Microsoft

# SAP NetWeaver: Building a Disaster Recovery Solution using Azure Site Recovery


Authors

Cameron Gardiner, Principal Program Manager, Microsoft Azure CAT

Ashish Gangwar, Program Manager, Azure Site Recovery



This white paper provides a step-by-step guidance for building a disaster recovery solution for SAP applications, based on Azure Site Recovery by Microsoft.



Version: 2.0

Date of Last Change: May 15, 2019

# Table of Contents

# 1. Introduction

Most large and medium sized SAP solutions have some form of Disaster Recovery solution. The importance of robust and testable Disaster Recovery solutions has increased as more core business processes are moved to applications such as SAP. Azure Site Recovery has been tested and integrated with SAP applications and exceeds the capabilities of most on-premises Disaster Recovery solutions and does so at a lower TCO than competing solutions

Benefits of Azure Site Recovery for SAP Customers:

1. Azure Site Recovery substantially lowers the cost of DR solutions. Site Recovery does not start up Azure VMs until an actual or test failover so compute charges are not incurred unless there is a DR event. Only the Storage cost is charged under normal replication.
2. Azure Site Recovery allows customers to perform non-disruptive DR Tests at any time without the need to roll back the DR solution after the test. Site Recovery Test Failovers mimic actual failover conditions and can be isolated to a separate test network. Test failovers can also be run for as long as required.
3. The resiliency and redundancy built into Azure far exceeds what most customers and hosting providers can provide in their own datacenters.
4. Site Recovery "Recovery Plans" allow customers to orchestrate sequenced DR failover / failback procedures or runbooks, giving you the ability to achieve true Application DR.
5. Azure Site Recovery is a heterogeneous solution and works with Windows and Linux VMs, supports VMware and Hyper-V and works well with a range of database solutions.
6. Azure Site Recovery has been tested with many SAP NetWeaver and non-NetWeaver applications.

# 2. Purpose of this Document

This document does not replace the existing Azure Site Recovery documentation. Prior to implementing Azure Site Recovery, it recommended to fully review the Site Recovery documentation for the scenario(s) proposed.

This document details how you can use implement a DR solution using Azure Site Recovery for the following scenarios:

- SAP systems running in one Azure datacenter replicating to another Azure datacenter (Azure-to-Azure DR), as architected here.
- SAP systems running on VMWare (or Physical) servers on-premises replicating to a DR site in an Azure datacenter (VMware-to-Azure DR), which requires some additional components as architected here.
- SAP systems running on Hyper-V on-premises replicating to a DR site in an Azure datacenter (Hyper-V-to-Azure DR), which requires some additional components as architected here.

# 3. Latest Updates & Feature Support

Since the first version of this documentation several new features and capabilities have been added to the Azure Site Recovery product. Always check the ASR Support Matrix for the latest support status here.

1. ASR A2A supports Windows 2016 + 2019, Suse 12.x (**select kernels only**), RHEL 7.5 and Oracle 7.x
2. ASR A2A supports target Availability Zones in another region (example ASR from HK to a specific Availability Zone in another region)
3. ASR supports Azure Disk Encryption ADE (A2A) on Windows VMs – Full Portal Experience
4. Replicating Linux VMs with ADE is not supported as at April 2019. Check the support matrix for the release of this feature
5. ASR A2A fully supports Accelerated Networking
6. SAP ASCS on Windows can be deployed without a shared disk - Shared disk clusters are quite complex for ASR to handle
7. ASR A2A has been tested with SIOS
8. ASR A2A has been tested with SoFS/S2D
9. Transcontinental ASR A2A – example Primary in Australia and DR site in USA West or Primary in Amsterdam and DR in USA West – ask your Microsoft technical resource for more information
10. Support for iSCSI disks for Linux VMs

More news and updates about feature support can be found here.

# 4. Moving from On-premises to Azure

You can use Azure Site Recovery to migrate VMs and physical servers to Azure, so that users can access them as Azure VMs. Migration entails replication, and failover from the primary site to Azure, and a complete migration gesture as detailed here.

With Site Recovery you can:

- Migrate workloads running on on-premises Hyper-V VMs, VMware VMs, and physical servers, to run on Azure VMs.
- Migrate Azure IaaS VMs between Azure regions.
- Migrate AWS Windows instances to Azure IaaS VMs.

SAP also provides safe, fast and well documented tools for copying SAP systems from source infrastructure to a new target infrastructure. The SAP Homogeneous (no change of OS and/or DB) and SAP Heterogeneous (change of OS and/or DB) system copy procedure is documented here. It is now common for SAP customer to retire UNIX based servers and move to Azure using the SAP Heterogeneous System Copy procedure.

SAP customers moving from on-premises to Azure can do so via the Homogeneous or Heterogeneous SAP System Copy procedure. Often this is combined with changing the DBMS and/or updating to the latest OS, DBMS and SAP kernels. The SAP System Copy procedure also allows a customer to consolidate, re-architect HA/DR and cost optimize infrastructure during a migration to Azure.
At the time of writing (April 2019) using ASR to move shared disk cluster based ASCS VMs is not possible.

The table below compares using ASR and the SAP System Copy process functionalities

| | ASR Replication | SAP System Copy | Comment |
|---|---|---|---|
| Update to Latest Supported Operating System | NO | YES | ASR will copy "as is". SAP System copy allows change |
| Update to Latest Supported DBMS + Patch | NO | YES | ASR will copy "as is". SAP System copy allows change |
| Change OS and/or DB | NO | YES | ASR will copy "as is". SAP System copy allows change |
| Supports Migrating UNIX or Mainframe system to Azure | NO | YES | SAP System copy handles proprietary UNIX platforms and conversion from big endian OS |
| Migrate to Hana | NO | YES – with DMO | ASR will copy "as is". SAP System copy allows change |
| Upgrade SAP Release | NO | YES – with DMO | ASR will copy "as is". SAP System copy allows change |
| Update to Latest SAP Kernel | NO | YES | ASR will copy "as is". SAP System copy allows change |
| Restructure Disk Configuration | NO | YES | Optimize for Azure disk designs |
| Restructure HA/DR Solution | NO | YES | Can change from 2-tier to 3-tier |
| Infrastructure Team can handle complete project | YES | NO | SAP System Copy process has the disadvantage of requiring a deep SAP skillset |
| Project can be completed in a weekend | YES | YES | <20TB single DB size SAP systems can be moved in a weekend via either ASR or SAP System Copy process |

# 5. Block Diagram of Typical SAP Application Deployments

Large SAP customers usually deploy between 6 to 20 individual SAP applications. Most of these applications are based on the SAP NetWeaver ABAP or Java engines. Supporting these core NetWeaver applications are many smaller specific non-NetWeaver SAP standalone engines and typically some non-SAP applications.

It is critical to inventory all the SAP applications running in a landscape and to determine the deployment mode (either 2-tier or 3-tier), versions, patches, sizes, churn rates and disk persistence requirements. After collecting accurate information, the appropriate DR tool can be deployed as suggested below.

## Database Layer

The SAP Database persistence layer should be protected via the native DBMS tools such as SQL Server AlwaysOn, Oracle DataGuard or Hana System Replication.

## ASCS Layer

The SAP Single Point of Failure (SPOF) is called the Central Services components. For ABAP systems, the SPOF is called "ASCS" and for Java based systems it is called "SCS".

The Central Services can either be installed on a standalone single server. This configuration is called a "Distributed Installation". Depending on the SLA of the SAP systems, sometimes a Distributed System and the Azure Single VM SLA of 99.9% is sufficient.

If the Central Services are made highly available using operating system level clustering this is called a "High Available Installation". Until recently the Central Services deployment required a Cluster Shared Disk. Azure does not natively support Cluster Shared Disks. To present a Cluster Shared Disk a 3rd party tool such as SIOS. The setup and configuration of SIOS is documented here.

> Recently SAP has removed the requirement for a shared disk and replaced this with a **File Share Cluster ASCS**. Instead of using a Shared Disk a UNC File Share is used. Check this blog for more information about the availability of the File Share Cluster ASCS.

## Application Layer

There can be between one and up to 20-30 SAP Application Servers on large systems. SAP application servers have little disk IO and are easily replicable with Azure Site Recovery. SAP Application servers must never be used as file server or for storing interface files as this creates security and performance problems.

## Client Layer

The third tier in the 3-tier client server model is the client. The client layer is not protected by Azure Site Recovery, but it is important to consider topics that impact this layer such as DNS Propagation delay, security, single sign on and remote access to the DR datacenter

## SAP Non-NetWeaver Based Standalone SAP Engines and Gateways

Many SAP solutions depend on non-NetWeaver based engines and gateways. Common examples of these are Business Objects, TREX, Livecache, Content Server or WebDispatcher

## Non-SAP Applications

Most SAP customers require at least some non-SAP applications to run common business processes. Examples include payment gateways, a file server for interface file or SAP TMS transport files, custom developed Web Frontend applications or External Customer Facing portals. These applications must be part of the overall SAP Azure Site Recovery implementation as the business process is not complete without this capability.

## SAP 3-Tier vs. SAP 2-Tier Systems

3-Tier SAP Systems are recommended for Azure Site Recovery with the following considerations:

1. Strictly 3-tier systems with no critical SAP software installed on the DBMS server
2. Replication of the DBMS layer by the native DBMS replication tool (such as SQL Server AlwaysOn or HSR).
3. SAP Application Server layer is replicated by Azure Site Recovery.
4. ASCS layer can be replicated by Azure Site Recovery in most scenarios.
5. Non-NetWeaver and non-SAP applications need to be assessed on a case by case basis to determine if they are suitable for replication by Azure Site Recovery or some other mechanism.
6. Only Azure Resource Manager is supported for SAP systems using Site Recovery for DR purposes.

> Note: SAP Host Monitoring agents are not considered critical and may be installed on a 3-tier DBMS server.

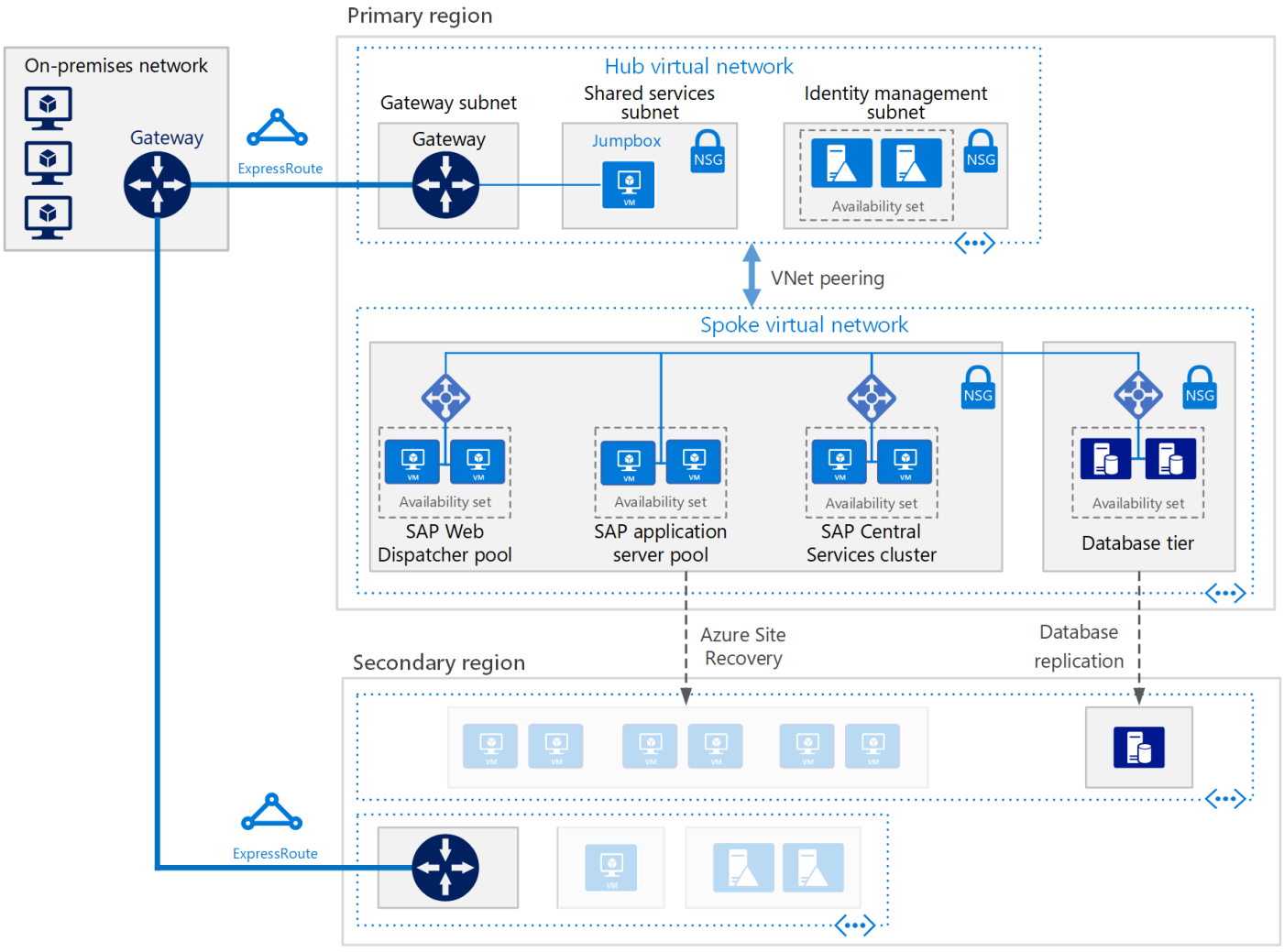
The use of Azure Site Recovery for a 2-tier SAP system needs to be analyzed on a case by case basis. Customers evaluating considering using Azure Site Recovery to replicate a 2-tier SAP system, or a Standalone engine with a file system dependency (such as TREX) should test extensively. If required, a SAP system can be changed from 2-tier to 3-tier using the SAP System Copy procedure

## 7. Example Azure-2-Azure Deployment

In the diagram below the Azure Site Recovery Azure-to-Azure DR scenario is depicted:

- The Primary Datacenter is in Singapore (Azure South-East Asia) and the DR datacenter is Hong Kong (Azure East Asia). In this scenario local High Availability is provided by having two VMs running SQL Server AlwaysOn in Synchronous mode in Singapore
- The File Share ASCS is used to provide HA for the SAP single points of failure (this does not require a cluster shared disk and SIOS is not required)
- DR protection for the DBMS layer is achieved using Asynchronous replication
- This scenario shows "symmetrical DR" – a term used to describe a DR solution that is an exact replica of production, therefore the DR SQL Server solution has local High Availability. The use of symmetrical DR is not mandatory, and many customers leverage the flexibility of cloud deployments to build a local High Availability Node quickly after a DR event
- The diagram depicts the SAP NetWeaver ASCS and Application server layer replicated by Azure Site Recovery

Note: SAP now supports deploying the ASCS without the requirement to have a shared disk (called SAP ASCS File Share Cluster). Azure Site Recovery also supports SIOS Shared Cluster Disks




More information on the setup and configuration of Azure cross DC networking and Windows clustering and Quorum calculation can be found in these sites:

- https://aka.ms/saponazureblog
- https://docs.microsoft.com/en-us/azure/virtual-machines/workloads/sap/get-started

# 8. Required Foundation Services

This documentation, internal testing and existing customers have all been deployed with the following foundation services deployed:

- ExpressRoute or Site-2-Site VPN
- At least one Active Directory Domain Controller and DNS server running in Azure
- At least one Management Station running on a small low cost VM

It is strongly recommended to ensure the infrastructure above is established prior to deploying Azure Site Recovery

# 9. Azure Site Recovery Deployment Considerations

## Application consistent recovery point

A recovery point is application consistent if, in addition to being write-order consistent, running applications complete all their operations and flush their buffers to disk (application quiescing). Application consistent recovery points can be used if Azure Site Recovery is used to protect DBMS type applications such as SQL Server or Oracle. For SAP applications, it is recommended to use the native DBMS tools (such as AlwaysOn or HSR).

Application consistent recovery points are recommended for all application workloads and guarantee that all disks attached to a single VM are failed over at precisely the same instant of time. This is achieved using the Windows Volume Snap Shot service (and similar on Linux). There is a small performance impact if there is a very high rate of data change on the underlying disks. In all cases it is recommended to test application consistent recovery points carefully with SAP applications such as TREX, Content Server and Business Objects.

## Recovery Group Structure

One SAP application per Recovery Group is generally recommended. For example, it is recommended to create a Recovery Group for SAP ECC and another separate Recovery Group for SAP BW. Each Recovery Group can have its own configuration and own Recovery Plan. DR testing with the ASR "Test Failover" functionality is simpler and easier with individual Recovery Plans per SAP application.

Individual Recovery Plans also allow failover of a specific SAP application if needed without impacting other SAP applications. For example. the BW application could be moved to DR and all other SAP applications remain untouched. In event of a total datacenter failure, multiple Recovery Plans would need to be run to failover all systems.

## Preservation of IP Address after Failover to DR Site

SAP applications, gateways, standalone components and external RFC or HTTP calls should all be configured to connect to hostnames. It is strongly advised not to configure connectivity directly to IP addresses.

Users and RFC or Web connections will be made to the ASCS or SCS and then load balanced (SMLG) to the optimal SAP application server. The only hostname that end user PCs need to resolve to an IP address is the IP address of the SAP Central Services. SAP end users never connect directly to the database server and should not directly logon to SAP application servers

It is strongly recommended to review the Software Provisioning Manager 1.0 documentation. High Availability concepts are explained in detail. SWPM documentation and the tool can be download here.

Azure VMs are provisioned after a failover, by default, with a DHCP address. If required, static IP can be assigned by script after failover or manually configured under the "Compute and Network -> Network Interface Card" menu in the Recovery Vault setting for the virtual machine. It is strongly recommended to plan networking design for on-premises VM and Azure VM DR as the case may be.

Discussion on DNS propagation delay can be found here.

## Setup of Internal Load Balancer in DR Location

All clustered Virtual Machines replicated with Azure Site Recovery require the setup of an ILB. If more than one virtual IP address is configured, the script contained in this article can be used. This script can be incorporated as an automation step in the Recovery Plan as detailed here. The ILB may also be created in advance on a specific vNet provided static IP addresses are configured for the ASCS and/or DBMS VMs

Information on high availability for SAP NetWeaver on Azure VMs can be found here.

## Non-Production Test Landscape

SAP change management procedures should be followed when deploying Azure Site Recovery. Deploying the Site Recovery agents onto a non-production system is recommended prior to deploying on production. Often non-production SAP environments (such as Dev or QAS) may not be 3-tier. This limits the usefulness of testing on these environments.

There are several options for Site Recovery agent deployment depending on the non-production configuration:

- Deploy on Dev, QAS and Production – Dev & QAS may be 2-tier, therefore this is not a useful test.
- Deploy on Prod directly without testing on non-prod – not recommended.
- Deploy on a non-Prod 3-tier system – some customers have a pre-production 3-tier non-prod system.
- Deploy on a "mock" 3-tier copy of production system – especially for the Azure-to-Azure DR scenario, it is possible to create a temporary environment that logically resembles production.

## Azure Resource Manager vs. ASM Classic for SAP on Azure with Azure Site Recovery

ARM deployments have been the default pattern for SAP customers for some time. ARM offers new features, capabilities and advantages that are unavailable in ASM. Multiple customers have migrated their ASM deployments to ARM. Therefore only ARM deployments are documented in this guide

## Resource Group Structure

One possible option is to place all the Azure Site Recovery objects into a single Resource Group dedicated for DR allows an organization to quickly and easily calculate the cost of operating a DR solution. Alternatively, customers can use tagging to calculate the cost of DR.

## Supported Configurations (frequently updated)

The support of new operating systems, features such as Windows ReFS, Managed Disks and Advanced Disk Encryption (ADE) are all documented centrally in the Azure Site Recovery Support Matrix.

Please check the support matrix for On-premises-to-Azure and Azure-to-Azure scenarios regularly as this information is continuously updated.

## Installation and Configuration of Host Monitoring Agent

SAP applications running on Azure VMs are only supported if the SAP Host Monitoring Agents are installed as described in Note 2015553 – SAP on Microsoft Azure: Support Requirements.

After an Azure-to-Azure failover, the Host Monitoring Agent may stop working. Running the script again will resolve the problem.

## SAP Landscape Inventory & Deployment Analysis

After reviewing the latest SAP on Azure and Azure Site Recovery documentation, create an inventory of all the SAP applications, including details of any 2-tier SAP NetWeaver systems, standalone engines (such as Content Server or TREX) and any critical non-SAP applications integrated with the SAP landscape.

The inventory should contain information such as:

- OS & DB versions and patches
- Cluster configuration
- Internal Load Balancer configuration
- NSG configuration
- Resource Group
- Availability Set configuration
- 2-tier vs. 3-tier configuration
- Disk size and disk configuration*
- DBMS size, replication tool and configuration
- DBMS encryption configuration (if used)
- Scripting requirements (such as Azure Automation scripts to create ILB or update DNS entries)
- Planned Recovery Group structure
- Features that need to be checked on the support matrix such as ReFS, Managed Disks, Storage Spaces, SIOS and ADE Disk Encryption
- Standalone Engine versions and details and non-SAP applications

After collecting all this information, perform an analysis to determine which replication technology and tools to use and the support status of all components. If unsure about the support status of SAP specific components open an OSS Message to BC-OP-NT-AZR.

> Implementing Azure Site Recovery is a mini project and should have a Technical Design Document. Customers that follow the detailed process in this guide, inventory their current landscape and build a good quality Technical Design Document are welcome to contact the authors of this document for review

Determine a deployment plan for the Azure Site Recovery solution and identify a non-production infrastructure that is a logical replica of production environment. Also formulate a testing plan for each component such as DBMS, ASCS, Application Server, 2-tier system, standalone engine and non-SAP application.

*There are two competing points of view around disk configuration for SAP application servers
Option 1. Provision a small disk for the boot disk. Place the swapfile onto the non-persistent disk. Provision another additional disk for /usr/sap/<SID>
Option 2. Increase the size of the boot disk to 128GB or more. Place the swapfile onto the non-persistent disk. Boot, OS and /usr/sap/<SID> are all on the same disk. There are no additional disks. The VM has only a single large boot disk
Either Option 1 or 2 can be deployed.
Those in favor of Option 1 consider this solution less likely to run out of space on the OS disk and is similar to what is done on-premises today
Those in favor of Option 2 observe SAP application servers are very unlikely to fill up 128GB disk and that the simplest solution is typically the best and most reliable, especially when replicating VMs
Azure VM boot disks can be up to 1TB and have many thousands of IOPS.

## 10. Support Matrix for SAP on Azure Guest Operating Systems

The most up to date information is contained in SAP Note 1928533 – SAP Applications on Azure: Supported Products and Azure VM types
As of April 2019, the following Operating Systems are supported by SAP on Azure:

- Microsoft Windows Server 2008 R2, 2012 (R2), 2016 & 2019
- SUSE Linux Enterprise Server 12 (SLES12)
- SUSE SLES for SAP Applications (based on SLES12)
- Red Hat Enterprise Linux 7 (RHEL7)
- Red Hat RHEL for SAP (based on RHEL7)
- Red Hat RHEL for SAP HANA (based on RHEL7)

Windows versions Windows 2016 and Windows 2019 are recommended for SAP deployments either on-premises or Azure.
Suse 11.x and Redhat 6.x are not supported on Azure due to security and support reasons.
New OS support and features are being continuously added to Azure Site Recovery. Please check the Site Recovery support matrix for On-premises-to-Azure and Azure-to-Azure scenarios regularly as this information is continuously updated.

## 11. Protecting SAP Systems: Azure to Azure Scenario

### Planning and Preparation

Review the SAP on Azure documentation to confirm the latest support and certification information
https://docs.microsoft.com/en-us/azure/virtual-machines/workloads/sap/get-started

Review the Azure Site Recovery A2A documentation and support matrix
https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-azure-to-azure
https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-support-matrix-azure-to-azure

### Deployment & Testing

Follow the ASR A2A documentation to protect (A)SCS and SAP NetWeaver Application servers on 3-tier SAP systems.

If SAP standalone applications and non-SAP application can leverage the ASR A2A toolset then deploy the agents onto these VMs. Configure application consistent snapshots on non-NetWeaver applications that have filesystem dependencies.

Protect DBMS workloads with the native DBMS replication technology (such as AlwaysOn, Dataguard or Hana System Replication)

It is generally recommended to configure Application Consistent Snapshot = 0 for SAP application servers with only one disk. This is the simplest and fastest recommended configuration.
2-tier systems, SAP standalone engines and non-SAP applications need to be assessed and tested on case-by-case basis
https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-create-recovery-plans
https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-runbook-automation

Failover documentation
https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-test-failover-to-azure
https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-how-to-reprotect-azure-to-azure

### Troubleshooting & Monitoring

ASR provides the capability to generate email alerts if a VM is unprotected or when Recovery Plans finish

https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-azure-to-azure-troubleshoot-errors

## 12. Protecting SAP Systems: VMWare to Azure Scenario

Review the documentation in these links:
https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-vmware-to-azure

https://blogs.msdn.microsoft.com/saponsqlserver/2016/05/06/protecting-sap-systems-running-on-vmware-with-azure-site-recovery/

Updated documentation with a flow chart can be found here: https://docs.microsoft.com/en-us/azure/site-recovery/vmware-walkthrough-overview

It recommended to review these SAP Notes
2229228 VMware vSphere 6.0: possible data corruption
2447884 VMware vSphere with VMware Tools 9.10.0 up to 10.1.5: Performance Degradation on Windows
2381942 Virtual Machines Hanging with VMware ESXi 5.5 p08 and p09
2293740 Performance degradation due to high network latency with vSphere 6

### Planning and Preparation

https://docs.microsoft.com/en-us/azure/site-recovery/vmware-walkthrough-overview#step-2-review-prerequisites

### Setup and Initial Replication

Follow the ASR V2A documentation to protect (A)SCS and SAP NetWeaver Application servers on 3-tier SAP systems.

If SAP standalone applications and non-SAP application can leverage the ASR V2A toolset then deploy the agents onto these VMs. Configure application consistent snapshots on non-NetWeaver applications that have filesystem dependencies.

Protect DBMS workloads with the native DBMS replication technology (such as AlwaysOn or Log Shipping for SQL Server)

It is generally recommended to configure Application Consistent Snapshot = 0 for SAP application servers with only one disk. This is the simplest and fastest recommended configuration.
2-tier systems, SAP standalone engines and non-SAP applications need to be assessed and tested on case-by-case basis
https://docs.microsoft.com/en-us/azure/site-recovery/vmware-walkthrough-enable-replication

### Setup Recovery Plan

Recovery plan documentation is detailed here

https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-create-recovery-plans

### Test Failover Procedure

https://docs.microsoft.com/en-us/azure/site-recovery/vmware-walkthrough-test-failover

### Failback procedure

https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-failback-azure-to-vmware

Troubleshooting and Monitoring

https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-vmware-to-azure-protection-troubleshoot

## 13. Protecting SAP Systems: Windows Hyper-V to Azure Scenario

SAP applications running on Hyper-V can be replicated to Azure using the Host based replication technology built into Hyper-V.

Replication of shared disk clusters with Hyper-V to Azure ASR are difficult and complex to setup. It is recommended to use the File Share Cluster ASCS solution if a Highly Available ASCS is required.

Follow the existing links and documentation

### Planning and Preparation

Azure Site Recovery for Hyper-V has two deployment options:

1. Hyper-V replication to Azure – with System Center Virtual Machine Manager

https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-vmm-to-azure

2. Hyper-V replication to Azure – without System Center Virtual Machine Manager

https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-hyper-v-site-to-azure

Additional links are listed below:

Setup and replication is documented in this link

https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-vmm-to-azure#enable-replication
https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-create-recovery-plans
https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-test-failover-to-azure

# Appendix

## 14. Frequently Asked Questions

**Q1. Is Azure Site Recovery supported for 2-tier SAP NetWeaver systems?**
A1. It is generally recommended to convert SAP 2-tier systems to 3-tier using the SAP System Copy procedure. Converting from 2-tier to 3-tier is simple, safe and quick using the latest SWPM tool and System Copy Guide.

**Q2. How much network bandwidth is required?**
A2. Bandwidth requirements depend very heavily on the daily data churn of the protected VMs. Identify your daily change (churn) rate for replicated data. To do this:

- If you're replicating Hyper-V VMs, then download the Hyper-V capacity planning tool to get the change rate. Learn more about this tool. We recommend you run this tool over a week to capture averages.
- If you're replicating VMware virtual machines, use the Azure Site Recovery Deployment Planner to figure out the churn rate.
- If you're replicating physical servers, you need to estimate manually.

**Q3. Which Azure VM types are supported for SAP NetWeaver applications?**
A3. Review SAP Note 1928533 – SAP Applications on Azure: Supported Products and Azure VM types

**Q4. Is encryption of the DBMS mandatory on Azure?**
A4. No, there is no requirement to encrypt the DBMS. Many customers running SQL Server choose to use SQL Server TDE because there is a simple and easy integration to Azure Key Vault. More information is linked here:
More Questions From Customers About SQL Server Transparent Data Encryption – TDE + Azure Key Vault
Customers running Hana or other DBMS are advised to evaluate using DB and Backup encryption

**Q5. How to assess if a non-SAP application or SAP standalone application such as TREX will work with ASR?**
A5. Each application needs to be analyzed and tested individually. There are many factors that influence if an application will failover consistently. These factors include:

- Specific details about each application and version
- Operating system and version
- DBMS and version
- Disk layout (example if all files are stored on one disk failover is consistent, but if files are spread across multiple disks the application might become corrupted)
- Churn rate on the disk(s)

In all cases it is strongly recommended to do extensive testing on applications that need file system level consistency. ASR allows test failovers even during peak load periods.

**Q6. What is the difference between an Application Consistent recovery point and a non-Application Consistent recovery point?**
A6. App-consistent snapshots are taken at the "app-consistent snapshot frequency" set in replication policy. The minimum possible frequency is "1 hour". The default setting is 4 hours for Azure-to-Azure replication. (You can change it in "Vault -> Settings -> Site Recovery infrastructure -> For Azure VMs -> Replication policy -> Select policy -> Change the app consistent snapshot frequency -> Save".)
Crash consistent snapshots are generated every few minutes. The replication itself is continuous and hence your RPO will be in the order of minutes (and not tied with any specific setting).

**More details on Crash consistency and app consistency**
**Crash consistent recovery point** - A recovery point is crash consistent if all of the interrelated data components are as they were (write-order consistent) at the instant the recovery point is created. To better understand this type of consistency, imagine the status of the data on your PC's hard drive after a power outage or similar event. A crash-consistent recovery point is usually sufficient if your application is designed to recover from a crash without any data inconsistencies.

**Application consistent recovery point** - A recovery point is application consistent if, in addition to being write-order consistent, running applications complete all their operations and flush their buffers to disk (application quiescing). Application-consistent recovery points are recommended for database applications such as SQL, Oracle, and Exchange.

**Q7. Does Azure-to-Azure DR support replication across different Azure subscriptions?**
A7. Yes

**Q8. What are the networking requirements for using Azure Site Recovery?**
A8. Refer to the Site Recovery guidance to plan networking for Azure-to-Azure DR and On-premises-to-Azure DR.

**Q9. How to protect non-NetWeaver SAP software? How to determine if an application consistent snapshot is sufficient to guarantee a consistent failover?**
A9. If unsure about the support status of SAP specific components open an OSS Message to BC-OP-NT-AZR after collecting all this information about version, file system layout, disk sizes etc.

**Q10. Will the SAP License be valid after failover?**
A10. During failover the SAP License will likely become invalid. A temporary license may need to be applied immediately. After the system is running and the service is restored a permanent license can be applied.
SAP Note 2413104 - How to get a license key after the hardware exchange

**Q11. Does ASR Help Ensure Intra-System Database Consistency?**
A11. No. Customers are advised to exercise extreme care when activating a DR solution. It is not possible to provide specific guidance for all customers as each customer scenario varies greatly. Large Enterprise Customers should evaluate if the following scenario applies to them:

a. The SAP landscape is composed of 6-12 different applications such as S4, ECC, BW, PO, CRM, GRC, SCM, Enterprise Warehouse Management, Customer Activity Repository (CAR) etc
b. These SAP applications are deeply integrated into non-SAP applications such as 3rd party Warehouse Management solutions, Credit Card/payment gateways, DHL or FEDEX trace & trace, 3rd party custom developed solutions
c. Both SAP and non-SAP on-prem systems are also integrated to Software-as-a-Service (SaaS) type cloud applications that are not directly under the control of the DBA or system administrator (meaning it is not possible to restore the database and roll forward to a nominated point in time)
d. If the Primary Datacenter is in USA West and the DR is in USA East only Asynchronous DBMS level replication technologies may be used. It is impossible to use Synchronous DB replication tools at these distances due to the finite speed of light through fiber cables
e. Different SAP and non-SAP applications will have different transaction volumes. Busier Databases will have a higher RPO than idle Databases. For example an S4HANA system might be very busy and consequentially the DR Database replica might be 30 minutes behind Production but CAR might only be 10 minutes behind Production
f. If a large scale DR event was to occur and all SAP and non-SAP applications were started the application level integrity would be corrupted. The S4HANA system might be 30 minutes behind the BW system. The S4HANA system might also be 30 minutes behind the non-SAP Warehouse Management System. Orders, Stock levels, Financial Documents and Deliveries would be inconsistent between applications

Customers with complex interconnected applications are advised to create an application landscape diagram and analyze the dependencies between SAP, non-SAP and SaaS or externally managed applications. Identify high priority interfaces such as those related to stock levels in a warehouse (eg. between S4 and a 3rd party WMS). It may be possible to create reconciliation programs or procedures to handle such situations.
Other customers ship full and log backups to their DR sites. If a DR event was to occur SAP and non-SAP databases are restored and roll forward to a common point in time.

It is highly recommended that customers carefully read and review these two SAP Notes
[434645 - Point-in-time recovery: What must I be aware of?]
[434647 - Point-in-time recovery in an SAP system group]
These notes explain that restoring SAP databases to different points in time is very dangerous and should generally be avoided.

| Option | PIT Variants | RESET Status | Inconsistencies | Data loss |
|---|---|---|---|---|
| 1 | Point-in-time recovery only in the affected system | only the affected system is reset to a previous version. | the number of inconsistencies is at its highest | the amount of data lost is restricted to one system. It may be possible to recover the missing data from the data in the other components/databases |
| 2 | Point-in-time recovery for all components that are part of the SAP system landscape | All SAP components in the landscape are reset to the same version | If the system clocks on all SAP servers are synchronized the SAP landscape will be consistent. Application inconsistencies between SAP and non-SAP applications very likely | The amount of data lost is higher than in the first variant and there is no option to restore the data from the other components. |
| 3 | Restore a consistent backup of the entire SAP and non-SAP landscape (if this exists) | All SAP and non-SAP components in the landscape are reset to the same version | no inconsistencies exist between SAP and non-SAP applications. External SaaS applications and physical inventory may be inconsistent | The restore point must be the "lowest common denominator"; meaning the restore point is determined by the system with the highest RPO loss. Therefore the amount of data lost is greatest in this variant |

## 15. High-level Steps for a Test Failover for Azure-to-Azure DR

The steps listed below give a high-level procedure for conducting a Test Failover with Azure Site Recovery.
In this test example, the OS and DB are Windows 2016 and SQL Server 2016, but the same or similar steps apply to other OS and DB combinations.

The following infrastructure is deployed:

- Medium size ECC 6.0 EHP 8, BW 7.5, PO 7.5, Solman 7.2 and BusinessObjects 4.2 landscape is protected using ASR. All systems run Windows 2016 & SQL Server 2016
- Primary DC is Europe West. DR DC is Europe North West
- A ExpressRoute, VPN or Global Peered gateway has been created from EU West to EU North West. SQL Server is replicating the databases across this network
- There is a single 2 node File Share Cluster for the ASCS. ECC, BW, PO and Solman run their (A)SCS on this cluster with different system numbers (00, 01, 02 etc) and different virtual IP and virtual Hostnames
- ASR agents have been installed on the SAP application servers and the ASCS cluster. Each SAP application has 2 application server VMs. The VMs are replicated to EU North West, but as they are in synchronization mode they are shutdown (no compute costs)
- There is one AD/DNS server in EU North West A2 VMs running 24 x 7. To secure the AD server in Azure the boot and data disks have been encrypted with ADE (thus preventing unauthorized cloning of a Domain Controller)
- The DB VMs in Production are DS15v2 for ECC and BW. Others SAP applications use DS13v2 as DB servers
- The DB VMs in DR are much smaller DS12v2 (these will be increased if there is a failover DR). These VMs run 24x7
- SQL Server is configured to backup off the AlwaysOn secondary replica in the DR datacenter to URL each night. Transaction log backups are configured to backup off the DR replica to URL every 5 minutes
- Monitoring of the DR solution is via the AlwaysOn dashboard and Azure Portal for ASR
- There is a Management server in Production with SAPGUI and other SAP client software installed. Interface and Transport Directories are located on this small A2 server. The Management Server is protected with ASR
- The SAP Basis team have Azure RBAC access to do all the Azure tasks they need
- There is a single Resource Group for DR so all costs of the DR solution are transparent including Testing Costs

On Tuesday morning at 11am the Datacenter Manager does a "surprise test" and asks the SAP Basis and Server team to do a full DR test. The Basis and Server team cooperate on the following tasks:

- SAP Basis and Server team request written confirmation to involve a Test DR from Management
- A Test vNet with no external connectivity is created. This will prevent problems with duplicate Windows hostnames and prevent SAP from sending purchase orders or printing delivery notes from the DR Test system
- Clone the AD Domain Controller and copy to the Test vNet (requires ADE key)

- Run a Test Failover Recovery Plan to failover the management server. Assign an external IP to this VM. RDP to the Management Station

These are extra steps required in a Test Failover scenario. The DB servers are already existing in case of a "real" DR event.

- Run a Recovery Plan called zBuild_Test_DB_Servers-1. This Recovery Plan has an Azure Automation script to provision DS15v2 and DS13v2 VMs from a pre-created custom gallery image.
- *Run zBuild_Test_DB_Servers-2 – this script does a SQL Restore from the previous full backup (URL – key is required)
- *Run zBuild_Test_DB_Servers-3 – this script does a SQL Restore of all current transaction logs (URL – key is required)
- Run zBuild_Test_DB_Servers-4 – this script ensures the databases are online, recovered, single node AlwaysOn AG created, ILB created for the Listener vIP and creates the users/schema as needed

- In the Azure Portal select the Recovery Plan for Combined (A)SCS and press "Test Failover". Select the Test vNet created earlier and select Lowest RTO. (Recovery plan also creates the ILB and assigns vIP)
- In the Azure Portal select the Recovery Plan for ECC 6.0 EHP 8 and press "Test Failover". Select the Test vNet created earlier and select Lowest RTO.
- Repeat for all the SAP applications
- Run a Recovery Plan called zStart_SAP_All – this will start all the SAP application servers (the SAP (A)SCS have been defaulted to autostart in their instance profiles and cluster admin) or alternatively start each SAP application manually
- Use the Management server to test connectivity and functionality
- When testing is complete continue the Recovery Plans and Cleanup the ASR resources
- Run a script to shutdown and delete the DB servers
- Delete the Test vNet (ILBs will be deleted)

*Note: it is recommended to do a restore and log roll forward to fully test and prove the backup/restore process. If a shorter RTO is required consider using SQL Server Snapshot Backups on the AlwaysOn secondary

## 16. SAP Notes

Following is a list of useful SAP Notes for various requirements:

License key related
94998 – Requesting license keys and deleting systems
607141 – License key request for SAP J2EE Engine
870871 – License key installation
1288121 – How to download temporary license keys for Analytics Solutions from SAP (BusinessObjects)
1644792 – License key/installation of SAP HANA
2035875 – Windows on Microsoft Azure: Adaption of your SAP License
2036825 – How to Get an Emergency Key from SAP
2413104 – How to get a license key after the hardware exchange

Supported scenarios
1380654 – SAP support in public cloud environments
1928533 – SAP Applications on Azure: Supported Products and Azure VM types
2015553 – SAP on Microsoft Azure: Support prerequisites
2039619 – SAP Applications on Microsoft Azure using the Oracle Database: Supported Products and Versions

Setup and installation
1634991 – How to install (A)SCS instance on more than 2 cluster nodes
2056228 – How to set up disaster recovery for SAP BusinessObjects

Troubleshooting
1999351 – Troubleshooting Enhanced Azure Monitoring for SAP

## 17. Microsoft Links & KB Articles

https://aka.ms/saponazureblog
https://azure.microsoft.com/en-us/blog/tag/azure-site-recovery/