Microsoft Azure - Starter Kits for Partners

Hands on Lab

Azure Site Recovery

Last Update: 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.

© 2015 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](#_Toc427788464)

[Deployment Scenarios 4](#_Toc427788465)

[Protection between an on-premises VMM site and Azure 5](#_Toc427788466)

[Protection between an on-premises Hyper-V site and Azure 6](#_Toc427788467)

[Protection between on-premises VMware virtual machines or physical servers and Azure 7](#_Toc427788468)

[Protection between on-premises VMM sites 8](#_Toc427788469)

[Protection between on-premises VMM sites with SAN 9](#_Toc427788470)

[Protection between on-premises VMware sites 10](#_Toc427788471)

## 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.

## 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.

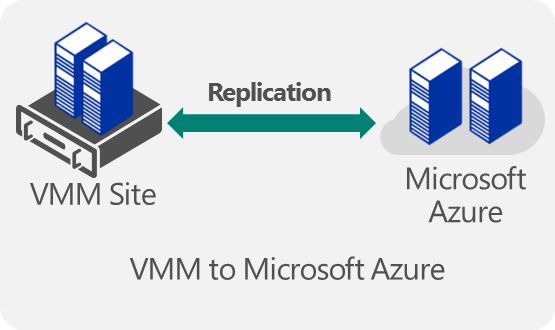
This table summarizes the replication scenarios supported by Site Recovery.

|  |  |  |
| --- | --- | --- |
| 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.

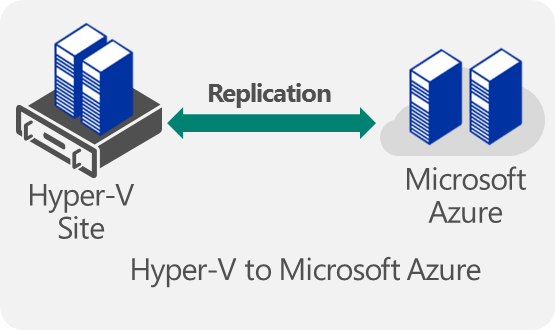
The guide includes prerequisites for the scenario and shows you how to set up a Site Recovery vault, get the Azure Site Recovery Provider installed on the source VMM server, register the server in the vault, add an Azure storage account, install the Azure Recovery Services agent on Hyper-V host servers, 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.



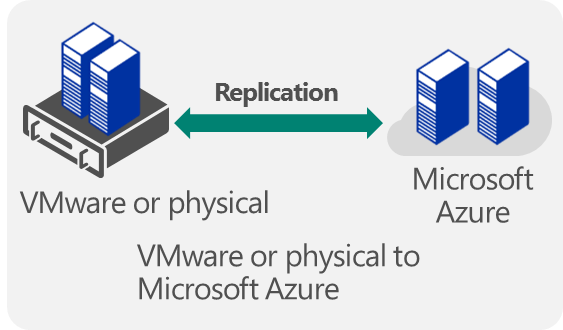
Scenario guide: <https://azure.microsoft.com/en-us/documentation/articles/site-recovery-hyper-v-site-to-azure/>

### 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.

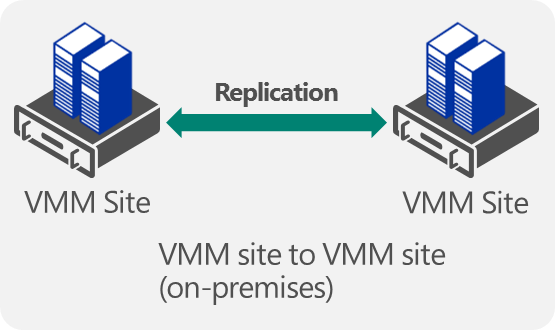


Scenario guide: <https://azure.microsoft.com/en-us/documentation/articles/site-recovery-vmware-to-azure/>

### 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.

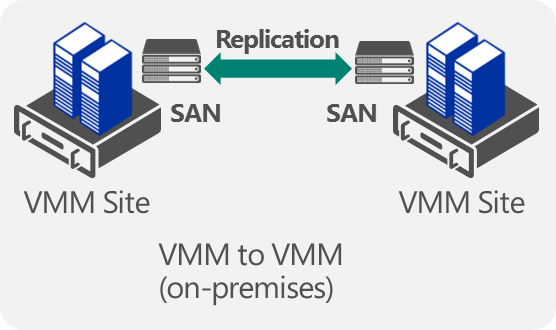
The guide includes prerequisites for the scenario and shows you how to set up a Site Recovery vault, get the Azure Site Recovery Provider installed on source and target VMM servers, register the servers in the vault, configure protection settings for VMM clouds that will be applied to all protected virtual 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

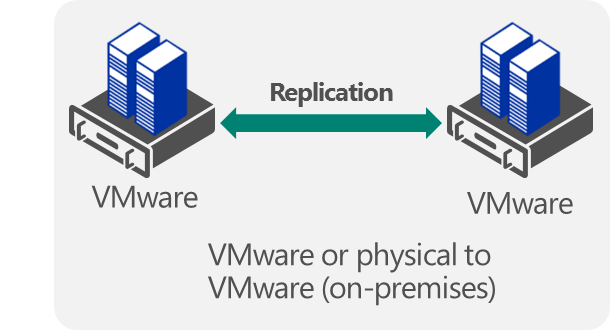
The article includes an overview and deployment prerequisites. It walks you through configuring and enable replication in VMM and the Site Recovery vault. You'll discover and classify SAN storage in VMM, provision LUNs, and allocate storage to Hyper-V clusters. It finishes up by testing failover to make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