. NetApp® SnapMirror® functionality is robust and provides enterprise with granular methods to protect and recover critical application data. Although Microsoft provides built-in VM replication capabilities utilizing Azure recovery services, a more robust data mirroring solution from NetApp can bring the entire solution to the next level. Azure site recovery with SAN replication to NetApp private storage (NPS) extends the functionality of ASR with SAN replication not only between private clouds, but also between private and Azure public clouds.

1.1 Purpose and Scope

This white paper delivers an overview of approaches for structuring a disaster recovery model for Microsoft Hyper-V Server using the comprehensive suite of NetApp hardware and software solutions.

The scenarios presented here are designed to achieve multiple levels of RPOs and RTOs.

1.2 Target Audience

This document assumes that the reader has read about, has formal training in, or has advanced working knowledge of Windows administration and VMM, as well as an understanding of NetApp storage concepts.

The target audience for this white paper includes the following roles:

- Information technology professionals
- Storage professionals
- Hyper-V infrastructure administrators responsible for virtualized-infrastructure management

To understand the methods and procedures covered in this white paper, NetApp assumes that the reader has working knowledge of the following Microsoft products and technologies:

- Microsoft Azure Site Recovery service
- Microsoft Azure Virtual Machine service
- Microsoft Azure ExpressRoute®
- Hyper-V component architecture
- Hyper-V infrastructure administration and management

- VMM infrastructure administration and management
- Service-level expertise of Hyper-V recovery options

NetApp assumes that the reader also has working knowledge of the following NetApp® products and solutions:

- Data ONTAP®
- SnapDrive® for Windows
- NetApp Data ONTAP SMI-S Agent (Storage Management Initiative Specification)
- NetApp SnapMirror
- NetApp Private Storage for Microsoft Azure | TR-4316 solution architecture and deployment guide

2 Disaster Recovery, High Availability, and Business Continuity Overview

Any business or organization can experience an incident that prevents it from continuing normal operations. This could be a flood or fire, or a serious computer malfunction or information security incident.

Disaster recovery requires an investment in a secondary storage site. When the primary production site is temporarily or permanently unusable, a effective disaster recovery plan allows the continued operation of virtual machines (VMs) hosted on Microsoft Hyper-V infrastructure at a secondary site, or on Microsoft Azure. With ASR SAN replication, the secondary site can be another private cloud data center, a service Agent–hosted private cloud, or Microsoft Azure with Azure ExpressRoute connectivity to NPS. A satisfactory DR solution balances three parameters—RPO, RTO, and manageability—and implementation requires careful preparation and planning.

Business continuity is the return of business processes to full capability following the disruption of service. Determining which applications are mission critical—essential to an organization's functioning in case of a disaster—is one of the first steps in high-availability (HA) and business-continuity planning. After the crucial components are identified, it is essential to identify the RPOs and RTOs for the identified crucial, mission-critical apportioning in terms of cost and acceptable risk. To appropriately architect a disaster recovery solution, one must be familiar with the following terms:

- **Availability.** Generally, availability refers to the degree to which a system, subsystem, service, or equipment is in an operable state and functional condition for a proportion of time.
- **Disaster recovery.** Disaster recovery (DR) is a process of regaining access to the data, hardware, and software necessary to resume critical business operations following a disaster. A robust disaster recovery plan consists of the IT, architecture, and processes to recover mission-critical data in a location other than the primary processing location.
- **High availability.** High availability (HA) is a system-design protocol and associated implementation that enables the operational continuity of a system, service, or equipment during a given measurement period. High-availability planning must include strategies to prevent single points of failure that could potentially disrupt the availability of mission-critical business operations.
- **Recovery point objective.** The RPO is the maximum amount of data loss, in terms of time, that an organization feels is acceptable.
- **Recovery time objective.** The RTO is the acceptable amount of downtime before the application is available to its users.
- **Manageability.** Manageability is a subjective measure of IT administrative resources that a particular DR solution requires.

- **Service-level agreement.** A service-level agreement (SLA) is a formal, negotiated agreement between a service Agent and a user (typically a customer) specifying the levels of availability, serviceability, performance, and operability of a system, service, or application.
- **Service levels.** To simplify business continuity and disaster recovery planning, it is common for an organization to implement service levels in which they associate a virtual machine (VM) or service to a class. These classes then define things such as backup intervals and data retention requirements. Classification of VM workloads, based on backup and availability characteristics, is based on three levels of service: gold, silver, and bronze, also called tier 1, tier 2, and tier 3 virtual machines. Mixing of these VM classes is required to maximize the efficiency of the underlying hardware because, at the gold level of service, for example, a set of small VMs quickly fills up a server. For more details on effectively designing your service levels, refer to NetApp for Microsoft Private Cloud or to FlexPod with Microsoft Private Cloud.

3 NetApp Solution Components

NetApp offers a rich set of functionality for data storage, management, and protection. In addition to storing data for different applications and work flows, NetApp software protects on-premises data with NetApp Snapshot® technologies and mirrors data to remote locations with NetApp SnapMirror replication. At the same time, NetApp integrates these technologies into Microsoft Windows Server® and Microsoft applications. SnapManager® products and NetApp Storage Management Initiative Specification (SMI-S) are integral for the seamless integration of storage and a Microsoft Private Cloud solution.

3.1 NetApp SnapMirror

NetApp SnapMirror technology provides fast, efficient data replication and disaster recovery for your critical data. It uses a single solution across all NetApp Data ONTAP storage arrays and protocols. SnapMirror technology works with any application—in both virtual and traditional environments—and in multiple configurations, including hybrid cloud. It is used to mirror data from one or more NetApp storage systems across a LAN or WAN. Efficiency of SnapMirror is based on NetApp deduplication and network compression capabilities and gives a leading edge to SnapMirror technology from the replication technology standpoint.

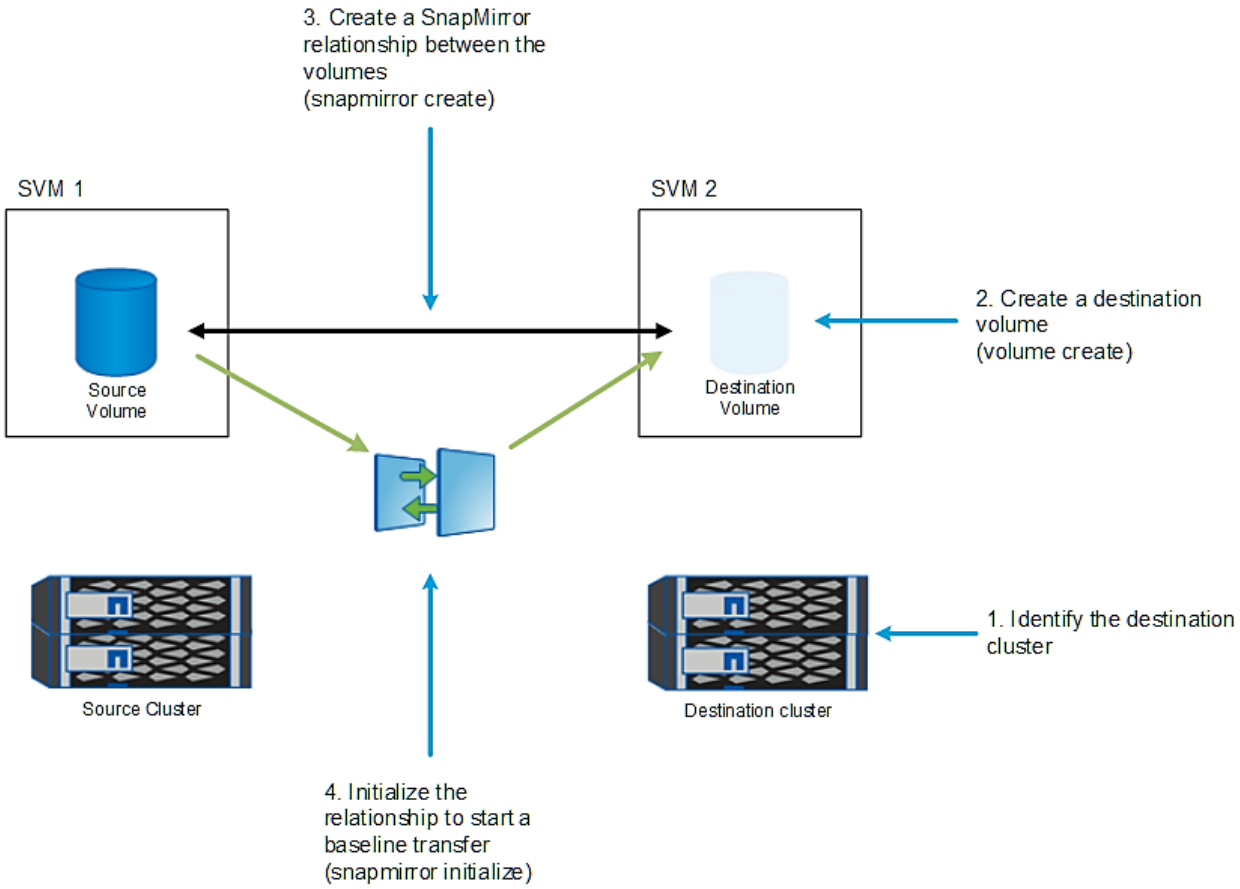
Cost-effective SnapMirror capabilities include:

- Network compression to reduce bandwidth utilization
- Accelerated data transfers to lower RPOs
- A single repository for both the active mirror and prior backup copies to enable selective failover points

With NetApp SnapMirror technology, a disaster recovery plan can be implemented to protect the entire data center. Using NetApp SnapMirror technology, volumes can be incrementally backed up to an off-site location. SnapMirror performs incremental, block-based replication as frequently as the required RPO. The block-level updates reduce bandwidth and time requirements, and data consistency is maintained at the DR site.

Figure 1 illustrates the procedure for initializing a SnapMirror relationship.

Figure 1) NetApp SnapMirror setup.



The first and most important step involves the creation of a one time, baseline transfer of the entire data set. This is required before incremental updates can be performed. This operation includes creating a Snapshot copy (baseline copy) of the source and transferring all of the data blocks referenced by it to the destination file system. After the initialization is complete, scheduled or manually triggered updates can occur. Each update transfers only the new and changed blocks from the source to the destination file system. This operation includes creating a Snapshot copy at the source volume, comparing it with the baseline copy, and transferring only the changed blocks to the destination volume. The new copy becomes the baseline copy for the next update.

Because the replication is periodic, SnapMirror is able to consolidate the changed blocks and conserve network bandwidth. The impact on write throughput and write latency is minimal.

NetApp FlexClone® technology can be leveraged to create instantaneous, space-efficient copies of replicated data. This allows you to perform DR testing, business intelligence, and development, and run tests without business interruptions.

3.2 NetApp SMI-S Agent

The NetApp Data ONTAP SMI-S 5.2 Agent allows administrators to manage and monitor NetApp FAS storage systems through open-standard protocols and classes defined by two organizations:

- Distributed Management Task Force (DMTF)
- Storage Networking Industry Association (SNIA)

VMM relies on SMI-S as the main integration component to plug storage into Microsoft-based private cloud systems. Storage can be provisioned by VMM in a unified manner, without the involvement of the storage administrator. VMM can also control and utilize storage mirroring functionality exposed by the SMI-S Agent.

Data ONTAP SMI-S 5.2 Agent can be installed on both Windows and Linux platforms. This SMI-S integration is designed to allow end-to-end discovery of logical and physical objects and the associations between them, add capacity to hosts and clusters, and rapidly provision VMs by using SAN and the SMB 3.0 protocol. The SMI-S Agent interface can also be used to accomplish simple tasks, such as using VMM to create and deploy new storage to individual hosts or clusters. The Data ONTAP SMI-S Agent 5.2 complies with SMI-S 1.5 and 1.6 specifications.

NetApp SMI-S Agent supports fully discovered models, meaning both primary and recovery storage and SVMs should be managed by each SMI-S Agent at primary and recovery sites.

The primary VMM server will manage primary storage and SVMs by using the primary site SMI-S Agent, and the recovery VMM server will manage recovery storage and SVMs through the recovery site SMI-S Agent.

At the recovery site, Azure is connected to collocated NPS through Azure ExpressRoute. The primary site is the data center located at the on-premises site.

3.3 NetApp Private Storage

The NetApp Private Storage for Microsoft Azure solution is a hybrid cloud architecture that allows enterprises to build an agile cloud infrastructure that combines the scalability and flexibility of the Microsoft Azure cloud with the control and performance of NetApp private storage.

NetApp storage is deployed at an Equinix collocation facility and is connected to Microsoft Azure compute resources through the Equinix Cloud Exchange and the Microsoft Azure ExpressRoute service.

The customer's data resides on its own NetApp storage in an Equinix Tier 1 data center that is directly connected to a Microsoft Azure data center. Direct connectivity of both data centers enables increased performance and security of applications running on Azure compute with data on NPS. In NetApp testing, it's been shown that Azure ExpressRoute connectivity between NetApp storage and Azure improves throughput by 36% compared to VPN over the Internet.

The NetApp Private Storage for Microsoft Azure solution deployed at Equinix can also be connected to on-premises data centers through a Multiprotocol Label Switching (MPLS) wide-area network (WAN) or through a point-to-point virtual private network (VPN). Customers can then use NetApp SnapMirror and SnapVault® storage replication to move data closer to Microsoft Azure compute resources.

Microsoft System Center, NetApp PowerShell Toolkit, and Azure PowerShell modules enable management and mobility of data between on-premises private cloud and private storage that's connected to Microsoft Azure through ExpressRoute.

3.4 NetApp Solution Advantages

Based on NetApp testing, the following key advantages can be achieved using this NetApp solution to create a DR plan for VMs hosted on Microsoft Hyper-V, to provide cross-site resiliency and high availability:

- Key NetApp technologies, such as thin provisioning, deduplication, and NetApp SnapMirror compression help reduce infrastructure costs.
- SnapMirror technology simplifies DR operations and allows customers to lower their RTO while achieving RPO, based on their SLA.
- Following an initial baseline transfer, NetApp SnapMirror decreases replication time across sites, and reduces network usage and storage costs, by replicating only changed blocks of data.

- NetApp SnapMirror can be deployed with no additional IT resources and supports frequent testing of your disaster recovery plan.

NetApp SnapMirror can be used to extend protection by replicating these consistent backups to a different storage system—located either within the same data center, at another data center located on the campus, or at a remote DR site.

In addition, the customer:

- Does not have to build or operate their own DR data center
- Does not have to purchase DR compute resources
- Can nondisruptively test DR scenarios by creating FlexClone volumes and Azure compute
- Can use clones of SnapMirror destination with Azure compute for development and testing

4 Microsoft Solution Components

This solution utilizes the Azure platform with Azure Site Recovery (ASR) with Azure recovery services, Azure SAN replication technologies, Azure Virtual Machine service, and ExpressRoute.

4.1 Microsoft Azure

Microsoft Azure is a public cloud compute platform and infrastructure for building, deploying, and managing applications and services through a global network of data centers managed by Microsoft.

The Azure cloud platform leverages a growing collection of integrated services—compute, storage, data, networking, and applications—that help you move faster, do more, and save money.

4.2 Microsoft ExpressRoute

Microsoft ExpressRoute provides a direct network connection between on-premises IT infrastructure and Azure data centers. ExpressRoute doesn't use public Internet, providing more secure and reliable connectivity with better performance and lower latencies. It brings the public cloud closer to the private cloud infrastructure, allowing business applications to span private and public clouds seamlessly.

ExpressRoute is a critical piece of this solution. Azure Recovery Services and NetApp SnapMirror utilize ExpressRoute to provide a more reliable replication channel between multiple locations.

4.3 Azure Site Recovery

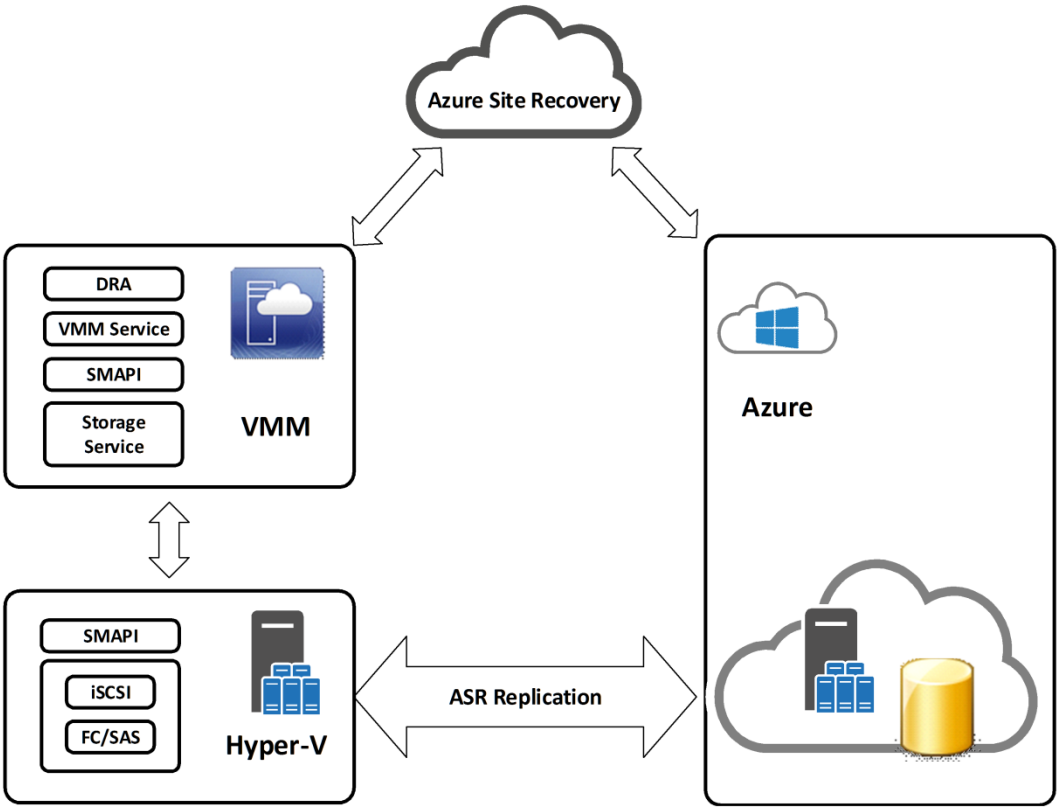
Azure Site Recovery (ASR) is a service run on Azure to protect customer environments by moving server virtual machines between on-premises and cloud-based infrastructures. ASR helps you to protect important applications by coordinating VM failover, utilizing storage replication between clouds. You can replicate to your own data center to a hosting service provider, or even to Azure to avoid the expense and complexity of building and managing your own secondary location.

Azure Recovery Services (ASR Replication)

Azure Recovery Services relies on a Hyper-V replica and is the primary replication technology used by ASR to replicate virtual machines between different locations. Azure Recovery Services enables asynchronous replication of Hyper-V VMs between two hosting servers. It is simple to configure and does not require either shared storage or any specific storage hardware. Any server workload that can be virtualized in Hyper-V can be replicated. Replication works over any ordinary IP-based network, and the replicated data can be encrypted during transmission. Azure Recovery Services works with standalone servers, failover clusters, or a mixture of both. The servers can be physically collocated or widely separated geographically. The physical servers do not need to be in the same domain or even joined to any domain at all.

Figure 2 illustrates the solution for Azure Site Recovery with Azure Recovery Services.

Figure 2) Azure Site Recovery with Azure Recovery Services.



Azure Site Recovery with SAN Replication

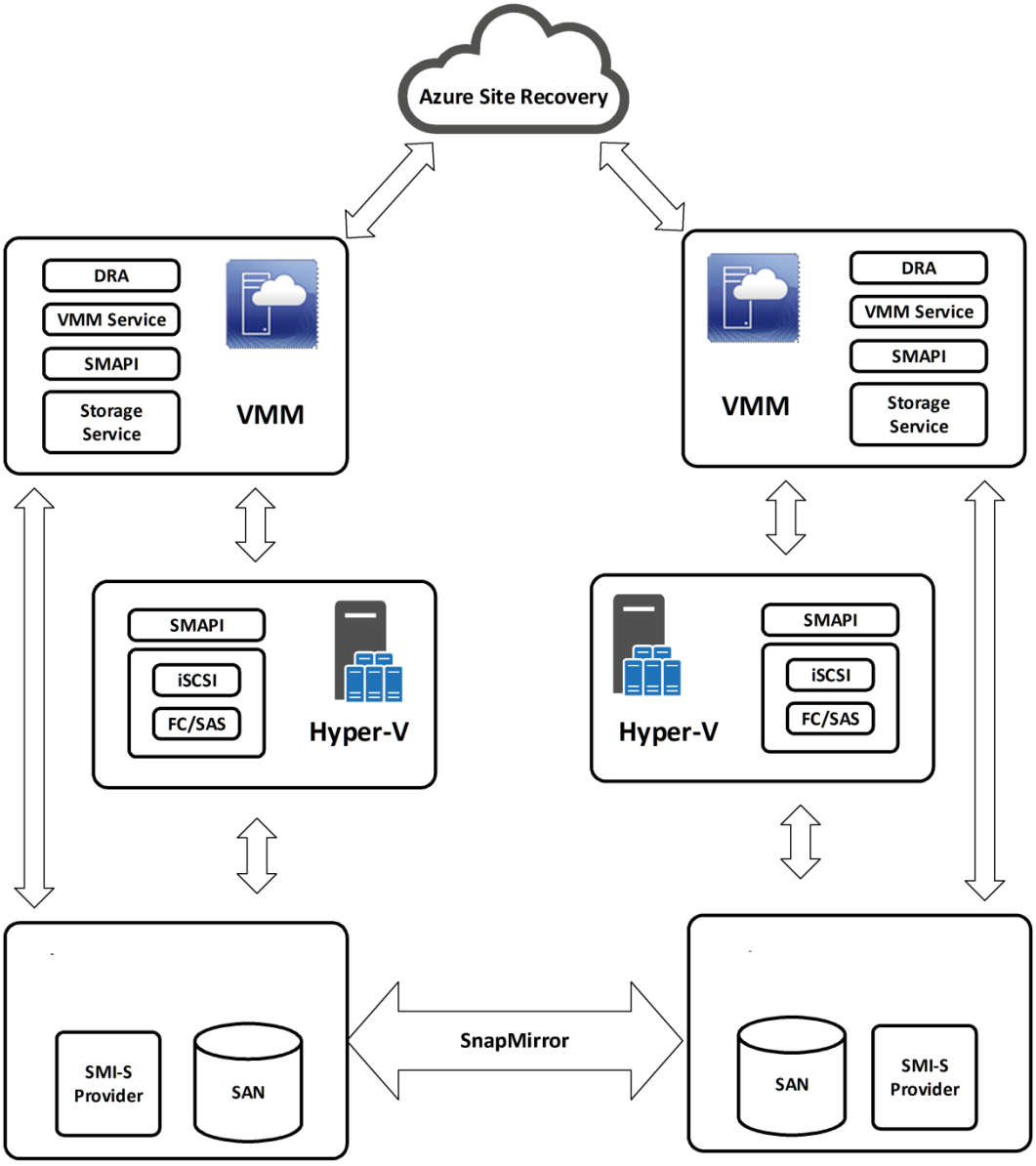
SAN replication technologies provided by storage vendors can extend functionality of Azure Site Recovery replication.

ASR enables you to leverage existing SAN infrastructure and use storage replication to protect your mission-critical applications.

SAN replication provides support for guest clusters and confirms replication consistency across different tiers of an application with synchronized replication. SAN replication also allows you to replicate guest-clustered VMs with iSCSI or FC storage.

Figure 3 illustrates ASR with SAN replication based on SnapMirror.

Figure 3) Azure Site Recovery with SnapMirror-based SAN replication.



5 Solution Configuration

This section describes best practices for deploying ASR with NetApp SAN. It includes information regarding ASR prerequisites, setting up your VMM infrastructure, PowerShell scripts for failover and recovery, and instructions for configuring settings in the ASR console.

A configuration of ASR with SAN replication to NetApp Private Storage combines both types of replication available through Azure Site Recovery:

- ASR replication to mirror OS drives of VMs between on-premises private cloud and Azure
- NetApp SnapMirror SAN replication using NetApp SMI-S Agent between the on-premises private cloud and NetApp Private Storage located at the Equinix data center and connected to collocated Microsoft Azure compute.

ASR acts as the main orchestration mechanism to coordinate the failover of the VM compute, OS, and data drives from one location to another.

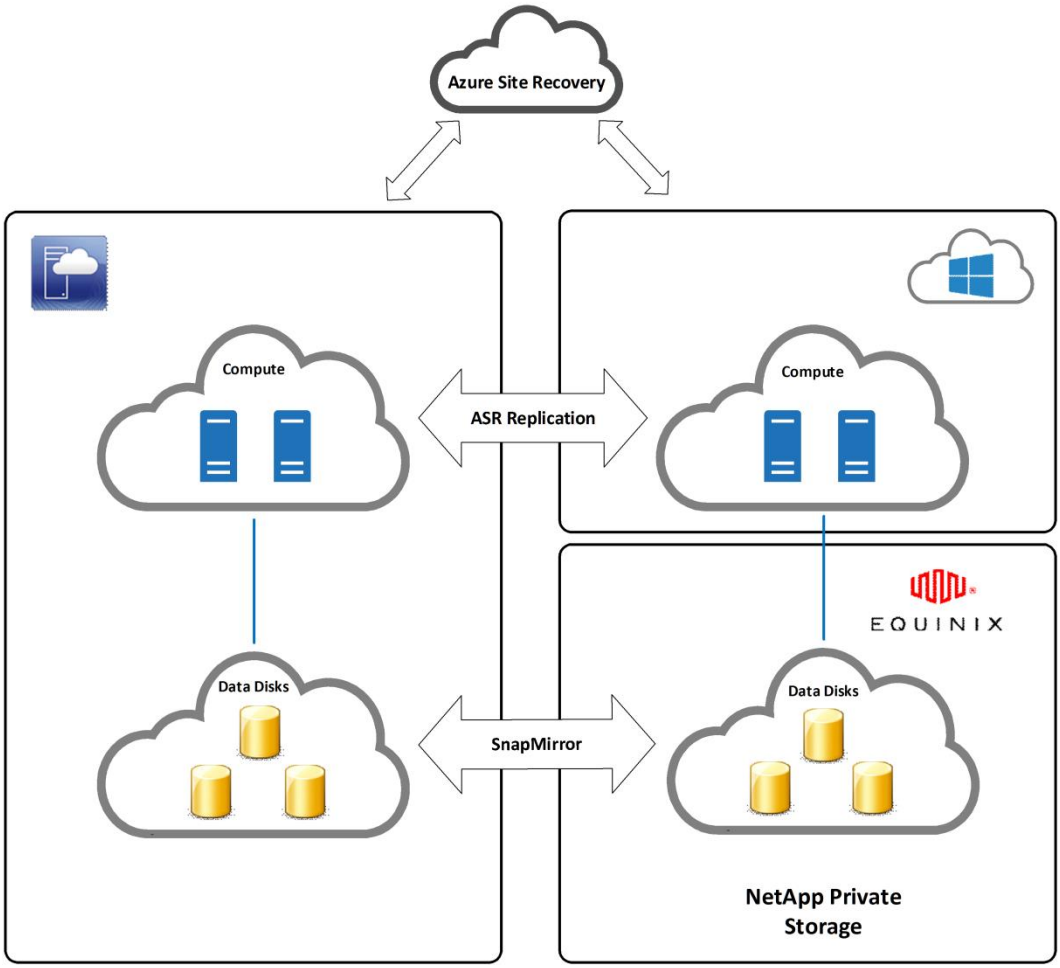
The following PowerShell scripts are used to make sure NetApp LUNs are properly unmasked and mapped to guest VMs:

- `MaskSourceLUNs.ps1`. This script masks iSCSI disks from guest VMs.
- `UnmaskTargetLUNs.ps1`. This script unmasks iSCSI disks to guest VMs.

Refer to the Appendixes A and B for the source of the scripts.

Figure 4 illustrates the solution for ASR with NetApp private storage.

Figure 4) ASR with NetApp private storage.



6 Solution Validation

6.1 Test Configuration

Overview

The Azure Site Recovery with SAN Replication to NetApp Private Storage for Microsoft Azure solution is validated for data replication and disaster recovery of a two-node SQL Server® guest VM cluster running on Hyper-V with VM storage backed up by clustered Data ONTAP.

ASR replication is used for replication of OS disk to Azure, while SnapMirror is used to replicate or protect data disks to NetApp Private Storage for Azure.

The end-to-end orchestration process is executed by ASR, which manages on-premises resources, including storage and compute, through VMM. Storage management uses Data ONTAP SMI-S Agent 5.2.

Software and Hardware Configuration

This solution uses the following software and hardware configuration:

- ASR with Azure Site Recovery Provider v3.5.700.0
- Private cloud management: System Center Virtual Machine Manager 2012 R2 with UR5 (KB3023914, KB3023195, and KB3035898)
- Storage management: Data ONTAP SMI-S Agent 5.2
- Compute: Fujitsu servers running Windows 2012 R2 Server with GUI
- Storage: NetApp FAS8080 cluster running Data ONTAP 8.2.3
- DR technologies: Azure Recovery Services for OS disk and SnapMirror for data disks

Environment Configuration

System Center Virtual Machine Manager Environment

- Primary VMM server: `vmm-01`
- Recovery VMM server: `vmm-02`

Hyper-V Compute Environment

- Primary Hyper-V cluster: `hv-cluster-01` (simulated on-premises compute)
- Recovery Hyper-V cluster: Azure

NetApp Storage Configuration Including NPS

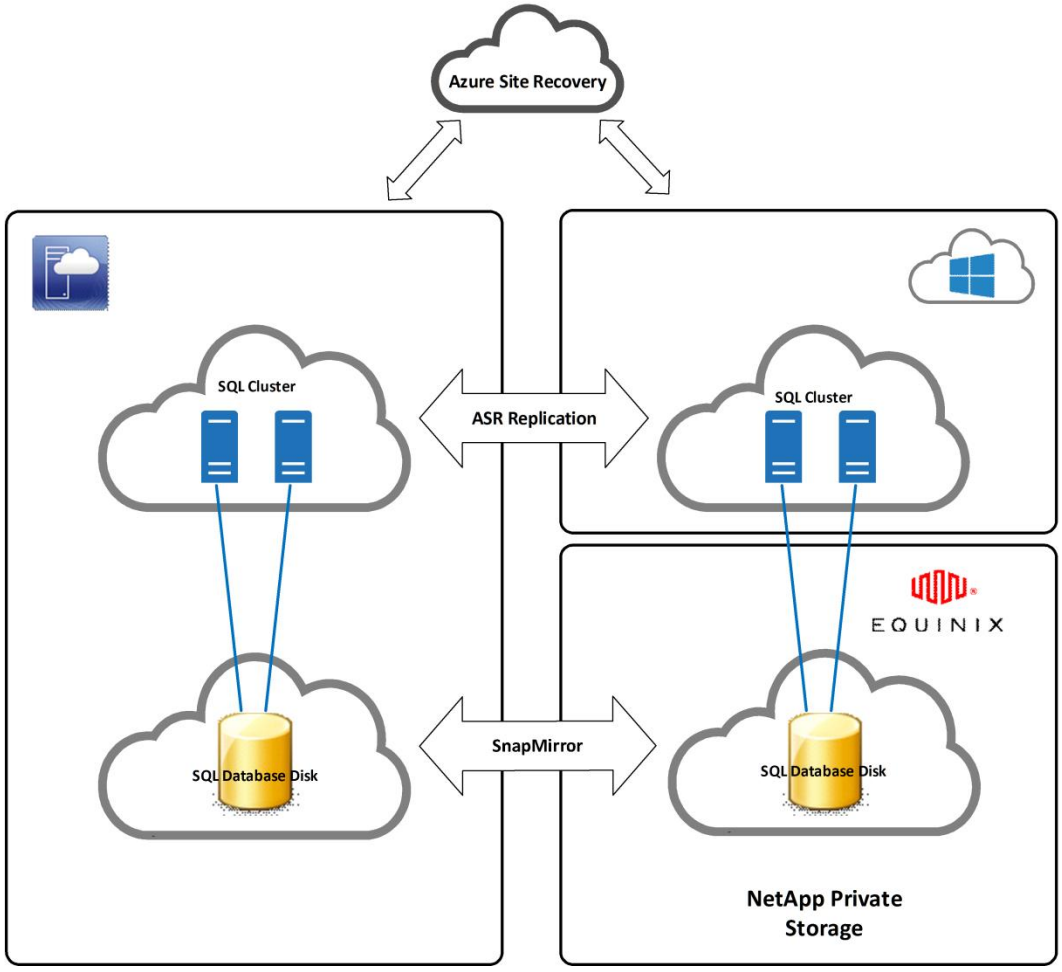
- Primary storage (SVM): `sv5-asr-01` (simulated on-premises storage)
- Recovery storage (SVM): `sv5-asr-02` (NPS at Equinix data center; single SMI-S agent managing primary and recovery SVM)
- Primary storage is managed by primary VMM Server `vmm-01`
- Recovery storage is managed by recovery VMM Server `vmm-02`

Primary and recovery VMM server registered to Azure Site Recovery through Azure Site Recovery Provider.

- Storage layout. NetApp FlexVol volumes exposed as VMM storage pool are as follows:
  - `quorum`. To host quorum disk
  - `sql_cluster_data`. To host shared disk for SQL Server cluster
- `VolumeToHostVMs`. To host CSV for VMs
- The following two pools form NPS to back storage for SQL Server cluster:
  - `quorum_dp`. To protect quorum from primary SVM
  - `sql_cluster_data_dp`. To protect `sql_cluster_data` from primary SVM

Figure 5 shows the ASR to NPS SAN workload used for replication testing.

Figure 5) SQL Server cluster workload in ASR to NPS SAN replication testing.



Additional Requirements

- Azure supports generation 1 and generation 2 VMs.
- Only highly available VMs can be protected to Azure.
- ExpressRoute is set up between NetApp Private Storage and the Azure network.
- NetApp Private Storage uses an ExpressRoute connection through an exchange provider (Equinix Cloud Exchange).
- Azure does not support first-class guest clusters. Therefore, internal load balancer (ILB) must be configured to direct cluster traffic for SQL Server service.
- Target Azure VMs should not be basic. Basic VMs don't support ILB. Also, Virtual Networks (Vnets) based on Affinity Group (AG) do not support ILB. Therefore, to test failover of guest cluster resources in Azure, ExpressRoute Vnet should be region scoped.

6.2 Test Scenarios

Enable Protection for Compute and Storage Clouds Between On Premises and Azure and NPS

To enable protection for compute and storage clouds between on-premises storage and Azure and NPS, we completed the following steps:

1. Install and configure SMI-S Agent. Integrate with the Microsoft System Center Manager environment (`vmm-01` and `vmm-02`). Bring the primary NetApp storage virtual machine (SVM) under the management of the primary VMM server (`vmm-01`) and the recovery SVM under the management of the recovery VMM server (`vmm-02`).
2. Using VMM, create a cluster shared volume (CSV) on a NetApp LUN using `vmm-01` and associate it with the Hyper-V host cluster at the primary site.
3. Create two highly available VMs `asr-test-vm-01` and `asr-test-vm-02` on the CSV share.
4. Using Failover Cluster Manager, create an in-guest cluster `asr-sql-cluster` with the previously created VMs.
5. Install and configure in-guest SQL Server 2012 Enterprise Edition `asr-sql-01` on both the VMs.
6. Create iSCSI session using iSCSI initiator on these VMs with the primary SVM (`sv5-asr-01`).
7. Create quorum and a shared disk on VMM pool `quorum` and `sql_cluster_data`, respectively, through VMM.
   - `quorum_lun`. This will be used as a witness disk for the in-guest cluster.
   - `sql_data_lun`. This will be used as storage for SQL Server DB.
8. Enable remote PowerShell on each guest VM, which will be used to run in-guest scripts to automate in-guest actions such as creating iSCSI session with SVM/target and bringing online the cluster resources.
9. Use the following two scripts for unmasking and masking LUNs during failover. Place them in primary and recovery VMM servers' library share.
   - `MaskSourceLUNs.ps1`. This script will mask iSCSI disks from guest SQL Server cluster VMs.
   - `UnmaskTargetLUNs.ps1`. This script will unmask iSCSI disks to guest SQL Server cluster VMs.
10. Create replication groups for pools `quorum` and `sql_cluster_data` with similar name as pools for consistency with guest cluster scripts and simplicity.
11. Create three VMM clouds:
    - `Primary_Compute`. Created on the primary VMM server. This is the compute cloud that holds the SQL Server guest cluster that will be protected to Azure.
    - `Primary_NAStorage`. Created on the primary VMM server. This is the SAN cloud and will hold the SAN replication groups (quorum, `sql_cluster_data`).
    - `Secondary_NPS`. Created on the recovery VMM server. This will be the recovery SAN cloud where `Primary_NAStorage` will fail over in NPS.
12. Assign the replication groups `quorum` and `sql_cluster_data` to VMM cloud `Primary_Compute`.
13. Log in to the ASR portal and execute a pool pairing between `quorum` to `quorum_dp` and `sql_cluster_data to sql_cluster_data_dp`.
14. Enable protection or pairing between `Primary_NAStorage` with `Secondary_NPS`.
15. For primary SAN, enable protection for the replication groups `quorum` and `sql_cluster_data`. This will establish and initialize the SnapMirror transfer through the NetApp SMI-S Agent.
16. Configure cloud protection for cloud `Primary_Compute` as follows:
    a. Before you enable protection, make sure to disable integration services component on virtual machines.
    b. Make sure cluster resources are online and you can move them between nodes.
    c. Power off both of the VMs. This is required because Azure Recovery Services performs an iSCSI check and will fail if any iSCSI disks are mounted on the VM. This is a workaround method published by Microsoft.
    d. Enable protection for each VM in ASR.

e. After protection is established, enable the Hyper-V integration services component.

Perform Compute and Storage Clouds Failover from On Premises to Azure and NPS Using VMM Scripts in Recovery Plan

To fail over compute and storage clouds from on-premises storage to Azure and NPS using VMM scripts in a recovery plan, we completed the following steps:

1. Create the following two recovery plans in ASR:
   - `RP-Compute`. This is the recovery plan for the compute cloud `Primary_Compute`. Include the SQL Server guest cluster VMs in this recovery plan.
   - `RP-NAStorage`. This is the recovery plan for the SAN cloud `Primary_NAStorage`. Include the NetApp RG (`quorum`, `sql_cluster_data`) to be failed over.
   - Insert script `MaskSourceLUNs.ps1` before failing over all the groups.
   - Insert script `UnmaskTargetLUNs.ps1` after failing over all the groups.
2. Verify that the SQL Server cluster is working correctly before failover to Azure by moving cluster resources between nodes of the cluster.
3. Execute `RP-Compute` recovery plan. This will fail over on-premises VMs to Azure.
4. Execute `RP-NAStorage` PowerShell script. This script will perform the following actions:
   a. Mask the cluster disks (`quorum_lun` and `sql_data_lun`) on primary site within `Primary_NAStorage`.
   b. Perform a SAN failover of replication groups to `Secondary_NPS`.
   c. Unmask the cluster disks on Azure IaaS VMs.
5. Log in to guest cluster SQL Server VMs and establish iSCSI connection to the recovery SVM.
6. Set up an internal load balancer (ILB) with endpoints to serve cluster traffic for SQL service. ILB is configured on the cloud service. Every failover creates a cloud service; therefore, ILB must be recreated. The following commands can be run from Azure Powershell to set up ILB for a guest cluster:

```
Add-AzureInternalLoadBalancer -InternalLoadBalancerName ILB_SQL_AO -SubnetName AzureVMs -
ServiceName RP-Compute-4b171504-7236-49dc-96cd-5067e1b4b641 -StaticVnetIPaddress 10.3.1.100

Get-AzureVM -ServiceName RP-Compute-aad5c81b-1088-4f71-b431-ac19fd4e7bce -Name asr-test-vm-01 |
Add-AzureEndpoint -Name "LisEUep" -LBSetName "ILBSet1" -Protocol tcp -LocalPort 1433 -PublicPort
1433 -ProbePort 59999 -ProbeProtocol tcp -ProbeIntervalInSeconds 10 –DirectServerReturn $true -
InternalLoadBalancerName ILB_SQL_AO | Update-AzureVM

Get-AzureVM -ServiceName RP-Compute-aad5c81b-1088-4f71-b431-ac19fd4e7bce -Name asr-test-vm-02 |
Add-AzureEndpoint -Name "LisEUep" -LBSetName "ILBSet1" -Protocol tcp -LocalPort 1433 -PublicPort
1433 -ProbePort 59999 -ProbeProtocol tcp -ProbeIntervalInSeconds 10 –DirectServerReturn $true -
InternalLoadBalancerName ILB_SQL_AO | Update-AzureVM
```

7. Log in to one of the failed-over guest VMs and change the IP of SQL service to match the IP of ILB (`10.3.1.100`). If the cluster disks (`quorumlun` and `sql_data_lun`) are offline in cluster manager, then reestablish the iSCSI session from each guest to the recovery target. Bring the SQL Server resource online and make sure other cluster resources are online. Test for success by moving SQL Server resource between the guests VMs. Core cluster resources cannot be failed over because we are using ILB for guest cluster traffic. Therefore, you will be able to access SQL Server only from the owner node.

Perform Failback of Compute and Storage Cloud from Azure/NPS to On Premises Storage

To fail back the compute and storage clouds from Azure and NPS to on-premises storage, we completed the following steps:

1. Perform `RP-Compute` for the following operations:
   - **Commit.** Prepares the VMs for failover. The VM state is checkpoint to failover.
   - **Planned failover.** Fails over VMs from Azure to `Primary_Compute` on the primary site. This will fail back the guest cluster to the on-premises site.
   - **Commit.** Prepares the VMs for reverse replication.
   - **Reverse replication.** Resyncs Hyper-V protection from `Primary_Compute` to Azure.
2. Perform `RP-NAStorage` for the following operations:
   - **Reverse replication.** Establishes the SnapMirror relationship from NPS to the on-premises site. Basically, it replicates replication groups from `Secondary_NPS` to `Primary_NAStorage`.
   - **Planned failover**. Fails back storage or breaks SnapMirror relationship between the NPS and on-premises site. Basically, it activates `Primary_NAStorage` to provide cluster disks (`quorum_lun` and `sql_data_lun`) to the guest cluster that was failed back from Azure to an on-premises site.
   - **Reverse replication**. Reestablishes/resyncs the SnapMirror relationship from the on-premises site to NPS. Basically, it reprotects replication groups from `Primary_NAStorage` to `Secondary_NPS`.
3. Log in to on-premises cluster VMs and reestablish iSCSI connection with primary SVM. Verify that cluster resources are online. Move cluster resources between nodes and confirm that the cluster is healthy.
4. Since we changed the IP of the SQL resource in Azure, it must be changed back to match the on-premises IP address (`192.168.1.81`). Verify that cluster resources are online. Move cluster resources between nodes and verify that everything works and the cluster is healthy.

7 Conclusion

Disasters affecting IT systems can happen. Physical hardware such as servers and network switches can fail without warning, bringing down critical IT infrastructure and severely affecting businesses. It's not only the vulnerability of system components that are exposed; bigger events could bring entire sites down.

Microsoft Hyper-V, as a building block of a virtualized infrastructure, supports an organization's mission-critical applications. In the event of a disaster in which mission-critical apps hosted on the hypervisor become unavailable, an organization's operational productivity can become crippled.

NetApp provides proven data-protection and disaster-recovery tools for Microsoft Hyper-V servers.

NetApp Private Storage for Microsoft Azure, along with Azure Site Recovery with SAN replication, provides a robust and cost-effective solution for simplified disaster recovery to protect and recover your VMs while meeting stringent RPOs and RTOs based on your business requirements.

Appendix A: PowerShell Scripts Used to Mask Source LUNs

- Source of the script and description can be downloaded from Microsoft TechNet at https://gallery.technet.microsoft.com/scriptcenter/Azure-Recovery-Recovery-b656835a

Appendix B: PowerShell Scripts Used to Unmask Target LUNs

- Source of the script and description can be downloaded from Microsoft TechNet at https://gallery.technet.microsoft.com/scriptcenter/Azure-Recovery-Recovery-27f37018

References

The following references were used in this paper:

- TR-4271: Best Practices and Implementation Guide for NetApp SMI-S Agent 5.2 http://www.netapp.com/us/media/tr-4271.pdf
- NetApp Unveils Support for Microsoft Azure SAN Replication with SMI-S and SnapMirror http://community.netapp.com/t5/Technology/NetApp-Unveils-Support-for-Microsoft-Azure-SAN-Replication-with-SMI-S-and/ba-p/94483
- Microsoft Azure Site Recovery SAN Replication with SMI-S 5.2 Deep Dive http://community.netapp.com/t5/Technology/Microsoft-Azure-Site-Recovery-SAN-Replication-with-SMI-S-5-2-Deep-Dive/ba-p/94575
- Leveraging SAN Replication for Enterprise Grade Disaster Recovery with Azure Site Recovery and System Center TechEd Europe 2014 Presentation http://video.ch9.ms/sessions/teched/eu/2014/CDP-B339.pptx
- TR-4316: NetApp Private Storage for Microsoft Azure Solution Architecture and Deployment Guide http://www.netapp.com/us/media/tr-4316.pdf

Acknowledgments

The authors would like to recognize the Microsoft team for working with and providing full support to NetApp:

- Abhishek Agrawal, Principal Program Manager
- Abhishek Hemrajani, Program Manager II
- Hector Linares, Principal Program Manager
- Krishan Kumar Attre, Principal Software Engineering Manager
- Madhu Jujare, Principal Software Engineering Manager
- Mohit Nagpal, Software Engineer II
- Vimalraj Thekkoot, Software Engineer II
- Gaurav Sinha, Senior Software Engineer
- Amit Virmani, Senior Software Engineer
- Jeff Li, Senior Software Engineer
- Siva Kotapati, Senior Software Engineer

Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.