INTRODUCTION TO AZURE SITE RECOVERY WITH SAN REPLICATION USING VMAX3 SNAPVX AND SRDF

EMC® VMAX3® Engineering White Paper

ABSTRACT
This white paper discusses the basic fundamentals of how to implement Microsoft’s Azure Site Recovery for SAN replication, using VMAX3 to perform site-to-site disaster recovery and protection of private clouds.

September, 2015
To learn more about how EMC products, services, and solutions can help solve your business and IT challenges, contact your local representative or authorized reseller, visit www.emc.com, or explore and compare products in the EMC Store.

Copyright © 2014 EMC Corporation. All Rights Reserved.

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

The information in this publication is provided "as is." EMC Corporation makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

EMC², EMC, and the EMC logo are registered trademarks or trademarks of EMC Corporation in the United States and other countries. All other trademarks used herein are the property of their respective owners.

For the most up-to-date listing of EMC product names, see EMC Corporation Trademarks on EMC.com.

Part Number H14528.1
# TABLE OF CONTENTS

## EXECUTIVE SUMMARY

- Audience: 6
- Terminology: 6

## PRODUCT OVERVIEW

- Azure Site Recovery Overview: 8
- VMAX3 Product Overview: 8

## EMC SMI-S PROVIDER FOR VMAX3 SETUP AND CONFIGURATION

- EMC SMI-S Provider for VMAX3 Configuration For System Center Virtual Machine Manager: 11
- EMC SMI-S Provider for VMAX3 Gatekeepers Considerations: 11
- EMC SMI-S Provider for VMAX3 Installation and Configuration: 13
- SRDF Consistency Groups And SCVMM Replication Groups: 14

## ASR SETUP AND CONFIGURATION

- Software Requirements: 15
- ASR High Level Configuration Steps: 16

## AZURE SITE RECOVERY USE CASES OVERVIEW

- Scale Limits for ASR Scenarios: 17
- Use Case 1: Create and Protect RGs And Resident VMs: 17
- Use Case 2: Planned Failover of RGs to Recovery Site and Reverse Role: 18
- Use Case 3: Unplanned Failover of RGs to Recovery Site and Reverse Role: 20
- Use Case 4: Failback to Primary Site: 20
- Use Case 5: Test Failover of RGs, for Non-Impact Production Site Testing: 21
- Use Case 6: Organize RGS and RESIDENT VMs in Flexible Recovery Plans: 21
- Use Case 7: Delete RGs and Disable Protection: 22

## APPENDIX I: SRDF GROUP CREATION AND MANAGEMENT

- Listing local and remote VMAX3 SRDF adapters: 23
- Creating dynamic SRDF groups: 23
- Listing the status of SRDF group: 23

## APPENDIX II: DETAILED SCVMM AND ASR SETUP

- SCVMM Configuration: 24
- ASR Configuration In Azure Portal: 37
Detailed ASR Operations Use Cases ................................................................. 52

APPENDIX III: SOLUTIONS ENABLER CLI EXAMPLES .............................. 59

APPENDIX IV: WINDOWS POWERSHELL EXAMPLES ................................ 63

APPENDIX V: MICROSOFT PRIVATE CLOUD STORAGE MANAGEMENT ON VMAX3 ............................................................... 65

Unisphere for VMAX3 ...................................................................................... 65
SCVMM with EMC SMI-S Provider for VMAX3 ............................................ 65
Solutions Enabler CLI .................................................................................... 66

REFERENCES .................................................................................................. 66
Executive Summary

Microsoft Azure Site Recovery (ASR) can help protect critical applications running in datacenters with a flexible recovery plan and low RTO/RPO. ASR’s powerful replication capabilities extend datacenters to Azure and enable disaster recovery, Dev testing, and migration of applications to Azure, and cloud bursting. ASR supports heterogenous datacenter environments including virtual machines running on VMware or Hyper-V and physical machines. In addition to DR to Azure, ASR also helps coordinate the replication and recovery of on-premises clouds running Windows Server Hyper-V across sites at scale for dozens or even hundreds of virtual machines. VMAX3™ offers Symmetrix® Remote Data Facility (SRDF®), which is a proven, industry leading, enterprise-wide, SAN-based data protection and disaster recovery solution. Synchronous SRDF protects critical application with zero data loss. Asynchronous SRDF protects local datacenters at very long distances with two to four site topologies. SRDF also integrates seamlessly with VMAX3 TimeFinder® SnapVX for local replication to allow creation of remote copies of the data for farther backups and repurposing as TEST/DEV. ASR with SAN replication integrates with VMAX3 SRDF and TimeFinder SnapVX to provide enterprise-class site-to-site disaster recovery for Windows Server Hyper-V environments. It does so by leveraging the SAN replication capabilities of VMAX3 SRDF and TimeFinder SnapVX. ASR for SAN replication is an automated, self-service, and continuous remote data protection solution that reduces complexity and improves confidence in a disaster recovery solution.

Advantages with Azure Site Recovery with SAN replication include:

- Automated protection of Windows Server VMs including shared disk guest clusters, providing an enterprise scalable replication solution.
- Leverages existing VMAX3 SAN infrastructure to protect mission-critical applications.
- Application consistency with low RTO and RPO for both synchronous and asynchronous VMAX3 replication.
- Applications that require multi-VM group consistency by leveraging native consistency group capabilities in VMAX3.
- Integration with SCVMM and standards-based EMC Storage Management Initiative Specification (SMI-S) for VMAX3.

ASR with SAN replication using VMAX3 delivers advanced capabilities for cloud protection, disaster recovery, and non-disruptive testing and failover of virtual machines. It manages planned and unplanned failover from primary data centers to target recovery sites. ASR uses VMAX3 array remote replication to protect Windows Server Hyper-V environments using SRDF/Synchronous (SRDF/S) and SRDF/Asynchronous (SRDF/A) modes of operation. When using SRDF with Azure Site Recovery, targeted set of VMs can be protected and the desired boot order maintained during failover and reverse replication using a write order that is consistency natively available with VMAX3 SRDF. ASR also enables creation of a test copy at the recovery site for DR testing, increasing the confidence and trust in the overall DR solution without disrupting ongoing remote replication. ASR can also leverage consistency replication groups in VMAX to replicate a group of VMs together and ensure Multi-VM replication for enterprise grade applications. Figure 1 is a diagrammatic representation of site-to-site disaster recovery using SAN replication. It shows EMC VMAX3 SRDF providing a scalable, simple, and end-to-end DR solution along with ASR.

Figure 1. Site to Site Disaster Recovery using SAN replication
This paper describes the components of ASR with SAN replication including VMAX3, SRDF, EMC SMI-S Provider for VMAX3 and SCVMM integration, and lists the steps needed to setup and register a Microsoft private cloud in Azure portal for DR orchestration. It also covers deployment considerations for scaling and grouping of Windows Server Hyper-V VMs for successful DR strategy. This paper also highlights several use cases supported by ASR with SAN replication and provides some troubleshooting guidance to ensure smooth deployment.

AUDIENCE
This white paper is intended for system administrators, storage administrators, and Microsoft Azure administrators who are responsible for implementing, managing, and maintaining their Private Cloud infrastructures on VMAX3 storage systems. It is intended for the teams that are responsible for DR implementation in environments utilizing VMAX storage and Windows Server Hyper-V virtualization. It is assumed that readers have familiarity with the EMC VMAX3 family of storage arrays, Microsoft Azure Site Recovery, and are interested in leveraging VMAX3 SRDF remote replication capabilities for enterprise level disaster recovery and protection of System Center Virtual Machine Manager (SCVMM) Cloud environments. This paper covers the required steps of configuring SMI-S Providers for SAN replication using SRDF and Azure site recovery. For an in-depth description of the configuration of the Azure Site Recovery portal for Recovery Plan VM automation for orchestrated disaster recovery, consult Microsoft’s online documentation.

Note: Support exists for both VMAX and VMAX3, though the rest of this whitepaper will refer to VMAX3 for simplicity. Hence VMAX3 arrays refer to both VMAX® and VMAX3™ throughout the document, unless explicitly called out.

TERMINOLOGY
The following table provides an explanation for important terms used in this paper.

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Site</td>
<td>The primary site, where the production VM workload is running. It is also referred to as protection site, production site, or R1 site in this document.</td>
</tr>
<tr>
<td>Target Site</td>
<td>The secondary site, where production data is mirrored to by using synchronous or asynchronous replication. It could be located in the same region as the production site or at a distant location. It is also referred to as recovery site, bunker site, remote site, or R2 site in this document.</td>
</tr>
<tr>
<td>Replication Group</td>
<td>Replication Group (RG) is SCVMM terminology used to describe a group of LUNs that need to be protected and replicated as a singular entity. See VMAX3 Consistency Group.</td>
</tr>
<tr>
<td>EMC SMI-S Provider for VMAX3</td>
<td>EMC VMAX3 storage arrays can be discovered in SCVMM using EMC SMI-S Provider for VMAX3. SMI-S supports the Storage Networking Industry Association (SNIA) Storage Management Initiative Specification (SMI-S), an American National Standards Institute (ANSI) standard for storage management.</td>
</tr>
<tr>
<td>SCVMM</td>
<td>System Center Virtual Machine Manager.</td>
</tr>
<tr>
<td>Azure Site Recovery (ASR)</td>
<td>Microsoft Azure Site Recovery (ASR) service contributes to a robust business continuity and disaster recovery (BCDR) solution that protects your on-premises physical servers and virtual machines by orchestrating and automating replication and failover to Azure, or to a secondary on-premises datacenter. Azure Site Recovery for SAN replication refers to on-premises protection with SAN.</td>
</tr>
<tr>
<td>Storage consistent replication</td>
<td>Storage consistent replications refer to storage replications (local or remote) that maintain write-order fidelity at the target devices, even while the application is running.</td>
</tr>
<tr>
<td>VMAX3 Consistency Group</td>
<td>A device group comprised of VMAX3 RDF devices, which have been enabled for remote consistency. The devices in the consistency group are specially configured to act in unison to maintain the integrity of data when distributed across multiple devices within an array. A consistency group will allow control operations to be performed at the group level.</td>
</tr>
</tbody>
</table>
| VMAX3 HYPERMAX OS | HYPERMAX OS is the industry’s first open converged storage hypervisor and operating system. It
enables VMAX3 to embed storage infrastructure services like cloud access, data mobility and data protection directly on the array. This delivers new levels of data center efficiency and consolidation by reducing footprint and energy requirements. In addition, HYPERMAX OS delivers the ability to perform real-time and non-disruptive data services.

<table>
<thead>
<tr>
<th><strong>VMAX3 FAST</strong></th>
<th>Fully automated storage tiering (FAST) automatically moves active data to high-performance storage tiers and inactive data to low-cost, high-capacity storage tiers.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>VMAX3 Storage Group (SG)</strong></td>
<td>A collection of host addressable VMAX3 devices. Storage Group can be used to (a) present devices to host (LUN masking), (b) specify FAST Service Levels (SLOs) to a group of devices, and (c) manage grouping of devices for replications software such as SnapVX and SRDF. Storage Groups can be cascaded. For example, the child storage groups can be used for setting FAST Service Level Objectives (SLOs) and the parent used for LUN masking of all the database devices to the host.</td>
</tr>
<tr>
<td><strong>VMAX3 Storage Pool</strong></td>
<td>Storage Resource Pool (SRP) is a collection of data pools that provides a domain for capacity and performance management. By default, a single default SRP is factory pre-configured. Additional SRPs can be created with an EMC service engagement. The data movements performed by FAST are done within the boundaries of the SRP.</td>
</tr>
<tr>
<td><strong>VMAX3 RDF Group</strong></td>
<td>An RDF group is a collection of paths between two VMAX3 systems. When you create an RDF pair it is associated to an RDF group to define communication paths that will be used to synchronize data between the Primary Site VMAX3 devices and Secondary Site VMAX3 devices.</td>
</tr>
<tr>
<td><strong>VMAX3 TimeFinder SnapVX</strong></td>
<td>TimeFinder SnapVX is the latest development in TimeFinder local replications software. With VMAX3, TimeFinder SnapVX snapshots are always space-efficient. When they are linked to host-addressable target devices, the user can choose to keep the target devices space-efficient, or perform full copying.</td>
</tr>
</tbody>
</table>
Product Overview

ASR SAN Replication with VMAX3 solution is based on Microsoft on-premises cloud DR configuration using SRDF on VMAX3, System Center Virtual Machine Manager (SCVMM), monitoring and management using EMC SMI-S Provider for VMAX3, and overall orchestration using Azure. The following sections provide an overview of these components.

AZURE SITE RECOVERY OVERVIEW

Microsoft Azure Site Recovery (ASR) offers robust business continuity and disaster recovery to protect on-premises physical servers and virtual machines by orchestrating and automating replication and failover to Azure, or to a secondary on-premises data center. ASR provides various deployment scenarios to replicate a Windows Server Hyper-V site, HyperV virtual machine or a physical server to Azure or to a secondary data center. In this document, we will focus on site to site scenario with ASR. In this deployment, ASR service connects with SCVMM environment on-premises and requires only metadata associated with virtual machine such as VM Name to orchestrate for replication and failover. When using ASR in this model, no application data is ever sent to Azure, ensuring a high degree of security and trust in the solution. It leverages Windows Server Hyper-V Replica for the replication process and it can also use SAN replication when orchestrating replication between two on-premises data centers.

This paper focuses on replication and orchestration using ASR with Synchronous and Asynchronous SAN replication for two site-to-site on-premises data centers on VMAX3 using SRDF. For other deployment scenarios please refer to: https://azure.microsoft.com/en-us/documentation/articles/site-recovery-overview/.

ASR SAN replication with VMAX3 allows orchestration of VMAX3-based Windows Server Hyper-V Clouds configured by Microsoft System Center Virtual Machine Manager (SCVMM). SCVMM uses EMC SMI-S Provider for VMAX3 to orchestrate VMAX3 array management functions for SAN-based operations. The SAN replication and topologies and EMC SMI-S Provider for VMAX3 integrations are described in subsequent sections.

VMAX3 PRODUCT OVERVIEW

The EMC VMAX3 family of storage arrays is built on the strategy of simple, intelligent, modular storage, and incorporates a Dynamic Virtual Matrix interface that connects and shares resources across all VMAX3 engines, allowing the storage array to seamlessly grow from an entry-level configuration into the world’s largest storage array. It provides the highest levels of performance and availability featuring new hardware and software capabilities.

The newest additions to the EMC VMAX family—VMAX3 100K, 200K and 400K—deliver the latest in Tier-1 scale-out multi-controller architecture with consolidation and efficiency for the enterprise. They offer dramatic increases in floor tile density, high capacity flash and hard disk drives in dense enclosures for both 2.5” and 3.5” drives, and support both block and file (eNAS) storage.

1 – 8 redundant VMAX³ Engines
Up to 4 PB usable capacity
Up to 256 FC host ports
Up to 16 TB global memory (mirrored)
Up to 384 Cores, 2.7 GHz Intel Xeon E5-2697-v2
Up to 5,760 drives
SSD Flash drives 200/400/800/1,600 GB 2.5”/3.5”
300 GB – 1.2 TB 10K RPM SAS drives 2.5”/3.5”
300 GB 15K RPM SAS drives 2.5”/3.5”
2 TB/4 TB SAS 7.2K RPM 3.5”

Figure 2. VMAX3 storage array

VMAX3 family of storage arrays come pre-configured from the factory to simplify deployment at customer sites and minimize time to first I/O. Each array uses Virtual Provisioning to allow the user easy and quick storage provisioning. VMAX3 can ship as an all-flash array with the combination of EFDs (Enterprise Flash Drives) and large persistent cache that accelerates both writes
and reads even farther. It can also ship as hybrid, multi-tier storage that excels in providing FAST\(^1\) (Fully Automated Storage Tiering) enabled performance management based on Service Level Objectives (SLO). VMAX3’s new hardware architecture comes with more CPU power, larger persistent cache, and a new Dynamic Virtual Matrix dual InfiniBand fabric interconnect that creates an extremely fast internal memory-to-memory and data-copy fabric. Figure 2 lists possible VMAX3 components. Refer to EMC documentation and release notes to find the most up-to-date supported components.

**VMAX3 SnapVX Local Replication**

EMC TimeFinder SnapVX software delivers instant and storage-consistent point-in-time replicas of host devices that can be used for purposes such as the creation of gold copies, patch testing, reporting and test/dev environments, backup and recovery, data warehouse refreshes, or any other process that requires parallel access to, or preservation of the primary storage devices.

Some of the main SnapVX capabilities related to native snapshots:

- With SnapVX, snapshots are natively targetless. They only relate to source devices and can't be otherwise accessed directly. Instead, snapshots can be restored back to the source devices, or linked to another set of target devices which can be made host-accessible.
- Each source device can have up to 256 snapshots, and can be linked to up to 1024 targets.
- SnapVX snapshots themselves are always space-efficient such as they are simply a set of pointers pointing to the original data when it is unmodified, or to the original version of the data when it is modified. Multiple snapshots of the same data utilize both storage and memory savings by pointing to the same location and consuming very little metadata.
- SnapVX snapshots are always consistent. That means that snapshot creation always maintains write-order fidelity. This allows easy creation of restartable database copies. Snapshot operations such as establish and restore are also consistent – that means that the operation either succeeds or fails for all the devices as a unit.

**Note:** TimeFinder SnapVX is the default method for creating a production test environment at the recovery site, when triggering test failover at the Azure Site recovery portal.

**References:** [SnapVX TechNote EMC VMAX3 Local Replication](#) and [Solutions Enabler Product Docs](#).

---

\(^1\) Fully Automated Storage Tiering (FAST) allows VMAX\(^1\) storage to automatically and dynamically manage performance service level goals across the available storage resources to meet the application I/O demand, even as new data is added, and access patterns continue to change over time.
VMAX3 SRDF Remote Replication

EMC Symmetrix Remote Data Facility (SRDF) family of software is the gold standard for remote replications in mission critical environments. Built for the industry leading high-end VMAX3 storage array, the SRDF family is trusted for disaster recovery and business continuity. SRDF offers a variety of replication modes that can be combined in different topologies, including two, three, and even four sites. SRDF and TimeFinder are closely integrated to offer a combined solution for local and remote replications.

- **SRDF modes of operation supported by ASR:**
  - SRDF/S is used to create a committed transactions solution with no data loss.
    - In SRDF/S, each host-write to an R1 device is acknowledged only after the I/O is copied to the R2 storage system persistent cache.
    - SRDF/S makes sure that data on both the source and target devices is exactly the same.
    - Host I/O latency will be affected by the distance between the storage arrays.
  - SRDF/A is used to create consistent replicas at unlimited distances, without write response time penalty to the application.
    - In SRDF/A each host-write to an R1 device is acknowledged immediately after it registered with the local VMAX3 persistent cache, preventing any write response time penalty to the application.
    - The R2 target devices maintain a consistent replica of the R1 devices, though slightly behind, depending on how fast the links can transmit the cycles and the cycle time. For example, when cycles are received every 15 seconds at the remote storage array its data will be 15 seconds behind production (if transmit cycle was fully received), or 30 seconds behind (if transmit cycle was not fully received it will be discarded during failover to maintain R2 consistency).

- **SRDF Groups:**
  - An SRDF group is a collection of matching devices in two VMAX3 storage arrays together with the SRDF ports that are used to replicate these devices between the arrays. HYPERMAX OS allows up to 250 SRDF groups per SRDF director. The source devices in the SRDF group are called R1 devices, and the target devices are called R2 devices.
  - SRDF operations are performed on a group of devices contained in an SRDF group. This group is defined by using either a text file specifying the list of devices, a ‘device-group’ (DG), ‘composite/consistency-group’ (CG), or a ‘storage group’ (SG). The recommended way is to use a storage group.

- **SRDF Consistency:**
  - SRDF Consistency Group is an SRDF group to which consistency was enabled.
  - Consistency can be enabled for either Synchronous or Asynchronous replication mode.
  - An SRDF consistency group always maintains write-order fidelity (also called: dependent-write consistency) to make sure that the target devices always provide a restartable replica of the source application. Even when consistency is enabled the remote devices may not yet be consistent while SRDF state is sync-in-progress. This happens when SRDF initial synchronization is taking place before it enters a consistent replication state.
  - SRDF consistency also implies that if a single device in a consistency group can’t replicate, then the whole group will stop replicating to preserve target devices consistency.

- **SRDF Topologies**
  - Two-site SRDF topology include SRDF sessions in SRDF/S and SRDF/A between two storage arrays, where each RDF group can be set in different mode, and each array may contain R1 and R2 devices of different groups.
  - Three and four-site topologies are beyond the scope of this paper.

References: Please refer to SRDF documentation for details on SRDF modes, and topologies details.

Note: Since ASR by design, is a two-site paradigm, only two sites of a three SRDF sites solution can be directly managed at once. In other words, recovery can only occur between two sites, and which sites those are depends upon by which are being managed by the Azure ASR portal, and where the compute resources are physically located.
EMC SMI-S Provider for VMAX3 and EMC CIM Object Manager (ECOM)

EMC SMI-S Provider for VMAX3 supports the Storage Networking Industry Association (SNIA) Storage Management Initiative Specification (SMI-S), an American National Standards Institute (ANSI) standard for storage management. It defines the open storage management interface that enables the interoperability of multiple storage management technologies for monitoring and controlling storage resources in SAN topologies. The EMC SMI-S Provider for VMAX3 is paired with the EMC CIM Object Manager (ECOM) server to provide an SMI-S compliant interface for EMC VMAX3 arrays. SCVMM also uses EMC SMI-S Provider for VMAX3 to perform VMAX3 storage provisioning, management and replication operations. The EMC SMI-S Provider for VMAX3 installation and configuration comprises of EMC SMI-S Provider for VMAX3, EMC Common Interface Module (CIM) server and required Solutions Enabler. The ECOM is a cross-platform server that receives requests from SMI clients and translates each request into a provider specific operation. It then passes the operation to the EMC SMI-S Provider for VMAX3 for processing.

EMC SMI-S PROVIDER FOR VMAX3 SETUP AND CONFIGURATION

EMC SMI-S PROVIDER FOR VMAX3 CONFIGURATION FOR SYSTEM CENTER VIRTUAL MACHINE MANAGER

The SCVMM topology is shown in Figure 3. Windows Server Hyper-V hosts get the SAN LUNs (FC or iSCSI), from VMAX3 directly by communicating via Windows SMAPI (Storage Management API). The volume automation, as handled by the Hyper-V hosts, essentially provides the disks, partitions and Clustered Shared Volumes (CSVs) that Windows Server Hyper-V hosts use for consumption as storage for their VMs. The SCVMM uses WMI to communicate to the Windows Server Hyper-V hosts, and CIMXML to communicate to the EMC SMI-S Provider for VMAX3 over the network. The EMC SMI-S Provider for VMAX3 enables SAN orchestration by helping to discover and manage VMAX3 arrays. This provides and end-to-end picture of an entire site as managed by System Center Virtual Machine Manager (SCVMM).

Note: SCVMM does neither pair the VMAX3 SRDF links, nor does it manage it. The SRDF configuration and initial setup is done out-of-band by SAN administrators.

SCVMM Topology

Figure 3.

EMC SMI-S PROVIDER FOR VMAX3 GATEKEEPERS CONSIDERATIONS

Size of the VMAX3 Gatekeepers

EMC SMI-S Provider for VMAX3 uses EMC Solutions Enabler, a software infrastructure to control the features of VMAX3 arrays. Solutions Enabler receives requests from EMC SMI-S Provider for VMAX3 and generates low-level commands (syscalls) that are transmitted to the VMAX3 array for action as needed. Gatekeeper devices are VMAX3 devices that act as the target of these command requests in the form of disk I/O. Gatekeepers require only a small amount of space, 3 cylinders (~3MB).
Note: SAN Administrators are discouraged from building Gatekeepers in larger sizes as the Solutions Enabler uses size to automatically identify and use devices as Gatekeepers.

Presenting a Gatekeeper from an array to the Solutions Enabler will cause that array to be seen as a local array.

**Presentation of VMAX3 Gatekeepers to EMC SMI-S Provider for VMAX3 Virtual Machine**

Present Gatekeepers to EMC SMI-S Provider for VMAX3 VM using either pass through devices or Virtual Fibre Channel adapters.

Windows Server 2012 provides the Virtual Fibre Channel feature to provide direct Fibre Channel connectivity to VMAX3 arrays from virtual machines, giving full protocol access.

**Note:** For EMC SMI-S Provider for VMAX3 virtual machine both EMC and Microsoft recommend the use of Virtual Fibre Channel adapters instead of pass-through devices.

When Gatekeepers are presented to a VM over a Virtual Fibre Channel adapter, no additional steps are required.

It is recommended to have at least two virtual adapters that are zoned and registered across redundant virtual SANs allowing device access through redundant VMAX3 array ports. When EMC SMI-S Provider for VMAX3 is installed in a VM environment, and has Gatekeeper access via Virtual Fibre Channel adapters, the provider is free to move from one Windows Server Hyper-V server to another as part of live migration while maintaining Fibre Channel connectivity to the VMAX3. The overall recommended base topology is shown in Figure 4.

**References:** The Virtual Fibre Channel feature is explained in *EMC Storage with Microsoft Hyper-V virtualization.*

---

**Figure 4.** Virtual Fibre Channel configuration for EMC SMI-S Provider for VMAX3 VM

**Number of VMAX3 Gatekeepers**

The number of Gatekeepers needed to service the commands is determined by the number of commands issued from Solutions Enabler, and by the complexity and time of the actions required to service those commands. Any array that does not have Gatekeepers present to an instance of Solutions Enabler, but has an SRDF connection to an array that does, will appear in that Solutions Enabler instance as a remote array. In most cases Gatekeeper devices must be mapped and masked to a single server and should not be shared across servers. Likewise, it is a best practice to minimize the number of SMI-S Providers servicing a single VMAX3 (virtualized environments offer an exception). The minimum requirement of six Gatekeepers per VMAX3 should prove sufficient for most EMC SMI-S Provider for VMAX3 servers (or VMs). However where scale is taken into consideration, the number of Gatekeepers given to an SMI-S server varies. The calculation is as follows:
Gatekeepers needed for Replication Group operation = [Number of Replication Groups] * 0.3
Round the result of calculations to a whole integer and then do the following addition:
Total number of Gatekeepers provisioned per VMAX3 = 6 + (GKs needed for RG operation)

References:  
- Solutions Enabler Installation Guide, details about VMAX3 Gatekeepers at EMC primus 255976,  
- Automation with System Center and EMC Storage Systems using SMI-S Reference Architecture.

**EMC SMI-S Provider for VMAX3 Installation and Configuration**

**EMC SMI-S Provider for VMAX3 installation**

EMC SMI-S Provider for VMAX3 is packaged as part of the VMAX3 Solutions Enabler kit. Execute the following steps at both the source and target sites.

1. In the Setup type dialog, select **Custom** and choose SMISPROVIDER_COMPONENT as shown in Figure 5.

![Figure 5. SMISPROVIDER_COMPONENT custom setup](image)

2. While installing EMC SMI-S Provider for VMAX3, choose the **Solutions Enabler Base Daemon**, **EMC Solution Enabler RDF Daemon**, **EMC Solutions Enabler GNS Daemon**, **EMC SE Event Daemon** and **Solutions Enabler SYMAPI Server Daemon** to be installed and started. See Figure 6.

![Figure 6. Service daemons that need to be chosen for ASR](image)

3. In the specify lockbox password fields, click Next to select the default value, or enter a value in the fields. The default lockbox password generated by the installation program for ECOM/SMI-S is **admin/#1Password**.

4. Edit C:\Program Files\EMC\SYMAPI\config\daemon_options to enable the following parameters.
   Be sure to remove the leading “#” character.
   SYMAPI_USE_GNS = ENABLE
   SYMAPI_USE_RDFD = ENABLE

5. For 2-site dual EMC SMI-S Provider for VMAX3 configuration, edit C:\Program Files\EMC\SYMAPI\config\daemon_options: storgnsd:GNS_REMOTE_MIRROR = enable

6. Optionally use TCP/IP port no. 5988, non-SSL or port no. 5989 SSL connection as desired.

7. Edit C:\Program Files\EMC\ECIM\ECOM\conf\Security_settings.xml
   Change default value NonCIMRequest_AuthenticationEnabled to “false”
   Change default value ExternalConnectionLimit 100 to 600
   Change default value for ExternalConnectionLimitPerHost 100 to 600
   Change SSLClientAuthentication to “None”
   Save Security_settings.xml

8. For 2-site dual EMC SMI-S Provider for VMAX3 configuration, edit C:\Program Files\EMC\ECIM\ECOM\Providers\OSLSProvider.conf
   Modify or Add the following line
   OSLSPRovider/com.emc.cmp.osls.se.symm.ReplicationService.offline = false

9. Stop ECOM and the solutions enabler daemons and restart them.

Azure Site recovery 2-site configuration requires two separate EMC SMI-S Providers for VMAX3, one in each location.

Note: It is not supported to have a single EMC SMI-S Provider for VMAX3 manage arrays on both sites as local. Each EMC SMI-S Provider for VMAX3 must manage their local arrays as local (have direct access to them via Gatekeepers) and their respective paired arrays as “remote” (have indirect access to them via SRDF connection). Both EMC SMI-S Providers for VMAX3 have full knowledge of the other VMAX3 to enable ASR orchestration of failover/failback between sites.

EMC SMI-S provide for VMAX3 admin authentication

EMC SMI-S Provider for VMAX3 post-installation tasks requires setting up an administrator role to query the EMC SMI-S Provider for VMAX3. An initial setup is required on the EMC SMI-S Provider for VMAX3 VM to create a user using URL https://<SMT-S Provider IP Address>:5989/ecomconfig, and using default credentials of username admin and password #1Password (or the appropriate password if a non-default lockbox password was selected during Solutions Enabler installation). Once logged in another user with the role of Administrator can be created. For security reasons, it is recommended to change the default password of the user admin.

References: Solutions Enabler installation Guide for SMI-S authentication and certificate management

EMC SMI-S Provider for VMAX3 hosts and Solutions Enabler daemons

SRDF control and management operations are enabled by an RDF daemon (storrdfd) running on all attached EMC SMI-S Provider for VMAX3 hosts. Along with storrdfd the Group Name Services (GNS) daemon (storgnsd) is enabled as well. It provides a common repository to store and maintain consistency group definitions across VMAX3 arrays. This shared GNS repository is available and visible to any GNS-enabled locally-attached EMC SMI-S Provider for VMAX3 hosts to perform control operations. Storrdfd relies on the GNS daemon to propagate updated consistency group (CG) definitions to the other remote EMC SMI-S Providers for VMAX3 locally attached to the remote VMAX3 arrays. The propagated CG at the remote site has the same name as the local one, has identical contents, and reflects the perspective of the primary local array. By default, no longer than 60 seconds after the CG is created in one site, it is available for use on the recovery site.

References: An in-depth discussion of GNS can be found in the SRDF Product Guide.

SRDF CONSISTENCY GROUPS AND SCVMM REPLICATION GROUPS

A consistency group is a device group or composite group comprised of RDF devices, which has been enabled for remote consistency. The devices in the consistency group are set to act in unison to maintain the integrity of data when distributed across multiple devices within an array. SRDF consistency protection software preserves the dependent-write consistency of
devices within the group by monitoring data propagation from source devices to their corresponding target devices. If a source R1 device in the consistency group cannot propagate data to its corresponding R2 device, SRDF consistency software suspends data propagation from all the R1 devices in the group. This protection leaves the remote data consistent, and allows for a quick recovery from certain types of failures or physical disasters by maintaining a consistent environment.

SRDF consistency group protection is available for both SRDF/S and SRDF/A. SRDF consistency protection is managed and maintained by the SRDF Daemon (storrdfd) running on the Solutions Enabler servers.

SCVMM uses Solutions Enabler Consistency Groups to create Replication Groups. Replication Group creation in SCVMM is completed manually. The Virtual machines and the corresponding group of LUNs that are holding them must be identified in advance. These LUNs are then included as part of the consistency group as shown in Figure 7. Carefully naming the replication groups to identify the priority and the business use of these LUNs and their Virtual machines helps simplify replication tasks like choosing between Synchronous and Asynchronous operations, and also virtual machine startup order in the recovery plans in the Azure portal.

![Diagram of Virtual Machines, LUNs, Replication Groups mappings for recovery plans](image)

**Figure 7. Virtual Machines, LUNs, Replication Groups mappings for recovery plans**

**ASR Setup and Configuration**

**SOFTWARE REQUIREMENTS**

**SCVMM and ASR software requirements**
1. Windows Server 2012 or 2012 R2 Hyper-V clusters must be setup on both primary and secondary sites.
2. System Center Virtual Machine Manager 2012 R2 must be on both sites with at least Update Rollup 6 installed.
3. Azure Site Recovery Provider (latest version) must be installed on each SCVMM server.

**References:** For details, refer to the [Azure Site Recovery Deployment Guide](#).

**VMAX3 software requirements for ASR**

This section details the general pre-requisites that need to be met. Table 1 shows VMAX3 storage environment and EMC SMI-S Provider for VMAX3 kit used for the test cases.

<table>
<thead>
<tr>
<th>Configuration aspect</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMAX3 Array</td>
<td>100K, 200K, 400K</td>
</tr>
</tbody>
</table>
16

VMAX3 Enginuity Build Version | 5977.596.583 or higher
---|---
EMC SMI-S Provider for VMAX3 | V8.0.3.20 or higher
Kit: se80320-WINDOWS-x64.exe

References: The latest support details for VMAX and VMAX3 can be found in the Azure Site Recovery SAN Integration document.

1. Ensure that SRDF physical connectivity and zoning between SRDF directors exist and SRDF groups for SRDF/S, and SRDF/A are created.

2. It highly recommended to pre-create LUNs at the recovery site to be used as TimeFinder SnapVX linked targets, in a test failover scenario. EMC SMI-S Provider for VMAX3 will try to first locate suitable target LUNs for linking. If none are found, the Provider will try to create them, although this operation could take some time.

3. A separate SRDF group exists for every Replication Group. SCVMM will use EMC SMI-S Provider for VMAX3 to automatically choose the existing, available SRDF groups.

4. For a two-site dual SMI-S Provider model, each site must see their local arrays as "local" (have access to them via Gatekeepers) and their respective paired arrays as "remote" (have indirect access to them via SRDF connection). The EMC SMI-S Provider for VMAX3 should not see the arrays from both sides of an SRDF pair as "local". In a two-site model, both SMI-S Providers should have full knowledge of other site.

ASR HIGH LEVEL CONFIGURATION STEPS

The steps below outline the high-level steps executed at both sites (Primary and Recovery). Granular step-by-step operations for ASR setup and recovery use cases are explained in Appendix II.

Setup using System Center Virtual Machine Manager (SCVMM)

1. Conduct SAN discovery via EMC SMI-S Provider for VMAX3.
2. Browse available Storage Pools as managed by SCVMM.
3. Allocate Storage pools to Host group.
4. Create SAN volumes (LUNs) for VMs (Primary)^2.
5. Create Cluster Shared Volumes (CSVs) on the LUNs and use quick format (Primary).
6. Create Replication Groups (RGs) (Primary).
7. Create Primary and Recovery clouds.
8. Add RGs to cloud (Primary).

Operations at the Microsoft Azure Site Recovery Portal

1. Create a Site Recovery Vault.
2. Register Primary and Recovery site SCVMM servers by setting up providers.
3. Create storage array and storage pool mapping for the Primary and Recovery Sites.
4. Configure cloud protection settings for primary and recovery site clouds.
5. Protect RGs.
6. Create VMs and protect them (SCVMM only).
7. Perform SAN operations like enable protection, failover, reverse role and test failover.

References: For more details, refer to the Azure Site Recovery SAN Integration Guide and the ASR advanced recovery plan options.

^2 It is assumed that the Hyper-V clusters have access to VMAX source and target devices when surfaced because of pre-existing host masking views created out of band using SYMCLI or Unisphere for VMAX.
Azure Site Recovery Use Cases Overview

**Note:** The following is a high-level overview of the use cases tested. Please refer to the [Appendix II](#) for detailed steps.

This section covers the scale limits tested with ASR with SAN Replication on VMAX3. The following use cases are covered in this section and more details about them can be found in Appendix II as well:

1. **CREATE AND PROTECT RGs AND RESIDENT VMs**
2. **PLANNED FAILOVER OF RGs TO RECOVERY SITE AND REVERSE ROLE**
3. **UNPLANNED FAILOVER OF RGs TO RECOVERY SITE AND REVERSE ROLE**
4. **FAILBACK TO PRIMARY SITE**
5. **TEST FAILOVER OF RGs, FOR NON-IMPACT PRODUCTION SITE TESTING**
6. **DELETE RGs AND DISABLE PROTECTION**

**SCALE LIMITS FOR ASR SCENARIOS**

The scale limits for ASR deployment with VMAX3 are described in Table 2 below.

<table>
<thead>
<tr>
<th>Scale aspect</th>
<th>Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum number of replicating LUNs at both sites</td>
<td>100</td>
</tr>
<tr>
<td>Maximum number of LUNs in a RG</td>
<td>20</td>
</tr>
<tr>
<td>Maximum number of parallel operations</td>
<td>5 RGs x 10 LUNs</td>
</tr>
<tr>
<td>Maximum number of LUNs in parallel operations</td>
<td>10 RGs x 5 LUNs</td>
</tr>
</tbody>
</table>

**References:** Refer to [Azure Site Recovery SAN Integration Guide](#) for most recent support notes.

**USE CASE 1: CREATE AND PROTECT RGs AND RESIDENT VMs**

This use case deals with preparing VMAX3 arrays to be discovered within SCVMM, and then placing VMs to be protected using Azure Site recovery orchestration. These VMs are located on protected storage that is part of a Replication Group (RG). The VMAX3 storage aspect of this use case is illustrated in Figure 8.

![Figure 8](#)  
**Figure 8.** Enabling protection for RGs for synchronous or asynchronous replication
These are the steps for creating replication groups and protecting the VMs:

1. Discover Source and Target site EMC SMI-S Providers for VMAX3.
2. At both sites, bring storage pools under management, create classification, and allocate discovered storage to host groups.
3. Configure network and add Hyper-V servers to both sites, and add hosts to SCVMM.
4. Create storage volumes on VMAX3 arrays, and allocate them to host groups.
5. Prepare these storage volumes as clustered shared volumes, and format them for use.
6. Create RGs with these storage volumes and designate them for replication.
7. Create a source site cloud, then assign logical network, storage classifications and RGs to this cloud.
8. Create a target site cloud, then assign logical network and storage classifications to this cloud.
9. Sign up for an account in Azure Site Portal, and create a recovery services Vault for SAN replication.
10. Download the management certificate and ASR provider (DRA plugin), and register both SCVMM servers to the portal.
11. Pair logical networks, storage pools, and arrays for source and target sites in the portal.
12. Discover Source and Primary site clouds, and configure protection for them.
13. Enable RG protection for the discovered source site RGs.
14. Create a VM template in the source site SCVMM instance.
15. Use the new VM wizard in source site SCVMM to select a VM template and specify Advanced option Azure Site Recovery and corresponding RG for cloud protection.
16. Verify the creation of placeholder-database-only VMs, in stopped state, to reserve host resources on the target site.

USE CASE 2: PLANNED FAILOVER OF RGS TO RECOVERY SITE AND REVERSE ROLE

This use case describes the situation when a planned failover or migration is triggered from the ASR portal. The RG and the LUNs containing the protected VMs are failed over to the target site. This is done gracefully, so that the VMs that need to be failed over are shut down, and are started up in order. This graceful migration of VMs is triggered from the source site. The VMAX3 SAN storage aspect of this use case is illustrated in Figure 9.

---

2 It is assumed that the Hyper-V clusters have access to VMAX source and target devices when surfaced because of pre-existing host masking views created out of band using SYMCLI or Unisphere for VMAX.
These are the steps for performing planned failover and reversing the replication flow:

1. Follow steps described in Use Case 1.
2. Trigger the failover of the protected RG from the source site to the target site.
3. Ensure that the VMs are shut down, and storage LUNs within those RGs are properly failed over.
4. Ensure that the LUNs on the target site are surfaced on the Windows Server Hyper-V hosts.
5. Verify that the failed over VMs and their corresponding configurations are registered to the Hyper-V hosts and powered-on.
6. Verify that on the source site the VMs are removed, and that the LUNs are unmounted and unregistered from the Hyper-V hosts.
7. Verify that the source LUNs are write disabled, the links are in “Failed Over” status, and the target LUNs are read/write enabled.
8. Reverse replicate the RGs once the failover is successful since the changes in the target site need to be committed to the source site as well. This swap operation allows RGs to be recovered quickly and continue to be protected, at the original site.

The VMAX3 SAN operation from the reverse replication perspective is illustrated in Figure 10.

---

4 It is assumed that the Hyper-V clusters have access to VMAX source and target devices when surfaced because of pre-existing host masking views created out-of-band using SYMCLI or Unisphere for VMAX.
USE CASE 3: UNPLANNED FAILOVER OF RGS TO RECOVERY SITE AND REVERSE ROLE

This use case describes the situation when the source site has experienced a site outage. This could be caused by a massive power outage, actual physical destruction of the infrastructure, or network failure of replication traffic. It is assumed that the target site is not impacted, and is still available for use. In this situation, an unplanned failover to the target site is triggered by the ASR portal for all VMs and RGS. In an unplanned failover, minimal attempts are made to contact the source site. Everything is triggered from the target site and run to completion, even if errors are encountered on the source site.

These are the steps after unplanned failover:

1. Follow steps mentioned in Use Case 1 to protect the RGs and VMs and trigger replication between the source site and the target site.
2. When a source site outage occurs, trigger an unplanned failover of RGs and their VMs.
3. Ensure that the LUNs on the target site are surfaced on the Windows Server Hyper-V hosts.
4. Verify that the failed over VMs and their corresponding configurations are registered to the Hyper-V hosts and are started.
5. Optionally check whether the SRDF pair state is “Partitioned” or “TransmitIdle” in a true disaster or unplanned migration. If the SRDF pair is in a “Split” mode this indicates that user has executed a planned migration of the RGs, the link is still up, and a storage failure has not occurred (or has been resolved).
6. Once the source site is repaired and verified to be up and healthy, reverse replicate the RGs back to it. This allows the RGs to continue to be protected.

USE CASE 4: FAILBACK TO PRIMARY SITE

This use case describes the situation when the source site that temporarily assumed the role of the target site as part of planned or unplanned failover, is made primary site again. This essentially is a return back to its primary site role. This is possible after reverse role has ensured that data replication and synchronization have been established to the source site. The workflow is similar to the planned failover operation previously discussed in Use Case 3, except it is in the other direction.

These are the steps to failback to primary site:

1. Follow the steps mentioned in Use Case 1 to protect the RGs and VMs, and to trigger replication between the source site and the target site.
2. Follow the steps mentioned in either Use Case 2 or Use Case 3, to failover RGs to the Recovery site and reverse replicate.
3. Execute a planned failover or unplanned failover back to source site to make it the primary again. This essentially is equivalent to a failback.
4. Verify that all VMs that were initially migrated to the target site have been moved back to the source site.
USE CASE 5: TEST FAILOVER OF RGS, FOR NON-IMPACT PRODUCTION SITE TESTING

This use case supports the test failover workflow that involves creation of remote snapshots. Test failovers are achieved through the use of local replication technology provided by VMAX3: in this case, SnapVX linked replicas of the target RGS. Test failovers happen while the replication from source site to target continues. This helps create a separate VM environment used for test purposes. Test failover incorporating SnapVX is illustrated in Figure 11.

These are the steps to D/R testing using remote snapshot:
1. Follow the steps in Use Case 1 to protect the RGs and VMs, and to trigger replication between the source site and the target site.
2. While replication from source site to target site is still going on, trigger a test failover of the RGS.
3. Verify that failed over test VMs are created and spun up in a separate bubble IP-network environment on the target site.
4. Check that no operations are disrupted at the source site, and that the replication from source site to target site is unimpeded.
5. Verify the success of any custom scripts, application functionality, networking, etc. Once all facets of the test are verified, acknowledge test failover complete in the ASR portal.
6. Ensure that the test environment is cleaned up, the snapshot linked target LUNs unregistered, removed from the target site Hyper-V hosts and deleted. This cleanup operation is needed to execute another test failover attempt if needed.

USE CASE 6: ORGANIZE RGS AND RESIDENT VMS IN FLEXIBLE RECOVERY PLANS
1. In Microsoft Azure Portal for Azure Site Recovery, create a Recovery Plan to organize RGs and resident VMs for failover sequence.
2. Select the RGs and resident VMs that need to be included in this plan. All VMs that are part of an RG will get selected.
3. Organize the VMs into different boot up groups. For example, DB VMs can be in group 1 and web VMs can be in group 2.
4. Customize recovery plan with additional PowerShell scripts or manual actions and save the script.
5. Once Recovery Plan has been saved, it can be used to perform planned, unplanned and test failover for all the RGs and VMs included in the group. Recovery Plan will ensure the shutdown and boot order and also execute custom scripts and enable a one click end to end DR of the application.
USE CASE 7: DELETE RGS AND DISABLE PROTECTION

This use case explains how to clean up and delete RGs from the target site after protection is deleted.

These are the steps for cleanup:

1. Follow steps mentioned in Use Case 1 to protect the RGs and VMs.
2. Delete protection for VMs, before deleting RG protection. Confirm removal of target LUNs, and target site RGs.
3. Ensure that the cleanup happens, and the RGs are removed from the source site and target site clouds.
4. Repeat the above steps at various failover and failback stages, when the RGs are failed over at the target site, or when reverse replication is in progress from target site to source site.

Conclusion

VMAX3 SRDF is the industry-leading Enterprise business continuity and DR solution offering synchronous and asynchronous modes of operation and various topologies for two to four sites. Azure Site recovery with SAN Replication is a business continuity solution that provides orchestration of DR support for Microsoft on-premises clouds leveraging existing VMAX3 SRDF investments. ASR integrates with SCVMM and EMC SMI-S Provider for VMAX3 to manage storage-based replication functions for Hyper-V clouds. ASR provides users with a simple, consistent, and unified experience via Azure Site Recovery portal to orchestrate replication, planned and unplanned failovers, and creation of remote test and dev copies for DR testing for on-premises Hyper-V Clouds on VMAX3 storage. ASR SAN replication with SRDF provides zero RPO/Near sync RPO solutions to enterprise class applications running on Windows Server Hyper-V by allowing user defined group consistency across a desired group of VMs.
**Appendix I: SRDF Group Creation and Management**

**LISTING LOCAL AND REMOTE VMAX3 SRDF ADAPTERS**

Figure 12 shows the physical connectivity between the source site and the target site.

![Physical connectivity listing between Source and Target VMAX3 arrays](image)

**Figure 12. Physical connectivity listing between Source and Target VMAX3 arrays**

To further confirm a full listing of existing SRDF directors, available ports, and dynamic SRDF groups, run the command listed below on both local and remote VMAX3 arrays:

```
# symcfg -sid 536 list -ra all
Symmetrix ID: 000196700536 (Local)
 SYMMETRIX RDF DIRECTORS
Remote Local Remote Status
Ident Port SymmID RA Grp RA Grp Dir Port
----- ---- -------------- ------ ------ ------ -------
RF-1E 7 000196700535 11 (0A) 11 (0A) Online Online
RF-2E 7 000196700535 11 (0A) 11 (0A) Online Online

# symcfg -sid 535 list -ra all
Symmetrix ID: 000196700535 (Remote)
 SYMMETRIX RDF DIRECTORS
Remote Local Remote Status
Ident Port SymmID RA Grp RA Grp Dir Port
----- ---- -------------- ------ ------ ------ -------
RF-1H 10 000197200056 1 (00) 1 (00) Online Online
RF-2H 10 000197200056 1 (00) 1 (00) Online Online
```

**CREATING DYNAMIC SRDF GROUPS**

This command shows how to create a dynamic SRDF group. Based on the output generated from the prior command, a new dynamic SRDF group can be created with proper director ports and group numbers.

```
# symrdf addgrp -label Async80 -rdfg 80 -remote_rdfg 80 -dir "1e:7,2e:7" -remote_dir "1h:10,2h:10" -sid 000196700536 -remote_sid 000196700535
Execute a Dynamic RDF Addgrp operation for group
'Async80' on Symm: 000196700536 (y/[n]) ? y
Successfully Added Dynamic RDF Group 'Async80' for Symm: 000196700536
```

**LISTING THE STATUS OF SRDF GROUP**

This command shows how to get information about the existing SRDF group:

```
# symrdf -sid 536 list -rdfg 80
Symmetrix ID: 000196700536
 Local Device View
--------------------------------------------
Sym Sym RDF STATUS MODES RDF STATES
--------------------------------------------
```
Appendix II: Detailed SCVMM and ASR Setup

SCVMM CONFIGURATION

Discovering the EMC SMI-S Provider for VMAX3 into SCVMM

The EMC SMI-S Provider for VMAX3 discovers and manages the VMAX3 arrays, and hence needs to have network connectivity to the SCVMM server by IP address or FQDN. The next few steps outline the discovery of SMI-S Provider into SCVMM.

1. In the Fabric workspace, click storage

2. In the Providers section or from Home, select Add Resources > Storage Devices. (See Figure 13).

![Figure 13. Storage Devices to add EMC SMI-S Provider for VMAX3](image-url)
3. In the Add Storage Devices wizard, select the storage provider type select the option **SAN devices discovered and managed by the EMC SMI-S Provider for VMAX3** (See Figure 14).

![Add Storage Devices Wizard](image)

**Figure 14. SAN devices by SMI-S Provider**

4. Specify the protocol as **SMI-S CIMXML**, include address for the EMC SMI-S Provider for VMAX3 virtual machine IP address or FQDN, and select a suitable Run As account. This SCVMM "Run As account" should have access into the provider, and should have privileges to discover the provider (see Figure 15).

![Specify Discovery Scope](image)

**Figure 15. Specify SMI-S FQDN and discovery scope**
5. Once the discovery scope is defined with TCP/IP port 5989, discovery and import of storage device information will be started. Both the source VMAX3 and target VMAX3 storage arrays are discovered as part of storage device Scan Provider (See Figure 16). Select the source VMAX3 array at the primary site, and the target VMAX3 array at the recovery site.

![Source and Target VMAX3 arrays discovered as part of RDF relationship](image)

**Figure 16. Source and Target VMAX3 arrays discovered as part of RDF relationship**

6. The discovery process discovers the VMAX3 array, its SRP, manufacturer, model and capacity. Once the Storage Resource Pool is discovered to get them under SCVMM control; this source can now be used by SCVMM for replication (See Figure 17). The LUNs that are unmasked to Hyper-V host initiators are also detected and their end-to-end connections mapped.

![Selecting VMAX3 SRP for allocation to Host Group](image)

**Figure 17. Selecting VMAX3 SRP for allocation to Host Group**
7. Confirming the final settings in the summary page enables final discovery of VMAX3 assets, storage pools, masking sets, and LUNs in SCVMM, as seen in the job progress window. The status window shows the command set-SCStorageArray job enumerating the sequence of steps taken by SCVMM in discovery of these VMAX3 arrays. (See Figure 18)

![VMAX3 storage discovery progress](image18.png)

**Figure 18.** VMAX3 storage discovery progress

8. The classifications and pools section in SCVMM shows the LUNS that are under SCVMM control as part of the SRP discovery. (See Figure 19)

![SRP and its LUNs under SCVMM management](image19.png)

**Figure 19.** SRP and its LUNs under SCVMM management
9. Click on **All Hosts** or specific Host Group properties and if not already allocated, allocate the discovered SRP and LUNs to satisfy a particular host group’s need for storage provisioning of VMs. Do not miss this important step which assures allocation of storage to the cluster. (See Figure 20)

![Allocating VMAX3 SRP to Host Storage](image)

**Figure 20.** Allocating VMAX3 SRP to Host Storage

### Replication group creation for remote replication

Replication Groups are also called consistency groups (CGs). These contain all the LUNs that are needed to be replicated together. Multiple LUNs, multiple applications, and multiple VMs need to be consistent at the target site when failover happens; the replication group guarantees this consistency. ASR with SCVMM and EMC SMI-S Provider for VMAX3 is able to automatically create LUNs on the target site, group it into a Replication Group (RG), and then enable replication. The actual protection and replication itself is offloaded to the VMAX3 arrays. These steps outline the RG creation process:

1. The storage array properties dialog box provides a listing of replication groups. These replication groups can be created, edited or deleted here (see Figure 21).

![Create RG wizard](image)

**Figure 21.** Create RG wizard
2. Create a replication group and associate LUNs from the Create Replication Group Wizard. These LUNs can be out-of-band pre-created storage, or newly created storage LUNs that contain Clustered Shared Volumes (CSVs), that will take part in replication. Once Replication Groups are created on the primary array, they can be made part of the cloud. These RGs are added to the cloud that is subsequently exposed to the ASR portal. (See Figure 22)

![Replication group or consistency group as part of Array properties](Image)

**Creating private SCVMM Clouds**

There should be at least one cloud on the source SCVMM server, and one on the target SCVMM server, that you want to protect. Add SCVMM host groups, Hyper-V clusters, and virtual machines to the source cloud. Add replication groups to the cloud as well. The protection starts with the discovery of the cloud in the ASR portal.

1. Create the Source R1 Cloud in SCVMM (see Figure 23).

![Create source R1 Cloud](Image)
2. Populate the cloud by selecting the appropriate resources, logical networks, templates, and classifications for port and storage. Choose the capability profile as Hyper-V. (See Figure 24)

3. Finally choose the RGs that are going to be part of this cloud that can be exposed to the ASR portal for replication. Confirm the settings in the Cloud summary window. (See Figure 25)
4. Follow similar steps to create the target (recovery) cloud, note that the replication groups are not populated here, as they are currently not yet created by ASR (see Figure 26).

![Figure 26. Target Cloud created on R2 site](image)

5. Create the source (R1.Cloud) and target cloud (R2.Cloud) in the primary SCVMM instance and secondary SCVMM instance, as shown in Figure 27. R1.Cloud on the source site has the RG that needs to be protected and replicated to the target site.

![Figure 27. R1 and R2 Clouds as created in source and target SCVMM instances](image)
Enabling protection for virtual machine

1. Map the VMAX3 Logical Units IDs to Hyper-V host storage through the disk properties. This information is useful when trying to deploy VMs on RGs that have VMAX3 LUNs formatted as clustered shared volumes. (Figure 28)

![Hyper-V host storage mapping to VMAX3 LUN ids](image)

Figure 28. Hyper-V host storage mapping to VMAX3 LUN ids

2. Create a new logical unit as a clustered shared volume for use as VM storage via cluster local properties shared volumes option. This eliminates the use of multiple click streams and the use of the failover cluster manager. (See Figure 29)

![Creating CSVs from cluster host](image)

Figure 29. Creating CSVs from cluster host

3. The process of creating a CSV to be used as shared clustered volumes consists of registering the storage logical unit, modifying the masking view, creating a host volume, formatting it, and then mounting it as a CSV. (See Figure 30)

![Mounting a host cluster disk](image)

Figure 30. Mounting a host cluster disk
4. VMs can be protected after a RG is already replicating. Protected VMs are then added to recovery plans, so they can be part of replication operations within ASR. The next steps show how to deploy a VM into the cloud and also make it part of the Replication Group (RG) for failover. We use SCVMM to select the VMs to enable for recovery. In advanced options in VM properties, choose the replication group, to be used as part of Enable Microsoft Azure Site Recovery protection for this virtual machine. (Figure 31)

Figure 31.  **Enabling ASR at the VM level**

5. Modify properties of the virtual machine to deploy the virtual machine to a private cloud. Choose the destination Hyper-V server for the virtual machine in the cloud. Be sure to check Details, Rating Explanation, and Deployment explanations for validity. It is required that the destination is available for SAN migrations, in order to be protected as part of ASR. (See Figure 32). Then click **Finish** at the summary page to trigger the VM creation in the private cloud.

Figure 32.  **Deploying VM to a private cloud, and checking rating explanation**
6. A corresponding progress is also noted in the primary site. The replication status will also be noted as configuring replica for the VM is being created. The job progress in the Jobs tab should have a description about checking for prerequisites, creating and configuring replica virtual machines, and updating states. Deploying a file using Fast File Copy is invoked, for rapid deployment. This offloads to VM creation to VMAX3. (See Figure 33)

![Figure 33. Deploying VM into the cloud](image)

7. Once the protected VM is created in the Private Cloud on the source site, a DB only VM with reserved capacity is automatically created on the target site and has a status of “reserved”. The replicated LUNs and VHDs are still hidden from the target Hyper-V host cluster. CSVs are not exposed to the servers, DB only VM exists in the context of the SCVMM database with capacity, and other resources reserved in preparation for failover at some point. This ensures a good failover of the VMs. (See Figure 34)

![Figure 34. Creation of DB only VM with reserved capacity on target site](image)
8. Invoking planned failover on the Replication Group also invokes the containing VMs within it, to be brought online. The detailed steps that are invoked during failover are creating new storage logical units, creating new replication group, changing the host cluster, setting the storage logical unit, registering the Storage Logical Unit to cluster, and mounting the storage disk to the remote cluster. (See Figure 35)

![Figure 35. VM in running state after failover to the target site](image)

**Deleting VMs, RGs and disabling protection**
- Before disabling protection for RGs, delete the VMs from the ASR portal. Deleting a VM from the ASR portal will only delete its entry there, while the source and target SCVMMs will still think the VM is protected. Therefore, it is important to either clean up protected VMs manually between both the sites, or migrate the protected VMs out of the protected RGs control to trigger disable ASR protection for the VMs.

**References:** Refer to the [Azure documentation on site recovery management registration and protection](#).
- Manual deletion procedure for primary site virtual machines is detailed as such. On the Source site server SCVMM console, remove protection flag settings as seen in the following script example:

1. In the SCVMM console click the PowerShell button to open the SCVMM PowerShell console. Replace SQLVM1 with the name of your virtual machine.

   ```powershell
   $vm = get-scvirtualmachine -Name "DB_VM"; Set-SCVirtualMachine -VM $vm -ClearDRProtection
   ```

2. On the target site SCVMM server run this script to clean up the settings for the secondary virtual machines.

   ```powershell
   $vm = get-scvirtualmachine -Name "DB_VM"; Remove-SCVirtualMachine -VM $vm -Force
   ```

- As noted, before triggering a delete RG at the portal, it is important to first disable and delete all VMs associated with that RG from the source and target SCVMMs. If these associated RG objects and VMs that are in a replication relationship in the cloud are not removed, then the delete will fail, and manual out-of-band cleanup is necessary.
Deleting and disabling RG protection involves disabling protection on the source location, disabling protection on the target location, removing LUNs, RGs on the target location (if selected), and finally updating the provider states. (See Figure 36)

Figure 36. Disabling RG protection
ASR CONFIGURATION IN AZURE PORTAL

Creating recovery vault in ASR portal

It is assumed that the Cloud administrator has subscription to Azure Site Recovery Management Portal as part of initial Azure account sign-up.

References: See details on access and pricing on the Azure home page.

To create a recovery vault in ASR portal:

1. Sign in to the Management Portal, expand Data services, recovery services, and create an Azure Site recovery vault (see Figure 37).

![Creating recovery vault in the portal](image1)

Figure 37. **Creating recovery vault in the portal**

2. Give the site recovery vault a friendly site name using Quick Create. Next, choose the geographic region as per Azure Site Recovery Pricing. Check status to see if successfully created. (See Figure 38)

![ASR friendly name and Region selection](image2)

Figure 38. **ASR friendly name and Region selection**
3. Once the Azure Site Recovery vault is created, you will be at the dashboard landing page for Quick start. Here, set up recovery for two on-premises SCVMM sites, and then follow the steps for preparing SCVMM servers, configuring cloud protection, Mapping network and storage resources, and finally protecting VMs. (See Figure 39)

![ASR dashboard page for quick start steps](image)

**Figure 39.** ASR dashboard page for quick start steps

4. You may notice a message about not having any servers registered yet. This is because the ASR provider (DRA plugin), has not been downloaded and the SCVMM servers have not been registered with the management registration key. (See Figure 40)

![Protected items SCVMM clouds not having SCVMM servers](image)

**Figure 40.** Protected items SCVMM clouds not having SCVMM servers
5. Preparing SCVMM servers can be achieved by downloading and installing SCVMMASRProvider_x64.exe on the SCVMM servers. Run this provider kit on both the source and target SCVMM servers. Before installing the ASR provider kit, you will have to generate a registration key file in ASR. This file is used for SCVMM authentication into the vault. This is shown as a registration step below (Figure 41). This key file is valid for five days, can be stored locally in a safe place or on a secured share, to be used during Provider Setup. It should be accessible to all the SCVMM servers. If Provider setup was not run within five days, and new registration key file can always be generated.

Figure 41. Download provider and registration key

**Azure Site Recovery provider setup**

Follow these steps to set up Azure site recovery for providers. The next steps show the process of installing the agent, SCVMMASRProvider_x64.exe on the SCVMM servers:

1. Before installing the provider, stop the SCVMM service as automatically prompted by the installer. (See Figure 42)
2. Choose proxy settings to specify how Provider connects to Azure Site Recovery, and select the Registration Key file that was downloaded from Quick Start page in Azure Site Recovery portal. (See Figure 43)

![VMM server page with registration key](Image)

**Figure 43.** VMM server page with registration key

3. The Vault credentials file helps in the ASR provider (DRA plugin) installation, and ultimately authenticating with ASR, so the SCVMM clouds can be published. The registration file is a certificate file that was previously created in the Azure Site Recovery Portal, when the recovery vault was initialized. (See Figure 44)

![Choosing the registration file](Image)

**Figure 44.** Choosing the registration file

4. Synchronize the Cloud Metadata so that the portal gets all SCVMM specific information into Azure Site Recovery. This starts the synchronization phase, and successful initial registration of the SCVMM servers. This needs to happen once for each of
the SCVMM servers at the source and target sites. (See Figure 45)

Figure 45.  **Synchronize with Cloud ASR portal**

At the end of the registration completion, you get a summary of the client certificate, with the creation and expiry dates. After this step, you should notice the clouds populated in the Azure Site Recovery portal, and this helps configure cloud protection settings. Also the source and target VSCMM servers will be shown as connected but not protected, in the recovery vault. The metadata from the SCVMM servers are now retrieved by Azure Site Recovery, and changes in state are also reflected in ASR. (See Figure 46)

![Registration Completed Successfully](image)

Figure 46.  **Registration successful page**
Pairing Clouds in ASR to configure protection

- After the provider is installed and registered, detect the published SCVMM clouds, pair them, and finally configure protection settings. This also means pairing the resources like networks, storage classifications, and storage pools. In the recovery vault notice that the Source and Target SCVMM servers and their corresponding clouds showing up not configured for protection in protected items tab. (See Figure 47) To pair clouds in ASR for protection configuration, follow these steps:

**Figure 47. Not configured clouds**

1. Click on **Source Cloud** to configure protection settings for virtual machines in the cloud. In the menu for configuring replication location and frequency, select the target as SCVMM in the drop down, select target SCVMM server, a suitable target cloud and then choose SAN as replication type (See Figure 48). Notice that the Source and Target arrays are not paired currently. They are paired as a later step. Once the VMAX3 arrays are paired, then replication is triggered. Also keep in mind that the Replication type as SAN is only available after ASR verifies that the clouds have access to SAN replication capable VMAX3 storage.

**Figure 48. Configure replication location**
2. Save the protection settings to trigger a series of steps to register servers, prepare the cloud for protection configuration, prepare SCVMM servers, check the prerequisites for pairing clouds, and also configure cloud for SAN replication. (See Figure 49)

![Figure 49. Configure protection job progress](image1)

3. Once the Clouds are configured for protection, to make any sort of modifications to protection, you must first remove protection to delete the cloud pairings. Then redo the configure protection operations listed above. (See Figure 50)

![Figure 50. Remove protection for configured clouds](image2)
Mapping storage arrays and pairing their pools

Pair VMAX3 storage resources like the classifications and pools to create mapping between VMAX3 arrays and storage resource pools (SRPs) in the primary and secondary sites. Check the servers tab to check status and provider version. Certificates can be renewed here as well. (See Figure 51)

Figure 51. Checking status of connected SCVMM servers

The Add Storage Array Mappings consists of mapping the source and target pools, and their classifications. (See Figure 52)

Figure 52. Resources server storage tab
To map a storage array, follow these steps:

4. Click on **Resources > Server Storage > Map Source and Target Array**. Select the VMAX3 array on the source site and map them to the VMAX3 arrays on the target site, by selecting classifications. (See Figure 53)

Figure 53. **Mapping classifications and storage pools**

5. Confirm storage classification and storage pool mappings in the job properties window. Once resources are mapped, they can be unmapped here. (See Figure 54) This is an important step to keep in mind. Failing to execute steps for storage pool mapping will disable protection on Replication Groups. A message about storage pool pairing has not been completed will be displayed.
Figure 54. Job progress with mapped classifications and storage pools
Enabling SAN replication with Replication Group protection

To enable SAN replication with RG protection, follow these steps:

1. Add SCVMM replication groups associated with the clouds for protection. This enables protecting the virtual machines that are residing on LUNs comprising these replication groups (see Figure 55).

2. Choose the replication group on the source array, and then the target array, and also the replication type (synchronous or asynchronous) (See Figure 56).

Figure 55.  Add replication groups

Figure 56.  Adding and enabling protection for RG
3. Monitor progress of enable protection in the jobs window, as well as in SCVMM on the target site. Notice that as part of the protection, recovery storage logical units, and recovery replication groups are being created on the target site. This operation is executed by SCVMM in conjunction with EMC SMI-S Provider for VMAX3, to provision target site storage and to enable replication (See Figure 57).

Figure 57. **Recovery LUNs created on target site as part of RG protection**

4. The RG protection also enables creation of consistency groups or Replication Groups on the target site, with the replicated LUNs in them (See Figure 58).

Figure 58. **RGs as seen in target site SCVMM**
5. Progress at ASR consists of prerequisite check, identifying replication target, enable replication, and initiating replication, including updating provider states. The duration tab, gives you the timing for each step, to keep you informed as to the expected completion times (See Figure 59).

![Figure 59. Enable protection progress at ASR portal](image)

6. Once protection is enabled and is in state complete, the LUNs themselves are in state synchronized or consistent, depending on the replication type (synchronous or asynchronous). This can be verified in Solutions Enabler SYMCLI. (See Figure 60)

![Figure 60. Verifying device states via Solutions Enabler](image)
7. Also execute refresh in ASR to get the current replication status of the Replication group. Clicking on protection details gives you the ability to delete RG protection, or re-enable it. Typically VMs in Replication groups can undergo the following operations: failover (planned or unplanned), Test Failover, and Delete Protection operation, which tears down the replication groups, on the target site. There is also an intermediate operation after failover; the Reverse replication operation which reverses the role. (See Figure 61)

![Failover states, and ASR protection status](image)

**Figure 61.** Failover states, and ASR protection status

**Recovery plan for orchestrated VM recovery**

A recovery plan groups Virtual machines together for purposes of failover and recovery. Orchestrated recovery using Recovery Plans in the ASR portal have the same consistent experience, as site-to-site DR, using Hyper-V Replica and DR to Azure. Many of the features, like script integration, manual actions that are used as part of a basic Azure recovery flow are available here to make sure that Application VMs come up consistently.

**References:** [Customized recovery plans for on-premises to on-premises protection](#)

8. To create a recovery plan, choose a suitable user defined name and the target SCVMM site with replication type as SAN. Next, select the VMs to be grouped together for specific failover and power-up order. (See Figure 62)

![VM recovery plan creation](image)

**Figure 62.** VM recovery plan creation
Customize recovery plans to add additional groups for specified startup order, additional virtual machines, scripts or manual actions. Scripts can be run, before or after a specific group in a recovery plan. Manual actions can be performed during failover, planned, unplanned or test. Once the group order is set, the recovery plan can be saved, and run from the main recovery plans dashboard in the portal. (See Figure 63)

Figure 63. **Customizing recovery plan**
DETAILED ASR OPERATIONS USE CASES

Planned workload failover

In planned Workload failover, LUNs in the replication group exist in the source site; before they are removed a clean shutdown of the VMs is executed before failover to the target site. This creates consistency from an application perspective. Checks are made to make sure that the data is fully synchronized to the secondary site. Once RG with these LUNs has failed over, the LUNs are then exposed and made ready on the target site. LUNs are then got online, registered to SCVMM, and the Hyper-V cluster or Hyper-V server. The process also startups the VMs in the replication plan in a proper order.

These steps are performed by ASR during the planned fail over:

1. Choose the failover direction to execute a planned failover. (Figure 64)

![Confirm Planned Failover of ‘APP_RG’](image)

Figure 64.  **Executing a planned failover**

2. Once initiated, the status is noted in the windows as planned failover initiated, and the job progress will detail the steps being taken. First failover prerequisites checks are done, then the Virtual machines are shut down in preparation for failover. Once failover is completed, replica virtual machines are created and started. (See Figure 65)

![app_rg (planned failover)](image)

Figure 65.  **Failover in progress**
3. After failover, the Replication Status in ASR will show the following planned failover finished. As seen by the action buttons available in the bottom, Reverse Replicate is the only operation available in this state. Also, at the end of planned failover, the LUNs participating in the Replication group, will show a status of "Failed Over" when queried using Solutions Enabler SYMCLI. (See Figure 66)

**Figure 66. Planned failover finished**

**Reverse replicate procedures**

- Run the reverse replication operation to have any application changes on the target (recovery) site committed back to the primary site. Notice that the active location currently is the target site, and not the source site.

These steps are performed by ASR during reverse replication:

- Prerequisite check
- Commit
- Prepare for reverse replication
- Start reverse replication
- Update provider stats.

The duration for each step can be noted in the job properties window. (See Figure 67)

**Figure 67. Reverse replication progress**
4. The LUNs participating in reverse replication will have the state “Synchronized”, after this operation is successfully executed. The Active Location in a reverse replication state is still the Secondary (recovery) site, while the Replication status gets the Protected-OK tag. Also other operations like Failover and Test Failover get enabled. Users can go through another round of Planned Failover, and Reverse Replication, to set the Active Location back to Primary Site. (See Figure 68)

Figure 68. Reverse replication device status on complete protection

Unplanned workload failover overview

In case of unplanned workload failover, the assumption is that the source site is down. When the communication is broken to the source site, failover can be initiated from the target site. The target site now becomes the primary site. ASR assumes that the available site is the target site, and starts to execute steps there. (See Figure 69)

Figure 69. Unplanned failover of RG

These steps are performed by ASR during unplanned fail over:

- Prerequisites check
- Start failover
- Prepare replica virtual machines
• Start replica virtual machines (See Figure 70)

![Figure 70. Unplanned failover progress](image)

The Replication status during an unplanned failover is shown by the state "unplanned failover completed". The only action button that is available during this state is **Reverse Replicate**, for synching back changes to the unavailable source site once it is available and functional. Triggering a reverse replication to sync the updates back to the Source site on availability will return back the LUNs to synchronized state. Depending on the nature of the unplanned failure on the source site, the state of the failed over LUNs in the Replication Group, using solutions enabler SYMCLI may be "Failed Over". There may be manual intervention required to resume replication. (See Figure 71). Triggering a reverse replication at this stage, should sync the updates back to the source site based on its availability, and will return back the LUNs to synchronized state or consistent state.

![Figure 71. Unplanned failover complete and respective device states](image)
Test failover of workloads overview

- A Workload test failover leverages VMAX3 SnapVX technology on the target site. Once the SnapVX replica is created and linked to target LUNs, it is surfaced to another set of test Hyper-V hosts for testing VM application failover in an isolated environment. The test RGs that were created on the target site are cleaned out once the test is done. It is to be noted that all of the test failover happens while the source site is still replicating to the target site. This allows for testing of the failover process in itself without disrupting protection. Changes will be made to the test failover VMs, their networks, and their storage during this operation. (See Figure 72)

![Confirm Test Failover of 'APP_RG'](image)

Figure 72. Test failover

These steps are performed by ASR during test failover of a workload on remote site (D/R testing):
- Prerequisite checks
- Create test environment
- Create a test virtual machine
- Add the test virtual machine to the cloud
- Attach the network
- Start the virtual machine
- Complete testing
- Clean up the virtual machines
- Remove and finalize LUNs

Figure 73. **Test failover steps**

From a solutions enabler SYMCLI perspective, when SnapVX snapshots are created for test failover they are Copy-On-Write, when linking to the target, as opposed to, Full-Copy which copies all the data to the target. This will help create snapshots instantaneously once the target volume is created. (See Figure 74)

Figure 74. **SnapVX snapshot view for test failover**

For test failover to work at the ASR management portal, add a SCVMM registry entry at the target site or source site, depending on the location of test bed creation. This allows the ASR solution to use pre-created target LUNs for SnapVX linking. The registry key is as follows:

- [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft System Center Virtual Machine Manager Server\DRAdapter]
  Value: StorageProvidersToF0LunAssociationNotImplemented
Type: REG_MULTI_SZ
Value: The SCVMM IDs for all the storage providers, space delimited

- Example "8c775939-54a8-4d9b-a299-766bd901857d 057af7b4-0ea0-4b32-9a9a-4c2137664cbe"

- Example cmdlet to get SCVMM IDs.
  $provider=Get-SCStorageProvider -Name "smi-s.contoso.com"; Write-host $provider.ID
Appendix III: Solutions Enabler CLI Examples

This Appendix shows a brief listing of some useful SYMCLI commands used for out-of-band management of VMAX3 arrays, used frequently in the ASR solution.

References: Solutions Enabler Product Docs

- Command: `symcfg`

`symcfg -version`
`symcfg -hotfix`
`symcfg list`
`symcfg list -pool -sid <array-id>`
`symcfg list -ra all -sid <array-id>`
`symcfg -sid <array-id> list -lock -lockn ALL`
`symcfg -sid SymmID -lockn 15 release`
`symcfg list -ra all -switched -sid <array-id>`
`symcfg list -sid <array-id> -rdfg <rdf group-number> -rdfa (see for sample output in Figure 75)`

```
PS C:\program files\emc\symcli\bin> symcfg list -sid S36 -rdfg 80 -rdfa

SYMMETRIX RDFA GROUPS

RA-Grp Group Name Consistency Cycle Pri Thr Transmit Delay Thr GRP DEV PLG
00 (MP) Async00 XAX XAX 15 33 50 000100100 000000 00000 0 0 0 0 0 0 0

Legend:

- RDFA Flags
  - Consistency
  - Status
  - Mode
  - MSC Cleanup
  - Modified
  - SE Status
  - AutoStart

- Write Pacing Flags
  - Group-Level Pacing
  - Device-Level Pacing

- Supported

(DEV) Device-Level Pacing:
  - Status
  - AutoStart

(FLG) Flags for Group-Level and Device-Level Pacing:
  - Device:

Figure 75. Sample out of symcfg
```

- Command: `symsg`

`symsg list -v`
`symsg delete <Storage group name> -force`

- Command: `symcg`

`symcg list -v`
`symcg delete <Consistency group name> -force (See example in Figure 76 showing cleanup of invalid composite groups)"
Cleanup of invalid consistency group

- **Command:** symrdf

<table>
<thead>
<tr>
<th>Command</th>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>symrdf list</td>
<td>-sid &lt;Primary-array-id&gt;</td>
</tr>
<tr>
<td>symrdf list</td>
<td>-sid &lt;Remote-array-id&gt;</td>
</tr>
<tr>
<td>symrdf -cg &lt;cgname&gt; query -detail</td>
<td></td>
</tr>
<tr>
<td>symrdf -sid &lt;array-id&gt; -rdfg &lt;ra-group-number&gt; -file dev.txt split -force -nop</td>
<td></td>
</tr>
<tr>
<td>symrdf -sid &lt;array-id&gt; -rdfg &lt;ra-group-number&gt; -file dev.txt disable -force -nop</td>
<td></td>
</tr>
<tr>
<td>symrdf -sid &lt;array-id&gt; -rdfg &lt;ra-group-number&gt; -file dev.txt deletepair -force -nop</td>
<td></td>
</tr>
<tr>
<td>symrdf -sid &lt;array-id&gt; -rdfg &lt;ra-group-number&gt; -file dev.txt suspend -force -nop</td>
<td></td>
</tr>
</tbody>
</table>

Notice in the above example dev.txt is a file that contains the source and target device pairings(see Figure 77)

**Figure 77.** Example of dev.txt used as input file to symrdf command
Command: symsnapvx

```
symsnapvx -sid <array-id> list -sg <storage group name> -detail (See Figure 78 for defined linked copy)
symsnapvx -sid <array-id> list -sg <storage group name> -detail -linked (See Figure 79 for linked target clones)
```
Command: symsan

```
> symsan list -sanrdf -sid <array-id> -dir all  (See Figure 80 for example output)
```

![Symsan output to check physical connectivity between sites](image)

Figure 80. *Symsan output to check physical connectivity between sites*
Appendix IV: Windows PowerShell Examples

Some frequently used storage related Windows PowerShell examples are listed below, and should help automate some of the ASR related tasks.

- Retrieving EMC SMI-S Provider for VMAX3 - SCVMM specific ID, see example shown in Figure 81

```powershell
$provider = Get-SCStorageProvider -Name "dsib2079.R2.local"
write-host $provider.id
```

Figure 81. SCVMM ID for provider

- EMC SMI-S Provider for VMAX3 rescan from within SCVMM.

```powershell
get-scstorageprovider | read-scstorageprovider -force
```

- Replication group creation for a LUN named PRIMARY_LUN01

```powershell
$sourcelun = Get-SCStorageLogicalUnit | where {$_.Name -eq "PRIMARY_LUN01"}
New-SCReplicationGroup -Name "PRI_RG01" -StorageLogicalUnit $sourcelun
```

- Remove a replication group

```powershell
$PriGrp = Get-SCReplicationGroup -Name "PRI_RG01"
Remove-SCReplicationGroup $PriGrp
```

- Remove a VM named "DB_VM" by force

```powershell
$vm = get-vm "DB_VM"
Remove-vm $vm -force
```

- Get a list of LUNs discovered in SCVMM

```powershell
$rg = Get-screplicationgroup
$rg.storagelogicalunits
```

- Get the paired target replica LUN for a source LUN named "PRILUN68_1a0_1",

```powershell
$vd = get-virtualdisk "PRILUN68_1a0_1"
get-virtualdisk -SourceVirtualDisk $vd (See example shown in Figure 82 )
```

Figure 82. Listing of a target LUN, for a given Source LUN
• Important storage related powershell query commands

Get-scstoragearray
Get-screplicationgroup
Get-scstoragelogicalunit
Get-storageprovider
Get-storagesubsystem
Get-storagepool
Appendix V: Microsoft Private Cloud Storage Management on VMAX3

UNISPHERE FOR VMAX3

Unisphere for VMAX3 is a web-based interface used to discover, monitor, configure and control VMAX3 arrays. It provides a wide range of functions that involve managing, replicating and protecting storage. It has monitoring capabilities, performance trend analysis and dashboards to analyze data. It displays alerts, array attributes, jobs and other VMAX3 related tasks. Figure 83 shows the snapshot for Unisphere for VMAX3.

References: Refer to VMAX3 Family with HYPERMAX OS Product Guide

Figure 83. Unisphere for VMAX3 dashboard

SCVMM WITH EMC SMI-S PROVIDER FOR VMAX3

Microsoft System Center Virtual Machine Manager (SCVMM) is used to manage a Hyper-V environment that can incorporate hundreds of physical servers. SCVMM integrates with high availability clusters, and provides a single pane of glass with centralized management, reporting and alerts. SCVMM provides standards-based discovery and automation of VMAX3 storage resources, using EMC SMI-S Provider for VMAX3. EMC SMI-S Provider for VMAX3 enables SCVMM to manage multiple arrays. EMC SMI-S Provider for VMAX3 and SCVMM together help provide on-demand storage for private cloud environments, enable automation via Windows storage-specific cmdlets, and support rapid provisioning of VMs to Hyper-V hosts. They take full advantage of VMAX3 array capabilities. Figure 84 shows the snapshot of SCVMM that has VMAX3 arrays discovered by EMC SMI-S Provider for VMAX3.

References: Storage Automation with System Center and EMC Storage Systems using EMC SMI-S Provider for VMAX3

Figure 84. Snapshot of System Center Virtual Machine Manager Fabric resource page
SOLUTIONS ENABLER CLI

EMC Solutions Enabler CLI (SYMCLI) is installed as part of EMC SMI-S Provider for VMAX3 installation. It provides a command line interface for VMAX3 arrays. It is equivalent to the CLI functionality that Unisphere for VMAX3 provides. It is built on top of API library functions, which use system calls to generate low-level I/O SCSI commands to the VMAX3 arrays, hence providing a comprehensive command set for management and control. This appendix has numerous examples on how to use SYMCLI to perform out-of-band array level management tasks without SCVMM. Figure 85 shows a sample output of a symcli command to list the arrays discovered by the EMC SMI-S Provider for VMAX3.

References: VMAX3 Family with HYPERMAX OS Product Guide

Figure 85. SYMCLI output for arrays discovered by EMC SMI-S Provider for VMAX3

References
- Support and training on VMAX3 SRDF technology, including setup and configuration, at http://support.emc.com
- Microsoft blog
- EMC blog (with demo video)
- Microsoft Azure Site to Site Recovery documentation
- Microsoft Azure Site Recovery wiki at TechNet
- EMC and Microsoft Azure Site Recovery SAN Integration Guide for most recent support notes.
- Storage Automation with System Center 2012 and EMC Storage Systems using EMC SMI-S Provider for VMAX3- Reference Architecture and Best Practices
- Using EMC SMI-S Provider for VMAX3 with SCVMM blog post at TechNet
- EMC VMAX3 Family with HYPERMAX OS Product Guide
- EMC VMAX3 Local Replication Tech Note