

|  |
| --- |
| SAP NetWeaver: Building a Hyper-V & Microsoft Azure–based Disaster Recovery Solution |
| This document provides a step-by-step guidance for building a disaster recovery solution, based on  Microsoft Hyper-V and Microsoft Azure technologies. |

Version: 1.5

Date of Last Change: August 13, 2015



Authors

Cameron Gardiner, Senior Program Manager, Microsoft Azure CAT

Anoob Backer, Program Manager, Microsoft Azure Site Recovery Services Development IDC

Technical Reviewers

Juergen Thomas, Principal Lead Program Manager, Microsoft Azure CAT

Hermann Daeubler, Senior Program Manager, Microsoft Azure CAT

Troy Shane, Microsoft-SAP Technology Center

Contents

[1 Overview 3](#_Toc427234249)

[1.1 Introducing Azure Site Recovery 3](#_Toc427234250)

[1.2 How to use this document 4](#_Toc427234251)

[1.3 Before you start 4](#_Toc427234252)

[2 Topology 6](#_Toc427234253)

[2.1 Site-to-site virtual private network (VPN) device or ExpressRoute 6](#_Toc427234254)

[2.2 System Center Virtual Machine Manager 6](#_Toc427234255)

[2.3 Active Directory Directory Services and domain name system (DNS) 6](#_Toc427234256)

[2.4 SQL Server and other DBMS 6](#_Toc427234257)

[3 Azure Site Recovery requirements 8](#_Toc427234258)

[3.1 Active Directory 8](#_Toc427234259)

[3.2 System Center 2012 R2 8](#_Toc427234260)

[3.3 Unsupported configurations 8](#_Toc427234261)

[3.4 Agents 9](#_Toc427234262)

[3.4.1 Azure Site Recovery Provider 9](#_Toc427234263)

[3.4.2 Azure Recovery Services Agent 9](#_Toc427234264)

[4 Protecting SAP application layers 12](#_Toc427234265)

[4.1 SAP database layer 12](#_Toc427234266)

[4.2 SAP application server layer 12](#_Toc427234267)

[4.3 SAP SPOF layer (ASCS) 13](#_Toc427234268)

[4.3.1 Emulating the on-premises ASCS 13](#_Toc427234269)

[4.3.2 Testing failover 14](#_Toc427234270)

[4.4 SAP stand-alone layer 16](#_Toc427234271)

[5 Implementation checklists 17](#_Toc427234272)

[5.1 Important blogs and articles 17](#_Toc427234273)

[5.1.1 Important blogs 17](#_Toc427234274)

[5.1.2 Important KB articles 17](#_Toc427234275)

[5.1.3 Recommended software versions and updates 17](#_Toc427234276)

[5.2 Capacity planning and readiness assessment 18](#_Toc427234277)

[5.3 Implementation checklist 19](#_Toc427234278)

[6 Testing Azure Site Recovery Solution for SAP 21](#_Toc427234279)

[6.1 Network isolated failover scenario 21](#_Toc427234280)

[6.2 Network integrated failover scenario 22](#_Toc427234281)

[7 Monitoring, troubleshooting, and exceptional handling 23](#_Toc427234282)

[7.1 Monitoring 23](#_Toc427234283)

[7.2 Troubleshooting 23](#_Toc427234284)

[7.3 Exception handling 24](#_Toc427234285)

[8 Azure Site Recovery for VMware and Linux 26](#_Toc427234286)

[Appendix: Recommended resources 27](#_Toc427234287)

[Glossary 28](#_Toc427234288)

# Overview

To provide exceptional customer experiences, IT organizations must stay prepared. Downtime can represent a loss of revenue, employee productivity, and cash flow, in addition to fines and penalties. Downtime can even give competitors an opportunity to gain market share. Increasingly, the expectations of customers, employees, and other key stakeholders are put at risk if there are no DR plans in place to support critical computing workloads. Your organization’s success can depend on having DR plans that are properly tested at regular intervals—only then can you attest with confidence that your recovery plans will work reliably.

Yet planning and implementing a DR solution can be challenging. In many organizations, the budget for business continuity and disaster recovery (BCDR) is a small percentage of overall IT spending. In addition, data capacity requirements are growing, while the landscape of heterogeneous applications is gaining in complexity.

This document provides a step-by-step guidance for implementing a DR solution for SAP NetWeaver systems, based on Microsoft Azure and Microsoft Hyper-V technologies. The guidance offers principles but does not cover the whole procedure including auxiliary systems of a SAP landscape. Also, not all of the covered aspects are necessary for a DR exercise.

Microsoft Azure Cloud Services differ from other cloud platforms in the integration between your on-premises private cloud and the Azure public cloud platform. Microsoft Azure Site Recovery is the key to providing DR to Azure functionality. It can help you protect virtual machines (VMs) by coordinating the replication and recovery of private clouds to your own secondary site, to a hoster’s site, or to an Azure DR site.

## Introducing Azure Site Recovery

Azure Site Recovery provides disaster recovery as a service (DRaaS) in the following ways:

* On-premises to on-premises protection: You can recover your applications to your own second site or to a hoster’s site.

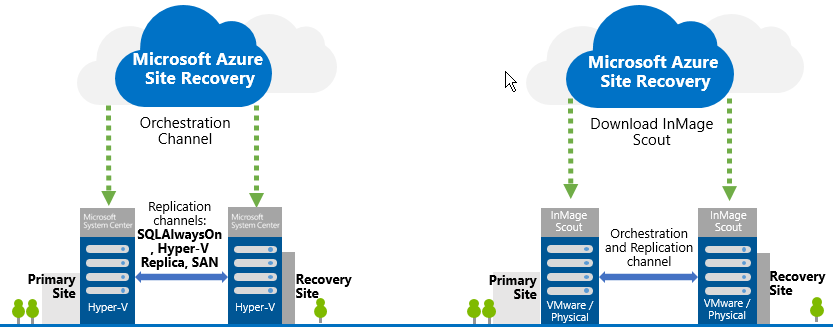


Figure 1. Using Azure Site Recovery for on-premises to on-premises protection.

* Migrate or protect to Azure: You can use Azure as your disaster recovery site and avoid the expense and complexity of building and managing your own secondary location, or you can engage a hoster to provide a DR site.

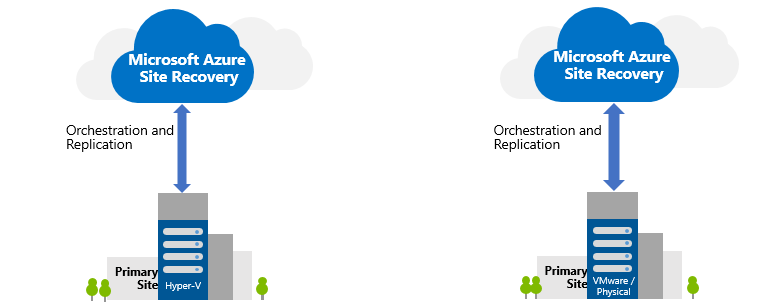


Figure 2. Using Azure Site Recovery to facilitate a disaster recovery site.

## How to use this document

This document describes the protection and recovery of an on-premises SAP application to Azure.

This document is intended for experienced SAP Basis administrators, Windows administrators, and database administrators. It assumes the following:

* A basic familiarity with the [Microsoft Azure Management Portal](https://manage.windowsazure.com/) (account required) at https://manage.windowsazure.com/.
* Working knowledge of Microsoft Hyper-V.
* Knowledge of how to set up and configure database-level replication technologies, such as SQL Server AlwaysOn. For more information, see [Overview of AlwaysOn Availability Groups (SQL Server)](http://msdn.microsoft.com/en-us/library/ff877884.aspx), at http://msdn.microsoft.com/en-us/library/ff877884.aspx.
* Detailed knowledge about the proxy server and user ID (if required) to authenticate and allow external Internet traffic.
* Basic SAP Basis knowledge.

## Before you start

This document is not intended to replace the existing documentation about installation and configuration of Azure Site Recovery. Before you start, we recommend that you:

* Test the deployment of Azure Site Recovery using a non-SAP test VM, before implementing Azure Site Recovery for a SAP landscape.
* Become familiar with the setup and operation of Azure Site Recovery on a non-SAP test VM, and practice tasks, such as planned and unplanned failovers.

The following guides are available for the topic of SAP deployments on Azure:

* SAP NetWeaver on Microsoft Azure Virtual Machine Services – Planning and Implementation Guide.
* SAP NetWeaver on Microsoft Azure Virtual Machine Services – Deployment Guide.
* DBMS Deployment Guide for SAP on Microsoft Azure Virtual Machine Services.
* SAP NetWeaver: Building a Microsoft Azure–based Disaster Recovery Solution.
* Clustering SAP ASCS Instance using Windows Server Failover Cluster on Azure with SIOS DataKeeper.

The guides can be downloaded under the section **SAP** at <http://go.microsoft.com/fwlink/p/?LinkId=397566>.

Before you proceed, for all SAP NetWeaver application servers and SAP NetWeaver Central Services (SCS) VMs, verify that the SAP applications are supported in Azure. For details, see the following:

* [1928533 – SAP Applications on Azure: Supported Products and Azure VM types](http://service.sap.com/sap/support/notes/1928533), on the SAP Service Marketplace (logon required), at <http://service.sap.com/sap/support/notes/1928533>.
* [2015553 – SAP on Microsoft Azure: Support Requirements](http://service.sap.com/sap/support/notes/2015553), on the SAP Service Marketplace (logon required), at <http://service.sap.com/sap/support/notes/2015553>.

NOTE For VMs containing SAP NetWeaver components, running in Azure, make sure that Azure Enhanced Monitoring for SAP is installed or gets installed. See [Running SAP Applications on the Microsoft Platform](http://blogs.msdn.com/b/saponsqlserver/archive/2014/06/24/azure-extended-monitoring-for-sap.aspx), on the Microsoft Servers and Tools Blog, at <http://blogs.msdn.com/b/saponsqlserver/archive/2014/06/24/azure-extended-monitoring-for-sap.aspx>.

# Topology

The following sections describe the key components you must deploy for protection and recovery. Figure 3 shows the datacentre-Azure topology.

## Site-to-site virtual private network (VPN) device or ExpressRoute

To operate hybrid/cross-premises or complete SAP landscapes between on-premises datacenters and Azure, transparent network connectivity is required to be established between your site(s) and Azure. You can do this through site-to-site connectivity using VPN devices, Windows Server 2012 R2, or Azure ExpressRoute.

The Microsoft Azure platform supports a very broad range of VPN devices. For more information, see [About VPN Devices for Virtual Network](http://msdn.microsoft.com/en-us/library/azure/jj156075.aspx), at <http://msdn.microsoft.com/en-us/library/azure/jj156075.aspx>. The Azure Portal can be used to generate a VPN configuration script.

A Windows 2012 R2 server can also function as an Azure VPN device. For more information, see [Azure Virtual Machine Services—Planning and Implementation Guide](http://go.microsoft.com/fwlink/p/?LinkId=397963), at <http://go.microsoft.com/fwlink/p/?LinkId=397963>.

For Azure ExpressRoute, you must find multiprotocol label switching (MPLS) providers or network providers that cover your region. For a list of current providers, see [ExpressRoute Technical Overview](http://msdn.microsoft.com/library/azure/dn606309.aspx), at <http://msdn.microsoft.com/library/azure/dn606309.aspx>.

## System Center Virtual Machine Manager

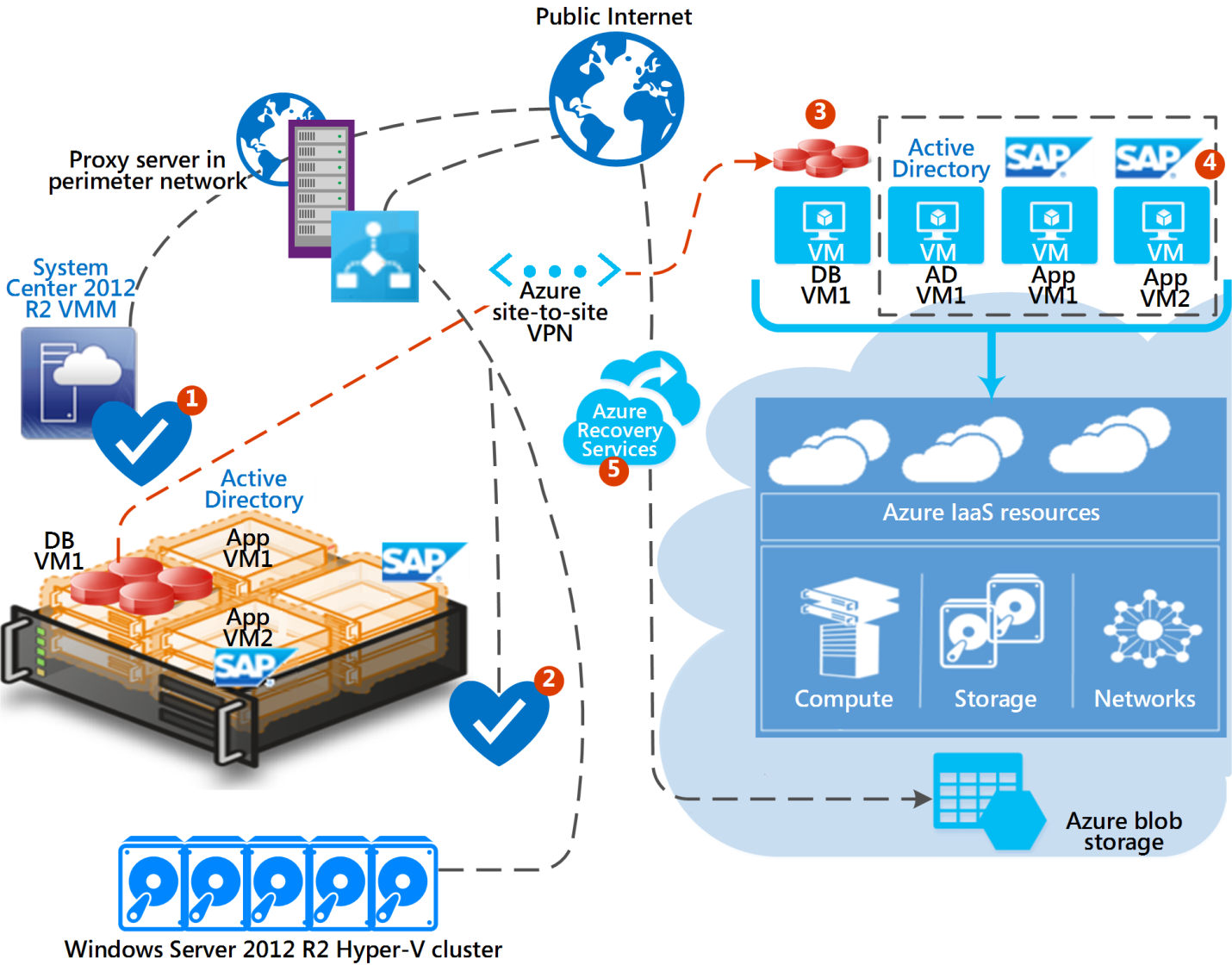
The Azure Site Recovery replication channel, based on Hyper-V, has an option to use System Center Virtual Machine Manager (SCVMM) to orchestrate the site recovery process. SCVMM 2012 is supported; however, the solution described in this document has been tested on SCVMM 2012 R2 with Update Rollup 3. SCVMM 2012 R2 [Rollup 6](https://support.microsoft.com/en-us/kb/3050317) is now released

## Active Directory Directory Services and domain name system (DNS)

Many business applications, including SAP, have a dependency on Active Directory services. Azure Site Recovery has been tested with Windows Server 2008 R2 and Windows Server 2012 R2 domain controllers running in Windows Server 2003, Windows Server 2008, and native Windows Server 2012 R2 mode.

## SQL Server and other DBMS

SQL Server 2008 R2 (and later), Oracle, and SAP ASE are supported for SAP on Azure. For high availability and disaster recovery (HA/DR) scenarios, we recommend database methods like SQL Server 2012 (and later) AlwaysOn or Oracle Data Guard.



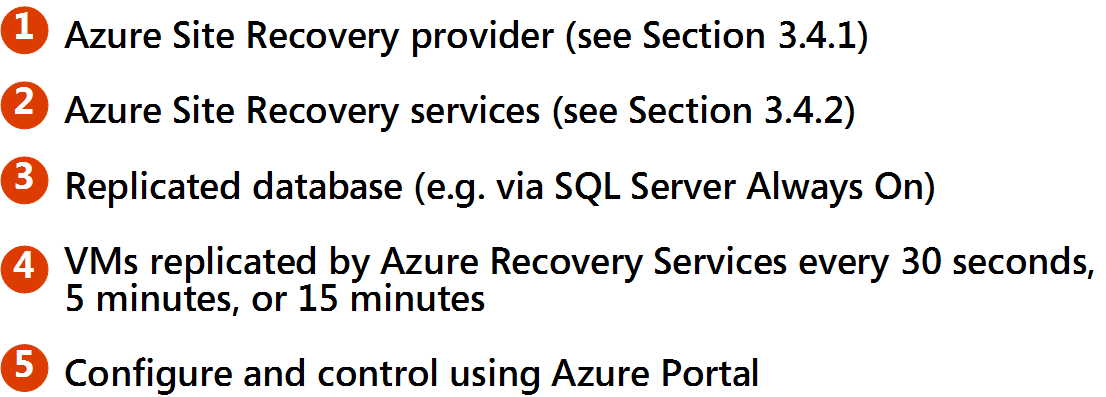


Figure 3. A sample organization's datacenter is on the left; the Azure region on the right.

# Azure Site Recovery requirements

Before deploying Azure Site Recovery services, make sure you have Active Directory and System Center 2012 R2.

## Active Directory

SAP servers and services are dependent on Active Directory for authentication and DNS. The virtual machines in Azure must be able to communicate with at least one domain controller. Three-tier SAP deployments should be domain-based installations; therefore, Active Directory Directory Services and DNS services must be available in Azure.

## System Center 2012 R2

System Center 2012 R2 is optional and can be used to manage and coordinate failover and failback activities.

Azure Recovery Services replicates VMs that are defined within a System Center cloud. The SCVMM server normally runs on your site.

You must install Update Rollup 1, 2, and 3[[1]](#footnote-2) for System Center 2012 R2 with Windows Update. Rollup 6 is now released and available.

## Unsupported configurations

The following technologies *are not supported* by Azure Site Recovery Services, as of July 2015:

* Linux Generation 2 Hyper-V VMs.
* VMs with a boot disk or C: drive larger than 1023GB.
* The addition or removal of disks (virtual hard disks [VHDs]) to the replicated VM. Doing so needs manual intervention to enable replication of the newly added disk for the VM. If you need to add or remove a disk, remove Azure Site Recovery protection, change the disk status by attaching or detaching it, and then re-enable Azure Site Recovery protection.
* Replication of VMs that are within a Windows Server Failover Cluster Configuration with access to Cluster Shared Disks.
* Booting from disks secured by BitLocker.
* VM names that contain special characters or are very long. A VM can be renamed in Azure Portal, after a warning is issued, during the initial replication.
* SAP or other executables installed on D: drive. We recommend that you avoid using the D: drive, although it is technically possible.[[2]](#footnote-3) This disk is reserved on Azure VMs.

In addition, Active Directory domain controllers can be replicated using Azure Site Recovery; however, consider the following recommendations:

* + Place the DS data, log, and SYSVOL on at least one separate data disk, with disk caching switched off.[[3]](#footnote-4)
  + Build the VMs based on Azure Gallery images, which you can download.
  + Install the Azure agent when the gallery image is first created.
  + Configure the diskpart SAN policy to **onlineall** (diskpart.exe san policy=onlineall).
  + If the VM does not come online, validate that all the data disks have come online in the same sequence as on Hyper-V.

NOTE Periodically check the blogs referenced in this document. Future releases of Azure Site Recovery Services may support these features. We recommend you run the Azure Virtual Machine Readiness Assessment Tool.[[4]](#footnote-5)

## Agents

To replicate VM metadata and VHDs to Azure, two agents must be installed on the System Center host or Hyper-V host: Microsoft Azure Site Recovery Provider and Microsoft Azure Recovery Services Agent. You do not need to install an agent or other software within the VMs with the Hyper-V Azure Site Recovery replication channel.

### Azure Site Recovery Provider

This agent coordinates the startup and shutdown of the Hyper-V VM and replicates metadata about the VMs and System Center clouds. This agent must be installed on the System Center host if System Center is deployed.

The latest agent can be found on the Azure Site Recovery Quick Start page in the Azure Portal.

This agent does not require any configuration, and it normally communicates to Azure by an SSL connection over public Internet via a corporate proxy server. Alternatively, communication can be via Azure VPN or ExpressRoute. For more information, see [Step 2: Install the Azure Site Recovery Provider: On-premises to Azure](http://msdn.microsoft.com/en-us/library/azure/dn788914.aspx), on MSDN, at <http://msdn.microsoft.com/en-us/library/azure/dn788914.aspx>.

### Azure Recovery Services Agent

This agent replicates the VM storage. You must install it on all Hyper-V hosts. For more information, see [Step 3: Install the Azure Recovery Services Agent: On-premises to Azure](http://msdn.microsoft.com/en-us/library/azure/dn788913.aspx), on MSDN, at <http://msdn.microsoft.com/en-us/library/azure/dn788913.aspx>.

For the latest agent, see the Azure Site Recovery Quick Start page in the Azure Portal.

This agent usually communicates to Azure by an SSL connection over public Internet via a corporate proxy server. Alternatively, communication can be via Azure VPN or ExpressRoute. This channel of communication is needed to control flows of replication and failover activity. Therefore, it’s better to route the communication through the corporate proxy server and not through VPN or ExpressRoute, where the replication workload traffic is handled. That way, you help make sure that a full site outage does not take down all the corporate proxy servers.

You must configure the Microsoft Azure Recovery Services Agent, provide proxy server details, and enter a username to authenticate.[[5]](#footnote-6)

You can configure Microsoft Azure Recovery Services Agent using the Microsoft Management Console (MMC) (go to **Add/Remove Snap-In**, and then select **Microsoft Azure Backup**).

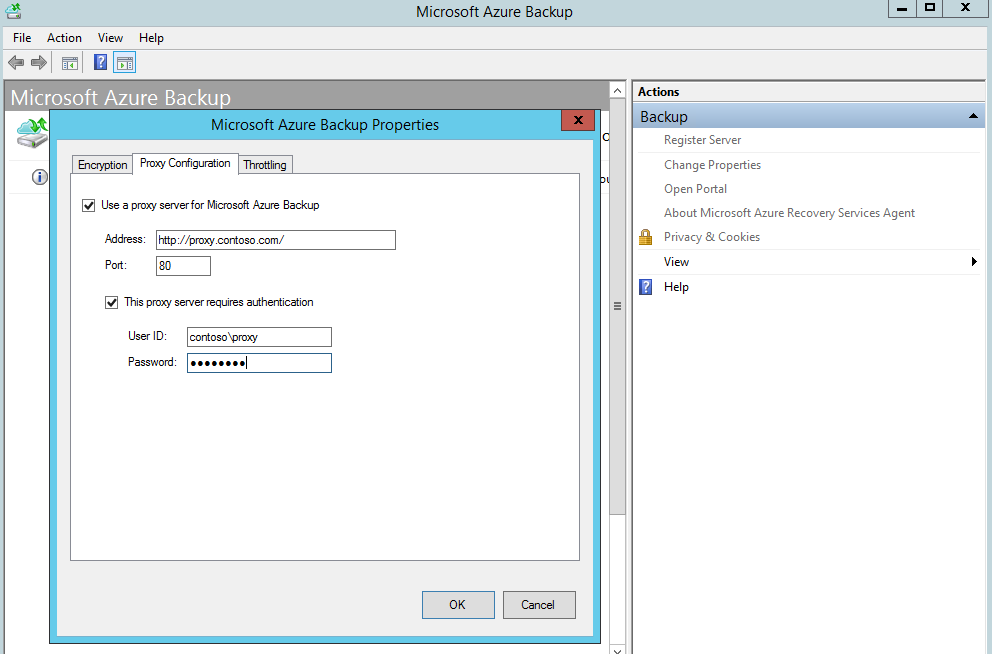


Figure 4. Configuring Azure Recovery Services Agent using MMC.

CmdLet:

$spwd = ConvertTo-SecureString -String Notag00pa55word -AsplainText –Force

Set-OBMachineSetting -ProxyServer [http://proxycontoso.com](http://msdn.microsoft.com/en-us/library/azure/jj156075.aspx) -ProxyPort 80 -ProxyUsername contoso\proxy -ProxyPassword $spwd

Additional configuration-limiting bandwidth is also possible.

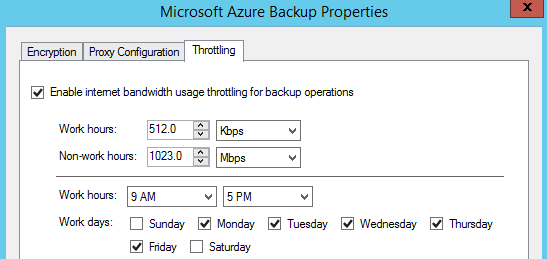


Figure 5. MMC agent properties: configuring additional limits.

CmdLet:

$mon = [System.DayOfWeek]::Monday

$tue = [System.DayOfWeek]::Tuesday

$wed = [System.DayOfWeek]::Wednesday

$thu = [System.DayOfWeek]::Thursday

$fri = [System.DayOfWeek]::Friday

Set-OBMachineSetting -WorkDay $mon, $tue, $wed, $thu, $fri -StartWorkHour "9:00:00" -EndWorkHour "18:00:00" -WorkHourBandwidth (512\*1024) -NonWorkHourBandwidth (1023\*1024\*1024)

NOTE If you use ExpressRoute or VPN, you may not need to configure a proxy.

# Protecting SAP application layers

Database and SAP application server layers require different mechanisms to protect against DR events. For more information about deploying SAP on Windows Hyper-V private cloud, see [How to Deploy SAP on Microsoft Private Cloud with Hyper-V 3.0](http://blogs.msdn.com/b/saponsqlserver/archive/2013/06/30/how-to-deploy-sap-on-microsoft-private-cloud-with-hyper-v-3-0.aspx), on the Running SAP Applications on the Microsoft Platform Blog, at <http://blogs.msdn.com/b/saponsqlserver/archive/2013/06/30/how-to-deploy-sap-on-microsoft-private-cloud-with-hyper-v-3-0.aspx>.

## SAP database layer

The SAP Database service should be protected by native database management systems (DBMS) level replication technologies.

SQL Server 2012 (and later) includes SQL Server AlwaysOn. In addition to SQL Server AlwaysOn, you can use database mirroring[[6]](#footnote-7) and log shipping[[7]](#footnote-8) to synchronize on-premises databases to Azure. In general, the replication technology for Azure is asynchronous—transactions are committed on-premises before they are confirmed on the DR system on Azure.

Other DBMSs have technologies[[8]](#footnote-9) like AlwaysOn or log shipping.[[9]](#footnote-10) Some of these technologies do not provide functionality like the SQL Server AlwaysOn listener. High-availability features operating without a virtual name, which is used to connect the SAP application layer, might force a revision to the SAP profile, changing it to the VM name after failover to Azure. The following SAP profile parameters must be changed: **dbs/<db platform>/server** and **Java ConfigTool**.

The SQL Server AlwaysOn listener preserves the listener host name. No reconfiguration is required for connecting the replicated SAP application server instances.

For more information about configuring SQL Server AlwaysOn in a hybrid, on-premises to Azure configuration, see [Connecting to Availability Group Listener in Hybrid IT](http://blogs.msdn.com/b/sqlalwayson/archive/2013/02/14/connecting-to-availability-group-listener-in-hybrid-it.aspx), at <http://blogs.msdn.com/b/sqlalwayson/archive/2013/02/14/connecting-to-availability-group-listener-in-hybrid-it.aspx>. For more information about AlwaysOn for SAP systems, see [Running SAP Applications on the Microsoft Platform](http://blogs.msdn.com/saponsqlserver/), at <http://blogs.msdn.com/saponsqlserver/>.

We recommend that you plan a backup mechanism for the DBMS layer in case the DR system is activated. For details, see [DBMS Deployment Guide for SAP on Microsoft Azure Virtual Machine Services](http://msdn.microsoft.com/library/dn745892.aspx), at <http://msdn.microsoft.com/library/dn745892.aspx>.

## SAP application server layer

SAP application servers running on Hyper-V can be replicated to Azure using the Azure Recovery Services framework and agents.

The application server does not contain any business data and does not need to be replicated to Azure very often. The only content that changes periodically is the SAP kernel after a kernel upgrade. Replication every 15 minutes is recommended.

For a step-by-step tutorial, see [Getting Started with Azure Site Recovery: On-Premises VMM Site to Azure protection with Hyper-V Replication](http://azure.microsoft.com/en-us/documentation/articles/hyper-v-recovery-manager-azure/), at <http://azure.microsoft.com/en-us/documentation/articles/hyper-v-recovery-manager-azure/>.

NOTE Do not use SAP application servers as file servers. Instead, store interface files, downloads, and other file system business data separately on a file server. For security reasons, do not permit user PCs to have access to SAP application servers. SAP ABAP programs should reference Logical File Names defined in transaction FILE,[[10]](#footnote-11) which, in turn, reference UNC paths, such as \\fileserver\share.

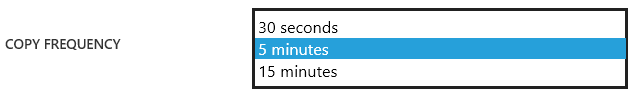


Figure 6. Replication every 15 minutes is recommended.

## SAP SPOF layer (ASCS)

The single point of failure (SPOF) for the SAP component is called the *ASCS/SCS* or *Central Services*. This component is made up of a virtual IP, virtual host name, enqueue server, message server, and highly available shared disk.

Azure Site Recovery Services does not support replication of VMs with shared disks. The Azure platform does not natively support shared disks.

To help protect the SAP components of ASCS/SCS/Central Services, you should:

* Have an Active Directory server running in Azure. This Active Directory server would be the primary Active Directory server in case of a failover to the DR site. The Active Directory domain controller in Azure must be regularly synchronized with the on-premises Active Directory domain controllers.
* While not running in Azure (the normal case), have a VM in Azure which is up and running for every running SAP ASCS/SCS/Central Services. If a DR event occurs, these VMs will take over the role of the ASCS/SCS/Central Services. You would need to make sure that the content of the sapmnt share(s) of the VMs running on-premises is copied on a regular basis into the VM(s) in Azure.
* In case of a failover to the DR site, assume that the Active Directory server that has been in Azure or is rebuilt in Azure is taking over the Windows Domain services.

NOTE In this procedure, you make a change to the DNS entries for the Virtual Windows Cluster names by changing their IP addresses to the IP addresses of the VMs in Azure that should run ASCS/SCS/Central Services. You also assign the virtual name of the cluster to the VMs in Azure designated to run ASCS/SCS/Central Services.

### Emulating the on-premises ASCS

You can assign a virtual host name to a Windows Server. In the following procedure, you use this capability, together with Active Directory and DNS changes, to emulate the on-premises ASCS:

1. Ensure that an Active Directory domain controller is in Azure with DS and DNS roles. We recommend that you use Windows Server 2012 R2[[11]](#footnote-12) for Active Directory domain controller, even if the domain functional level is lower.
2. Provision a new VM in Azure with physical host name = **p.hostname** (can be any host name, such as **azure-ascs**). The VM should be in the same VNET as the domain controller. This VM is designated to run ASCS/SCS/Central Services after a failover to the Azure DR site is executed.
3. Join the VM in Azure to the same domain that your other SAP VMs are running in on-premises.
4. Assign a static Azure IP address with the following command to the VM that is designated to run the ASCS/SCS/Central Services in Azure:

Get-AzureVM -servicename "<cloud service>" -name "<azure VM name>" | Set-AzureStaticVNetip -ipaddress xx.xx.xx.xx | Update-AzureVM

For details, see [Configure a Static Internal IP Address (DIP) for a VM](http://msdn.microsoft.com/library/azure/dn630228.aspx), at http://msdn.microsoft.com/library/azure/dn630228.aspx.

1. Add these keys to the ASCS/SCS/Central Services VM target in Azure:
   1. HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters -> DisableStrictNameChecking of type DWORD set to 1.
   2. HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\MSV1\_0 -> BackConnectionHostNames of type MULTI STRING set to the short virtual host name and FQDN of the on-premises ASCS cluster (example: vsapascs and vsapascs.domain.com).
2. Install Azure Enhanced Monitoring for SAP as described in [SAP NetWeaver on Microsoft Azure Virtual Machine Services - Deployment Guide](http://msdn.microsoft.com/library/dn745892.aspx), at <http://msdn.microsoft.com/library/dn745892.aspx>.
3. Restart the Azure VM.
4. Log on to the Azure VM, and open Windows Explorer. Type **\\p.hostname** (physical host name). The shared network resources on the Azure VM are shown. You may want to create a test shared folder.
5. Create a Windows scheduled task to ROBOCOPY the on-premises ASCS \sapmnt to a directory on the designated Azure VM once per day.

### Testing failover

To continue the installation, you must perform a test failover as follows:

1. Disconnect the VPN connectivity from Azure to on-premise resources. This step isolates the Active Directory and DNS services in Azure from the on-premise resources.
2. Confirm that there is no network connectivity between Azure and the on-premises servers.

WARNING Performing the following Active Directory changes will *offline the on-premises ASCS cluster* if the VPN is connected. Ensure that VPN network connectivity is disabled and blocked. Ensure that the domain controller is never synchronized back to the server on-premises. By default, test failover VMs are never synchronized back to the on-premises server.

1. Open **Active Directory Users and Computers**, and find the ASCS cluster virtual host name.
2. Right-click the object, and click **disable**.
3. Open **DNS Manager**, and find the ASCS/SCS/Central Services name. Double-click the cluster virtual host name, and change the IP address to the specified static IP address (see step 4 in section 4.3.1, “Emulating the on-premises ASCS.”).
4. In Windows Explorer, enter the assigned virtual host name (see step 5b in section 4.3.1, “Emulating the on-premises ASCS.”) **\\v.hostname** (short name) and **\\v.hostname.domain.com** (fully qualified domain name). Confirm that you see the same resources as in step 7 of section 4.3.1. Confirm the configuration with **net view** **\\v.hostname** and **net view \\v.hostname.domain.com**. /etc/hosts file should not be required.
5. In the designated VM, run sapinst.exe SAPINST\_USE\_HOSTNAME=<v.hostname> > System   
   Copy > Target System > Distributed, and install a stand-alone ASCS system.

IMPORTANT Start sapinst with the parameter and the virtual host name instead of with the physical name assigned to the VM in step 4.3.1.2.

1. After the installation is complete, manually copy the data that has been replicated or copied (see step 4.3.1.8) to \sapmnt in the Azure VM.
2. Do a test failover or planned failover of the SAP application server VMs.

NOTE In case of test failover, Azure Site Recovery creates another copy of the VMs in Azure instead of bringing the original copies online. That way, the asynchronous replication continues undisturbed. At the end of the test failover, the additional copies that were created are destroyed. For more information about the test failover functionality, see section 6, [Testing Azure Site Recovery Solution for SAP](#_Testing_Azure_Site) later this document.

1. Recover the database side.
2. Start the SAP application servers.
3. Check SAP Basis functionality, such as Remote Function Call (RFC) and transports.
4. To failback, complete the test failover step. This step destroys the VMs copied by the test failover for the test. It leaves the Hyper-V replicas running in Azure untouched.

WARNING  Before establishing the VPN or ExpressRoute connectivity, make sure that the VM running Active Directory and DNS is destroyed. Failure to destroy the Active Directory and DNS servers in Azure before reestablishing the VPN take the production cluster resources offline.

1. After the test failover is completed and the VM running Active Directory and DNS services is destroyed (to prevent replication of DNS and CNO changes), reconnect Azure VPN/ExpressRoute and check connectivity.
2. Change the Windows copy job (see step 4.3.1.8) to target the sapmnt share in the designated VM in Azure as destination directory of the copy job.

After these steps, the configuration is functional for DR site failovers. In a real failover, you need to make sure that you can rebuild the Active Directory and DNS VM in Azure. Make sure that the Active Directory and DNS services are the only items running. Then, the changes described in steps 12, 13, and 14 need to be executed. Steps 16 and 17 aren’t needed anymore, because the VM has preinstalled ASCS/ASCS/Central instances already. Instead of performing a test failover, as mentioned in step 18, perform a real failover.

## SAP stand-alone layer

Besides SAP NetWeaver, SAP stand-alone components can be categorized into the following types.

Table 1. Support for various types of stand-alone SAP components.

|  |  |  |
| --- | --- | --- |
| Stand-alone component | Description | Example |
| File-system based | These components can be protected by Azure Recovery Services by simply replicating the VM asynchronously. In general, we recommend minimizing the number of disks on the VM and, ideally, implementing the operating system and application on C: drive, if possible.. | CTM Optimizer  Adobe Document Server  KW |
| DBMS-based | These SAP stand-alone components use a database and, therefore, must be protected using database tools and Azure Recovery Services. For more information, see the appropriate SAP guidance, such as the LiveCache High Availability Guide.[[12]](#footnote-13) | LiveCache  Business Objects  Content Server |

# Implementation checklists

## Important blogs and articles

Before you start to implement Azure Site Recovery Services for SAP, we recommend that you review the following blogs, Knowledge Base (KB) articles, and software updates.

### Important blogs

Refer to the following:

* [Plan for Azure Site Recovery Deployment](http://msdn.microsoft.com/en-us/library/azure/dn469074.aspx), on the MSDN website, at <http://msdn.microsoft.com/en-us/library/azure/dn469074.aspx>.
* [Networking 101 for Disaster Recovery to Microsoft Azure using Site Recovery](http://blogs.technet.com/b/virtualization/archive/2014/09/09/networking-101-for-disaster-recovery-to-microsoft-azure-using-site-recovery.aspx) on the Azure Blog, at <http://blogs.technet.com/b/virtualization/archive/2014/09/09/networking-101-for-disaster-recovery-to-microsoft-azure-using-site-recovery.aspx>.
* Refer <http://azure.microsoft.com/blog/tag/azure-site-recovery/> for recent blogs about Azure Site Recovery.
* [Monitor and troubleshoot protection for VMware, VMM, Hyper-V and Physical sites](https://azure.microsoft.com/documentation/articles/site-recovery-monitoring-and-troubleshooting/) on the Azure documentation, at https://azure.microsoft.com/documentation/articles/site-recovery-monitoring-and-troubleshooting/
* [Monitoring Azure Site Recovery](http://blogs.technet.com/b/scvmm/archive/2014/10/30/monitoring-azure-site-recovery.aspx) on the Technet website, at <http://blogs.technet.com/b/scvmm/archive/2014/10/30/monitoring-azure-site-recovery.aspx>.

<https://azure.microsoft.com/documentation/articles/site-recovery-best-practices/>

### Important KB articles

During the setup of Azure Recovery Services, an error message about Hyper-V Broker appears. To resolve this issue, see Microsoft Knowledge Base article KB 2961977, ["Hyper-V Replica Cluster Broker is not installed" error when you replicate private clouds to Microsoft Azure](http://support.microsoft.com/kb/2961977), at <http://support.microsoft.com/kb/2961977>.

Broker is not required for Azure Recovery Services.

Refer How to manage on-premises to Azure protection network bandwidth usage to understand more about different network bandwidth settings at <https://support.microsoft.com/kb/3056159>

### Recommended software versions and updates

The Azure Recovery Services solution described in this document has been tested and validated with the software shown in the following table. In theory, Windows Server 2008 R2 should also work; however, all NetWeaver 7.xx systems now support Windows Server 2012 R2. If you are running an earlier version, we recommend upgrading to a newer operating system and database version.

Table 2. Software used to test and deploy the solution in this white paper.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Version | Service pack | Updates |
| Hyper-V host | Windows Server 2012 R2 | None | All Rollups |
| Guest OS | Windows Server 2012 R2 | None | All Rollups |
| System Center | System Center Virtual Machine Manager 2012 R2 | None | Rollup 1, 2, and 3 |
| Database | SQL Server 2012 | Service Pack 2 | CU 1 |
| SAP kernel | 721\_EXT  7.41 | 300  Due to memory leaks in the 7.4x kernel, you must use the latest patch. Do not use the kernel on the installation media. | DBSL patch 316  Due to memory leaks in the 7.4x kernel, you must use the latest patch. Do not use the kernel on the installation media. |

For more information, see [List of Rollup Updates for Windows 8.1 and Windows Server 2012 R2](http://social.technet.microsoft.com/wiki/contents/articles/23823.list-of-rollup-updates-for-windows-8-1-and-windows-server-2012-r2.aspx), on the TechNet website, at <http://social.technet.microsoft.com/wiki/contents/articles/23823.list-of-rollup-updates-for-windows-8-1-and-windows-server-2012-r2.aspx>.

## Capacity planning and readiness assessment

You can run the Azure Virtual Machine Readiness Assessment tool[[13]](#footnote-14) on VMs to ensure that they are compatible with Azure VMs and Azure Site Recovery Services. The Readiness Assessment Tool checks VM configurations and warns when configurations are incompatible with Azure. For example, it issues a warning if a C: drive is larger than 1TB.

Capacity planning is made up of at least two important components:

* Mapping on-premises Hyper-V VMs to Azure VM sizes (such as A6, A7, A8, and A9).
* Determining the required Internet bandwidth.

For more information about mapping the on-premises VMs to the certified and supported VM SKU in Azure, see the existing SAP on Azure documentation,[[14]](#footnote-15) in addition to SAP Note [1928533 – SAP Applications on Azure: Supported Products and Azure VM types](http://service.sap.com/sap/support/notes/1928533) at <http://service.sap.com/sap/support/notes/1928533>.

SAP application servers do not contain any business data; therefore, the expected data change rate is quite small. The amount of traffic generated by a SAP VM is not large. If you observe a large amount of replication traffic, you should investigate to determine root cause. Possible causes include using SAP application servers as file servers and writing text or CSV files to a SAP application server (a security risk and poor operational practice that we strongly discourage) or tracing and logging, such as audit logs, job logs, or ST05 traces.

You should monitor DBMS replication traffic carefully. The amount of log shipping or AlwaysOn traffic can be estimated based on the size of the transaction log backups. AlwaysOn uses compression by default. If log shipping is used, configure Backup Compression, in all cases.

## Implementation checklist

The Azure Portal provides step-by-step procedures for implementing Azure Site Recovery on the main page of the Site Recovery Vault dashboard.

Table 3. Implementation checklist.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Step 1** |  |  |  |  |  |
| Configure the vault. | | | |  |  |
| Download Registration Key | | | |  |  |
|  | |  |  |  |  |
|  |  |  |  |  |  |
| **Step 2** |  |  |  |  |  |
| Prepare VMM servers. | | | | |  |
| Download Microsoft Azure Site Recovery Provider, and install it on VMM servers. | | | | | |
|  |  |  |  |  |  |
| **Step 3** |  |  |  |  |  |
| Prepare resources. | | | |  |  |
| Add an Azure Storage account. | | |  |  |  |
| Download the Microsoft Azure Recovery Services Agent, and install it on Hyper-V host servers. | | | | | |
| Configure agent proxy, as needed. | | | | |  |
|  |  |  |  |  |  |
| **Step 4** |  |  |  |  |  |
| Configure cloud protection. | | | | | |
| Set up protection for VMM clouds. | | | |  |  |
|  |  |  |  |  |  |
| **Step 5** |  |  |  |  |  |
| Map resources. Map on-premise networks to Azure VNET. | | | |  |  |
|  |  |  |  |  |  |
| **Step 6** |  |  |  |  |  |
| Protect virtual machines, enable virtual machines. | | | | | |
| Define VM system boot disk in System Center. | | | | | |
| Add VM to System Center cloud. | | | | |  |
| Enable protection for VMs. | | | |  |  |
|  | | | |  |  |
| **Step 7** |  |  |  |  |  |
| Configure recovery plans. | | | | | |
| Perform test failover on individual VMs. | | | | | |
| Ensure that all VMs have access to required resources, such as Active Directory. | | | | | |
| Ensure that network redirections for SAP ASCS are working. | | | | | |
|  | | | | | |
| **Step 8** | | | | |  |
| Perform DR simulation with technical validation only. | | | |  |  |
| Perform technical validation of SAP system—check SM51, SM21, system connectivity, interface connectivity, and more. | | | |  |  |
|  | | | |  |  |
| **Step 9** | | | |  |  |
| Perform DR simulation with end-user functional validation. | | | |  |  |

# Testing Azure Site Recovery Solution for SAP

## Network isolated failover scenario

Azure Site Recovery Services includes test failover, which differs from planned/unplanned failover procedures in the following ways:

* A test failover does not stop the on-premises VMs; it simply activates the copy of the VM in Azure.
* Test failover can direct the VMs to a different VNET, which does not need to have a VPN connection back to the on-premises network. Because of this, the VMs can operate in an isolated network bubble, disconnected from VPNs and the on-premises network.
* The test failover Azure Site Recovery job pauses after the VMs start up. After pausing, the VMs are automatically destroyed and *are not replicated* back to the on-premises environment.
* A test failover does not interrupt or compromise the DR solution. A test failover copies the underlying storage and creates a new temporary copy attached to a temporary VM.
* To enable communication between a temporary, test VNET and other VNETs—where Active Directory or SQL Server AlwaysOn VMs are running—VNET-to-VNET connectivity is used.

We recommend using test failover for most DR test scenarios, especially when changes to the Active Directory cluster name object (CNO), server principal name (SPN), or other properties are required. Using the test failover mechanism guarantees that Active Directory changes do *not* replicate back to the on-premises Active Directory and impact the production systems.

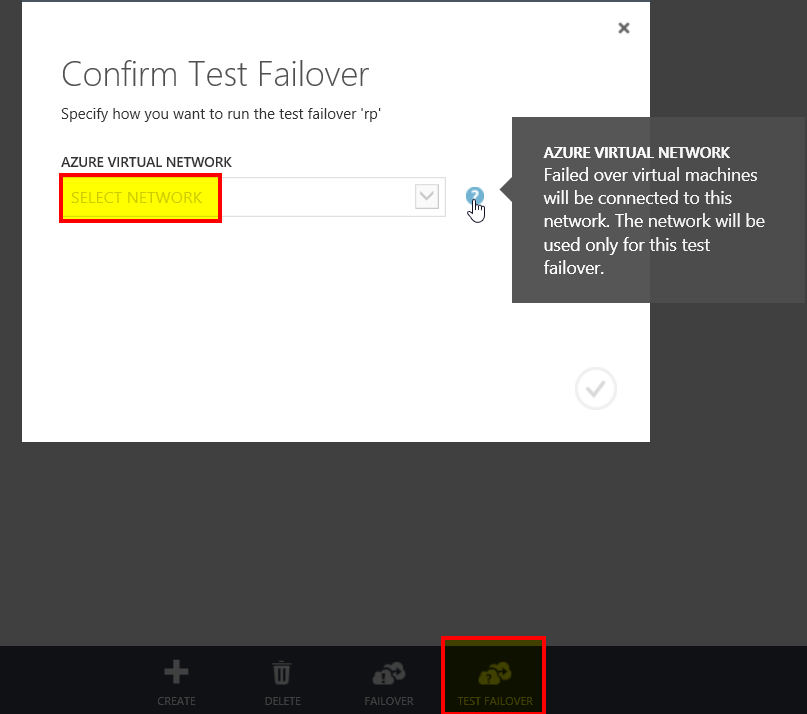


Figure 7. Azure Site Recovery Services includes test failover.

## Network integrated failover scenario

Planned failover (PFO) is executed in an anticipated event—a power outage, network outage, or server maintenance. PFO ensures that there is no data loss in the recovery process by making sure that primary side VMs are shut down and that the last delta replication has been sent to Azure *before* initiating the failover.

Unplanned failover (UFO) is executed in the event of a disaster or unexpected outage—an event you cannot plan. UFO incurs some data loss as configured during the protection. UFO ensures that VMs are brought online in Azure immediately. Executing UFO pauses the on-premises VMs.

NOTE In SAP scenarios, we do not recommend the use of UFO.

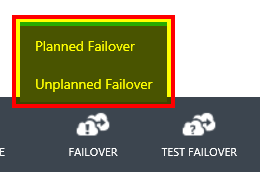


Figure 8. Azure Portal Failover control.

# Monitoring, troubleshooting, and exceptional handling

## Monitoring

As of September 2014, the Azure Portal indicates the VM synchronization status only when clicking each protected cloud. Inconsistent replication status is indicated in the Azure Portal and in the Event Viewer. Further alerting options are being evaluated.

Open **Windows Task Manager** > **Performance** > **Resource Monitor**, and then filter by image **cbengine.exe**, **vmmservice.exe**, and **vmmagent.exe**.

Resource Monitor can be used to measure the network throughput. As a minimum, 3–5 megabytes per second (MBPS) should be achieved.

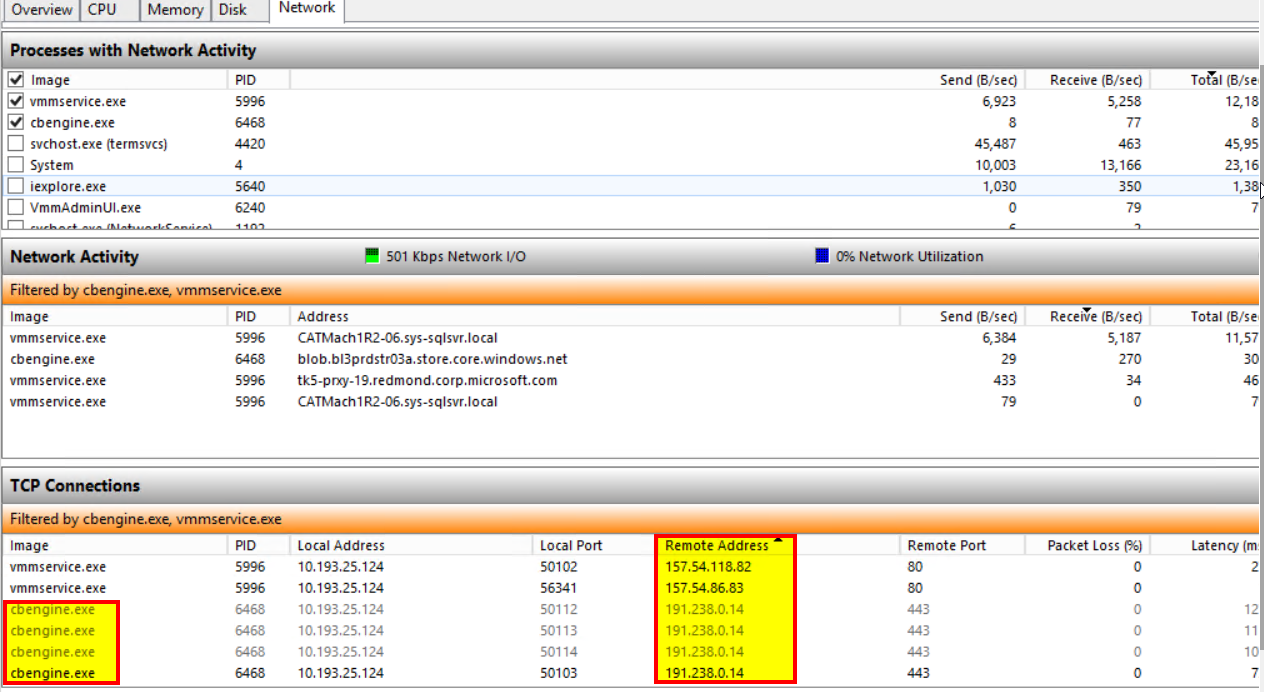


Figure 9. Resource Monitor can be used to measure the network throughput.

## Troubleshooting

The Azure Recovery Services agent logs information into the Windows Event Viewer. We recommend periodically checking the Event Viewer.

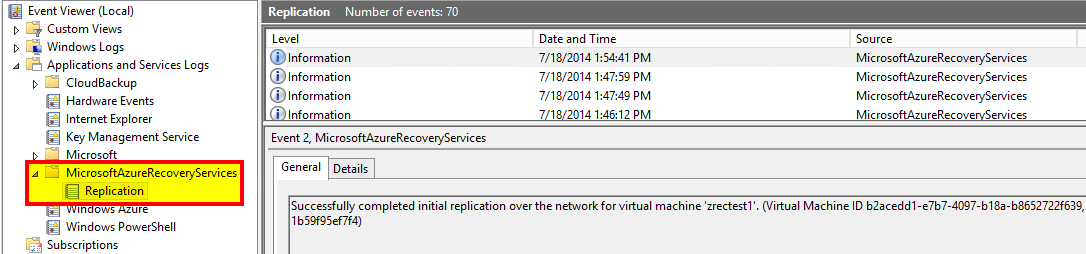


Figure 10. Event Viewer in Azure Recovery Services agent.

Further information is logged in trace files in the following directory on the Hyper-V hosts:

C:\Program Files\Microsoft Azure Recovery Services Agent\Temp

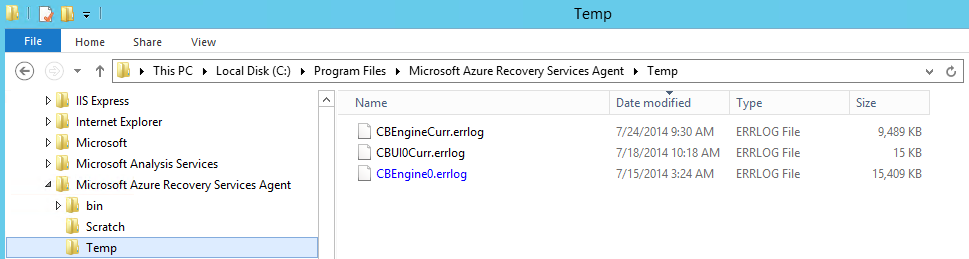


Figure 11. Trace files contains logs of important events.

The following cmdlets can be used to retrieve the same replication status:

Get-VMReplication -ComputerName "<hostname>" -VMName "<vmname>"

Measure-VMReplication -ComputerName "<hostname>" -VMName "<vmname>"

To collect VMM logs, see [How to enable debug logging in Virtual Machine Manager](http://support.microsoft.com/kb/2913445) at <http://support.microsoft.com/kb/2913445>.

<https://azure.microsoft.com/en-us/documentation/articles/site-recovery-monitoring-and-troubleshooting/>

## Exception handling

If you see the following error message, restart the Azure Site Recovery agent on the System Center Virtual Machine Manager host and then verify that the certificate is valid.

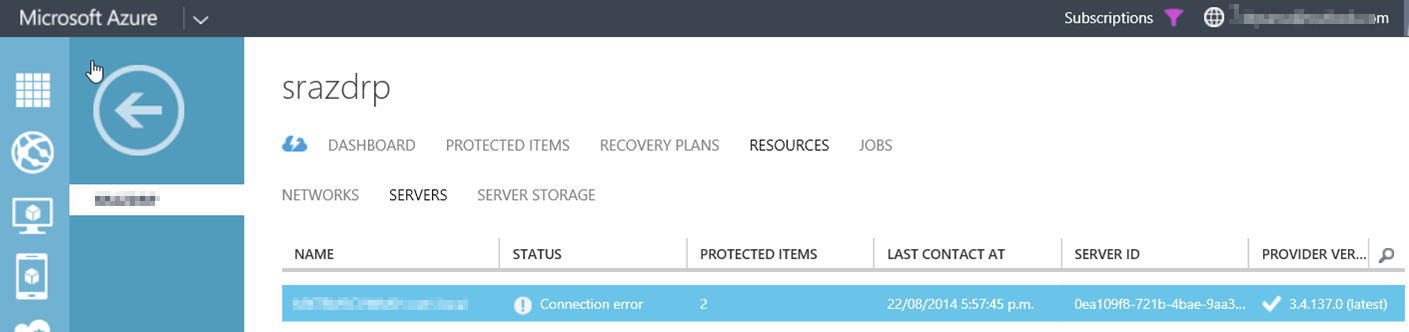


Figure 12. Error message in Azure Site Recovery agent.

When you execute a command, such as **net view \\servername** or **net view \\virtualhostname**, you may receive an error (“Error 5 Access Denied” or “Error 53 Path not found”). If this happens, and if the following Kerberos error also occurs when you choose **Event Viewer** > **System**, the Active Directory CNO object for the ASCS is still enabled. For more information, see the “[3.3 Agents](#_Agents)” section of this document.

The Kerberos client received a KRB\_AP\_ERR\_MODIFIED error from the server <azure vm>$. The target name used was cifs/<physical\_host\_name>.DOMAIN.local. This indicates that the target server failed to decrypt the ticket provided by the client. This can occur when the target server principal name (SPN) is registered on an account other than the account the target service is using. Please ensure that the target SPN is registered on, and only registered on, the account used by the server. This error can also happen when the target service is using a different password for the target service account than what the Kerberos Key Distribution Center (KDC) has for the target service account. Please ensure that the service on the server and the KDC are both updated to use the current password. If the server name is not fully qualified, and the target domain (DOMAIN.LOCAL) is different from the client domain (DOMAIN.LOCAL), check if there are identically named server accounts in these two domains, or use the fully qualified name to identify the server.

# Azure Site Recovery for VMware and Linux

It is technically possible to replicate VMware, Linux, and physical deployments to Azure using the InMage toolset. However, this document only describes how to replicate the Hyper-V private cloud to Azure using the Hyper-V Replica replication channel.

InMage provides an additional replication channel. A future paper will describe the setup and configuration of InMage for SAP systems.

<http://azure.microsoft.com/blog/2015/07/09/announcing-the-ga-of-disaster-recovery-for-vmware-virtual-machines-and-physical-machines-to-azure-using-asr/>

For more information about InMage, see [Acquisition of InMage Systems](http://blogs.technet.com/b/in_the_cloud/archive/2014/07/24/acquisition-of-inmage-systems.aspx), on the In the Cloud blog at http://blogs.technet.com/b/in\_the\_cloud/archive/2014/07/24/acquisition-of-inmage-systems.aspx.

Appendix: Recommended resources

* [Getting Started with Azure Site Recovery: On-Premises to On-Premises VMM Site Protection with Hyper-V Replication](file:///C:\Users\anbacker\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\SJC862BN\Getting%20Started%20with%20Azure%20Site%20Recovery:%20On-Premises%20to%20On-Premises%20VMM%20Site%20Protection%20with%20Hyper-V%20Replication), on the MSDN website, at <http://azure.microsoft.com/en-us/documentation/articles/hyper-v-recovery-manager-configure-vault/>.
* [Microsoft Azure Site Recovery: Leveraging Azure as Your Disaster Recovery Site](https://channel9.msdn.com/Events/TechEd/Europe/2014/CDP-B314) on the Channel 9 website at https://channel9.msdn.com/Events/TechEd/Europe/2014/CDP-B314.
* [Episode 149: Azure Site Recovery with Praveen Vijayaraghavan](http://channel9.msdn.com/Shows/Cloud+Cover/Episode-149-Azure-Site-Recovery-with-Praveen-Vijayaraghavan), on the Channel 9 website, at http://channel9.msdn.com/Shows/Cloud+Cover/Episode-149-Azure-Site-Recovery-with-Praveen-Vijayaraghavan.
* [Active Directory Virtualization Safeguards and Domain Controller Cloning with Windows Server 2012](http://channel9.msdn.com/Events/TechEd/Europe/2012/SIA317), on the Channel 9 website, at http://channel9.msdn.com/Events/TechEd/Europe/2012/SIA317.
* [Microsoft Azure Site Recovery: Your DR Site in Microsoft Azure](http://blogs.technet.com/b/systemcenter/archive/2014/07/01/microsoft-azure-site-recovery-your-dr-site-in-microsoft-azure.aspx), on the System Center Team Blog, at http://blogs.technet.com/b/systemcenter/archive/2014/07/01/microsoft-azure-site-recovery-your-dr-site-in-microsoft-azure.aspx.
* [Update Rollup 3 for System Center 2012 R2 is now available](http://blogs.technet.com/b/systemcenter/archive/2014/07/29/update-rollup-3-for-system-center-2012-r2-is-now-available.aspx), on the System Center Team Blog, at <http://blogs.technet.com/b/systemcenter/archive/2014/07/29/update-rollup-3-for-system-center-2012-r2-is-now-available.aspx>.
* <https://channel9.msdn.com/Shows/Edge/Disaster-Recovery-using-Azure-Site-Recovery-for-SMB-Hyper-V-Replication>
* <https://channel9.msdn.com/events/TechEd/Europe/2014/CDP-B319>
* <https://channel9.msdn.com/events/TechEd/Europe/2014/CDP-B314>
* <https://channel9.msdn.com/events/Ignite/2015/BRK3503>

Glossary

Azure Site Recovery components (A–Z)

**Active Directory**

SAP on Azure solutions must have an Active Directory domain controller in Azure to continue to work in the expected way.

**Azure Site Recovery agents**

Azure Site Recovery requires two agents. One agent is installed on the Hyper-V host(s) and another is installed on the System Center Virtual Machine Manager server. For more information, see the “[3.3 Agents](#_Agents)“ section in this document.

**Azure Site Recovery Portal—site recovery vault**

Azure Site Recovery is a service within Azure Portal and requires a site recovery vault. Azure supports backup vaults and site recovery vaults. A site recovery vault holds the metadata for a site protected by Azure Site Recovery and links to a storage account that holds the VM Virtual Hard Disks (VHDs).

**Azure storage account**

Azure Site Recovery Services replicates the VHD(x) of VMs and stores them on Azure Blob Page Store. At a configurable interval of 30 seconds, 5 minutes, or 15 minutes, a delta replication is synchronized from Hyper-V to Azure. All the file objects are kept on a storage account. For more information, see [How To Create a Storage Account](http://azure.microsoft.com/en-us/documentation/articles/storage-create-storage-account/), at http://azure.microsoft.com/en-us/documentation/articles/storage-create-storage-account/.

**database servers**

In the scenario described in this document, database servers are not protected with Azure Site Recovery. We recommend using native database tools for your specific SAP scenario.

**Hyper-V cluster**

Azure Site Recovery replicates Hyper-V VMs to Azure. Azure Site Recovery uses the Hyper-V replication mechanism to synchronize the VMs with Azure. For more information about deploying SAP on Hyper-V, see [How to Deploy SAP on Microsoft Private Cloud with Hyper-V 3.0](http://blogs.msdn.com/b/saponsqlserver/archive/2013/06/30/how-to-deploy-sap-on-microsoft-private-cloud-with-hyper-v-3-0.aspx), at http://blogs.msdn.com/b/saponsqlserver/archive/2013/06/30/how-to-deploy-sap-on-microsoft-private-cloud-with-hyper-v-3-0.aspx.

**proxy server**

Azure Site Recovery agents require network connectivity to Azure. Communication between the agents and Azure can either be routed via VPN and ExpressRoute or more commonly via public Internet over an SSL connection on port 443 (optional certificate encryption).

**System Center 2012 R2**

System Center Virtual Machine Manager is required to orchestrate the Azure Site Recovery failover and failback process. We recommend deploying the most recent System Center Rollup.

**VPN or ExpressRoute**

VPN security connects the local network to the Azure public cloud network via Internet cross-premises connectivity. (See [Configure and monitor virtual networks in Azure](http://azure.microsoft.com/en-us/documentation/services/virtual-network/), at http://azure.microsoft.com/en-us/documentation/services/virtual-network/.) ExpressRoute connects the local network to the Azure public cloud network via a dedicated private wide area network (WAN) link. (See [Create private connections between your on-premises or co-located infrastructure and Azure datacenters](http://azure.microsoft.com/en-us/documentation/services/expressroute/), at http://azure.microsoft.com/en-us/documentation/services/expressroute/.) For more information about network requirements, see [Using SAP on Azure VMs](file:///C:\Users\anbacker\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\SJC862BN\Using%20SAP%20on%20Azure%20VMs), at http://msdn.microsoft.com/library/dn745892.aspx. VPN or ExpressRoute can be used to handle replication traffic, but, more commonly, the Azure Site Recovery agents are communicating via a corporate proxy server.

1. See [Update Rollup 3 for System Center 2012 R2 is now available](http://blogs.technet.com/b/systemcenter/archive/2014/07/29/update-rollup-3-for-system-center-2012-r2-is-now-available.aspx) on the System Center Team Blog, at http://blogs.technet.com/b/systemcenter/archive/2014/07/29/update-rollup-3-for-system-center-2012-r2-is-now-available.aspx. [↑](#footnote-ref-2)
2. See [How To Change the Drive Letter of the Windows Temporary Disk](http://azure.microsoft.com/en-us/documentation/articles/virtual-machines-windows-change-drive-letter/), at <http://azure.microsoft.com/en-us/documentation/articles/virtual-machines-windows-change-drive-letter/>. <https://support.microsoft.com/en-us/kb/3031135> [↑](#footnote-ref-3)
3. See [Step 3: Install Windows Server Active Directory](http://azure.microsoft.com/en-us/documentation/articles/active-directory-new-forest-virtual-machine/#installad), at <http://azure.microsoft.com/en-us/documentation/articles/active-directory-new-forest-virtual-machine/#installad>. [↑](#footnote-ref-4)
4. Available at <http://azure.microsoft.com/en-us/downloads/vm-readiness-assessment/>. [↑](#footnote-ref-5)
5. For information about enterprise deployment using System Center Configuration Manager, see [Agent install and configuration for Hyper-V hosts when using Microsoft Azure Site Recovery for disaster recovery to Azure](http://blogs.technet.com/b/scvmm/archive/2014/07/22/agent-install-and-configuration-for-hyper-v-hosts-when-using-microsoft-azure-site-recovery-for-disaster-recovery-to-azure.aspx), on the System Center Virtual Machine Manager Engineering Blog, at <http://blogs.technet.com/b/scvmm/archive/2014/07/22/agent-install-and-configuration-for-hyper-v-hosts-when-using-microsoft-azure-site-recovery-for-disaster-recovery-to-azure.aspx>. [↑](#footnote-ref-6)
6. See SAP Note [965908 - SQL Server Database Mirroring and SAP Applications](http://service.sap.com/sap/support/notes/965908), at http://service.sap.com/sap/support/notes/965908. [↑](#footnote-ref-7)
7. See SAP Note [493290 - Configuring SQL server Log shipping](http://service.sap.com/sap/support/notes/493290), at <http://service.sap.com/sap/support/notes/493290>. [↑](#footnote-ref-8)
8. Oracle Dataguard <http://www.oracle.com/us/solutions/sap/wp-ora4sap-dataguard11g-303811.pdf> [↑](#footnote-ref-9)
9. See [Configuring Oracle Data Guard for Azure](http://msdn.microsoft.com/en-us/library/azure/dn614680.aspx), at <http://msdn.microsoft.com/en-us/library/azure/dn614680.aspx>. [↑](#footnote-ref-10)
10. See [Logical File Names](http://help.sap.com/saphelp_nw73/helpdata/en/48/d59192982b424be10000000a421937/frameset.htm), at <http://help.sap.com/saphelp_nw73/helpdata/en/48/d59192982b424be10000000a421937/frameset.htm>. [↑](#footnote-ref-11)
11. Windows 2012 adds protections for virtual environments. See [Safe virtualization of domain controllers](http://technet.microsoft.com/en-us/library/hh831734.aspx#safe_virt_dc), at <http://technet.microsoft.com/en-us/library/hh831734.aspx#safe_virt_dc>. [↑](#footnote-ref-12)
12. See SAP Note [952783 - FAQ: SAP MaxDB high availability](http://service.sap.com/sap/support/notes/952783), at <http://service.sap.com/sap/support/notes/952783>. [↑](#footnote-ref-13)
13. Download the [Azure Virtual Machine Readiness Assessment](http://azure.microsoft.com/en-us/downloads/vm-readiness-assessment/) at <http://azure.microsoft.com/en-us/downloads/vm-readiness-assessment/> . [↑](#footnote-ref-14)
14. See [Using SAP on Azure Virtual Machines (VMs)](http://msdn.microsoft.com/library/dn745892.aspx), at <http://msdn.microsoft.com/library/dn745892.aspx> . [↑](#footnote-ref-15)