Microsoft Azure - Starter Kits for Partners

Hands on Lab

Azure Site Recovery

Last Update: 19 September 2015





**MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.**

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The descriptions of other companies’ products in this document, if any, are provided only as a convenience to you. Any such references should not be considered an endorsement or support by Microsoft. Microsoft cannot guarantee their accuracy, and the products may change over time. Also, the descriptions are intended as brief highlights to aid understanding, rather than as thorough coverage. For authoritative descriptions of these products, please consult their respective manufacturers.

© 2014 Microsoft Corporation. All rights reserved. Any use or distribution of these materials without express authorization of Microsoft Corp. is strictly prohibited.

Microsoft and Windows are either registered trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Contents

[Introduction 4](#_Toc430420918)

[Best Practices for Azure Site Recovery 4](#_Toc430420919)

[Features and Scenarios 4](#_Toc430420920)

[Deployment Scenarios 8](#_Toc430420921)

[Protection between an on-premises VMM site and Azure 9](#_Toc430420922)

[Protection between an on-premises Hyper-V site and Azure 10](#_Toc430420923)

[Protection between on-premises VMware virtual machines or physical servers and Azure 11](#_Toc430420924)

[Protection between on-premises VMM sites 12](#_Toc430420925)

[Protection between on-premises VMM sites with SAN 13](#_Toc430420926)

[Protection between on-premises VMware sites 14](#_Toc430420927)

# Introduction

Azure Site Recovery contributes to your business continuity and disaster recovery (BCDR) strategy by orchestrating replication, failover and recovery of virtual machines in a number of deployment scenarios.

This document is designed to assist the consultant responsible for delivering this solution and is a reference for the online documentation about each Azure Site Recovery scenario.

# Best Practices for Azure Site Recovery

Before start your Azure Site Recovery deployment, make sure you read and implement the best practices available here:

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

# Features and Scenarios

This table summarizes the main Site Recovery features and how they are handled during replication to Azure, replication to a secondary site using the default Hyper-V Replica replication, and using SAN.

|  |  |  |  |
| --- | --- | --- | --- |
| Feature | Replicate to Azure | Replicate to a secondary site (Hyper-V Replica) | Replicate to a secondary site (SAN) |
| Data replication | Metadata about on-premises servers and virtual machines is stored in the Site Recovery vault.  Replicated data is stored in Azure storage. | Metadata about on-premises servers and virtual machines is stored in the Site Recovery vault.  Replicated data is stored in the location specified by the target Hyper-V server. | Metadata about on-premises servers and virtual machines is stored in the Site Recovery vault.  Replicated data is stored in the target array storage. |
| Vault requirements | Azure account with the Site Recovery service | Azure account with the Site Recovery service | Azure account with the Site Recovery service |
| Replication | Replicate virtual machine from source Hyper-V host to Azure storage. Fail back to the source location. | Replicate virtual machine from source Hyper-V host to target Hyper-V host. Fail back to the source location. | Replicate virtual machines from source SAN storage device to target SAN device. Fail back to the source location. |
| Virtual machine | Virtual machine hard disk stored in Azure storage | Virtual machine hard disk stored on Hyper-V host | Virtual machine hard disk stored on SAN storage array |
| Azure storage | Required to store replicated virtual machine hard disks | Not applicable | Not applicable |
| SAN storage array | Not applicable | Not applicable | SAN storage array must be available in both the source and target sites and managed by VMM |
| VMM server | VMM server only in the source site only. | VMM servers in source and target sites are recommended. You can replicate between clouds on a single VMM server. | VMM server in source and target VMM sites. Clouds must contain at least one Hyper-V cluster. |
| VMM version | System Center 2012 R2  System Center 2012 with SP1 | System Center 2012 R2 | System Center 2012 R2 with VMM Update Rollup 5.0 |
| VMM configuration | Set up clouds in source and target sites  Set up VM networks in source and target site  Set up storage classifications in source and target sites  Install the Provider on source and target VMM servers | Set up clouds in source site  Set up SAN storage  Set up VM networks in source site  Install the Provider on source VMM server  Enable virtual machine protection | Set up clouds in source and target sites  Set up VM networks in source and target sites  Install the Provider on source and target VMM server  Enable virtual machine protection |
| Azure Site Recovery Provider  Used to connected over HTTPS to Site Recovery | Install on source VMM server | Install on source and target VMM servers | Install on source and target VMM servers |
| Azure Recovery Services Agent  Used to connected over HTTPS to Site Recovery | Install on Hyper-V host servers | Not required | Not required |
| Virtual machine recovery points | Set recovery points by time.  Specifies how long a recovery point should be kept (0-24 hours) | Set recovery points by amount.  Specifies how many additional recovery points should be kept (0-15). By default a recovery point is created every hour | Configured in array storage settings |
| Network mapping | Map VM networks to Azure networks.  Network mapping ensures that all virtual machines that fail over in the same source VM network can connect after failover. In addition if there's a network gateway on the target Azure network then virtual machines can connect to on-premises virtual machines.  If mapping isn't enabled only virtual machines that fail over in the same recovery plan can connect to each other after failover to Azure. | Map source VM networks to target VM networks.  Network mapping is used to place replicated virtual machines on optimal Hyper-V host servers, and ensures that virtual machines associated with the source VM network are associated with the mapped target network after failover.  If mapping isn't enabled replicated virtual machines won't be connected to a network. | Map source VM networks to target VM networks.  Network mapping ensures that virtual machines associated with the source VM network are associated with the mapped target network after failover.  If mapping isn't enabled replicated virtual machines won't be connected to a network. |
| Storage mapping | Not applicable | Maps storage classifications on source VMM servers to storage classifications on target VMM servers.  With mapping enable virtual machine hard disks in the source storage classification will be located in the target storage classification after failover.  If storage mapping isn't enabled replicated virtual hard disks will be stored in the default location on the target Hyper-V host server. | Maps between storage arrays and pools in the primary and secondary sites. |

# Deployment Scenarios

The Site Recovery service contributes to a robust business continuity and disaster recovery (BCDR) solution that protects your on-premises physical servers and virtual machines by orchestrating and automating replication and failover to Azure, or to a secondary on-premises datacenter.

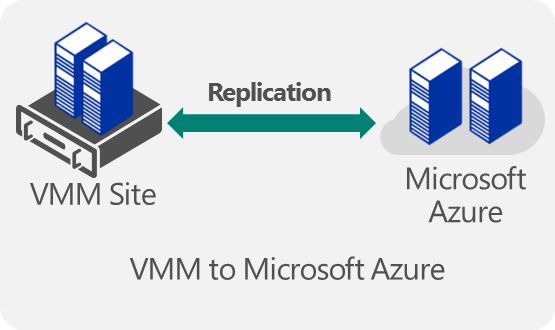
This table summarizes the replication scenarios supported by Site Recovery.

|  |  |  |
| --- | --- | --- |
| Replicate to | Replicate from (on-premises) | Details |
| Azure | Hyper-V site | Replicate virtual machine on one or more on-premises Hyper-V host servers that are defined as a Hyper-V site to Azure. No VMM server required. |
| Azure | VMM server | Replicate virtual machines on one or more on-premises Hyper-V host servers located in a VMM cloud to Azure. |
| Azure | Physical Windows server | Replicate a physical Windows or Linux server to Azure |
| Azure | VMware virtual machine | Replicate VMware virtual machines to Azure |
| Secondary datacenter | VMM server | Replicate virtual machines on on-premises Hyper-V host servers located in a VMM cloud to a secondary VMM server in another datacenter |
| Secondary datacenter | VMM server with SAN | Replicate virtual machines on on-premises Hyper-V host servers located in a VMM cloud to a secondary VMM server in another datacenter using SAN replication |
| Secondary datacenter | Single VMM server | Replicate virtual machines on on-premises Hyper-V host servers located in a VMM cloud to a secondary cloud on the same VMM server |

## Protection between an on-premises VMM site and Azure

This scenario guide describes how to deploy Site Recovery to orchestrate and automate protection for workloads running on virtual machines on Hyper-V host servers that are located in VMM private clouds. In this scenario virtual machines are replicated from a primary VMM site to Azure using Hyper-V Replica.

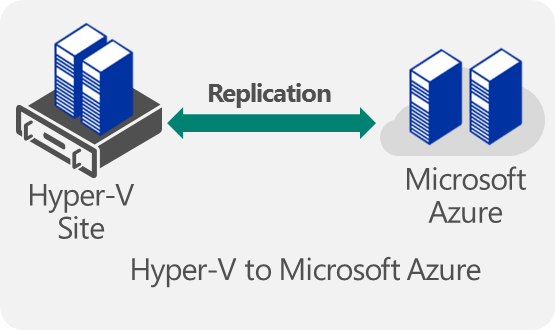
The guide includes prerequisites for the scenario and shows you how to set up a Site Recovery vault, get the Azure Site Recovery Provider installed on the source VMM server, register the server in the vault, add an Azure storage account, install the Azure Recovery Services agent on Hyper-V host servers, configure protection settings for VMM clouds that will be applied to all protected virtual machines, and then enable protection for those virtual machines. Finish up by testing the failover to make sure everything's working as expected.



Scenario guide: <https://azure.microsoft.com/en-us/documentation/articles/site-recovery-vmm-to-azure/>

## Protection between an on-premises Hyper-V site and Azure

This scenario guide describes how to deploy Site Recovery to replicate virtual machines located on on-premises Hyper-V servers running Windows Server 2012 R2. Replication to Azure storage is orchestrated by Site Recovery. This deployment is particularly useful if you're running Hyper-V servers but System Center Virtual Machine Manager (VMM) isn't deployed.



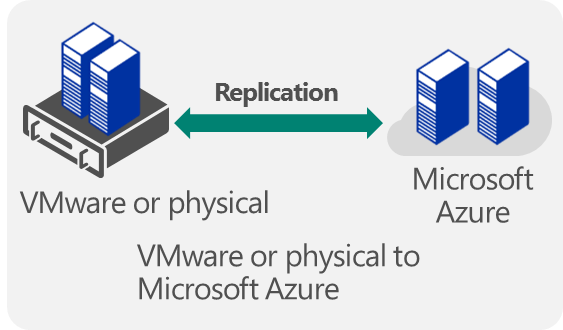
Scenario guide: <https://azure.microsoft.com/en-us/documentation/articles/site-recovery-hyper-v-site-to-azure/>

## Protection between on-premises VMware virtual machines or physical servers and Azure

This scenario guide describes how to deploy Site Recovery to:

* Protect VMware virtual machines—Coordinate replication, failover, and recovery of on-premises VMware virtual machines to Azure
* Protect physical servers—Coordinate replication, failover, and recovery of on-premises physical Windows and Linux servers to Azure using the Azure Site Recovery service.

The guide includes an overview, deployment prerequisites, and set up instructions. At the end of the article, your VMware virtual machines or physical servers will be replicating to Azure.

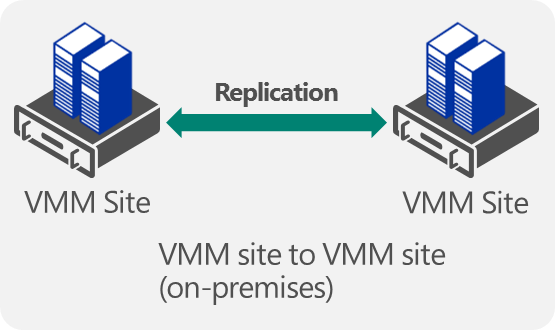


Scenario guide: <https://azure.microsoft.com/en-us/documentation/articles/site-recovery-vmware-to-azure/>

## Protection between on-premises VMM sites

This scenario guide describes how to deploy Site Recovery to orchestrate and automate protection for workloads running on virtual machines on Hyper-V host servers that are located in VMM private clouds. In this scenario, virtual machines are replicated from a primary VMM site to a secondary VMM site using Hyper-V Replica.

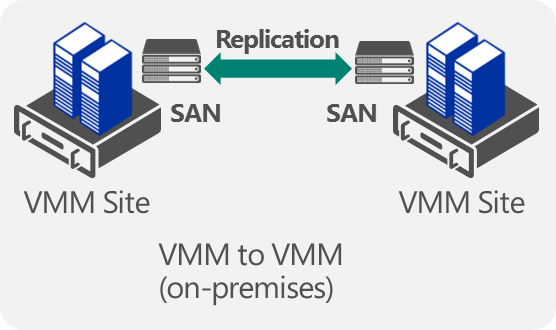
The guide includes prerequisites for the scenario and shows you how to set up a Site Recovery vault, get the Azure Site Recovery Provider installed on source and target VMM servers, register the servers in the vault, configure protection settings for VMM clouds that will be applied to all protected virtual machines, and then enable protection for those virtual machines. Finish up by testing the failover to make sure everything is working as expected.



Scenario guide: <https://azure.microsoft.com/en-us/documentation/articles/site-recovery-vmm-to-vmm/>

## Protection between on-premises VMM sites with SAN

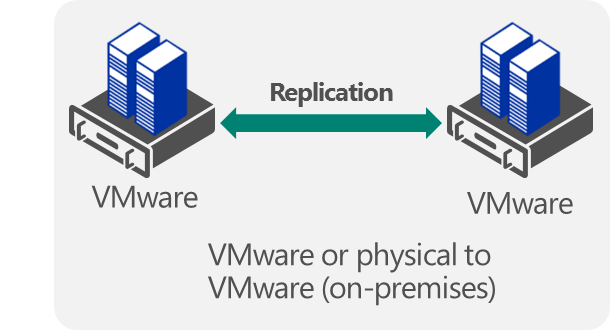
The article includes an overview and deployment prerequisites. It walks you through configuring and enable replication in VMM and the Site Recovery vault. You'll discover and classify SAN storage in VMM, provision LUNs, and allocate storage to Hyper-V clusters. It finishes up by testing failover to make sure everything's working as expected.



Scenario guide: <https://azure.microsoft.com/en-us/documentation/articles/site-recovery-vmm-san/>

## Protection between on-premises VMware sites

InMage Scout in Azure Site Recovery provides real-time replication between on-premises VMware sites. InMage Scout is included in Azure Site Recovery service subscriptions.



Scenario guide: <https://azure.microsoft.com/en-us/documentation/articles/site-recovery-vmware-to-vmware/>