

Contents

[Site Recovery Documentation](#)

[Overview](#)

[About Site Recovery](#)

[What's new in Site Recovery](#)

[Quickstarts](#)

[Replicate an Azure VM to another region](#)

[Tutorials](#)

[Azure VM disaster recovery to Azure](#)

[Enable replication](#)

[Run a disaster recovery drill](#)

[Run failover and reprotect](#)

[Run fallback](#)

[Move](#)

[Move Azure VMs to another region](#)

[Move Azure VMs to Availability Zones](#)

[Move Azure VMs between Government & Public regions](#)

[Move a vault to a different region](#)

[VMware VM disaster recovery to Azure](#)

[Prepare Azure](#)

[Prepare on-premises VMware](#)

[Set up replication](#)

[Run a disaster recovery drill](#)

[Fail over to Azure](#)

[Hyper-V VM disaster recovery to Azure](#)

[Prepare Azure](#)

[Prepare on-premises Hyper-V](#)

[Set up replication for Hyper-V VMs](#)

[Set up replication for Hyper-V VMs in VMM clouds](#)

[Run a disaster recovery drill](#)

[Fail over to Azure](#)

[Migrate to Azure](#)

[Prepare Azure for on-premises replication](#)

[Migrate on-premises machines to Azure](#)

[Migrate on-premises Windows Server 2008 servers to Azure](#)

[Migrate AWS instances to Azure](#)

[Concepts](#)

[Common questions about Site Recovery](#)

[About Azure VM disaster recovery](#)

[Azure to Azure architecture](#)

[Common questions](#)

[Azure to Azure support matrix](#)

[Using Site Recovery with Azure Backup](#)

[Accelerated networking for Azure VM disaster recovery](#)

[ExpressRoute with Azure VM disaster recovery](#)

[About moving Azure VMs to another region](#)

[About VMware VM disaster recovery](#)

[VMware disaster recovery overview](#)

[Common questions](#)

[VMware/physical to Azure support matrix](#)

[About Site Recovery components \(configuration/process/master target server\)](#)

[Support requirements for configuration and process servers](#)

[VMware to Azure architecture](#)

[About excluding disks from replication](#)

[Fallback location options from Azure to VMware](#)

[Multi-tenant support for VMware disaster recovery](#)

[About Hyper-V VM disaster recovery](#)

[Common questions](#)

[Support matrix](#)

[Hyper-V to Azure architecture](#)

[About excluding disks from replication](#)

[About physical server disaster recovery](#)

[VMware/physical to Azure support matrix](#)
[Physical server to Azure architecture](#)
[About excluding disks from replication](#)
[About networking for disaster recovery](#)
[Azure Traffic Manager with Site Recovery](#)
[ExpressRoute with Site Recovery](#)
[Network Security Groups with Site Recovery](#)
[Using public IP addresses with Site Recovery](#)
[About failover and fallback](#)
[About recovery plans](#)
[About migration to Azure](#)
[About role-based access control with Site Recovery](#)
[About disaster recovery to a secondary on-premises site](#)
[Support matrix for VMware/physical server](#)
[Architecture for VMware VM/physical server to a secondary site](#)
[Support matrix for Hyper-V](#)
[Architecture for Hyper-V VM to a secondary site](#)

How-to Guides

[Azure to Azure disaster recovery](#)

- [Set up networking](#)
 - [Prepare networking for Azure VM disaster recovery](#)
 - [Customize networking configurations of the target Azure VM](#)
 - [Set up network mapping and retain IP addresses after failover](#)
 - [Examples for retaining IP addresses after failover](#)
 - [Integrate ExpressRoute with Azure VM disaster recovery](#)
- [Set up disaster recovery](#)
 - [Enable Azure to Azure replication](#)
 - [Enable Azure to Azure replication for encrypted VMs](#)
 - [Enable Azure to Azure replication for VMs with CMK enabled disks](#)
 - [Enable Azure to Azure replication for S2D VMs](#)
 - [Enable replication for an added disk](#)
 - [Exclude disks](#)

- Reprotect Azure VMs after failover
 - Set up disaster recovery for Azure VMs after migration to Azure
- Manage
 - Update the Mobility Service for Azure VMs
 - Manage Site Recovery updates
 - Remove servers and disable protection
 - Delete a vault
- VMware to Azure disaster recovery
 - Set up disaster recovery at scale
 - Set up networking
 - Manage network interfaces for on-premises to Azure replication
 - Set up IP addressing for failover
 - Perform capacity planning
 - Plan capacity
 - Deployment Planner tool for VMware replication to Azure
 - Overview and prerequisites
 - Deployment Planner version history
 - Run the Deployment Planner tool
 - Analyze the generated report
 - Analyze the cost estimation report
 - Scale out process servers for VMware replication
 - Set up disaster recovery
 - Set up the source environment
 - Deploy the configuration server
 - Set up the target environment
 - Configure replication settings
 - Deploy the Mobility service
 - Mobility service overview and installation
 - Prepare for push installation
 - Automate Mobility service deployment
 - Enable replication for VMware VMs
 - Exclude disks from replication

Walkthrough-Set up replication with multi-tenancy and CSP for VMWare VMs

Run failover and failback

Set up recovery plans

Run a disaster recovery drill to Azure

Run a failover to Azure

Prepare for reprotection/failback

Reprotect from Azure to on-premises

Fail back from Azure to on-premises

Set up a failback process server in Azure

Set up a Linux master target server for failback

Manage

Manage the Mobility agent

Manage the configuration server for VMware

Manage process servers

Manage vCenter servers

Manage Site Recovery updates

Remove servers and disable protection

Delete a vault

Physical to Azure disaster recovery

Set up disaster recovery at scale

Set up networking

Manage network interfaces for on-premises to Azure replication

Set up IP addressing for failover

Set up disaster recovery

Walkthrough-Set up disaster recovery

Set up the source environment

Set up the target environment

Deploy the Mobility service

About Mobility service installation

Prepare for push installation of the Mobility service

Deploy the Mobility service with Configuration Manager

Run failover and failback

Manage

- Manage the Mobility service
- Manage the configuration server
- Manage process servers
- Remove servers and disable protection
- Manage Site Recovery updates
- Delete a vault

Azure Stack VM disaster recovery

Walkthrough-Set up disaster recovery for Azure Stack VMs

Hyper-V to Azure disaster recovery

- Set up networking
 - Manage network interfaces for on-premises to Azure replication
 - Set up IP addressing for failover
- Perform capacity planning
 - Deployment Planner tool for Hyper-V replication to Azure
 - Overview and prerequisites
 - Deployment Planner version history
 - Run the Deployment Planner tool
 - Analyze the generated report
 - Analyze the cost estimation report

Set up disaster recovery

- Prepare network mapping for Hyper-V VM disaster recovery
- Exclude disks from replication

Run failover and fallback

- Set up recovery plans
- Add VMM scripts to recovery plans
- Run a disaster recovery drill to Azure
- Run a failover to Azure
- Fail back from Azure to Hyper-V

Manage

- Deprecation of Site Recovery data encryption
- Upgrade Windows Servers configured with Site Recovery

[Remove servers and disable protection](#)

[Manage Site Recovery updates](#)

[Delete a vault](#)

[Disaster recovery for apps](#)

[About disaster recovery for on-premises apps](#)

[Active Directory and DNS](#)

[SQL Server](#)

[SharePoint](#)

[Dynamics AX](#)

[RDS](#)

[Exchange](#)

[SAP](#)

[File Server](#)

[IIS based web applications](#)

[Citrix XenApp and XenDesktop](#)

[Other workloads](#)

[Disaster recovery to a secondary site](#)

[VMware VMs/physical servers](#)

[Walkthrough-Disaster recovery of VMware VMs and physical servers to a secondary site](#)

[Hyper-V VMs](#)

[Deprecation of site-to-site scenario for Hyper-V VMs](#)

[Walkthrough-Disaster recovery of Hyper-V VMs in VMM clouds to a secondary site](#)

[Run a disaster recovery drill for Hyper-V VMs to a secondary site](#)

[Set up IP addressing for failover](#)

[Add VMM scripts to recovery plans](#)

[Run a failover and fallback between on-premises sites](#)

[Performance scale tests for disaster recovery to a secondary site](#)

[Automation](#)

[Set up disaster recovery of Azure VMs using PowerShell](#)

[Set up disaster recovery of VMware VMs to Azure using PowerShell](#)

[Set up disaster recovery of Hyper-V VMs to Azure using PowerShell](#)

[Set up disaster recovery of Hyper-V VMs \(with VMM\) using PowerShell](#)

[Add automation runbooks to recovery plans](#)

Monitoring

[Common questions about monitoring](#)

[Monitor Site Recovery](#)

[Monitor Site Recovery with Azure Monitor Logs](#)

[Monitor process servers](#)

Troubleshooting

[Troubleshoot Azure VMs](#)

[Troubleshoot Azure VM replication](#)

[Troubleshoot Azure VM connectivity issues](#)

[Troubleshoot ongoing replication](#)

[Troubleshoot Mobility service issues](#)

[Troubleshoot VMware VMs/physical servers](#)

[Troubleshoot VMware VM/physical server replication](#)

[Troubleshoot configuration servers](#)

[Troubleshoot process servers](#)

[Troubleshoot push installation of the Mobility service](#)

[Troubleshoot failover to Azure](#)

[Troubleshoot reprotection and failback of VMware VMs](#)

[Troubleshoot Provider upgrade failures](#)

[Troubleshoot vCenter discovery failures](#)

[Troubleshoot Hyper-V](#)

[Troubleshoot Hyper-V replication](#)

[Troubleshoot failover to Azure](#)

Reference

[Azure PowerShell](#)

[AzureRM PowerShell](#)

[Resource Manager template](#)

[REST](#)

Related

[Azure Automation](#)

Resources

[Azure Roadmap](#)

[Blog](#)

[Forum](#)

[Learning path](#)

[Pricing](#)

[Pricing calculator](#)

[Service updates](#)

About Site Recovery

9/9/2019 • 3 minutes to read • [Edit Online](#)

Welcome to the Azure Site Recovery service! This article provides a quick service overview.

As an organization you need to adopt a business continuity and disaster recovery (BCDR) strategy that keeps your data safe, and your apps and workloads up and running, when planned and unplanned outages occur.

Azure Recovery Services contribute to your BCDR strategy:

- **Site Recovery service:** Site Recovery helps ensure business continuity by keeping business apps and workloads running during outages. Site Recovery replicates workloads running on physical and virtual machines (VMs) from a primary site to a secondary location. When an outage occurs at your primary site, you fail over to secondary location, and access apps from there. After the primary location is running again, you can fail back to it.
- **Backup service:** The [Azure Backup](#) service keeps your data safe and recoverable by backing it up to Azure.

Site Recovery can manage replication for:

- Azure VMs replicating between Azure regions.
- On-premises VMs, Azure Stack VMs and physical servers.

What does Site Recovery provide?

FEATURE	DETAILS
Simple BCDR solution	Using Site Recovery, you can set up and manage replication, failover, and fallback from a single location in the Azure portal.
Azure VM replication	You can set up disaster recovery of Azure VMs from a primary region to a secondary region.
On-premises VM replication	You can replicate on-premises VMs and physical servers to Azure, or to a secondary on-premises datacenter. Replication to Azure eliminates the cost and complexity of maintaining a secondary datacenter.
Workload replication	Replicate any workload running on supported Azure VMs, on-premises Hyper-V and VMware VMs, and Windows/Linux physical servers.
Data resilience	Site Recovery orchestrates replication without intercepting application data. When you replicate to Azure, data is stored in Azure storage, with the resilience that provides. When failover occurs, Azure VMs are created, based on the replicated data.

FEATURE	DETAILS
RTO and RPO targets	Keep recovery time objectives (RTO) and recovery point objectives (RPO) within organizational limits. Site Recovery provides continuous replication for Azure VMs and VMware VMs, and replication frequency as low as 30 seconds for Hyper-V. You can reduce RTO further by integrating with Azure Traffic Manager .
Keep apps consistent over failover	You can replicate using recovery points with application-consistent snapshots. These snapshots capture disk data, all data in memory, and all transactions in process.
Testing without disruption	You can easily run disaster recovery drills, without affecting ongoing replication.
Flexible failovers	You can run planned failovers for expected outages with zero-data loss, or unplanned failovers with minimal data loss (depending on replication frequency) for unexpected disasters. You can easily fail back to your primary site when it's available again.
Customized recovery plans	Using recovery plans, can customize and sequence the failover and recovery of multi-tier applications running on multiple VMs. You group machines together in a recovery plan, and optionally add scripts and manual actions. Recovery plans can be integrated with Azure automation runbooks.
BCDR integration	Site Recovery integrates with other BCDR technologies. For example, you can use Site Recovery to protect the SQL Server backend of corporate workloads, with native support for SQL Server AlwaysOn, to manage the failover of availability groups.
Azure automation integration	A rich Azure Automation library provides production-ready, application-specific scripts that can be downloaded and integrated with Site Recovery.
Network integration	Site Recovery integrates with Azure for simple application network management, including reserving IP addresses, configuring load-balancers, and integrating Azure Traffic Manager for efficient network switchovers.

What can I replicate?

SUPPORTED	DETAILS

Supported	Details
Replication scenarios	<p>Replicate Azure VMs from one Azure region to another.</p> <p>Replicate on-premises VMware VMs, Hyper-V VMs, physical servers (Windows and Linux), Azure Stack VMs to Azure.</p> <p>Replicate AWS Windows instances to Azure.</p> <p>Replicate on-premises VMware VMs, Hyper-V VMs managed by System Center VMM, and physical servers to a secondary site.</p>
Regions	Review supported regions for Site Recovery.
Replicated machines	Review the replication requirements for Azure VM replication , on-premises VMware VMs and physical servers , and on-premises Hyper-V VMs .
Workloads	You can replicate any workload running on a machine that's supported for replication. In addition, the Site Recovery team have performed app-specific testing for a number of apps .

Next steps

- Read more about [workload support](#).
- Get started with [Azure VM replication between regions](#).

What's new in Site Recovery

2/6/2020 • 15 minutes to read • [Edit Online](#)

The [Azure Site Recovery](#) service is updated and improved on an ongoing basis. To help you stay up-to-date, this article provides you with information about the latest releases, new features, and new content. This page is updated on a regular basis.

You can follow and subscribe to Site Recovery update notifications in the [Azure updates](#) channel.

Supported updates

For Site Recovery components, we support N-4 versions, where N is the latest released version. These are summarized in the following table.

UPDATE	UNIFIED SETUP	CONFIGURATION SERVER OVA	MOBILITY SERVICE AGENT	SITE RECOVERY PROVIDER	RECOVERY SERVICES AGENT
Rollup 43	9.31.5449.1	5.1.5300.0	9.31.5449.1	5.1.5300.0	2.0.9165.0
Rollup 42	9.30.5407.1	5.1.5200.0	9.30.5407.1	5.1.5200.0	2.0.9165.0
Rollup 41	9.29.5367.1	5.1.5000.0	9.29.5367.1	5.1.5000.0	2.0.9165.0
Rollup 40	9.28.5345.1	5.1.4800.0	9.28.5345.1	5.1.4800.0	2.0.9165.0
Rollup 39	9.27.5308.1	5.1.4600.0	9.27.5308.1	5.1.4600.0	2.0.9165.0

[Learn more](#) about update installation and support.

Updates (January 2020)

Update rollup 44

[Update rollup 44](#) provides the following updates.

UPDATE	DETAILS
Providers and agents	There were no updates for the Site Recovery providers and agents.
Issue fixes/improvements	A number of fixes and improvements as detailed in the rollup.

Azure VMware disaster recovery

Azure virtual machines now support VMs enable for encryption-at-rest with customer-managed keys. [Learn more](#).

Update rollup 43

[Update rollup 43](#) provides the following updates.

UPDATE	DETAILS
Providers and agents	Updates to Site Recovery agents and providers (as detailed in the rollup)
Issue fixes/improvements	A number of fixes and improvements (as detailed in the rollup)

Updates (November 2019)

Update rollup 42

[Update rollup 42](#) provides the following updates.

UPDATE	DETAILS
Providers and agents	Updates to Site Recovery agents and providers (as detailed in the rollup)
Issue fixes/improvements	A number of fixes and improvements (as detailed in the rollup)

Azure VM disaster recovery

New features for Azure VM disaster recovery are summarized in the table.

FEATURE	DETAILS
UEFI	Site Recovery now supports disaster recovery for Azure VMs with UEFI-based boot architecture.
Linux	Site Recovery now supports Azure VMs running Linux with Azure Disk Encryption (ADE).
Generation 2	All generation 2 Azure VMs are now supported for disaster recovery.
Regions	You can now enable disaster recovery for Azure VMs in the Norway geo.

VMware to Azure disaster recovery

New features for VMware to Azure disaster recovery are summarized in the table.

FEATURE	DETAILS
UEFI	Site Recovery now supports disaster recovery for VMware VMs with UEFI-based boot architecture. Supported operating systems include Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, SLES 12 SP4, RHEL 8.

Update to servicing stack update/SHA-2

For disaster recovery of Azure VMs to a secondary region, or on-premises VMware VMs or physical servers to Azure, note the following:

- From version 9.30.5407.1 of the Mobility service extension (for Azure VMs), and Mobility service agent (for VMware/physical machines), some machine operating systems must be running the servicing stack update and SHA-2. Details are shown in the table below.
- Install the update and SHA-2 in accordance with the linked KB. SHA-1 isn't supported from September 2019, and if SHA-2 code signing isn't enabled the agent extension won't install/upgrade as expected.
- Learn more about [SHA-2 upgrade and requirements](#).

OPERATING SYSTEM	AZURE VM	VMWARE VM/PHYSICAL MACHINE
Windows 2008 R2 SP1	Servicing stack update SHA-2	Servicing stack update SHA-2
Windows 2008 SP2	Servicing stack update SHA-2	Servicing stack update SHA-2
Windows 7 SP1	Servicing stack update SHA-2	Servicing stack update SHA-2.

Updates (October 2019)

Update rollup 41

[Update rollup 41](#) provides the following updates.

UPDATE	DETAILS
Providers and agents	Updates to Site Recovery agents and providers (as detailed in the rollup)
Issue fixes/improvements	A number of fixes and improvements (as detailed in the rollup)

Azure VM disaster recovery

New features for Azure VM disaster recovery are summarized in the table.

FEATURE	DETAILS
Test failover settings	When setting up a test failover, you can now configure settings for the test failover VM and network, including IP address, NSG, internal load balance, and the public IP address for each machine NIC. These settings are optional and don't change current behavior. If you don't configure these settings, you can choose an Azure VNet at the time of test failover. Learn more .
Recovery plans	Recovery plans are now limited to 100 VMs, to ensure failover reliability.

VMware to Azure disaster recovery

New features for VMware to Azure disaster recovery are summarized in the table.

FEATURE	DETAILS
Recovery plans	Recovery plans are now limited to 100 VMs, to ensure failover reliability.

Updates (September 2019)

Update rollup 40

[Update rollup 40](#) provides the following updates.

UPDATE	DETAILS
Providers and agents	Updates to Site Recovery agents and providers (as detailed in the rollup)
Issue fixes/improvements	A number of fixes and improvements (as detailed in the rollup)

Azure VM disaster recovery

New features for Azure VM disaster recovery are summarized in the table.

FEATURE	DETAILS
Cleanup after failback	After failing over to the secondary Azure, and then failing back to the primary region, Site Recovery automatically cleans up machines in the secondary region. There's no need to manually delete VMs and NICs.
Test failover retains IP address	You can now retain the IP address of the source VM during a disaster recovery drill, and pick a static IP address for a test failover.

VMware/physical server disaster recovery

Features added this month are summarized in the table.

FEATURE	DETAILS
New process server alerts	We've added new process server alerts. Learn more .

Hyper-V disaster recovery

Features added this month are summarized in the table.

FEATURE	DETAILS
Storage account	Site Recovery now supports the use of storage accounts with firewall enabled for Hyper-V to Azure disaster recovery. You can select firewall-enabled storage accounts as a target account, or for cache storage. If you use firewall-enabled account, make sure that you enable the option to allow trusted Microsoft services. This is supported for Hyper-V VMs with or without System Center VMM.

Updates (August 2019)

Update rollup 39

[Update rollup 39](#) provides the following updates.

UPDATE	DETAILS
Providers and agents	Updates to Site Recovery agents and providers (as detailed in the rollup)
Issue fixes/improvements	A number of fixes and improvements (as detailed in the rollup)

Azure VM disaster recovery

New features for Azure VM disaster recovery are summarized in the table.

FEATURE	DETAILS
Encryption without Azure AD	Encryption without an Azure AD app is now supported for Azure VM replication to managed disks running Windows.
Network resources for failover	When failing over to another region, you can now attach network resource settings (NSGs, load balancing, public IP address) to a VM.

Updates (July 2019)

Update rollup 38

[Update rollup 38](#) provides the following updates.

UPDATE	DETAILS
Providers and agents	Updates to Site Recovery agents and providers (as detailed in the rollup)
Issue fixes/improvements	A number of fixes and improvements (as detailed in the rollup)

General

Site Recovery now supports the use of general purpose v2 storage accounts for cache storage or target storage. Previously only v1 was supported.

VMware to Azure disaster recovery

You can now replicate disks up to 8 TB, when replicating to an Azure VM with managed disks.

Updates (June 2019)

Update rollup 37

[Update rollup 37](#) provides the following updates.

UPDATE	DETAILS
Providers and agents	Updates to Site Recovery agents and providers (as detailed in the rollup)
Issue fixes/improvements	A number of fixes and improvements (as detailed in the rollup)

VMware/physical server disaster recovery

Features added this month are summarized in the table.

FEATURE	DETAILS
GPT partitions	From Update Rollup 37 onwards (Mobility service version 9.25.5241.1), up to five GPT partitions are supported in UEFI. Prior to this update, four were supported.

Updates (May 2019)

Update rollup 36

[Update rollup 36](#) provides the following updates.

UPDATE	DETAILS
Providers and agents	An update to Site Recovery agents and providers (as detailed in the rollup)
Issue fixes/improvements	A number of fixes and improvements (as detailed in the rollup)

Azure VM disaster recovery

Features added this month are summarized in the table.

FEATURE	DETAILS
Replicate added disks	Enable replication for data disks added to an Azure VM that's already enabled for disaster recovery. Learn more .
Automatic updates	When configuring automatic updates for the Mobility service extension that runs on Azure VMs enabled for disaster recovery, you can now select an existing automation account to use, instead of using the default account created by Site Recovery. Learn more .

VMware/physical server disaster recovery

Features added this month are summarized in the table.

FEATURE	DETAILS
Process server monitoring	For disaster recovery of on-premises VMware VMs and physical servers, monitor and troubleshoot process server issues with improved server health reporting and alerts. Learn more .

Updates (March 2019)

Update rollup 35

[Update rollup 35](#) provides the following updates.

UPDATE	DETAILS
Providers and agents	An update to Site Recovery agents and providers (as detailed in the rollup)
Issue fixes/improvements	A number of fixes and improvements (as detailed in the rollup)

VMware/physical server disaster recovery

Features added this month are summarized in the table.

FEATURE	DETAILS
Managed disks	Replication of on-premises VMware VMs and physical servers is now directly to managed disks in Azure. On-premises data is sent to a cache storage account in Azure, and recovery points are created in managed disks in the target location. This ensures you don't need to manage multiple target storage accounts.
Configuration server	Site Recovery now supports configuration servers with multiple NICs. Add additional adapters to the configuration server VM before you register the configuration server in the vault. If you add afterwards, you need to re-register the server in the vault.

Updates (February 2019)

Update rollup 34

[Update rollup 34](#) provides the following updates.

UPDATE	DETAILS
Providers and agents	An update to Site Recovery agents and providers (as detailed in the rollup).
Issue fixes/improvements	A number of fixes and improvements (as detailed in the rollup).

Update rollup 33

[Update rollup 33](#) provides the following updates.

UPDATE	DETAILS
Providers and agents	An update to Site Recovery agents and providers (as detailed in the rollup).
Issue fixes/improvements	A number of fixes and improvements (as detailed in the rollup).

Azure VM disaster recovery

Features added this month are summarized in the table.

FEATURE	DETAILS
Network mapping	For Azure VM disaster recovery, you can now use any available target network when you enable replication.
Standard SSD	You can now set up disaster recovery for Azure VMs using Standard SSD disks .
Storage Spaces Direct	You can set up disaster recovery for apps running on Azure VM apps by using Storage Spaces Direct for high availability. Using Storage Spaces Direct (S2D) together with Site Recovery provides comprehensive protection of Azure VM workloads. S2D lets you host a guest cluster in Azure. This is especially useful when a VM hosts a critical application, such as SAP ASCS layer, SQL Server, or scale-out file server.

VMware/physical server disaster recovery

Features added this month are summarized in the table.

FEATURE	DETAILS
Linux BTRFS file system	Site Recovery now supports replication of VMware VMs with the BTRFS file system. Replication isn't supported if: <ul style="list-style-type: none"> - The BTRFS file system sub-volume is changed after enabling replication. - The file system is spread over multiple disks. - The BTRFS file system supports RAID.
Windows Server 2019	Support added for machines running Windows Server 2019.

Updates (January 2019)

Accelerated networking (Azure VMs)

Accelerated networking enables single root I/O virtualization (SR-IOV) to a VM, improving networking performance. When you enable replication for an Azure VM, Site Recovery detects whether accelerated networking is enabled. If it is, after failover Site Recovery automatically configures accelerated networking on the target replica Azure VM, for both [Windows](#) and [Linux](#).

[Learn more.](#)

Update rollup 32

[Update rollup 32](#) provides the following updates.

UPDATE	DETAILS
Providers and agents	An update to Site Recovery agents and providers (as detailed in the rollup).
Issue fixes/improvements	A number of fixes and improvements (as detailed in the rollup).

Azure VM disaster recovery

Features added this month are summarized in the table.

FEATURE	DETAILS
Linux support	Support was added for RedHat Workstation 6/7, and new kernel versions for Ubuntu, Debian, and SUSE.
Storage Spaces Direct	Site Recovery supports Azure VMs using Storage Spaces Direct (S2D).

VMware VMs/physical servers disaster recovery

Features added this month are summarized in the table.

FEATURE	DETAILS
Linux support	Support was added for Redhat Enterprise Linux 7.6, RedHat Workstation 6/7, Oracle Linux 6.10 and Oracle Linux 7.6, and new kernel versions for Ubuntu, Debian, and SUSE.

Update rollup 31

[Update rollup 31](#) provides the following updates.

UPDATE	DETAILS
Providers and agents	An update to Site Recovery agents and providers (as detailed in the rollup).
Issue fixes/improvements	A number of fixes and improvements (as detailed in the rollup).

VMware VMs/physical servers replication

Features added this month are summarized in the table.

FEATURE	DETAILS
Linux support	Support was added for Oracle Linux 6.8, Oracle Linux 6.9 and Oracle Linux 7.0 with the Red Hat Compatible Kernel, and for the Unbreakable Enterprise Kernel (UEK) Release 5.
LVM	Support added for LVM and LVM2 volumes. The /boot directory on a disk partition and on LVM volumes is now supported.
Directories	Support was added for these directories set up as separate partitions, or file systems that aren't on the same system disk: /root, /boot, /usr, /usr/local, /var, /etc.
Windows Server 2008	Support added for dynamic disks.
Failover	Improved failover time for VMware VMs where storvsc and vsbus aren't boot drivers.

FEATURE	DETAILS
UEFI support	Azure VMs don't support boot type UEFI. You can now migrate on-premises physical servers with UEFI to Azure with Site Recovery. Site Recovery migrates the server by converting the boot type to BIOS before migration. Site Recovery previously supported this conversion for VMs only. Support is available for physical servers running Windows Server 2012 or later.

Azure VM disaster recovery

Features added this month are summarized in the table.

FEATURE	DETAILS
Linux support	Support was added for Oracle Linux 6.8, Oracle Linux 6.9 and Oracle Linux 7.0 with the Red Hat Compatible Kernel, and for the Unbreakable Enterprise Kernel (UEK) Release 5.
Linux BRTFS file system	Supported for Azure VMs.
Azure VMs in availability zones	You can enable replication to another region for Azure VMs deployed in availability zones. You can now enable replication for an Azure VM, and set the target for failover to a single VM instance, a VM in an availability set, or a VM in an availability zone. The setting doesn't impact replication. Read the announcement .
Firewall-enabled storage (portal/PowerShell)	<p>Support added for firewall-enabled storage accounts.</p> <p>You can replicate Azure VMs with unmanaged disks on firewall-enabled storage accounts to another Azure region for disaster recovery.</p> <p>You can use firewall-enabled storage accounts as target storage accounts for unmanaged disks.</p> <p>Supported in portal and using PowerShell.</p>

Updates (December 2018)

Automatic updates for the Mobility service (Azure VMs)

Site Recovery added an option for automatic updates to the Mobility service extension. The Mobility service extension is installed on each Azure VM replicated by Site Recovery. When you enable replication, you select whether to allow Site Recovery to manage updates to the extension.

Updates don't require a VM restart, and don't affect replication. [Learn more](#).

Pricing calculator for Azure VM disaster recovery

Disaster Recovery of Azure VMs incurs VM licensing costs, and network and storage costs. Azure provides a [pricing calculator](#) to help you figure out these costs. Site Recovery now provides an [example pricing estimate](#) that prices a sample deployment based on a three-tier app using six VMs with 12 Standard HDD disks and 6 Premium SSD disks.

- The sample presumes a data change of 10 GB a day for standard, and 20 GB for premium.
- For your particular deployment, you can change the variables to estimate costs.

- You can specify the number of VMs, the number and type of managed disks, and the expected total data change rate expected across the VMs.
- Additionally, you can apply a compression factor to estimate bandwidth costs.

[Read](#) the announcement.

Updates (October 2018)

Update rollup 30

[Update rollup 30](#) provides the following updates.

UPDATE	DETAILS
Providers and agents	An update to Site Recovery agents and providers (as detailed in the rollup).
Issue fixes/improvements	A number of fixes and improvements (as detailed in the rollup).

Azure VM disaster recovery

Features added this month are summarized in the table.

FEATURE	DETAILS
Region support	Site Recovery support added for Australia Central 1 and Australia Central 2.
Support for disk encryption	Support added for disaster recovery of Azure VMs encrypted with Azure Disk Encryption (ADE) with the Azure AD app. Learn more .
Disk exclusion	Uninitialized disks are now automatically excluded during Azure VM replication.
Firewall-enabled storage (PowerShell)	Support added for firewall-enabled storage accounts . You can replicate Azure VMs with unmanaged disks on firewall-enabled storage accounts to another Azure region for disaster recovery. You can use firewall-enabled storage accounts as target storage accounts for unmanaged disks. Supported using PowerShell only.

Update rollup 29

[Update rollup 29](#) provides the following updates.

UPDATE	DETAILS
Providers and agents	An update to Site Recovery agents and providers (as detailed in the rollup).
Issue fixes/improvements	A number of fixes and improvements (as detailed in the rollup).

Updates (August 2018)

Update rollup 28

[Update rollup 28](#) provides the following updates.

UPDATE	DETAILS
Providers and agents	An update to Site Recovery agents and providers (as detailed in the rollup).
Issue fixes/improvements	A number of fixes and improvements (as detailed in the rollup).

Azure VM disaster recovery

Features added this month are summarized in the table.

FEATURE	DETAILS
Linux support	Added supported for RedHat Enterprise Linux 6.10; CentOS 6.10.
Cloud support	Supported disaster recovery for Azure VMs in the Germany cloud.
Cross-subscription disaster recovery	Support for replicating Azure VMs in one region to another region in a different subscription, within the same Azure Active Directory tenant. Learn more .

VMware VM/physical server disaster recovery

Features added this month are summarized in the table.

FEATURE	DETAILS
Linux support	Support added for RedHat Enterprise Linux 6.10, CentOS 6.10. Linux-based VMs that use the GUID partition table (GPT) partition style in legacy BIOS compatibility mode are now supported. Review the Azure VM FAQ for more information.
Disaster recovery for VMs after migration	Support for enabling disaster recovery to a secondary region for an on-premises VMware VM migrated to Azure, without needing to uninstall the Mobility service on the VM before enabling replication.
Windows Server 2008	Support for migrating machines running Windows Server 2008 R2/2008 64-bit and 32-bit. Migration only (replication and failover). Failback isn't supported.

Updates (July 2018)

Update rollup 27 (July 2018)

Update rollup 27 provides the following updates.

UPDATE	DETAILS
Providers and agents	An update to Site Recovery agents and providers (as detailed in the rollup).
Issue fixes/improvements	A number of fixes and improvements (as detailed in the rollup).

Azure VM disaster recovery

Features added this month are summarized in the table.

FEATURE	DETAILS
Linux support	Support added for Red Hat Enterprise Linux 7.5.

VMware VM/physical server disaster recovery

Features added this month are summarized in the table.

FEATURE	DETAILS
Linux support	Support added for Red Hat Enterprise Linux 7.5, SUSE Linux Enterprise Server 12.

Next steps

Keep up-to-date with our updates on the [Azure Updates](#) page.

Set up disaster recovery to a secondary Azure region for an Azure VM

1/9/2020 • 2 minutes to read • [Edit Online](#)

The [Azure Site Recovery](#) service contributes to your business continuity and disaster recovery (BCDR) strategy by keeping your business apps up and running, during planned and unplanned outages. Site Recovery manages and orchestrates disaster recovery of on-premises machines and Azure virtual machines (VMs), including replication, failover, and recovery.

This quickstart describes how to set up disaster recovery for an Azure VM by replicating it to a different Azure region.

If you don't have an Azure subscription, create a [free account](#) before you begin.

NOTE

This article is a quick walkthrough for new users. It uses the simplest path, with default options and minimum customization. For a full walkthrough, review the tutorial [Enable replication](#).

Log in to Azure

Log in to the [Azure portal](#).

Enable replication for the Azure VM

1. On the Azure portal menu, select **Virtual machines**, or search for and select *Virtual machines* on any page. Select the VM you want to replicate.
2. In **Operations**, select **Disaster recovery**.
3. In **Configure disaster recovery > Target region** select the target region to which you'll replicate.
4. For this Quickstart, accept the other default settings.
5. Select **Review + Start replication**. Then select **Start replication** to start a job to enable replication for the VM.

The screenshot shows the Azure portal interface for configuring disaster recovery. On the left, a sidebar lists various operations like Bastion, Auto-shutdown, Backup, and Disaster recovery, with 'Disaster recovery' being the selected option and highlighted with a red box. The main content area is titled 'Welcome to Azure Site Recovery' and includes a map of the world with green dots indicating available regions. A dropdown menu for 'Target region' is open, showing 'East US 2' as the selected option. At the bottom of the page, there are two buttons: 'Review + Start replication' (highlighted with a red box) and 'Next : Advanced settings'.

Verify settings

After the replication job has finished, you can check the replication status, modify replication settings, and test the deployment.

1. On the Azure portal menu, select **Virtual machines**, or search for and select **Virtual machines** on any page. Select the VM you want to verify.
2. In **Operations**, select **Disaster recovery**.

You can verify replication health, the recovery points that have been created, and source, target regions on the map.

The screenshot shows the Azure portal interface for managing disaster recovery settings. The left sidebar shows various operations like Size, Security, Extensions, and Disaster recovery, with Disaster recovery being the selected option. The main content area displays the configuration for a specific vault named 'site-recovery-test-central-us'. It includes sections for 'Essentials' (containing vault details like location, resource group, storage account, and network), 'Replication' (showing healthy status, protected status, and 3-minute RPO), and 'Events' (showing 0 events). A 'Latest Recovery Points' table lists crash-consistent and app-consistent points from August 21, 2018, at 3:23:56 PM. To the right, there is a world map with green dots representing available regions for replication.

Clean up resources

The VM in the primary region stops replicating when you disable replication for it:

- The source replication settings are cleaned up automatically. The Site Recovery extension installed on the VM as part of the replication isn't removed, and must be removed manually.
- Site Recovery billing for the VM stops.

Stop replication as follows:

- On the Azure portal menu, select **Virtual machines**, or search for and select *Virtual machines* on any page. Select the VM you want to modify.
- In **Disaster recovery**, select **Disable Replication**.

Essentials

Recovery Services vault: **bcdr-recovery-west-central-us**
Region: **West Central US**
24-hour-retention-policy
Operating system: **Windows**
Protected disks: **1**
Target size: **Standard_DS2_v2**

Replication

Health	Events	Latest Recovery Points
Replication health: Healthy	0	Crash-consistent: 8/21/2018, 3:23:56 PM App-consistent: 8/21/2018, 3:23:56 PM
Status: Protected		
RPO: 3 minutes [As on 8/21/2018]		

Map

A world map showing the replication path from the primary location (East US) to the secondary location (South Central US). The path is indicated by a dashed blue line connecting the two regions.

Next steps

In this quickstart, you replicated a single VM to a secondary region. Now, try replicating multiple Azure VMs using a recovery plan.

[Set up disaster recovery for Azure VMs](#)

Set up disaster recovery for Azure VMs

1/24/2020 • 9 minutes to read • [Edit Online](#)

The [Azure Site Recovery](#) service contributes to your disaster recovery strategy by managing and orchestrating replication, failover, and fallback of on-premises machines and Azure virtual machines (VMs).

This tutorial shows you how to set up disaster recovery for Azure VMs by replicating them from one Azure region to another. In this tutorial, you learn how to:

- Create a Recovery Services vault
- Verify target resource settings
- Set up outbound network connectivity for VMs
- Enable replication for a VM

NOTE

This article provides instructions for deploying disaster recovery with the simplest settings. If you want to learn about customized settings, review the articles in the [How To section](#).

Prerequisites

To complete this tutorial:

- Review the [scenario architecture and components](#).
- Review the [support requirements](#) before you start.

Create a Recovery Services vault

Create the vault in any region, except the source region.

1. Sign in to the [Azure portal](#).
2. On the Azure portal menu or from the **Home** page, select **Create a resource**. Then, select **IT & Management Tools > Backup and Site Recovery**.
3. In **Name**, specify a friendly name to identify the vault. If you have more than one subscription, select the appropriate one.
4. Create a resource group or select an existing one. Specify an Azure region. To check supported regions, see geographic availability in [Azure Site Recovery Pricing Details](#).
5. To access the vault from the dashboard, select **Pin to dashboard** and then select **Create**.

The screenshot shows the Azure portal interface. On the left, there's a list of existing Recovery Services vaults: contosoassessment-Migr..., ContosoCorporation-Rec..., ContosoDemo, ContosoEmpty, ContosoScale, ContosoVMVault, ContosoVMVault, and Demo. On the right, a modal window titled "Recovery Services vault" is open, prompting the user to "Click here to try new preview create vault experience with Tags support." The form fields are as follows:

- Name:** Vault1 (highlighted with a green checkmark)
- Subscription:** <subscription-name>
- Resource group:** RG1 (highlighted with a blue border)
- Location:** West Central US

The new vault is added to the **Dashboard** under **All resources**, and on the main **Recovery Services vaults** page.

Verify target resource settings

Check your Azure subscription for the target region.

- Verify that your Azure subscription allows you to create VMs in the target region. Contact support to enable the required quota.
- Make sure your subscription has enough resources to support VM sizes that match your source VMs. Site Recovery picks the same size, or the closest possible size, for the target VM.

Set up outbound network connectivity for VMs

For Site Recovery to work as expected, you need to modify outbound network connectivity from the VMs that you want to replicate.

NOTE

Site Recovery doesn't support using an authentication proxy to control network connectivity.

Outbound connectivity for URLs

If you're using a URL-based firewall proxy to control outbound connectivity, allow access to these URLs:

URL	DETAILS
*.blob.core.windows.net	Allows data to be written from the VM to the cache storage account in the source region.
login.microsoftonline.com	Provides authorization and authentication to Site Recovery service URLs.

URL	DETAILS
*.hypervrecoverymanager.windowsazure.com	Allows the VM to communicate with the Site Recovery service.
*.servicebus.windows.net	Allows the VM to write Site Recovery monitoring and diagnostics data.

Outbound connectivity for IP address ranges

If you're using a network security group (NSG), create service-tag based NSG rules for access to Azure Storage, Azure Active Directory, Site Recovery service, and Site Recovery monitoring. [Learn more](#).

Verify Azure VM certificates

Check that the VMs you want to replicate have the latest root certificates. If they don't, the VM can't be registered to Site Recovery because of security constraints.

- For Windows VMs, install all the latest Windows updates on the VM, so that all the trusted root certificates are on the machine. In a disconnected environment, follow the standard Windows Update and certificate update processes for your organization.
- For Linux VMs, follow the guidance provided by your Linux distributor, to get the latest trusted root certificates and certificate revocation list on the VM.

Set permissions on the account

Azure Site Recovery provides three built-in roles to control Site Recovery management operations.

- Site Recovery Contributor** - This role has all permissions required to manage Azure Site Recovery operations in a Recovery Services vault. A user with this role, however, can't create or delete a Recovery Services vault or assign access rights to other users. This role is best suited for disaster recovery administrators who can enable and manage disaster recovery for applications or entire organizations.
- Site Recovery Operator** - This role has permissions to execute and manage Failover and Failback operations. A user with this role can't enable or disable replication, create or delete vaults, register new infrastructure, or assign access rights to other users. This role is best suited for a disaster recovery operator who can fail over virtual machines or applications when instructed by application owners and IT administrators. Post resolution of the disaster, the disaster recovery operator can reprotect and failback the virtual machines.
- Site Recovery Reader** - This role has permissions to view all Site Recovery management operations. This role is best suited for an IT monitoring executive who can monitor the current state of protection and raise support tickets.

Learn more about [Azure RBAC built-in roles](#).

Enable replication for a VM

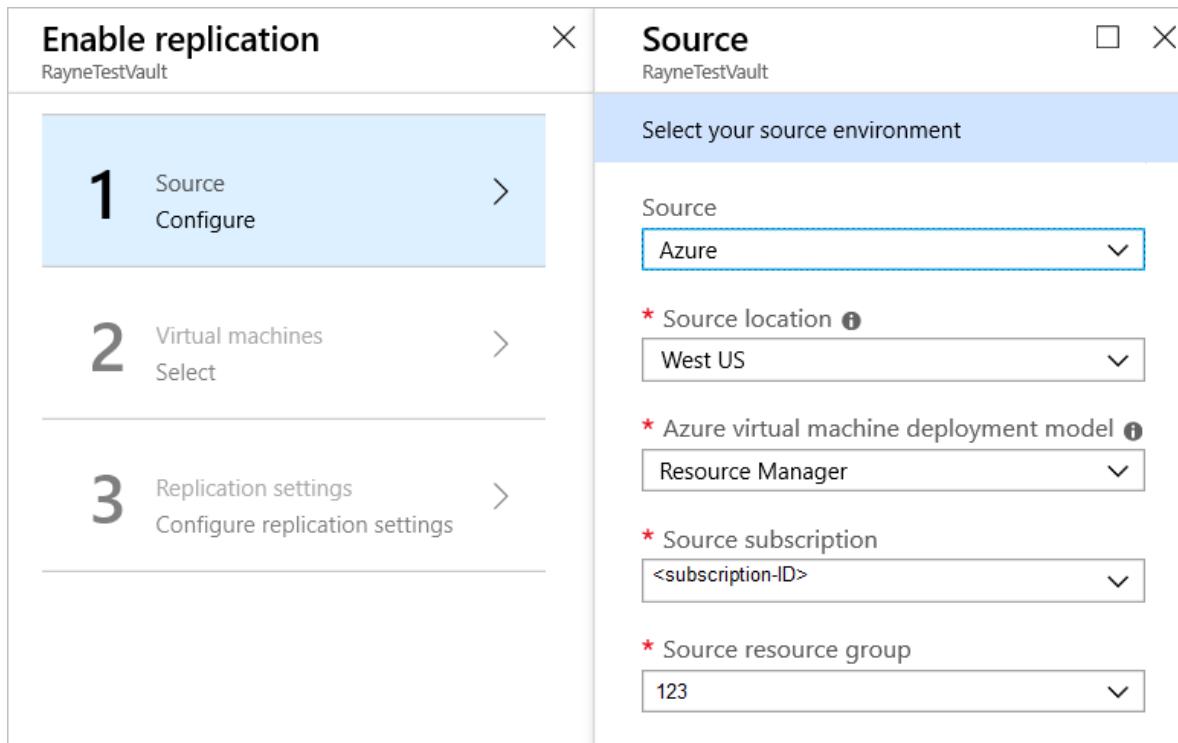
The following sections describe how to enable replication.

Select the source

To begin the replication set up, choose the source where your Azure VMs are running.

- Go to **Recovery Services vaults**, select the vault name, then select **+Replicate**.
- For the **Source**, select **Azure**.

3. In **Source location**, select the source Azure region where your VMs are currently running.
4. Select the **Source subscription** where the virtual machines are running. This can be any subscription within the same Azure Active Directory tenant where your recovery services vault exists.
5. Select the **Source resource group**, and select **OK** to save the settings.



Select the VMs

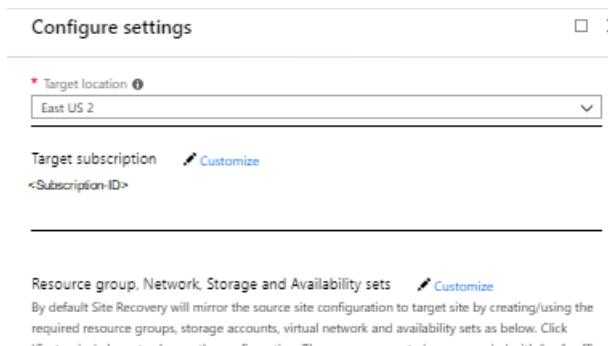
Site Recovery retrieves a list of the VMs associated with the subscription and resource group/cloud service.

1. In **Virtual Machines**, select the VMs you want to replicate.
2. Select **OK**.

Configure replication settings

Site Recovery creates default settings and replication policy for the target region. You can change these settings as required.

1. Select **Settings** to view the target and replication settings.
2. To override the default target settings, select **Customize** next to **Resource group, Network, Storage and Availability**.



3. Customize target settings as summarized in the table.

SETTING	DETAILS
Target subscription	By default, the target subscription is the same as the source subscription. Select Customize to select a different target subscription within the same Azure Active Directory tenant.
Target location	<p>The target region used for disaster recovery.</p> <p>We recommend that the target location matches the location of the Site Recovery vault.</p>
Target resource group	<p>The resource group in the target region that holds Azure VMs after failover.</p> <p>By default, Site Recovery creates a new resource group in the target region with an <code>asr</code> suffix. The location of the target resource group can be any region except the region in which your source virtual machines are hosted.</p>
Target virtual network	<p>The network in the target region that VMs are located after failover.</p> <p>By default, Site Recovery creates a new virtual network (and subnets) in the target region with an <code>asr</code> suffix.</p>
Cache storage accounts	<p>Site Recovery uses a storage account in the source region. Changes to source VMs are sent to this account before replication to the target location.</p> <p>If you're using a firewall-enabled cache storage account, make sure that you enable Allow trusted Microsoft services. Learn more. Also, ensure that you allow access to at least one subnet of the source Vnet.</p>
Target storage accounts (source VM uses non-managed disks)	<p>By default, Site Recovery creates a new storage account in the target region to mirror the source VM storage account.</p> <p>Enable Allow trusted Microsoft services if you're using a firewall-enabled cache storage account.</p>
Replica managed disks (If source VM uses managed disks)	By default, Site Recovery creates replica managed disks in the target region to mirror the source VM's managed disks with the same storage type (standard or premium) as the source VM's managed disk. You can only customize Disk type.
Target availability sets	By default, Azure Site Recovery creates a new availability set in the target region with name having <code>asr</code> suffix for the VMs part of an availability set in source region. In case availability set created by Azure Site Recovery already exists, it's reused.

SETTING	DETAILS
Target availability zones	<p>By default, Site Recovery assigns the same zone number as the source region in target region if the target region supports availability zones.</p> <p>If the target region doesn't support availability zones, the target VMs are configured as single instances by default.</p> <p>Select Customize to configure VMs as part of an availability set in the target region.</p> <p>You can't change the availability type (single instance, availability set, or availability zone) after you enable replication. To change the availability type, disable and enable replication.</p>

- To customize replication policy settings, select **Customize** next to **Replication policy**, and modify the settings as needed.

SETTING	DETAILS
Replication policy name	Policy name.
Recovery point retention	By default, Site Recovery keeps recovery points for 24 hours. You can configure a value between 1 and 72 hours.
App-consistent snapshot frequency	<p>By default, Site Recovery takes an app-consistent snapshot every 4 hours. You can configure any value between 1 and 12 hours.</p> <p>An app-consistent snapshot is a point-in-time snapshot of the application data inside the VM. Volume Shadow Copy Service (VSS) ensures that app on the VM are in a consistent state when the snapshot is taken.</p>
Replication group	If your application needs multi-VM consistency across VMs, you can create a replication group for those VMs. By default, the selected VMs are not part of any replication group.

- In **Customize**, select **Yes** for multi-VM consistency if you want to add VMs to a new or existing replication group. Then select **OK**.

NOTE

- All the machines in a replication group have shared crash consistent and app-consistent recovery points when failed over.
- Enabling multi-VM consistency can impact workload performance (it's CPU intensive). It should be used only if machines are running the same workload, and you need consistency across multiple machines.
- You can have a maximum of 16 VMs in a replication group.
- If you enable multi-VM consistency, machines in the replication group communicate with each other over port 20004. Make sure there's no firewall blocking the internal communication between the VMs over this port.
- For Linux VMs in a replication group, ensure the outbound traffic on port 20004 is manually opened in accordance with guidance for the Linux version.

Configure encryption settings

If the source VM has Azure disk encryption (ADE) enabled, review the settings.

1. Verify the settings:
 - a. **Disk encryption key vaults:** By default, Site Recovery creates a new key vault on the source VM disk encryption keys, with an `asr` suffix. If the key vault already exists, it's reused.
 - b. **Key encryption key vaults:** By default, Site Recovery creates a new key vault in the target region. The name has an `asr` suffix, and is based on the source VM key encryption keys. If the key vault created by Site Recovery already exists, it's reused.
2. Select **Customize** to select custom key vaults.

NOTE

Only Azure VMs running Windows operating systems and [enabled for encryption with Azure AD app](#) are currently supported by Azure Site Recovery.

Track replication status

After replication is enabled, you can track the job's status.

1. In **Settings**, select **Refresh** to get the latest status.
2. Track progress and status as follows:
 - a. Track progress of the **Enable protection** job in **Settings > Jobs > Site Recovery Jobs**.
 - b. In **Settings > Replicated Items**, you can view the status of VMs and the initial replication progress. Select the VM to drill down into its settings.

Next steps

In this tutorial, you configured disaster recovery for an Azure VM. Now you can run a disaster recovery drill to check that failover works as expected.

[Run a disaster recovery drill](#)

Run a disaster recovery drill to a secondary region for Azure VMs

1/17/2020 • 2 minutes to read • [Edit Online](#)

The [Azure Site Recovery](#) service contributes to your business continuity and disaster recovery (BCDR) strategy by keeping your business apps up and running available during planned and unplanned outages. Site Recovery manages and orchestrates disaster recovery of on-premises machines and Azure virtual machines (VMs), including replication, failover, and recovery.

This tutorial shows you how to run a disaster recovery drill for an Azure VM, from one Azure region to another, with a test failover. A drill validates your replication strategy without data loss or downtime, and doesn't affect your production environment. In this tutorial, you learn how to:

- Check the prerequisites
- Run a test failover for a single VM

NOTE

This tutorial helps you to perform a disaster recovery drill with minimal steps. To learn more about the various functions related to doing a disaster recovery drill, see the documentation for Azure VMs [replication](#), [networking](#), [automation](#), or [troubleshooting](#).

Prerequisites

Check the following items before you do this tutorial:

- Before you run a test failover, we recommend that you check the VM's properties to make sure it's configured for disaster recovery. Go to the VM's **Operations > Disaster Recovery > Properties** to view the replication and failover properties.
- **We recommend you use a separate Azure VM network for the test failover**, and not the default network that was set up when you enabled replication.
- Depending on your source networking configurations for each NIC, you can specify **Subnet**, **Private IP address**, **Public IP**, **Network security group**, or **Load balancer** to attach to each NIC under test failover settings in **Compute and Network** before doing a disaster recovery drill.

Run a test failover

This example shows how to use a Recovery Services vault to do a VM test failover.

1. Select a vault and go to **Protected items > Replicated items** and select a VM.
2. In **Test Failover**, select a recovery point to use for the failover:
 - **Latest**: Processes all the data in Site Recovery and provides the lowest RTO (Recovery Time Objective).
 - **Latest processed**: Fails the VM over to the latest recovery point that was processed by Site Recovery. The time stamp is shown. With this option, no time is spent processing data, so it provides a low RTO.
 - **Latest app-consistent**: This option fails over all VMs to the latest app-consistent recovery point. The time stamp is shown.
 - **Custom**: Fail over to particular recovery point. Custom is only available when you fail over a single VM, and not for failover with a recovery plan.

3. Select the target Azure virtual network that Azure VMs in the secondary region will connect to after the failover.

NOTE

If the test failover settings are pre-configured for the replicated item, the dropdown menu to select an Azure virtual network isn't visible.

4. To start the failover, select **OK**. To track the progress from the vault, go to **Monitoring > Site Recovery jobs** and select the **Test Failover** job.
5. After the failover finishes, the replica Azure VM appears in the Azure portal's **Virtual Machines**. Make sure that the VM is running, sized appropriately, and connected to the appropriate network.
6. To delete the VMs that were created during the test failover, select **Cleanup test failover** on the replicated item or the recovery plan. In **Notes**, record and save any observations associated with the test failover.

Next steps

[Run a production failover](#)

Fail over and reprotect Azure VMs between regions

8/5/2019 • 2 minutes to read • [Edit Online](#)

This tutorial describes how to fail over an Azure virtual machine (VM) to a secondary Azure region with the [Azure Site Recovery](#) service. After you've failed over, you reprotect the VM. In this tutorial, you learn how to:

- Fail over the Azure VM
- Reprotect the secondary Azure VM, so that it replicates to the primary region.

NOTE

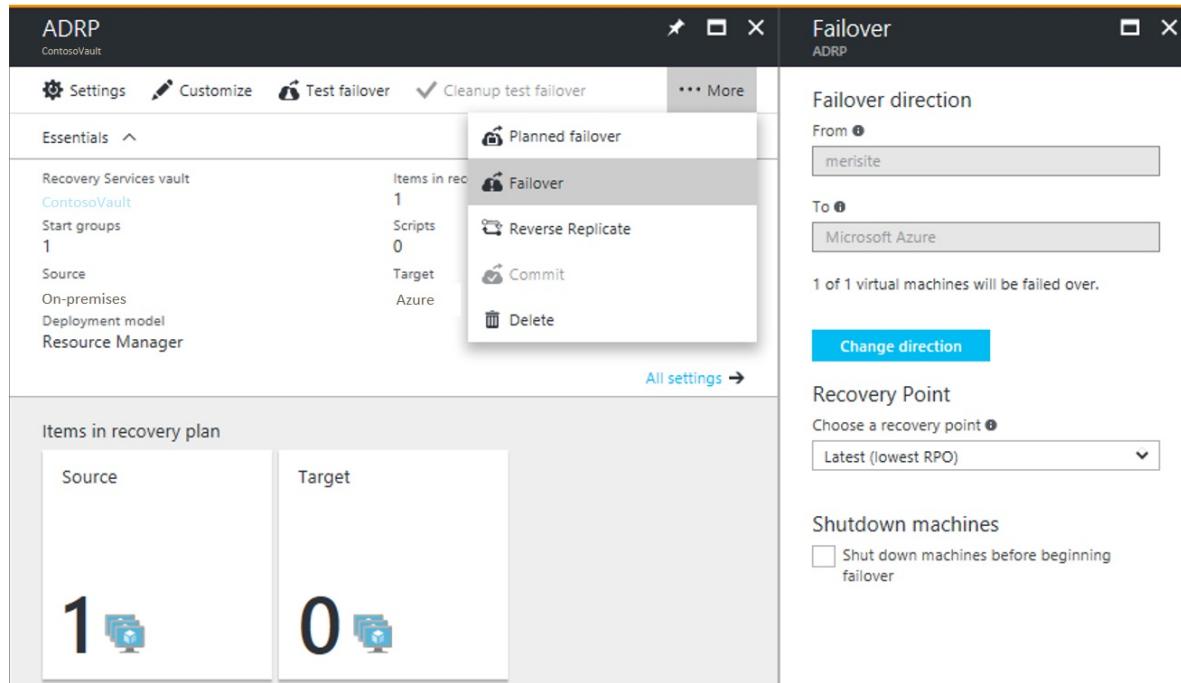
This tutorial contains the simplest path with default settings and minimum customization. For more complex scenarios, use the articles under 'How To' for Azure VMs.

Prerequisites

- Before you start, review [frequently asked questions](#) about failover.
- Make sure that you've completed a [disaster recovery drill](#) to check everything is working as expected.
- Verify the VM properties before you run the test failover. The VM must comply with [Azure requirements](#).

Run a failover to the secondary region

1. In **Replicated items**, select the VM that you want to fail over > **Failover**



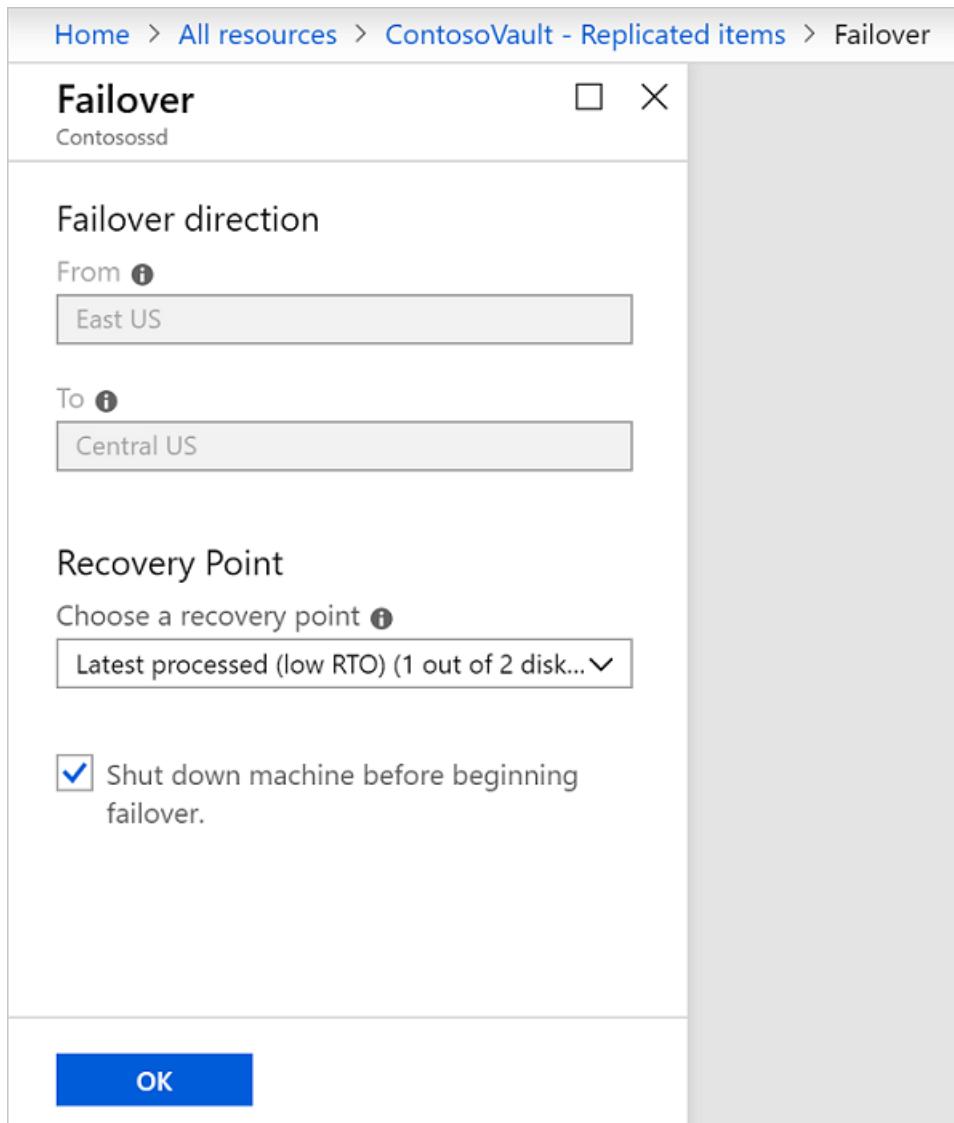
2. In **Failover**, select a **Recovery Point** to fail over to. You can use one of the following options:

- **Latest** (default): Processes all the data in the Site Recovery service and provides the lowest Recovery Point Objective (RPO).
- **Latest processed**: Reverts the virtual machine to the latest recovery point that has been processed by Site Recovery service.
- **Custom**: Fails over to a particular recovery point. This option is useful for performing a test failover.

3. Select **Shut down machine before beginning failover** if you want Site Recovery to attempt to do a shutdown of source VMs before triggering the failover. Shutdown helps to ensure no data loss. Failover continues even if shutdown fails. Site Recovery does not clean up the source after failover.
4. Follow the failover progress on the **Jobs** page.
5. After the failover, validate the virtual machine by logging in to it. If you want to go another recovery point for the virtual machine, then you can use **Change recovery point** option.
6. Once you are satisfied with the failed over virtual machine, you can **Commit** the failover. Committing deletes all the recovery points available with the service. You won't now be able to change the recovery point.

NOTE

When you fail over a VM to which you add a disk after you enabled replication for the VM, replication points will show the disks that are available for recovery. For example, if a VM has a single disk and you add a new one, replication points that were created before you added the disk will show that the replication point consists of "1 of 2 disks".

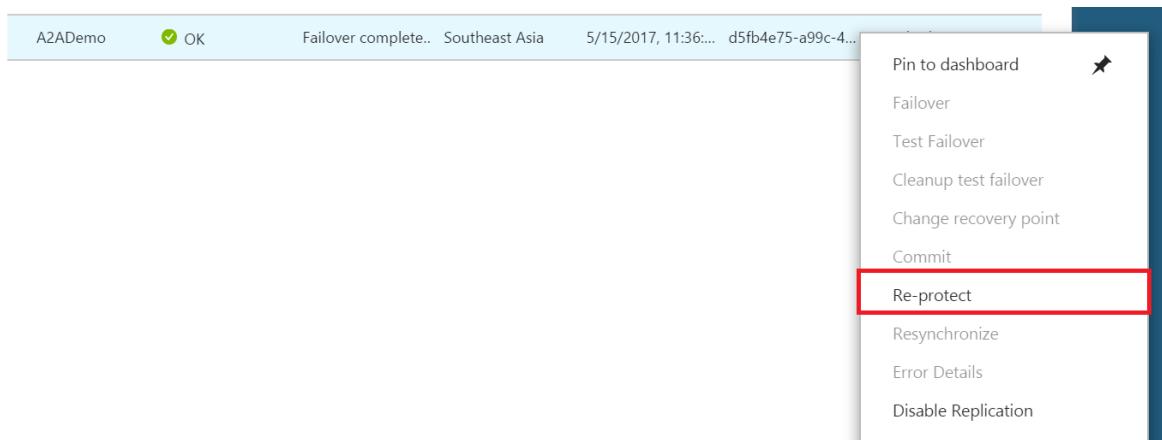


Reprotect the secondary VM

After failover of the VM, you need to reprotect it so that it replicates back to the primary region.

1. Make sure that the VM is in the **Failover committed** state, and check that the primary region is available, and you're able to create and access new resources in it.

2. In **Vault > Replicated items**, right-click the VM that's been failed over, and then select **Re-Protect**.



3. Verify that the direction of protection, secondary to primary region, is already selected.
4. Review the **Resource group, Network, Storage, and Availability sets** information. Any resources marked as new are created as part of the reprotect operation.
5. Click **OK** to trigger a reprotect job. This job seeds the target site with the latest data. Then, it replicates the deltas to the primary region. The VM is now in a protected state.

Next steps

- After reprotecting, [learn how to](#) fail back to the primary region when it's available.
- [Learn more](#) about the reprottection flow.

Fail back an Azure VM between Azure regions

11/14/2019 • 2 minutes to read • [Edit Online](#)

The [Azure Site Recovery](#) service contributes to your disaster recovery strategy by managing and orchestrating replication, failover, and failback of on-premises machines and Azure virtual machines (VMs).

This tutorial describes how to fail back a single Azure VM. After you've failed over, you must fail back to the primary region when it's available. In this tutorial, you learn how to:

- Fail back the VM in the secondary region.
- Reprotect the primary VM back to the secondary region.

NOTE

This tutorial helps you to fail over a few VMs to a target region and back to the source region with minimum customizations. For more in-depth instructions, review the [how-to guides on Azure VMs](#).

Before you start

- Make sure that the status of the VM is **Failover committed**.
- Check that the primary region is available, and that you're able to create and access new resources in it.
- Make sure that reprottection is enabled.

Fail back to the primary region

After VMs are reprotected, you can fail back to the primary region as needed.

1. In the vault, select **Replicated items**, and then select the VM that was reprotected.

The screenshot shows the Azure Site Recovery vault interface. At the top, there are several action buttons: Failover, Test Failover, Cleanup test failover, Commit, Resynchronize, Change recovery point, Re-protect, Disable Replication, Error Details, and Refresh. Below these are two main sections: 'Health and status' and 'Failover readiness'. The 'Health and status' section shows 'Replication Health' as 'Healthy' (green), 'Status' as 'Protected', and 'RPO' as '1 min [As on 2/27/2019, 5:46:54 PM]'. The 'Failover readiness' section shows 'Last successful Test Failover' as 'Never performed successfully' (yellow) and 'Configuration issues' as 'No issues' (green). To the right, a 'Latest recovery points' box is visible with the instruction 'Click above to see the latest recovery points.' At the bottom, there are tabs for 'Errors(0)', 'Events - Last 72 hours(0)', and 'Jobs(0)'.

2. In **Replicated items**, select the VM, and then select **Failover**.

3. In **Failover**, select a recovery point to fail over to:

- **Latest (default)**: Processes all the data in the Site Recovery service and provides the lowest recovery point objective (RPO).
- **Latest processed**: Reverts the VM to the latest recovery point that has been processed by Site Recovery.
- **Custom**: Fails over to a particular recovery point. This option is useful for performing a test failover.

4. Select **Shut down machine before beginning failover** if you want Site Recovery to attempt a shutdown of VMs in DR region before triggering the failover. The failover continues even if shutdown fails.

5. Follow the failover progress on the **Jobs** page.

6. After the failover is complete, validate the VM by logging in to it. You can change the recovery point as needed.
7. After you've verified the failover, select **Commit the failover**. Committing deletes all the available recovery points. The change recovery point option is no longer available.
8. The VM should show as failed over and failed back.

 ContosoWin2016	Running	Central US	contosoretail	1	-
 ContosoWin2016	Stopped (deallocated)	East US	contosoretail-asr	1	-

NOTE

For machines running the Site Recovery extension version 9.28.x.x onwards [Update rollup 40](#) Site Recovery cleans up machines in the secondary disaster recovery region, after failback is complete and VMs are re-protected. There is no need to manually delete VMs and NICs in the secondary region. If you completely disable replication after failing back, Site Recovery cleans up the disks in the disaster recovery region, in addition to the VMs and NICs.

Next steps

[Learn more](#) about the reprotection flow.

Move Azure VMs to another region

11/12/2019 • 6 minutes to read • [Edit Online](#)

There are various scenarios in which you'd want to move your existing Azure IaaS virtual machines (VMs) from one region to another. For example, you want to improve reliability and availability of your existing VMs, to improve manageability, or to move for governance reasons. For more information, see the [Azure VM move overview](#).

You can use the [Azure Site Recovery](#) service to manage and orchestrate disaster recovery of on-premises machines and Azure VMs for business continuity and disaster recovery (BCDR). You can also use Site Recovery to manage the move of Azure VMs to a secondary region.

In this tutorial, you will:

- Verify prerequisites for the move
- Prepare the source VMs and the target region
- Copy the data and enable replication
- Test the configuration and perform the move
- Delete the resources in the source region

NOTE

This tutorial shows you how to move Azure VMs from one region to another as is. If you need to improve availability by moving VMs in an availability set to zone pinned VMs in a different region, see the [Move Azure VMs into Availability Zones tutorial](#).

Prerequisites

- Make sure that the Azure VMs are in the Azure region from which you want to move.
- Verify that your choice of [source region - target region combination is supported](#), and make an informed decision about the target region.
- Make sure that you understand the [scenario architecture and components](#).
- Review the [support limitations and requirements](#).
- Verify account permissions. If you created your free Azure account, you're the administrator of your subscription. If you're not the subscription administrator, work with the administrator to assign the permissions that you need. To enable replication for a VM and essentially copy data by using Azure Site Recovery, you must have:
 - Permissions to create a VM in Azure resources. The Virtual Machine Contributor built-in role has these permissions, which include:
 - Permission to create a VM in the selected resource group
 - Permission to create a VM in the selected virtual network
 - Permission to write to the selected storage account
 - Permissions to manage Azure Site Recovery operations. The Site Recovery Contributor role has all the permissions that are required to manage Site Recovery operations in a Recovery Services vault.

- Make sure that all the latest root certificates are on the Azure VMs that you want to move. If the latest root certificates aren't on the VM, security constraints will prevent the data copy to the target region.
- For Windows VMs, install all the latest Windows updates on the VM, so that all the trusted root certificates are on the machine. In a disconnected environment, follow the standard Windows Update and certificate update processes for your organization.
- For Linux VMs, follow the guidance provided by your Linux distributor to get the latest trusted root certificates and certificate revocation list on the VM.
- Make sure that you're not using an authentication proxy to control network connectivity for VMs that you want to move.
- If the VM that you're trying to move doesn't have access to the internet, or it's using a firewall proxy to control outbound access, [check the requirements](#).
- Identify the source networking layout and all the resources that you're currently using. This includes but isn't limited to load balancers, network security groups (NSGs), and public IPs.
- Verify that your Azure subscription allows you to create VMs in the target region that's used for disaster recovery. Contact support to enable the required quota.
- Make sure that your subscription has enough resources to support VMs with sizes that match your source VMs. If you're using Site Recovery to copy data to the target, Site Recovery chooses the same size or the closest possible size for the target VM.
- Make sure that you create a target resource for every component that's identified in the source networking layout. This step is important to ensure that your VMs have all the functionality and features in the target region that you had in the source region.

NOTE

Azure Site Recovery automatically discovers and creates a virtual network when you enable replication for the source VM. You can also pre-create a network and assign it to the VM in the user flow for enable replication. As mentioned later, you need to manually create any other resources in the target region.

To create the most commonly used network resources that are relevant for you based on the source VM configuration, see the following documentation:

- [Network security groups](#)
- [Load balancers](#)
- [Public IP](#)
- For any other networking components, see the [networking documentation](#).

Prepare

The following steps shows how to prepare the virtual machine for the move using Azure Site Recovery as a solution.

Create the vault in any region, except the source region

1. Sign in to the [Azure portal](#) > **Recovery Services**.
2. Select **Create a resource** > **Management Tools** > **Backup and Site Recovery**.
3. In **Name**, specify the friendly name **ContosoVMVault**. If you have more than one subscription, select the appropriate one.
4. Create the resource group **ContosoRG**.

5. Specify an Azure region. To check supported regions, see geographic availability in [Azure Site Recovery pricing details](#).
6. In **Recovery Services vaults**, select **Overview > ContosoVMVault > +Replicate**.
7. In **Source**, select **Azure**.
8. In **Source location**, select the source Azure region where your VMs are currently running.
9. Select the Resource Manager deployment model. Then select the **Source subscription** and **Source resource group**.
10. Select **OK** to save the settings.

Enable replication for Azure VMs and start copying the data

Site Recovery retrieves a list of the VMs that are associated with the subscription and resource group.

1. In the next step, select the VM that you want to move, then select **OK**.
2. In **Settings**, select **Disaster recovery**.
3. In **Configure disaster recovery > Target region**, select the target region to which you'll replicate.
4. For this tutorial, accept the other default settings.
5. Select **Enable replication**. This step starts a job to enable replication for the VM.

The screenshot shows the 'Configure settings' dialog box for Azure Site Recovery. It includes sections for target resources, replication policy, and failover policy.

Configure settings

Resource group, Network, Storage and Availability sets [Customize](#)

By default Azure Site Recovery(ASR) will mirror the source site configuration to target site by creating/using the required resource groups, storage accounts, virtual network and availability sets as below. Click 'Customize' above to change the configuration. The resources created by ASR are appended with "asr" suffix.

Target resource group 	Target virtual network
ContosoRG	A2ATest2-vnet-asr(new)
Cache storage accounts 	Target storage accounts
a2atest2disks86cacheasr(new)	a2atest2disks864asr(new)
Target availability sets 	

Replication Policy [Customize](#)

Name: 24-hour-retention-policy
Recovery point retention: 24 hour(s)
App consistent snapshot frequency: 4 hour(s)

Move

The following steps shows how to perform the move to the target region.

1. Go to the vault. In **Settings > Replicated items**, select the VM, and then select **Failover**.
2. In **Failover**, select **Latest**.

3. Select **Shutdown machine before beginning failover**. Site Recovery attempts to shut down the source VM before triggering the failover. Failover continues even if shutdown fails. You can follow the failover progress on the **Jobs** page.
4. After the job is finished, check that the VM appears in the target Azure region as expected.

Discard

In case you checked the moved VM and need to make changes to point of failover or want to go back to a previous point, in the **Replicated items**, right-select the VM > **Change recovery point**. This step provides you the option to specify a different recovery point and failover to that one.

Commit

Once you have checked the moved VM and are ready to commit the change, in the **Replicated items**, right-select the VM > **Commit**. This step finishes the move process to the target region. Wait until the commit job finishes.

Clean up

The following steps will guide you through how to clean up the source region as well as related resources that were used for the move.

For all resources that were used for the move:

- Go to the VM. Select **Disable Replication**. This step stops the process from copying the data for the VM.

IMPORTANT

It's important to perform this step to avoid being charged for Azure Site Recovery replication.

If you have no plans to reuse any of the source resources, complete these additional steps:

1. Delete all the relevant network resources in the source region that you identified in [prerequisites](#).
2. Delete the corresponding storage account in the source region.

Next steps

In this tutorial, you moved an Azure VM to a different Azure region. Now you can configure disaster recovery for the VM that you moved.

[Set up disaster recovery after migration](#)

Move Azure VMs into Availability Zones

11/6/2019 • 7 minutes to read • [Edit Online](#)

Availability Zones in Azure help protect your applications and data from datacenter failures. Each Availability Zone is made up of one or more datacenters equipped with independent power, cooling, and networking. To ensure resiliency, there's a minimum of three separate zones in all enabled regions. The physical separation of Availability Zones within a region helps protect applications and data from datacenter failures. With Availability Zones, Azure offers a service-level agreement (SLA) of 99.99% for uptime of virtual machines (VMs). Availability Zones are supported in select regions, as mentioned in [What are Availability Zones in Azure?](#).

In a scenario where your VMs are deployed as *single instance* into a specific region, and you want to improve your availability by moving these VMs into an Availability Zone, you can do so by using Azure Site Recovery. This action can further be categorized into:

- Move single-instance VMs into Availability Zones in a target region
- Move VMs in an availability set into Availability Zones in a target region

IMPORTANT

Currently, Azure Site Recovery supports moving VMs from one region to another but doesn't support moving within a region.

Check prerequisites

- Check whether the target region has [support for Availability Zones](#). Check that your choice of [source region/target region combination is supported](#). Make an informed decision on the target region.
- Make sure that you understand the [scenario architecture and components](#).
- Review the [support limitations and requirements](#).
- Check account permissions. If you just created your free Azure account, you're the admin of your subscription. If you aren't the subscription admin, work with the admin to assign the permissions you need. To enable replication for a VM and eventually copy data to the target by using Azure Site Recovery, you must have:
 1. Permission to create a VM in Azure resources. The *Virtual Machine Contributor* built-in role has these permissions, which include:
 - Permission to create a VM in the selected resource group
 - Permission to create a VM in the selected virtual network
 - Permission to write to the selected storage account
 2. Permission to manage Azure Site Recovery tasks. The *Site Recovery Contributor* role has all permissions required to manage Site Recovery actions in a Recovery Services vault.

Prepare the source VMs

1. Your VMs should use managed disks if you want to move them to an Availability Zone by using Site Recovery. You can convert existing Windows VMs that use unmanaged disks to use managed disks. Follow the steps at [Convert a Windows virtual machine from unmanaged disks to managed disks](#). Ensure that the availability set is configured as *managed*.

2. Check that all the latest root certificates are present on the Azure VMs you want to move. If the latest root certificates aren't present, the data copy to the target region can't be enabled because of security constraints.
3. For Windows VMs, install all the latest Windows updates on the VM, so that all the trusted root certificates are on the machine. In a disconnected environment, follow the standard Windows update and certificate update processes for your organization.
4. For Linux VMs, follow the guidance provided by your Linux distributor to get the latest trusted root certificates and certificate revocation list on the VM.
5. Make sure you don't use an authentication proxy to control network connectivity for VMs that you want to move.
6. If the VM you're trying to move doesn't have access to the internet and uses a firewall proxy to control outbound access, check the requirements at [Configure outbound network connectivity](#).
7. Identify the source networking layout and the resources you currently use for verification, including load balancers, NSGs, and public IP.

Prepare the target region

1. Check that your Azure subscription lets you create VMs in the target region used for disaster recovery. If necessary, contact support to enable the required quota.
2. Make sure your subscription has enough resources to support VMs with sizes that match your source VMs. If you use Site Recovery to copy data to the target, it picks the same size or the closest possible size for the target VM.
3. Create a target resource for every component identified in the source networking layout. This action ensures that after you cut over to the target region, your VMs have all the functionality and features that you had in the source.

NOTE

Azure Site Recovery automatically discovers and creates a virtual network and storage account when you enable replication for the source VM. You can also pre-create these resources and assign to the VM as part of the enable replication step. But for any other resources, as mentioned later, you need to manually create them in the target region.

The following documents tell how to create the most commonly used network resources that are relevant to you, based on the source VM configuration.

- [Network security groups](#)
- [Load balancers](#)
- [Public IP](#)

For any other networking components, refer to the networking [documentation](#).

IMPORTANT

Ensure that you use a zone-redundant load balancer in the target. You can read more at [Standard Load Balancer and Availability Zones](#).

4. Manually [create a non-production network](#) in the target region if you want to test the configuration before you cut over to the target region. We recommend this approach because it causes minimal interference with

the production environment.

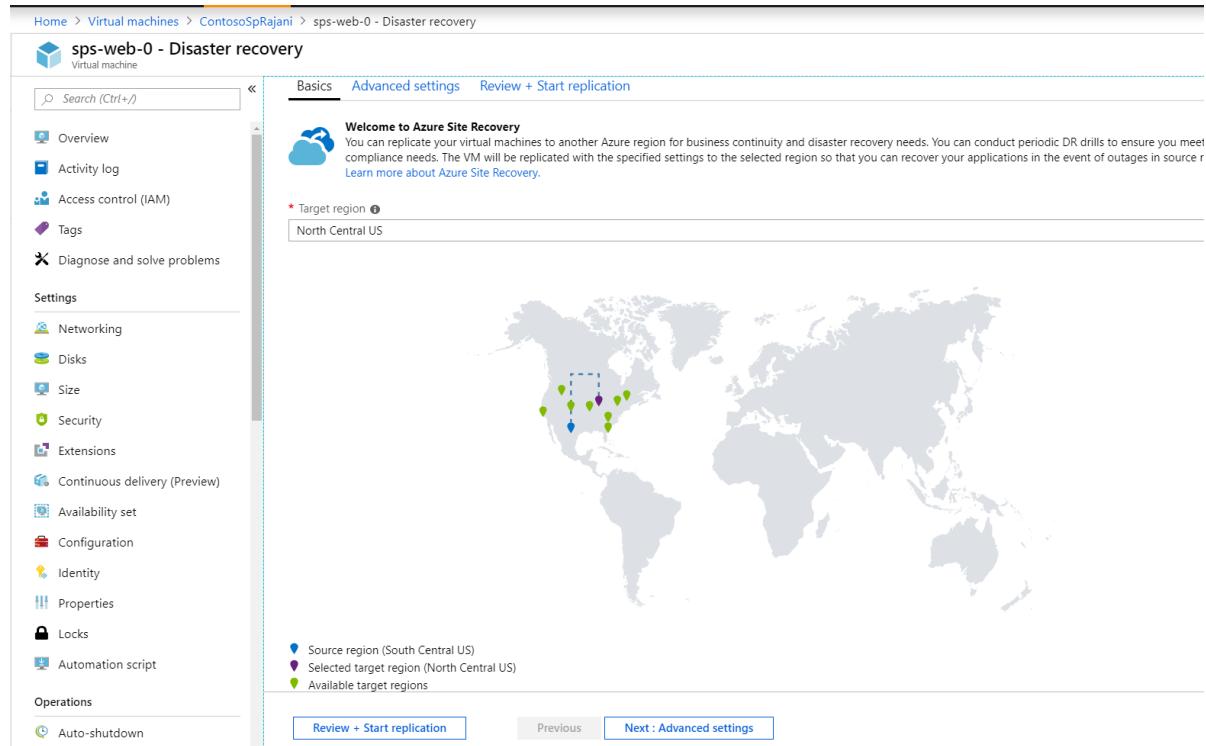
Enable replication

The following steps will guide you when using Azure Site Recovery to enable replication of data to the target region, before you eventually move them into Availability Zones.

NOTE

These steps are for a single VM. You can extend the same to multiple VMs. Go to the Recovery Services vault, select **+** **Replicate**, and select the relevant VMs together.

1. In the Azure portal, select **Virtual machines**, and select the VM you want to move into Availability Zones.
2. In **Operations**, select **Disaster recovery**.
3. In **Configure disaster recovery > Target region**, select the target region to which you'll replicate. Ensure this region **supports** Availability Zones.



4. Select **Next: Advanced settings**.
5. Choose the appropriate values for the target subscription, target VM resource group, and virtual network.
6. In the **Availability** section, choose the Availability Zone into which you want to move the VM.

NOTE

If you don't see the option for availability set or Availability Zone, ensure that the [prerequisites](#) are met and the [preparation](#) of source VMs is complete.

The screenshot shows the 'Review + Start replication' step in the Azure portal. Under 'Target settings', the 'Availability' section is highlighted with a red box. It shows three availability zones (1, 2, 3) listed under 'Availability zone'. Below this, there are sections for 'Storage settings', 'Replication settings', and 'Extension settings', each with a 'Show details' link.

7. Select **Enable Replication**. This action starts a job to enable replication for the VM.

Check settings

After the replication job has finished, you can check the replication status, modify replication settings, and test the deployment.

1. In the VM menu, select **Disaster recovery**.
2. You can check replication health, the recovery points that have been created and the source, and target regions on the map.

The screenshot shows the Disaster recovery blade for a specific VM. The left sidebar lists various management options. The main area displays replication settings, including active location (East US) and target location (South Central US). It also shows replication health (Healthy) and latest recovery points (Crash-consistent: 8/21/2018, 3:23:56 PM; App-consistent: 8/21/2018, 3:23:56 PM). A world map on the right shows the geographical distribution of replication points.

Test the configuration

1. In the virtual machine menu, select **Disaster recovery**.
2. Select the **Test Failover** icon.

3. In **Test Failover**, select a recovery point to use for the failover:

- **Latest processed:** Fails the VM over to the latest recovery point that was processed by the Site Recovery service. The time stamp is shown. With this option, no time is spent processing data, so it provides a low recovery time objective (RTO).
- **Latest app-consistent:** This option fails over all VMs to the latest app-consistent recovery point. The time stamp is shown.
- **Custom:** Select any recovery point.

4. Select the test target Azure virtual network to which you want to move the Azure VMs to test the configuration.

IMPORTANT

We recommend that you use a separate Azure VM network for the test failure, and not the production network in the target region into which you want to move your VMs.

5. To start testing the move, select **OK**. To track progress, select the VM to open its properties. Or, you can select the **Test Failover** job in the vault name > **Settings** > **Jobs** > **Site Recovery jobs**.

6. After the failover finishes, the replica Azure VM appears in the Azure portal > **Virtual Machines**. Make sure that the VM is running, sized appropriately, and connected to the appropriate network.

7. If you want to delete the VM created as part of testing the move, select **Cleanup test failover** on the replicated item. In **Notes**, record and save any observations associated with the test.

Move to the target region and confirm

1. In the virtual machine menu, select **Disaster recovery**.
2. Select the **Failover** icon.
3. In **Failover**, select **Latest**.
4. Select **Shut down machine before beginning failover**. Site Recovery attempts to shut down the source VM before triggering the failover. Failover continues even if shutdown fails. You can follow the failover progress on the **Jobs** page.
5. After the job is finished, check that the VM appears in the target Azure region as expected.
6. In **Replicated items**, right-click the VM > **Commit**. This finishes the move process to the target region. Wait until the commit job is finished.

Discard the resource in the source region

Go to the VM. Select **Disable Replication**. This action stops the process of copying the data for the VM.

IMPORTANT

Do the preceding step to avoid getting charged for Site Recovery replication after the move. The source replication settings are cleaned up automatically. Note that the Site Recovery extension that is installed as part of the replication isn't removed and needs to be removed manually.

Next steps

In this tutorial, you increased the availability of an Azure VM by moving into an availability set or Availability Zone. Now you can set disaster recovery for the moved VM.

[Set up disaster recovery after migration](#)

Move Azure VMs between Azure Government and Public regions

1/14/2020 • 13 minutes to read • [Edit Online](#)

You might want to move your IaaS VMs between Azure Government and Public regions to increase availability of your existing VMs, improve manageability, or for governance reasons, as detailed [here](#).

In addition to using the [Azure Site Recovery](#) service to manage and orchestrate disaster recovery of on-premises machines and Azure VMs for the purposes of business continuity and disaster recovery (BCDR), you can also use Site Recovery to manage move Azure VMs to a secondary region.

This tutorial shows you how to move Azure VMs between Azure Government and Public regions using Azure Site Recovery. The same can be extended to move VMs between region pairs that are not within the same geographic cluster. In this tutorial, you learn how to:

- Verify prerequisites
- Prepare the source VMs
- Prepare the target region
- Copy data to the target region
- Test the configuration
- Perform the move
- Discard the resources in the source region

IMPORTANT

This tutorial shows you how to move Azure VMs between Azure Government and Public regions, or between regions pairs that are not supported by the regular disaster recovery solution for Azure VMs. In case, your source and target regions pairs are [supported](#), please refer to this [document](#) for the move. If your requirement is to improve availability by moving VMs in an availability set to zone pinned VMs in a different region, refer to the tutorial [here](#).

IMPORTANT

It is not advisable to use this method to configure DR between unsupported region pairs as the pairs are defined keeping data latency in mind, which is critical for a DR scenario.

Verify prerequisites

NOTE

Make sure that you understand the [architecture and components](#) for this scenario. This architecture will be used to move Azure VMs, **by treating the VMs as physical servers**.

- Review the [support requirements](#) for all components.
- Make sure that the servers you want to replicate comply with [Azure VM requirements](#).
- Prepare an account for automatic installation of the Mobility service on each server you want to replicate.

- Note that after you fail over to the target region in Azure, you cannot directly perform a fail back to the source region. You will have to set up replication again back to the target.

Verify Azure account permissions

Make sure your Azure account has permissions for replication of VMs to Azure.

- Review the [permissions](#) you need to replicate machines to Azure.
- Verify and modify [role-based access](#) permissions.

Set up an Azure network

Set up a the target [Azure network](#).

- Azure VMs are placed in this network when they're created after failover.
- The network should be in the same region as the Recovery Services vault

Set up an Azure storage account

Set up an [Azure storage account](#).

- Site Recovery replicates on-premises machines to Azure storage. Azure VMs are created from the storage after failover occurs.
- The storage account must be in the same region as the Recovery Services vault.

Prepare the source VMs

Prepare an account for Mobility service installation

The Mobility service must be installed on each server you want to replicate. Site Recovery installs this service automatically when you enable replication for the server. To install automatically, you need to prepare an account that Site Recovery will use to access the server.

- You can use a domain or local account
- For Windows VMs, if you're not using a domain account, disable Remote User Access control on the local machine. To do this, in the register under **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System**, add the DWORD entry **LocalAccountTokenFilterPolicy**, with a value of 1.
- To add the registry entry to disable the setting from a CLI, type:

```
REG ADD HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v LocalAccountTokenFilterPolicy /t REG_DWORD /d 1.
```
- For Linux, the account should be root on the source Linux server.

Prepare the target region

1. Verify that your Azure subscription allows you to create VMs in the target region used for disaster recovery. Contact support to enable the required quota.
2. Make sure your subscription has enough resources to support VMs with sizes that match your source VMs. if you are using Site Recovery to copy data to the target, it picks the same size or the closest possible size for the target VM.
3. Ensure that you create a target resource for every component identified in the source networking layout. This is important to ensure that, post cutting over to the target region, your VMs have all the functionality and features that you had in the source.

NOTE

Azure Site Recovery automatically discovers and creates a virtual network when you enable replication for the source VM, or you can also pre-create a network and assign to the VM in the user flow for enable replication. But for any other resources, as mentioned below, you need to manually create them in the target region.

Please refer to the following documents to create the most commonly used network resources relevant for you, based on the source VM configuration.

- [Network Security Groups](#)
- [Load balancers](#)
- [Public IP](#)

For any other networking components, refer to the networking [documentation](#).

4. Manually [create a non-production network](#) in the target region if you wish to test the configuration before you perform the final cut over to the target region. This will create minimal interference with the production and is recommended.

Copy data to the target region

The below steps will guide you how to use Azure Site Recovery to copy data to the target region.

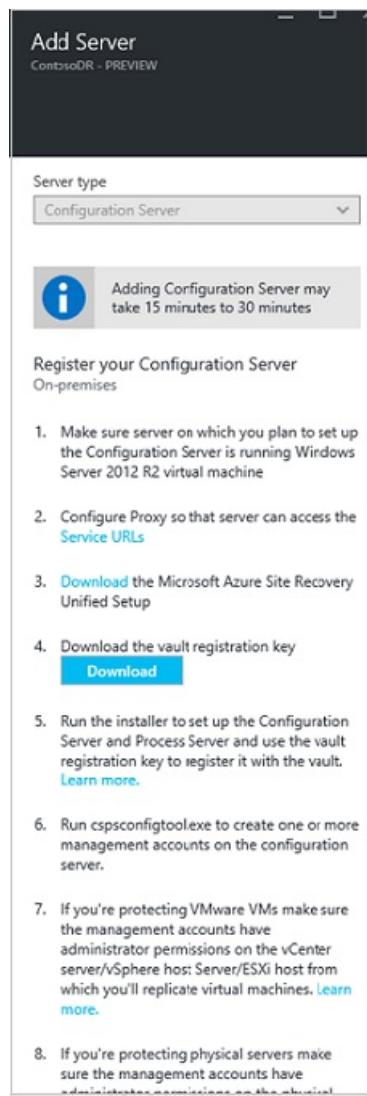
Create the vault in any region, except the source region.

1. Sign in to the [Azure portal](#) > **Recovery Services**.
2. Click **Create a resource** > **Management Tools** > **Backup and Site Recovery**.
3. In **Name**, specify the friendly name **ContosoVMVault**. If you have more than one a. subscription, select the appropriate one.
4. Create a resource group **ContosoRG**.
5. Specify an Azure region. To check supported regions, see geographic availability in [Azure Site Recovery Pricing Details](#).
6. In Recovery Services vaults, click **Overview** > **ConsotoVMVault** > **+Replicate**
7. Select **To Azure** > **Not virtualized/Other**.

Set up the configuration server to discover VMs.

Set up the configuration server, register it in the vault, and discover VMs.

1. Click **Site Recovery** > **Prepare Infrastructure** > **Source**.
2. If you don't have a configuration server, click **+Configuration server**.
3. In **Add Server**, check that **Configuration Server** appears in **Server type**.
4. Download the Site Recovery Unified Setup installation file.
5. Download the vault registration key. You need this when you run Unified Setup. The key is valid for five days after you generate it.



Register the configuration server in the vault

Do the following before you start:

Verify time accuracy

On the configuration server machine, make sure that the system clock is synchronized with a [Time Server](#). It should match. If it's 15 minutes in front or behind, setup might fail.

Verify connectivity

Make sure the machine can access these URLs based on your environment:

NAME	COMMERCIAL URL	GOVERNMENT URL	DESCRIPTION
Azure Active Directory	login.microsoftonline.com	login.microsoftonline.us	Used for access control and identity management by using Azure Active Directory.
Backup	*.backup.windowsazure.com	*.backup.windowsazure.us	Used for replication data transfer and coordination.
Replication	*.hypervrecoverymanager.windows.net	*.hypervrecoverymanager.usgovcloudapi.net	Used for replication management operations and coordination.
Storage	*.blob.core.windows.net	*.blob.core.usgovcloudapi.net	Used for access to the storage account that stores replicated data.

Name	Commercial URL	Government URL	Description
Telemetry (optional)	dc.services.visualstudio.com	dc.services.visualstudio.com	Used for telemetry.
Time synchronization	time.windows.com	time.nist.gov	Used to check time synchronization between system and global time in all deployments.

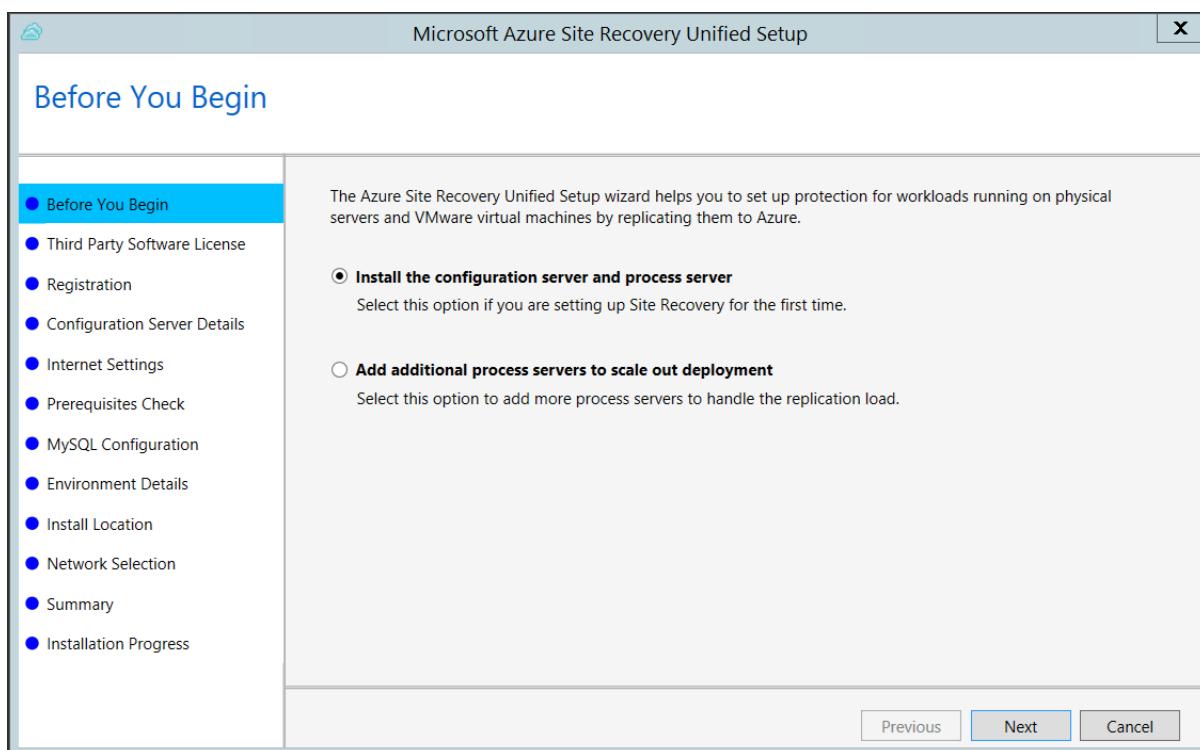
IP address-based firewall rules should allow communication to all of the Azure URLs that are listed above over HTTPS (443) port. To simplify and limit the IP Ranges, it is recommended that URL filtering be done.

- **Commercial IPs** - Allow the [Azure Datacenter IP Ranges](#), and the HTTPS (443) port. Allow IP address ranges for the Azure region of your subscription to support the AAD, Backup, Replication, and Storage URLs.
- **Government IPs** - Allow the [Azure Government Datacenter IP Ranges](#), and the HTTPS (443) port for all USGov Regions (Virginia, Texas, Arizona, and Iowa) to support AAD, Backup, Replication, and Storage URLs.

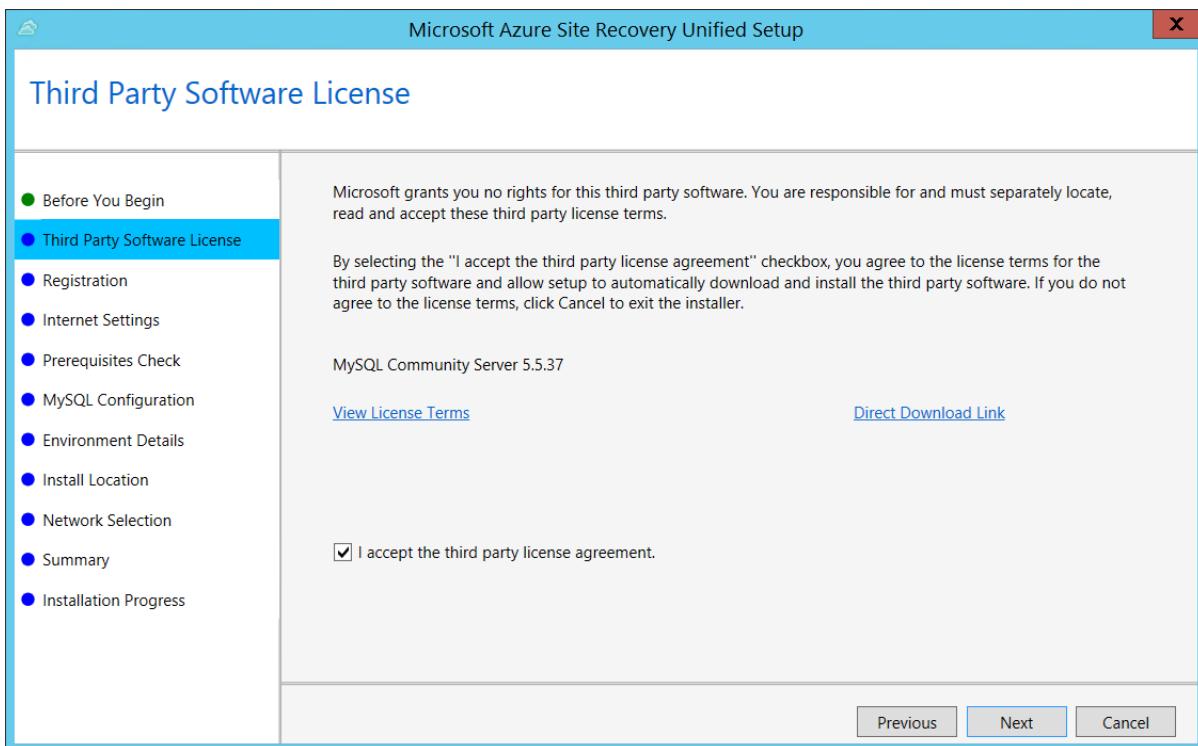
Run setup

Run Unified Setup as a Local Administrator, to install the configuration server. The process server and the master target server are also installed by default on the configuration server.

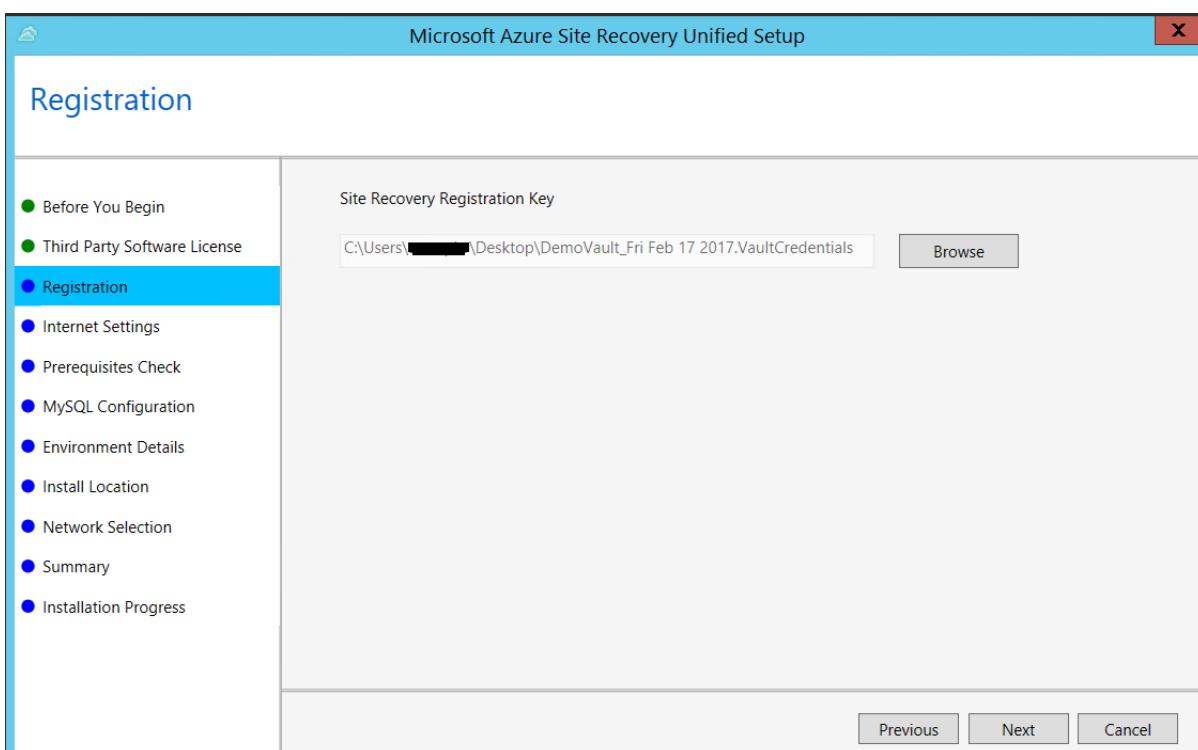
1. Run the Unified Setup installation file.
2. In **Before You Begin**, select **Install the configuration server and process server**.



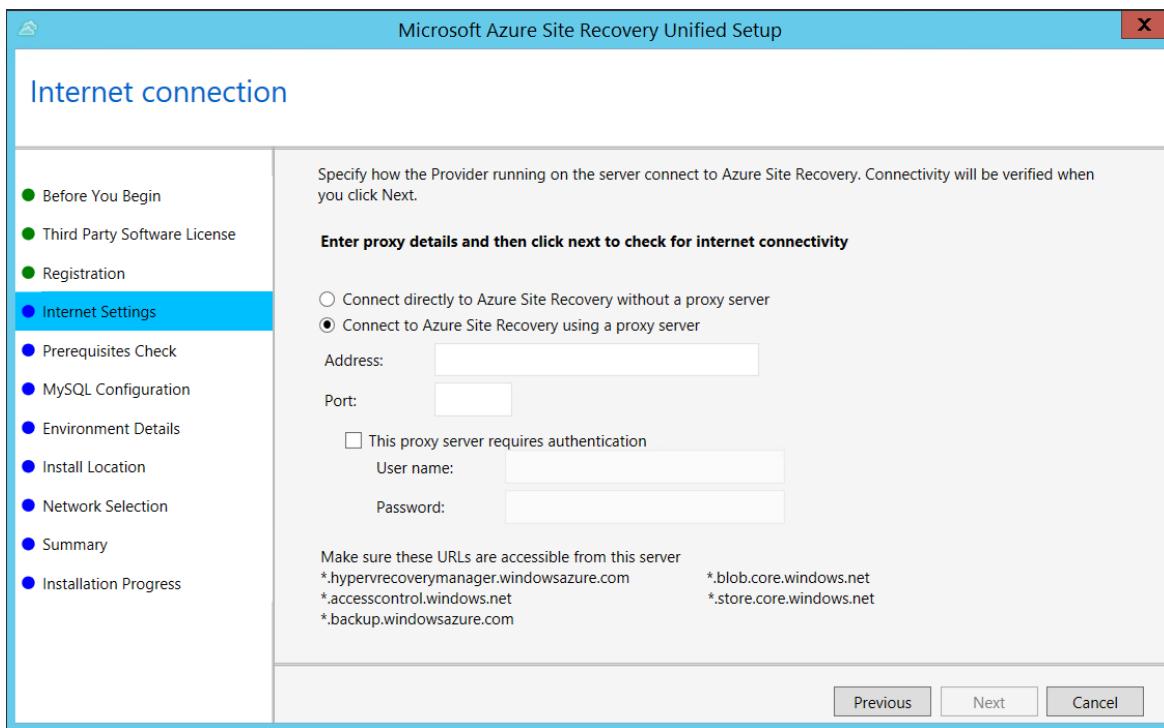
3. In **Third Party Software License**, click **I Accept** to download and install MySQL.



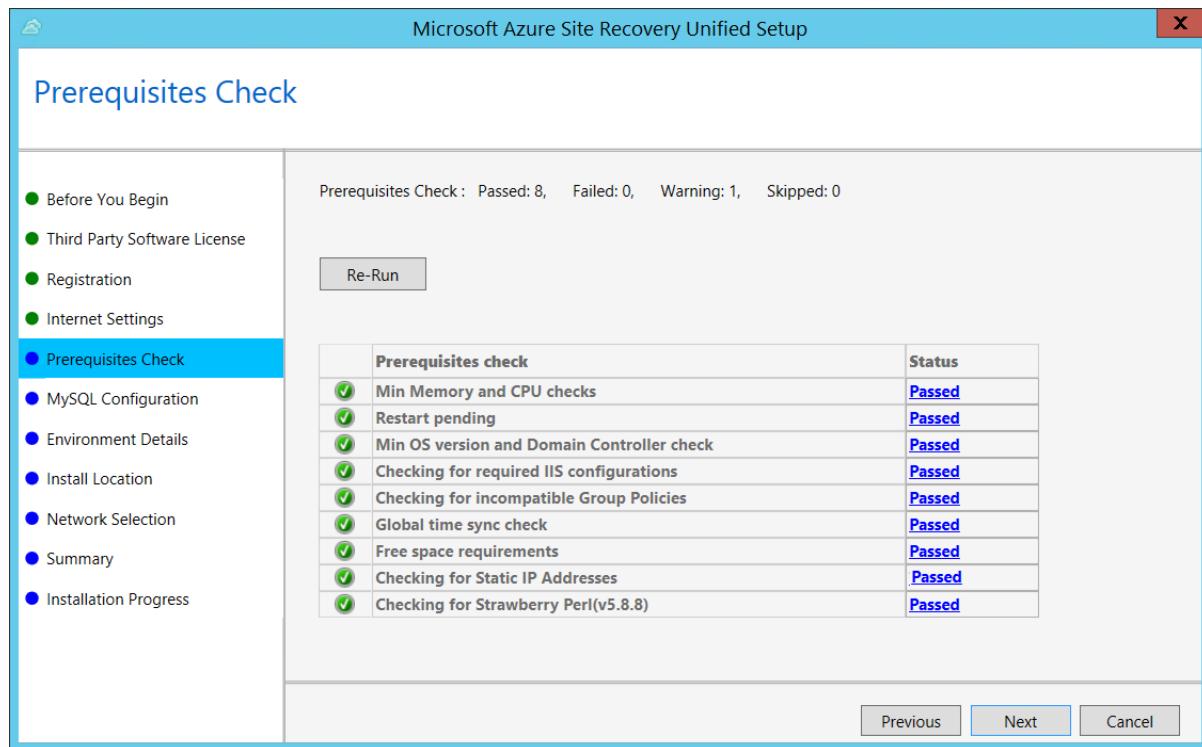
4. In **Registration**, select the registration key you downloaded from the vault.



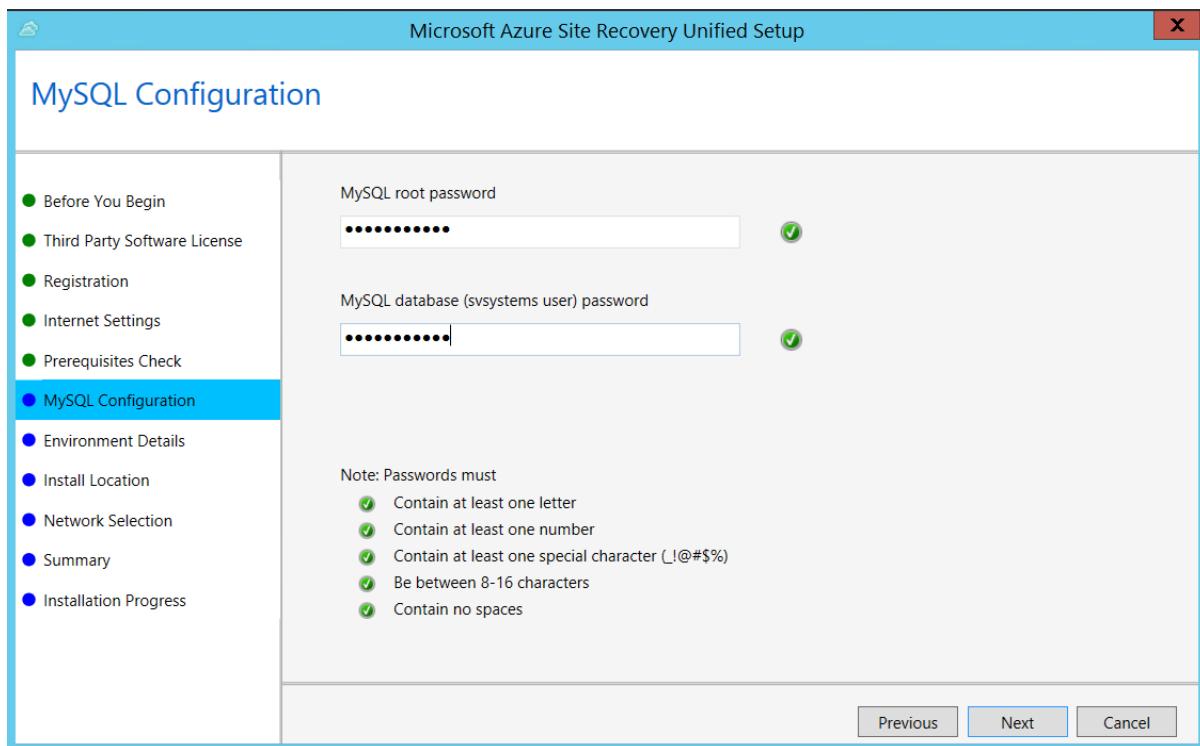
5. In **Internet Settings**, specify how the Provider running on the configuration server connects to Azure Site Recovery over the Internet. Make sure you've allowed the required URLs.
 - If you want to connect with the proxy that's currently set up on the machine, select **Connect to Azure Site Recovery using a proxy server**.
 - If you want the Provider to connect directly, select **Connect directly to Azure Site Recovery without a proxy server**.
 - If the existing proxy requires authentication, or if you want to use a custom proxy for the Provider connection, select **Connect with custom proxy settings**, and specify the address, port, and credentials.



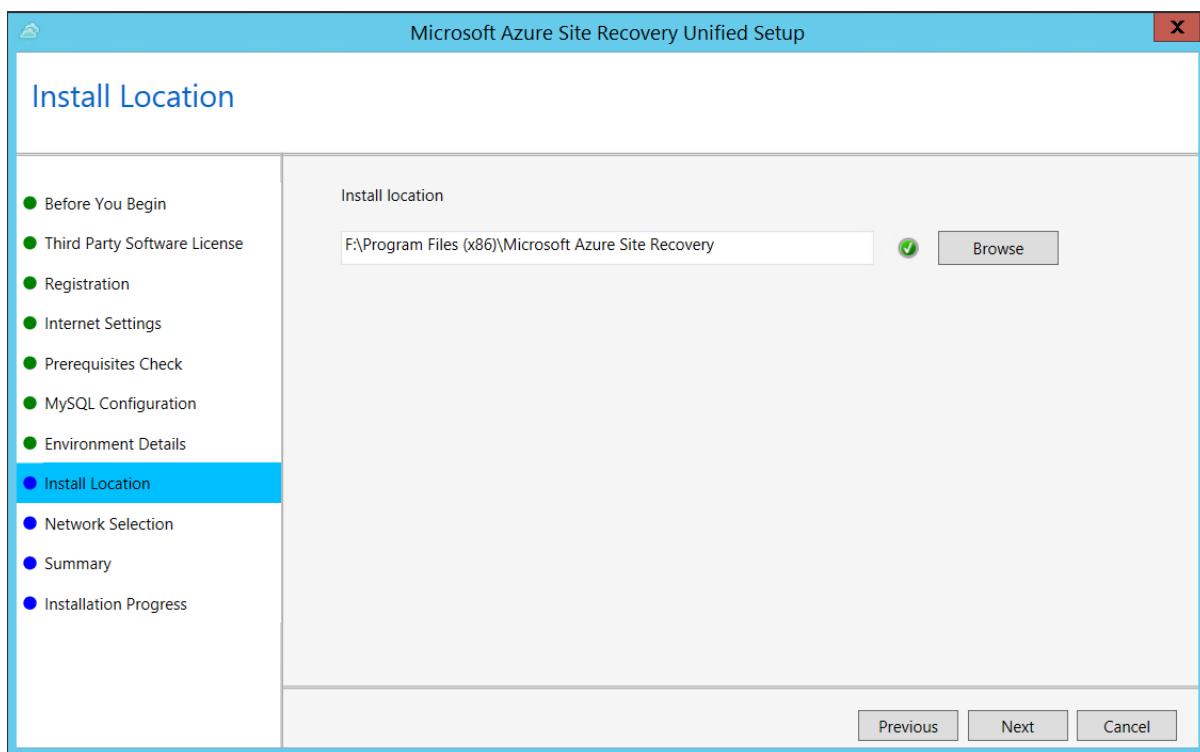
6. In **Prerequisites Check**, Setup runs a check to make sure that installation can run. If a warning appears about the **Global time sync check**, verify that the time on the system clock (**Date and Time** settings) is the same as the time zone.



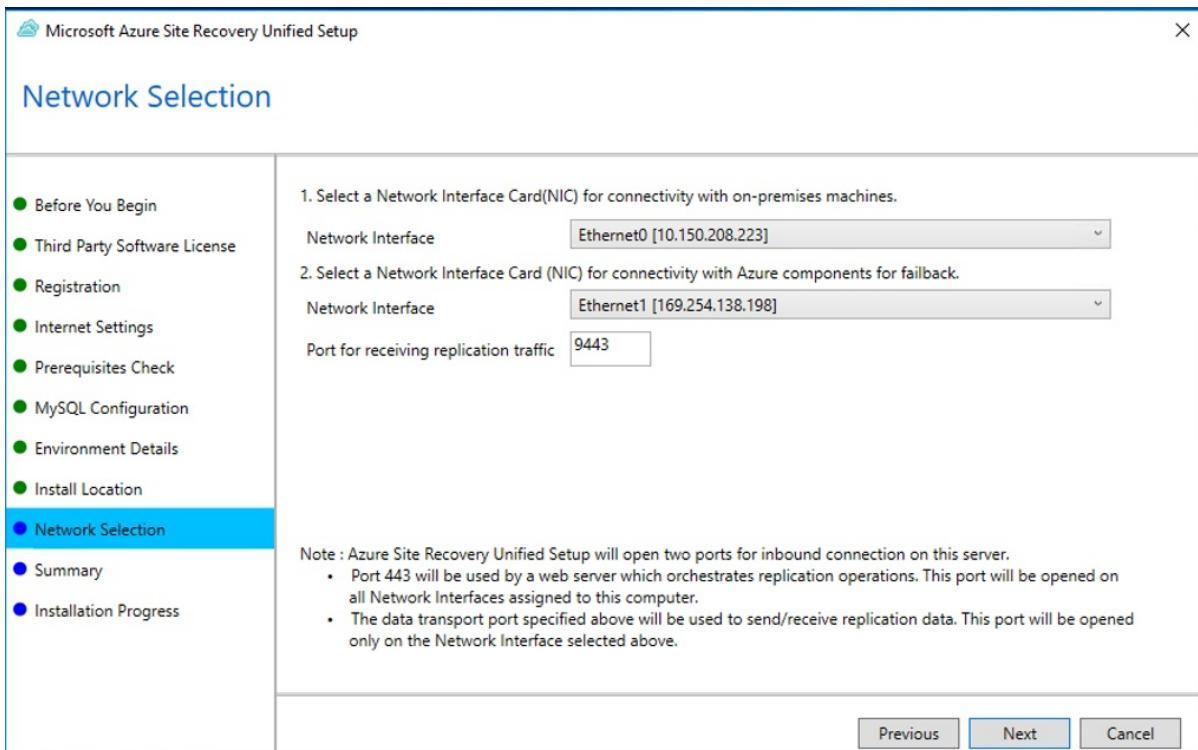
7. In **MySQL Configuration**, create credentials for logging on to the MySQL server instance that is installed.



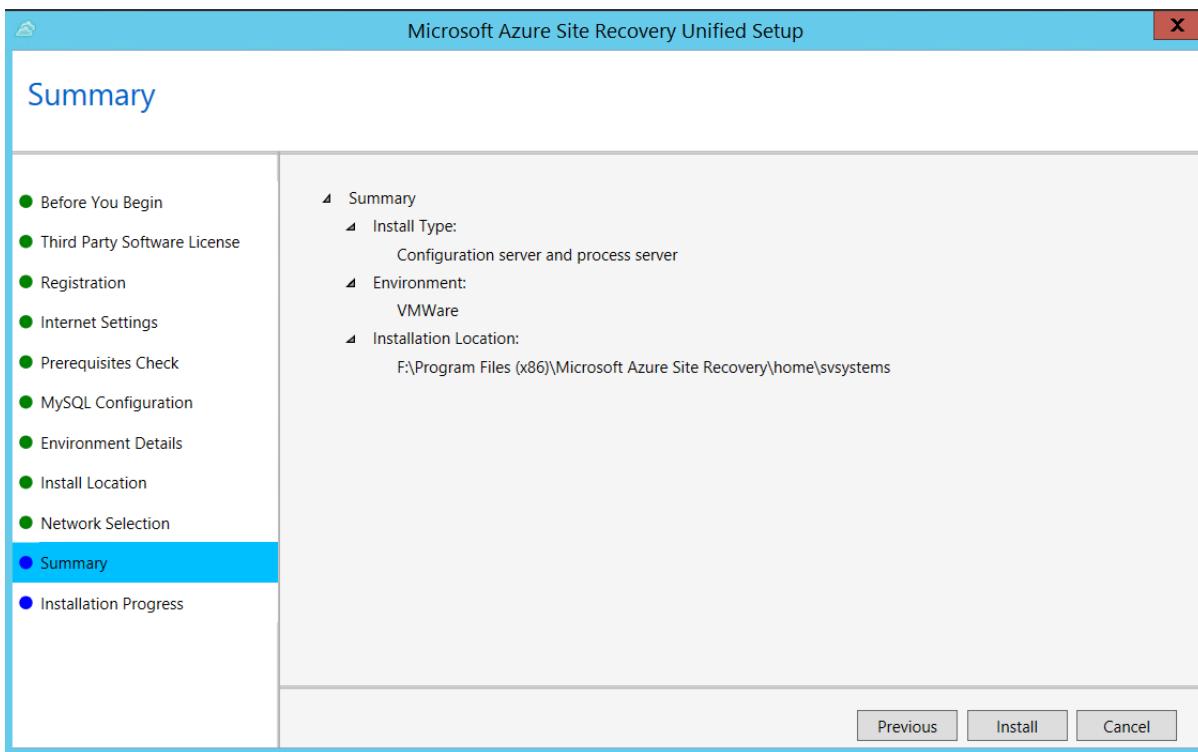
8. In **Environment Details**, select No if you're replicating Azure Stack VMs or physical servers.
9. In **Install Location**, select where you want to install the binaries and store the cache. The drive you select must have at least 5 GB of disk space available, but we recommend a cache drive with at least 600 GB of free space.



10. In **Network Selection**, first select the NIC that the in-built process server uses for discovery and push installation of mobility service on source machines, and then select the NIC that Configuration Server uses for connectivity with Azure. Port 9443 is the default port used for sending and receiving replication traffic, but you can modify this port number to suit your environment's requirements. In addition to the port 9443, we also open port 443, which is used by a web server to orchestrate replication operations. Do not use port 443 for sending or receiving replication traffic.



11. In **Summary**, review the information and click **Install**. When installation finishes, a passphrase is generated. You will need this when you enable replication, so copy it and keep it in a secure location.



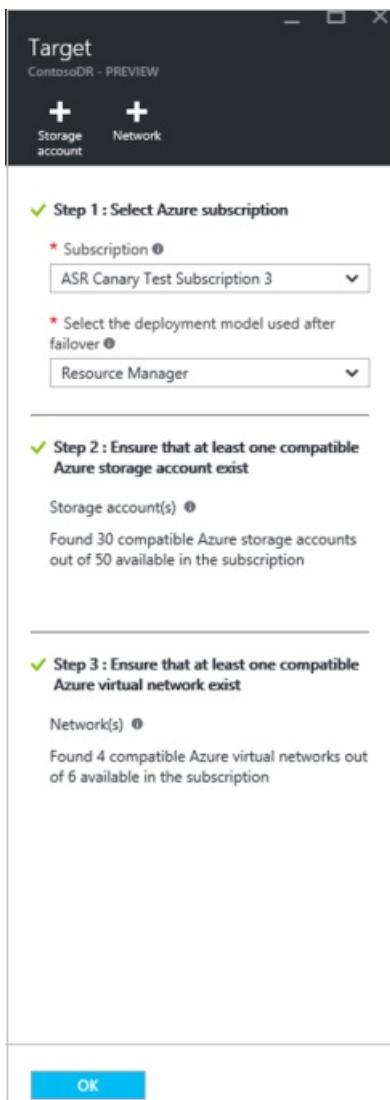
After registration finishes, the server is displayed on the **Settings > Servers** blade in the vault.

After registration finishes, the configuration server is displayed on the **Settings > Servers** page in the vault.

Configure target settings for replication

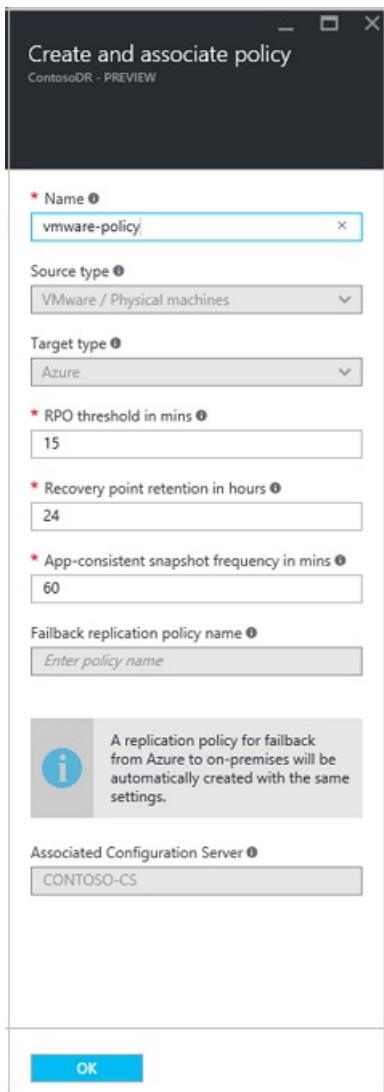
Select and verify target resources.

1. Click **Prepare infrastructure > Target**, and select the Azure subscription you want to use.
2. Specify the target deployment model.
3. Site Recovery checks that you have one or more compatible Azure storage accounts and networks.



Create a replication policy

1. To create a new replication policy, click **Site Recovery infrastructure > Replication Policies > +Replication Policy.**
2. In **Create replication policy**, specify a policy name.
3. In **RPO threshold**, specify the recovery point objective (RPO) limit. This value specifies how often data recovery points are created. An alert is generated if continuous replication exceeds this limit.
4. In **Recovery point retention**, specify how long (in hours) the retention window is for each recovery point. Replicated VMs can be recovered to any point in a window. Up to 24 hours retention is supported for machines replicated to premium storage, and 72 hours for standard storage.
5. In **App-consistent snapshot frequency**, specify how often (in minutes) recovery points containing application-consistent snapshots will be created. Click **OK** to create the policy.



The policy is automatically associated with the configuration server. By default, a matching policy is automatically created for failback. For example, if the replication policy is **rep-policy** then a failback policy **rep-policy-failback** is created. This policy isn't used until you initiate a failback from Azure.

Enable replication

- Site Recovery will install the Mobility service when replication is enabled.
- When you enable replication for a server, it can take 15 minutes or longer for changes to take effect, and appear in the portal.

- Click **Replicate application > Source**.
- In **Source**, select the configuration server.
- In **Machine type**, select **Physical machines**.
- Select the process server (the configuration server). Then click **OK**.
- In **Target**, select the subscription and the resource group in which you want to create the Azure VMs after failover. Choose the deployment model that you want to use in Azure (classic or resource management).
- Select the Azure storage account you want to use for replicating data.
- Select the Azure network and subnet to which Azure VMs will connect, when they're created after failover.
- Select **Configure now for selected machines**, to apply the network setting to all machines you select for protection. Select **Configure later** to select the Azure network per machine.
- In **Physical Machines**, and click **+Physical machine**. Specify the name and IP address. Select the

operating system of the machine you want to replicate. It takes a few minutes for the servers to be discovered and listed.

WARNING

You need to enter the IP address of the Azure VM you intend to move

10. In **Properties > Configure properties**, select the account that will be used by the process server to automatically install the Mobility service on the machine.
11. In **Replication settings > Configure replication settings**, verify that the correct replication policy is selected.
12. Click **Enable Replication**. You can track progress of the **Enable Protection** job in **Settings > Jobs > Site Recovery Jobs**. After the **Finalize Protection** job runs the machine is ready for failover.

To monitor servers you add, you can check the last discovered time for them in **Configuration Servers > Last Contact At**. To add machines without waiting for a scheduled discovery time, highlight the configuration server (don't click it), and click **Refresh**.

Test the configuration

1. Navigate to the vault, in **Settings > Replicated items**, click on the Virtual machine you intend to move to the target region, click **+Test Failover** icon.
2. In **Test Failover**, Select a recovery point to use for the failover:
 - **Latest processed**: Fails the VM over to the latest recovery point that was processed by the Site Recovery service. The time stamp is shown. With this option, no time is spent processing data, so it provides a low RTO (Recovery Time Objective)
 - **Latest app-consistent**: This option fails over all VMs to the latest app-consistent recovery point. The time stamp is shown.
 - **Custom**: Select any recovery point.
3. Select the target Azure virtual network to which you want to move the Azure VMs to test the configuration.

IMPORTANT

We recommend that you use a separate Azure VM network for the test failover, and not the production network into which you want to move your VMs eventually that was set up when you enabled replication.

4. To start testing the move, click **OK**. To track progress, click the VM to open its properties. Or, you can click the **Test Failover** job in the vault name > **Settings > Jobs > Site Recovery jobs**.
5. After the failover finishes, the replica Azure VM appears in the Azure portal > **Virtual Machines**. Make sure that the VM is running, sized appropriately, and connected to the appropriate network.
6. If you wish to delete the VM created as part of testing the move, click **Cleanup test failover** on the replicated item. In **Notes**, record and save any observations associated with the test.

Perform the move to the target region and confirm.

1. Navigate to the vault, in **Settings > Replicated items**, click on the virtual machine, and then click **Failover**.
2. In **Failover**, select **Latest**.
3. Select **Shutdown machine before beginning failover**. Site Recovery attempts to shut down the source VM before triggering the failover. Failover continues even if shutdown fails. You can follow the failover progress on

the **Jobs** page.

4. Once the job is complete, check that the VM appears in the target Azure region as expected.
5. In **Replicated items**, right-click the VM > **Commit**. This finishes the move process to the target region. Wait till the commit job completes.

Discard the resource in the source region

- Navigate to the VM. Click on **Disable Replication**. This stops the process of copying the data for the VM.

IMPORTANT

It is important to perform this step to avoid getting charged for ASR replication.

In case you have no plans to reuse any of the source resources please proceed with the next set of steps.

1. Proceed to delete all the relevant network resources in the source region that you listed out as part of Step 4 in [Prepare the source VMs](#)
2. Delete the corresponding storage account in the source region.

Next steps

In this tutorial you moved an Azure VM to a different Azure region. Now you can configure disaster recovery for the moved VM.

[Set up disaster recovery after migration](#)

Move a Recovery Services vault and Azure Site Recovery configuration to another Azure region

11/14/2019 • 2 minutes to read • [Edit Online](#)

There are various scenarios in which you might want to move your existing Azure resources from one region to another. Examples are for manageability, governance reasons, or because of company mergers and acquisitions. One of the related resources you might want to move when you move your Azure VMs is the disaster recovery configuration.

There's no first-class way to move an existing disaster recovery configuration from one region to another. This is because you configured your target region based on your source VM region. When you decide to change the source region, the previously existing configurations of the target region can't be reused and must be reset. This article defines the step-by-step process to reconfigure the disaster recovery setup and move it to a different region.

In this document, you will:

- Verify prerequisites for the move.
- Identify the resources that were used by Azure Site Recovery.
- Disable replication.
- Delete the resources.
- Set up Site Recovery based on the new source region for the VMs.

IMPORTANT

Currently, there's no first-class way to move a Recovery Services vault and the disaster recovery configuration as is to a different region. This article guides you through the process of disabling replication and setting it up in the new region.

Prerequisites

- Make sure that you remove and delete the disaster recovery configuration before you try to move the Azure VMs to a different region.

NOTE

If your new target region for the Azure VM is the same as the disaster recovery target region, you can use your existing replication configuration and move it. Follow the steps in [Move Azure IaaS VMs to another Azure region](#).

- Ensure that you're making an informed decision and that stakeholders are informed. Your VM won't be protected against disasters until the move of the VM is complete.

Identify the resources that were used by Azure Site Recovery

We recommend that you do this step before you proceed to the next one. It's easier to identify the relevant resources while the VMs are being replicated.

For each Azure VM that's being replicated, go to **Protected Items** > **Replicated Items** > **Properties** and identify the following resources:

- Target resource group

- Cache storage account
- Target storage account (in case of an unmanaged disk-based Azure VM)
- Target network

Disable the existing disaster recovery configuration

1. Go to the Recovery Services vault.
2. In **Protected Items > Replicated Items**, right-click the machine and select **Disable replication**.
3. Repeat this step for all the VMs that you want to move.

NOTE

The mobility service won't be uninstalled from the protected servers. You must uninstall it manually. If you plan to protect the server again, you can skip uninstalling the mobility service.

Delete the resources

1. Go to the Recovery Services vault.
2. Select **Delete**.
3. Delete all the other resources you [previously identified](#).

Move Azure VMs to the new target region

Follow the steps in these articles based on your requirement to move Azure VMs to the target region:

- [Move Azure VMs to another region](#)
- [Move Azure VMs into Availability Zones](#)

Set up Site Recovery based on the new source region for the VMs

Configure disaster recovery for the Azure VMs that were moved to the new region by following the steps in [Set up disaster recovery for Azure VMs](#).

Prepare Azure for on-premises disaster recovery to Azure

11/5/2019 • 3 minutes to read • [Edit Online](#)

This article describes how to prepare Azure resources and components so that you can set up disaster recovery of on-premises VMware VMs, Hyper-V VMs, or Windows/Linux physical servers to Azure, using the [Azure Site Recovery](#) service.

This article is the first tutorial in a series that shows you how to set up disaster recovery for on-premises VMs.

In this tutorial, you learn how to:

- Verify that the Azure account has replication permissions.
- Create a Recovery Services vault. A vault holds metadata and configuration information for VMs, and other replication components.
- Set up an Azure virtual network (VNet). When Azure VMs are created after failover, they're joined to this network.

NOTE

Tutorials show you the simplest deployment path for a scenario. They use default options where possible, and don't show all possible settings and paths. For detailed instructions, review the article in the How To section of the Site Recovery Table of Contents.

Before you start

- Review the architecture for [VMware](#), [Hyper-V](#), and [physical server](#) disaster recovery.
- Read common questions for [VMware](#) and [Hyper-V](#)

If you don't have an Azure subscription, create a [free account](#) before you begin. Then sign in to the [Azure portal](#).

Verify account permissions

If you just created your free Azure account, you're the administrator of your subscription and you have the permissions you need. If you're not the subscription administrator, work with the administrator to assign the permissions you need. To enable replication for a new virtual machine, you must have permission to:

- Create a VM in the selected resource group.
- Create a VM in the selected virtual network.
- Write to an Azure storage account.
- Write to an Azure managed disk.

To complete these tasks your account should be assigned the Virtual Machine Contributor built-in role. In addition, to manage Site Recovery operations in a vault, your account should be assigned the Site Recovery Contributor built-in role.

Create a Recovery Services vault

1. From the Azure portal menu, select **Create a resource**, and search the Marketplace for **Recovery**.

2. Select **Backup and Site Recovery** from the search results, and in the Backup and Site Recovery page, click **Create**.
3. In the **Create Recovery Services vault** page, select the **Subscription**. We're using **Contoso Subscription**.
4. In **Resource group**, select an existing resource group or create a new one. For this tutorial we're using **contosoRG**.
5. In **Vault name**, enter a friendly name to identify the vault. For this set of tutorials we're using **ContosoVMVault**.
6. In **Region**, select the region in which the vault should be located. We're using **West Europe**.
7. Select **Review + create**.

The screenshot shows the 'Create Recovery Services vault' wizard in the Microsoft Azure portal. The 'Basics' tab is active. In the 'Project Details' section, the 'Subscription' dropdown is set to 'Contoso Subscription'. Below it, the 'Resource group' dropdown is set to 'contosoRG' with a 'Create new' link. In the 'Instance Details' section, the 'Vault name' input field contains 'ContosoVMVault' with a green checkmark. The 'Region' dropdown is set to 'West Europe'. At the bottom, there are two buttons: 'Review + create' (highlighted in blue) and 'Next: Tags'.

The new vault will now be listed in **Dashboard > All resources**, and on the main **Recovery Services vaults** page.

Set up an Azure network

On-premises machines are replicated to Azure managed disks. When failover occurs, Azure VMs are created from these managed disks, and joined to the Azure network you specify in this procedure.

1. In the [Azure portal](#), select **Create a resource > Networking > Virtual network**.
2. Keep **Resource Manager** selected as the deployment model.
3. In **Name**, enter a network name. The name must be unique within the Azure resource group. We're using **ContosoASRnet** in this tutorial.
4. In **Address space**, enter the virtual network's address range in CIDR notation. We're using **10.1.0.0/24**.

- In **Subscription**, select the subscription in which to create the network.
- Specify the **Resource group** in which the network will be created. We're using the existing resource group **contosoRG**.
- In **Location**, select the same region as that in which the Recovery Services vault was created. In our tutorial it's **West Europe**. The network must be in the same region as the vault.
- In **Address range**, enter the range for the network. We're using **10.1.0.0/24**, and not using a subnet.
- We're leaving the default options of basic DDoS protection, with no service endpoint, or firewall on the network.
- Select **Create**.

Create virtual network

Name *	ContosoASRnet
Address space * ⓘ	10.1.0.0/24 10.1.0.0 - 10.1.0.255 (256 addresses)
<input type="checkbox"/> Add an IPv6 address space ⓘ	
Subscription *	Contoso Subscription
Resource group *	contosoRG Create new
Location *	(Europe) West Europe
Subnet	Name * default
Address range * ⓘ	10.1.0.0/24 10.1.0.0 - 10.1.0.255 (256 addresses)
DDoS protection ⓘ	<input checked="" type="radio"/> Basic <input type="radio"/> Standard
Service endpoints ⓘ	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled
Firewall ⓘ	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled
<input type="button" value="Create"/> Automation options	

The virtual network takes a few seconds to create. After it's created, you'll see it in the Azure portal dashboard.

Next steps

- For VMware disaster recovery, [prepare the on-premises VMware infrastructure](#).
- For Hyper-V disaster recovery, [prepare the on-premises Hyper-V servers](#).
- For physical server disaster recovery, [set up the configuration server and source environment](#)
- [Learn about Azure networks](#).
- [Learn about managed disks](#).

Prepare on-premises VMware servers for disaster recovery to Azure

1/10/2020 • 5 minutes to read • [Edit Online](#)

This article describes how to prepare on-premises VMware servers for disaster recovery to Azure using the [Azure Site Recovery](#) services.

This is the second tutorial in a series that shows you how to set up disaster recovery to Azure for on-premises VMware VMs. In the first tutorial, we [set up the Azure components](#) needed for VMware disaster recovery.

In this article, you learn how to:

- Prepare an account on the vCenter server or vSphere ESXi host, to automate VM discovery.
- Prepare an account for automatic installation of the Mobility service on VMware VMs.
- Review VMware server and VM requirements and support.
- Prepare to connect to Azure VMs after failover.

NOTE

Tutorials show you the simplest deployment path for a scenario. They use default options where possible, and don't show all possible settings and paths. For detailed instructions, review the article in the How To section of the Site Recovery Table of Contents.

Before you start

Make sure you've prepared Azure as described in the [first tutorial in this series](#).

Prepare an account for automatic discovery

Site Recovery needs access to VMware servers to:

- Automatically discover VMs. At least a read-only account is required.
- Orchestrate replication, failover, and fallback. You need an account that can run operations such as creating and removing disks, and powering on VMs.

Create the account as follows:

1. To use a dedicated account, create a role at the vCenter level. Give the role a name such as **Azure_Site_Recovery**.
2. Assign the role the permissions summarized in the table below.
3. Create a user on the vCenter server or vSphere host. Assign the role to the user.

VMware account permissions

TASK	ROLE/PERMISSIONS	DETAILS
------	------------------	---------

Task	Role/Permissions	Details
VM discovery	<p>At least a read-only user</p> <p>Data Center object -> Propagate to Child Object, role=Read-only</p>	<p>User assigned at datacenter level, and has access to all the objects in the datacenter.</p> <p>To restrict access, assign the No access role with the Propagate to child object, to the child objects (vSphere hosts, datastores, VMs and networks).</p>
Full replication, failover, fallback	<p>Create a role (Azure_Site_Recovery) with the required permissions, and then assign the role to a VMware user or group</p> <p>Data Center object -> Propagate to Child Object, role=Azure_Site_Recovery</p> <p>Datastore -> Allocate space, browse datastore, low-level file operations, remove file, update virtual machine files</p> <p>Network -> Network assign</p> <p>Resource -> Assign VM to resource pool, migrate powered off VM, migrate powered on VM</p> <p>Tasks -> Create task, update task</p> <p>Virtual machine -> Configuration</p> <p>Virtual machine -> Interact -> answer question, device connection, configure CD media, configure floppy media, power off, power on, VMware tools install</p> <p>Virtual machine -> Inventory -> Create, register, unregister</p> <p>Virtual machine -> Provisioning -> Allow virtual machine download, allow virtual machine files upload</p> <p>Virtual machine -> Snapshots -> Remove snapshots</p>	<p>User assigned at datacenter level, and has access to all the objects in the datacenter.</p> <p>To restrict access, assign the No access role with the Propagate to child object, to the child objects (vSphere hosts, datastores, VMs and networks).</p>

Prepare an account for Mobility service installation

The Mobility service must be installed on machines you want to replicate. Site Recovery can do a push installation of this service when you enable replication for a machine, or you can install it manually, or using installation tools.

- In this tutorial, we're going to install the Mobility service with the push installation.
- For this push installation, you need to prepare an account that Site Recovery can use to access the VM. You specify this account when you set up disaster recovery in the Azure console.

Prepare the account as follows:

Prepare a domain or local account with permissions to install on the VM.

- **Windows VMs:** To install on Windows VMs if you're not using a domain account, disable Remote User Access control on the local machine. To do this, in the registry > **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System**, add the DWORD entry **LocalAccountTokenFilterPolicy**, with a value of 1.
- **Linux VMs:** To install on Linux VMs, prepare a root account on the source Linux server.

Check VMware requirements

Make sure VMware servers and VMs comply with requirements.

1. Verify VMware server requirements.
2. For Linux VMs, check file system and storage requirements.
3. Check on-premises network and storage support.
4. Check what's supported for Azure networking, storage, and compute, after failover.
5. Your on-premises VMs you replicate to Azure must comply with Azure VM requirements.
6. In Linux virtual machines, device name or mount point name should be unique. Ensure that no two devices/mount points have the same names. Note that name aren't case-sensitive. For example, naming two devices for the same VM as *device1* and *Device1* isn't allowed.

Prepare to connect to Azure VMs after failover

After failover, you might want to connect to the Azure VMs from your on-premises network.

To connect to Windows VMs using RDP after failover, do the following:

- **Internet access.** Before failover, enable RDP on the on-premises VM before failover. Make sure that TCP, and UDP rules are added for the **Public** profile, and that RDP is allowed in **Windows Firewall > Allowed Apps**, for all profiles.
- **Site-to-site VPN access:**
 - Before failover, enable RDP on the on-premises machine.
 - RDP should be allowed in the **Windows Firewall -> Allowed apps and features** for **Domain** and **Private** networks.
 - Check that the operating system's SAN policy is set to **OnlineAll**. [Learn more](#).
- There should be no Windows updates pending on the VM when you trigger a failover. If there are, you won't be able to sign in to the virtual machine until the update completes.
- On the Windows Azure VM after failover, check **Boot diagnostics** to view a screenshot of the VM. If you can't connect, check that the VM is running and review these [troubleshooting tips](#).

To connect to Linux VMs using SSH after failover, do the following:

- On the on-premises machine before failover, check that the Secure Shell service is set to start automatically on system boot.
- Check that firewall rules allow an SSH connection.
- On the Azure VM after failover, allow incoming connections to the SSH port for the network security group rules on the failed over VM, and for the Azure subnet to which it's connected.
- [Add a public IP address](#) for the VM.
- You can check **Boot diagnostics** to view a screenshot of the VM.

Fallback requirements

If you plan to fail back to your on-premises site, there are a number of [prerequisites for fallback](#). You can prepare

these now, but you don't need to. You can prepare after you fail over to Azure.

Next steps

Set up disaster recovery. If you're replicating multiple VMs, plan capacity.

[Set up disaster recovery to Azure for VMware VMs](#) [Perform capacity planning](#).

Set up disaster recovery to Azure for on-premises VMware VMs

12/16/2019 • 10 minutes to read • [Edit Online](#)

This article describes how to enable replication for on-premises VMware VMs, for disaster recovery to Azure using the [Azure Site Recovery](#) service.

This is the third tutorial in a series that shows you how to set up disaster recovery to Azure for on-premises VMware VMs. In the previous tutorial, we [prepared the on-premises VMware environment](#) for disaster recovery to Azure.

In this tutorial, you learn how to:

- Set up the source replication settings, and an on-premises Site Recovery configuration server.
- Set up the replication target settings.
- Create a replication policy.
- Enable replication for a VMware VM.

NOTE

Tutorials show you the simplest deployment path for a scenario. They use default options where possible, and don't show all possible settings and paths. For detailed instructions, review the article in the How To section of the Site Recovery Table of Contents.

Before you start

Complete the previous tutorials:

1. Make sure you've [set up Azure](#) for on-premises VMware disaster recovery to Azure.
2. Follow [these steps](#) to prepare your on-premises VMware deployment for disaster recovery to Azure.
3. In this tutorial we show you how to replicate a single VM. If you're deploying multiple VMware VMs you should use the [Deployment Planner Tool](#). [Learn more](#) about this tool.
4. This tutorial uses a number of options you might want to do differently:
 - The tutorial uses an OVA template to create the configuration server VMware VM. If you can't do this for some reason, follow [these instructions](#) to set up the configuration server manually.
 - In this tutorial, Site Recovery automatically downloads and installs MySQL to the configuration server. If you prefer, you can set it up manually instead. [Learn more](#).

Select a protection goal

1. In **Recovery Services vaults**, select the vault name. We're using **ContosoVMVault** for this scenario.
2. In **Getting Started**, select Site Recovery. Then select **Prepare Infrastructure**.
3. In **Protection goal > Where are your machines located**, select **On-premises**.
4. In **Where do you want to replicate your machines**, select **To Azure**.
5. In **Are your machines virtualized**, select **Yes, with VMware vSphere Hypervisor**. Then select **OK**.

Set up the source environment

In your source environment, you need a single, highly available, on-premises machine to host these on-premises Site Recovery components:

- **Configuration server:** The configuration server coordinates communications between on-premises and Azure, and manages data replication.
- **Process server:** The process server acts as a replication gateway. It receives replication data; optimizes it with caching, compression, and encryption, and sends it to a cache storage account in Azure. The process server also installs the Mobility Service agent on VMs you want to replicate, and performs automatic discovery of on-premises VMware VMs.
- **Master target server:** The master target server handles replication data during failback from Azure.

All of these components are installed together on the single on-premises machines that's known as the *configuration server*. By default, for VMware disaster recovery, we set up the configuration server as a highly available VMware VM. To do this, you download a prepared Open Virtualization Application (OVA) template, and import the template into VMware to create the VM.

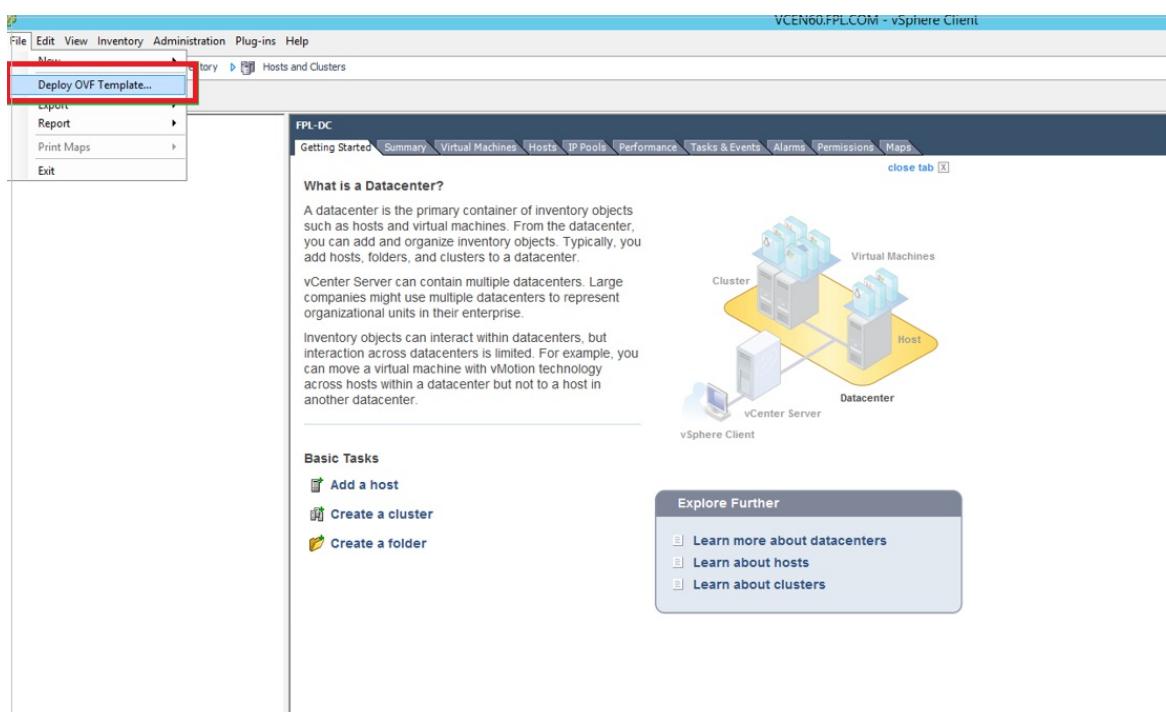
- The latest version of the configuration server is available in the portal. You can also download it directly from the [Microsoft Download Center](#).
- If for some reason you can't use an OVA template to set up a VM, follow [these instructions](#) to set up the configuration server manually.
- The license provided with OVF template is an evaluation license valid for 180 days. Windows running on the VM must be activated with the required license.

Download the VM template

1. In the vault, go to **Prepare Infrastructure > Source**.
2. In **Prepare source**, select **+Configuration server**.
3. In **Add Server**, check that **Configuration server for VMware** appears in **Server type**.
4. Download the OVF template for the configuration server.

Import the template in VMware

1. Sign in to the VMware vCenter server or vSphere ESXi host with the VMWare vSphere Client.
2. On the **File** menu, select **Deploy OVF Template** to start the **Deploy OVF Template Wizard**.



3. On **Select source**, enter the location of the downloaded OVF.
4. On **Review details**, select **Next**.
5. On **Select name and folder** and **Select configuration**, accept the default settings.
6. On **Select storage**, for best performance select **Thick Provision Eager Zeroed** in **Select virtual disk format**.
7. On the rest of the wizard pages, accept the default settings.
8. On **Ready to complete**, to set up the VM with the default settings, select **Power on after deployment > Finish**.

TIP

If you want to add an additional NIC, clear **Power on after deployment > Finish**. By default, the template contains a single NIC. You can add additional NICs after deployment.

Add an additional adapter

If you want to add an additional NIC to the configuration server, add it before you register the server in the vault. Adding additional adapters isn't supported after registration.

1. In the vSphere Client inventory, right-click the VM and select **Edit Settings**.
2. In **Hardware**, select **Add > Ethernet Adapter**. Then select **Next**.
3. Select an adapter type and a network.
4. To connect the virtual NIC when the VM is turned on, select **Connect at power on**. Select **Next > Finish**. Then select **OK**.

Register the configuration server

After the configuration server is set up, you register it in the vault.

1. From the VMWare vSphere Client console, turn on the VM.
2. The VM boots up into a Windows Server 2016 installation experience. Accept the license agreement, and enter an administrator password.
3. After the installation finishes, sign in to the VM as the administrator.
4. The first time you sign in, the Azure Site Recovery Configuration Tool starts within a few seconds.
5. Enter a name that's used to register the configuration server with Site Recovery. Then select **Next**.
6. The tool checks that the VM can connect to Azure. After the connection is established, select **Sign in** to sign in to your Azure subscription. The credentials must have access to the vault in which you want to register the configuration server. Ensure that necessary **roles** are assigned to this user.
7. The tool performs some configuration tasks and then reboots.
8. Sign in to the machine again. In a few seconds, the Configuration Server Management Wizard starts automatically.

Configure settings and add the VMware server

Finish setting up and registering the configuration server. Before proceeding, ensure all [pre-requisites](#) are met for successful set up of configuration server.

1. In the configuration server management wizard, select **Setup connectivity**. From the dropdowns, first select the NIC that the in-built process server uses for discovery and push installation of mobility service on source machines, and then select the NIC that Configuration Server uses for connectivity with Azure. Then select

Save. You cannot change this setting after it's configured.

2. In **Select Recovery Services vault**, select your Azure subscription and the relevant resource group and vault.
3. In **Install third-party software**, accept the license agreement. Select **Download and Install** to install MySQL Server. If you placed MySQL in the path, this step can be skipped. Learn [more](#)
4. In **Validate appliance configuration**, prerequisites are verified before you continue.
5. In **Configure vCenter Server/vSphere ESXi server**, enter the FQDN or IP address of the vCenter server, or vSphere host, where the VMs you want to replicate are located. Enter the port on which the server is listening. Enter a friendly name to be used for the VMware server in the vault.
6. Enter user credentials to be used by the configuration server to connect to the VMware server. Ensure that the user name and password are correct and is a part of the Administrators group of the virtual machine to be protected. Site Recovery uses these credentials to automatically discover VMware VMs that are available for replication. Select **Add**, and then select **Continue**.
7. In **Configure virtual machine credentials**, enter the user name and password that will be used to automatically install Mobility Service on VMs when replication is enabled.
 - For Windows machines, the account needs local administrator privileges on the machines you want to replicate.
 - For Linux, provide details for the root account.
8. Select **Finalize configuration** to complete registration.
9. After registration finishes, open the Azure portal and verify that the configuration server and VMware server are listed on **Recovery Services Vault > Manage > Site Recovery Infrastructure > Configuration Servers**.

After the configuration server is registered, Site Recovery connects to VMware servers by using the specified settings, and discovers VMs.

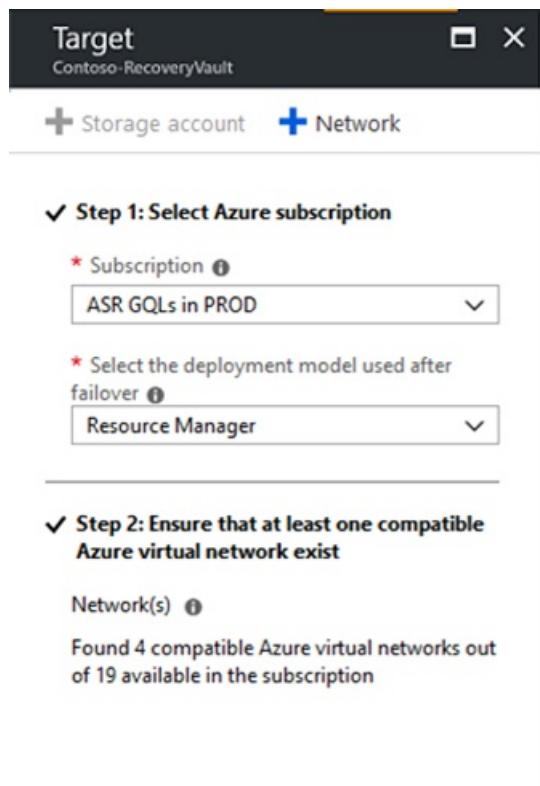
NOTE

It can take 15 minutes or more for the account name to appear in the portal. To update immediately, select **Configuration Servers > server name > Refresh Server**.

Set up the target environment

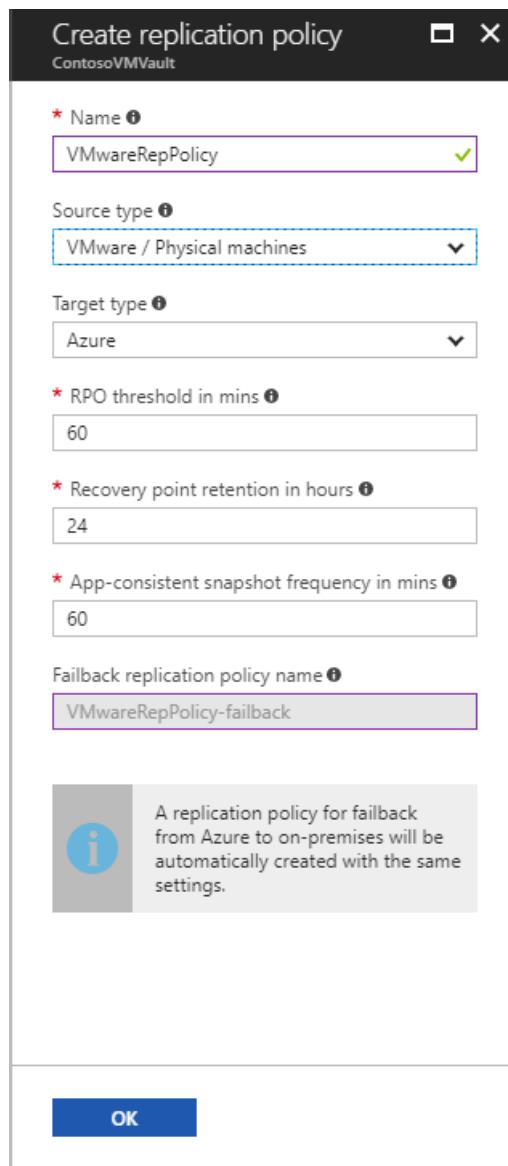
Select and verify target resources.

1. Select **Prepare infrastructure > Target**. Select the Azure subscription you want to use. We're using a Resource Manager model.
2. Site Recovery checks that you have one or more virtual networks. You should have these when you set up the Azure components in the [first tutorial](#) in this tutorial series.



Create a replication policy

1. Open the [Azure portal](#). Search for and select **Recovery Services vaults**.
2. Select the Recovery Services vault (**ContosoVMVault** in this tutorial).
3. To create a replication policy, select **Site Recovery infrastructure > Replication Policies > +Replication Policy**.
4. In **Create replication policy**, enter the policy name. We're using **VMwareRepPolicy**.
5. In **RPO threshold**, use the default of 60 minutes. This value defines how often recovery points are created. An alert is generated if continuous replication exceeds this limit.
6. In **Recovery point retention**, specify how longer each recovery point is retained. For this tutorial we're using 72 hours. Replicated VMs can be recovered to any point in a retention window.
7. In **App-consistent snapshot frequency**, specify how often app-consistent snapshots are created. We're using the default of 60 minutes. Select **OK** to create the policy.



- The policy is automatically associated with the configuration server.
- A matching policy is automatically created for failback by default. For example, if the replication policy is **rep-policy**, then the failback policy is **rep-policy-failback**. This policy isn't used until you initiate a failback from Azure.

Enable replication

Enable replication for VMs as follows:

1. Select **Replicate application > Source**.
2. In **Source**, select **On-premises**, and select the configuration server in **Source location**.
3. In **Machine type**, select **Virtual Machines**.
4. In **vCenter/vSphere Hypervisor**, select the vSphere host, or vCenter server that manages the host.
5. Select the process server (installed by default on the configuration server VM). Then select **OK**. Health status of each process server is indicated as per recommended limits and other parameters. Choose a healthy process server. A **critical** process server cannot be chosen. You can either **troubleshoot and resolve** the errors **or** set up a **scale-out process server**.
6. In **Target**, select the subscription and the resource group in which you want to create the failed-over VMs. We're using the Resource Manager deployment model.
7. Select the Azure network and subnet to which Azure VMs connect when they're created after failover.
8. Select **Configure now for selected machines** to apply the network setting to all VMs on which you enable replication. Select **Configure later** to select the Azure network per machine.

9. In **Virtual Machines** > **Select virtual machines**, select each machine you want to replicate. You can only select machines for which replication can be enabled. Then select **OK**. If you are not able to view/select any particular virtual machine, [learn more](#) about resolving the issue.
10. In **Properties** > **Configure properties**, select the account to be used by the process server to automatically install Mobility Service on the machine.
11. In **Replication settings** > **Configure replication settings**, verify that the correct replication policy is selected.
12. Select **Enable Replication**. Site Recovery installs the Mobility Service when replication is enabled for a VM.
13. You can track progress of the **Enable Protection** job in **Settings** > **Jobs** > **Site Recovery Jobs**. After the **Finalize Protection** job runs and a recovery point generation is complete, the machine is ready for failover.
14. It can take 15 minutes or longer for changes to take effect and appear in the portal.
15. To monitor VMs you add, check the last discovered time for VMs in **Configuration Servers** > **Last Contact At**. To add VMs without waiting for the scheduled discovery, highlight the configuration server (don't select it) and select **Refresh**.

Next steps

After enabling replication, run a drill to make sure everything's working as expected.

[Run a disaster recovery drill](#)

Run a disaster recovery drill to Azure

11/12/2019 • 4 minutes to read • [Edit Online](#)

This article describes how to run a disaster recovery drill for an on-premises machine to Azure using the [Azure Site Recovery](#) service. A drill validates your replication strategy without data loss.

This is the fourth tutorial in a series that shows you how to set up disaster recovery to Azure for on-premises machines.

In this tutorial, learn how to:

- Set up an isolated network for the test failover
- Prepare to connect to the Azure VM after failover
- Run a test failover for a single machine.

NOTE

Tutorials show you the simplest deployment path for a scenario. They use default options where possible, and don't show all possible settings and paths. If you want to learn about the disaster recovery drill steps in more detail, [review this article](#).

Before you start

Complete the previous tutorials:

1. Make sure you've [set up Azure](#) for on-premises disaster recovery of VMware VMs, Hyper-V VMs, and physical machines to Azure.
2. Prepare your on-premises [VMware](#) or [Hyper-V](#) environment for disaster recovery. If you're setting up disaster recovery for physical servers, review the [support matrix](#).
3. Set up disaster recovery for [VMware VMs](#), [Hyper-V VMs](#), or [physical machines](#).

Verify VM properties

Before you run a test failover, verify the VM properties, and make sure that the [Hyper-V VM](#), or [VMware VM](#) complies with Azure requirements.

1. In **Protected Items**, click **Replicated Items** > and the VM.
2. In the **Replicated item** pane, there's a summary of VM information, health status, and the latest available recovery points. Click **Properties** to view more details.
3. In **Compute and Network**, you can modify the Azure name, resource group, target size, availability set, and managed disk settings.
4. You can view and modify network settings, including the network/subnet in which the Azure VM will be located after failover, and the IP address that will be assigned to it.
5. In **Disk**, you can see information about the operating system and data disks on the VM.

Create a network for test failover

We recommend that for test failover, you choose a network that's isolated from the production recovery site network specific in the **Compute and Network** settings for each VM. By default, when you create an Azure virtual network, it is isolated from other networks. The test network should mimic your production network:

- The test network should have same number of subnets as your production network. Subnets should have the same names.
- The test network should use the same IP address range.
- Update the DNS of the test network with the IP address specified for the DNS VM in **Compute and Network** settings. Read [test failover considerations for Active Directory](#) for more details.

Run a test failover for a single VM

When you run a test failover, the following happens:

1. A prerequisites check runs to make sure all of the conditions required for failover are in place.
2. Failover processes the data, so that an Azure VM can be created. If you select the latest recovery point, a recovery point is created from the data.
3. An Azure VM is created using the data processed in the previous step.

Run the test failover as follows:

1. In **Settings > Replicated Items**, click the VM > **+Test Failover**.
2. Select the **Latest processed** recovery point for this tutorial. This fails over the VM to the latest available point in time. The time stamp is shown. With this option, no time is spent processing data, so it provides a low RTO (recovery time objective).
3. In **Test Failover**, select the target Azure network to which Azure VMs will be connected after failover occurs.
4. Click **OK** to begin the failover. You can track progress by clicking on the VM to open its properties. Or you can click the **Test Failover** job in vault name > **Settings > Jobs > Site Recovery jobs**.
5. After the failover finishes, the replica Azure VM appears in the Azure portal > **Virtual Machines**. Check that the VM is the appropriate size, that it's connected to the right network, and that it's running.
6. You should now be able to connect to the replicated VM in Azure.
7. To delete Azure VMs created during the test failover, click **Cleanup test failover** on the VM. In **Notes**, record and save any observations associated with the test failover.

In some scenarios, failover requires additional processing that takes around eight to ten minutes to complete. You might notice longer test failover times for VMware Linux machines, VMware VMs that don't have the DHCP service enabled, and VMware VMs that don't have the following boot drivers: storvsc, vmbus, storflt, intelide, atapi.

Connect after failover

If you want to connect to Azure VMs using RDP/SSH after failover, [prepare to connect](#). If you encounter any connectivity issues after failover, follow the [troubleshooting](#) guide.

Next steps

[Run a failover and fallback for VMware VMs](#) [Run a failover and fallback for Hyper-V VMs](#) [Run a failover and fallback for physical machines](#)

Fail over VMware VMs

12/26/2019 • 3 minutes to read • [Edit Online](#)

This article describes how to fail over an on-premises VMware virtual machine (VM) to Azure with [Azure Site Recovery](#).

This is the fifth tutorial in a series that shows you how to set up disaster recovery to Azure for on-premises machines.

In this tutorial, you learn how to:

- Verify that the VMware VM properties conform with Azure requirements.
- Fail over specific VMs to Azure.

NOTE

Tutorials show you the simplest deployment path for a scenario. They use default options where possible and don't show all possible settings and paths. If you want to learn about failover in detail, see [Fail over VMs and physical servers](#).

[Learn about](#) different types of failover. If you want to fail over multiple VMs in a recovery plan, review [this article](#).

Before you start

Complete the previous tutorials:

1. Make sure you've [set up Azure](#) for on-premises disaster recovery of VMware VMs, Hyper-V VMs, and physical machines to Azure.
2. Prepare your on-premises [VMware](#) environment for disaster recovery.
3. Set up disaster recovery for [VMware VMs](#).
4. Run a [disaster recovery drill](#) to make sure that everything's working as expected.

Verify VM properties

Before you run a failover, check the VM properties to make sure that the VMs meet [Azure requirements](#).

Verify properties as follows:

1. In **Protected Items**, select **Replicated Items**, and then select the VM you want to verify.
2. In the **Replicated item** pane, there's a summary of VM information, health status, and the latest available recovery points. Select **Properties** to view more details.
3. In **Compute and Network**, you can modify these properties as needed:
 - Azure name
 - Resource group
 - Target size
 - [Availability set](#)
 - Managed disk settings
4. You can view and modify network settings, including:
 - The network and subnet in which the Azure VM will be located after failover.

- The IP address that will be assigned to it.
5. In **Disks**, you can see information about the operating system and data disks on the VM.

Run a failover to Azure

1. In **Settings > Replicated items**, select the VM you want to fail over, and then select **Failover**.
2. In **Failover**, select a **Recovery Point** to fail over to. You can use one of the following options:
 - **Latest**: This option first processes all the data sent to Site Recovery. It provides the lowest Recovery Point Objective (RPO) because the Azure VM that's created after failover has all the data that was replicated to Site Recovery when the failover was triggered.
 - **Latest processed**: This option fails the VM over to the latest recovery point processed by Site Recovery. This option provides a low RTO (Recovery Time Objective) because no time is spent processing unprocessed data.
 - **Latest app-consistent**: This option fails the VM over to the latest app-consistent recovery point processed by Site Recovery.
 - **Custom**: This option lets you specify a recovery point.
3. Select **Shut down machine before beginning failover** to attempt to shut down source VMs before triggering the failover. Failover continues even if the shutdown fails. You can follow the failover progress on the **Jobs** page.

In some scenarios, failover requires additional processing that takes around 8 to 10 minutes to complete. You might notice longer test failover times for:

- VMware VMs running a Mobility service version older than 9.8.
- Physical servers.
- VMware Linux VMs.
- Hyper-V VMs protected as physical servers.
- VMware VMs that don't have the DHCP service enabled.
- VMware VMs that don't have the following boot drivers: storvsc, vmbus, storflt, intelide, atapi.

WARNING

Don't cancel a failover in progress. Before failover is started, VM replication is stopped. If you cancel a failover in progress, failover stops, but the VM won't replicate again.

Connect to failed-over VM

1. If you want to connect to Azure VMs after failover by using Remote Desktop Protocol (RDP) and Secure Shell (SSH), [verify that the requirements have been met](failover-fallback-overview.md#connect-to-azure-after-failover).
2. After failover, go to the VM and validate by [connecting](#) to it.
3. Use **Change recovery point** if you want to use a different recovery point after failover. After you commit the failover in the next step, this option will no longer be available.
4. After validation, select **Commit** to finalize the recovery point of the VM after failover.
5. After you commit, all the other available recovery points are deleted. This step completes the failover.

TIP

If you encounter any connectivity issues after failover, follow the [troubleshooting guide](#).

Next steps

After failover, reprotect the Azure VMs to on-premises. Then, after the VMs are reprotected and replicating to the on-premises site, fail back from Azure when you're ready.

[Reprotect Azure VMs Fail back from Azure](#)

Prepare Azure resources for Hyper-V disaster recovery

11/14/2019 • 4 minutes to read • [Edit Online](#)

Azure Site Recovery helps business continuity and disaster recovery (BCDR) by keeping business apps running during planned and unplanned outages. Site Recovery manages and orchestrates disaster recovery of on-premises machines and Azure virtual machines (VMs), including replication, failover, and recovery.

This tutorial is the first in a series that describes how to set up disaster recovery for on-premises Hyper-V VMs.

NOTE

We design tutorials to show the simplest deployment path for a scenario. These tutorials use default options when possible, and don't show all possible settings and paths. For more information, see the "How To" section for each corresponding scenario.

This tutorial shows you how to prepare Azure components when you want to replicate on-premises VMs (Hyper-V) to Azure. You'll learn how to:

- Verify that your Azure account has replication permissions.
- Create an Azure storage account, which stores images of replicated machines.
- Create a Recovery Services vault, which stores metadata and configuration information for VMs and other replication components.
- Set up an Azure network. When Azure VMs are created after failover, they're joined to this network.

If you don't have an Azure subscription, create a [free account](#) before you begin.

Sign in

Sign in to the [Azure portal](#).

Verify account permissions

If you just created a free Azure account, you're the administrator for that subscription. If you're not the administrator, work with the administrator to assign the permissions you need. To enable replication for a new virtual machine, you must have permission to:

- Create a VM in the selected resource group.
- Create a VM in the selected virtual network.
- Write to the selected storage account.

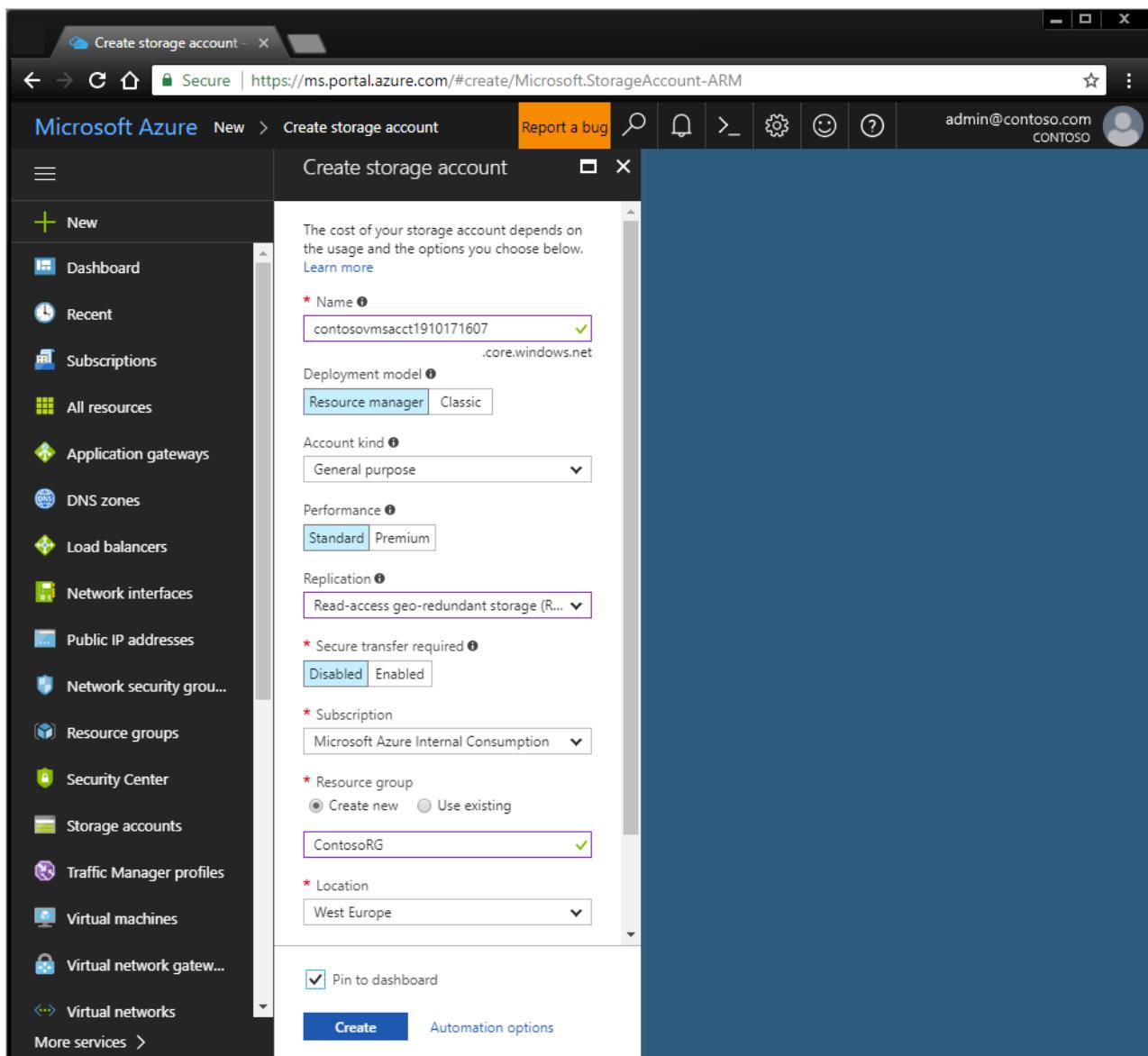
To complete these tasks, your account should be assigned the Virtual Machine Contributor built-in role. To manage Site Recovery operations in a vault, your account should be assigned the Site Recovery Contributor built-in role.

Create a storage account

Images of replicated machines are held in Azure storage. Azure VMs are created from the storage when you fail over from on-premises to Azure. The storage account must be in the same region as the Recovery Services vault.

1. In the [Azure portal](#) menu, select **Create a resource > Storage > Storage account - blob, file, table, queue**.

- In **Create storage account**, enter a name for the account. The name you choose must be unique within Azure, be from 3 to 24 characters long, and only use lowercase letters and numbers. For this tutorial, use **contosovmsacct1910171607**.
- In **Deployment model**, select **Resource Manager**.
- In **Account kind**, select **Storage (general-purpose v1)**. Don't select blob storage.
- In **Replication**, select the default **Read-access geo-redundant storage** for storage redundancy. Leave the Secure transfer required setting as **Disabled**.
- In **Performance**, select **Standard**. Next, in **Access tier**, select the default option of **Hot**.
- In **Subscription**, choose the subscription in which you want to create the new storage account.
- In **Resource group**, enter a new resource group. An Azure resource group is a logical container in which Azure resources are deployed and managed. For this tutorial, use **ContosoRG**.
- In **Location**, choose the geographic location for your storage account. For this tutorial, use **West Europe**.
- Select **Create** to create the storage account.



Create a recovery services vault

- In the Azure portal, select **+Create a resource**, and then search the Azure Marketplace for Recovery Services.
- Select **Backup and Site Recovery (OMS)**. Next, on the **Backup and Site Recovery** page, select **Create**.
- In **Recovery services vault > Name**, enter a friendly name to identify the vault. For this tutorial, use **ContosoVMVault**.
- In **Resource group**, select an existing resource group or create a new one. For this tutorial, use **contosoRG**.

5. In **Location**, select the region where the vault should be located. For this tutorial, use **West Europe**.
6. To quickly access the vault from the dashboard, select **Pin to dashboard > Create**.

The screenshot shows the 'Create Recovery Services vault' wizard in the Microsoft Azure portal. The title bar says 'Microsoft Azure' and 'Search resources, services, and docs (G+ /)'. The breadcrumb navigation shows 'Home > New > Backup and Site Recovery > Create Recovery Services vault'. The main title is 'Create Recovery Services vault'. Below it, there are three tabs: 'Basics *' (which is selected), 'Tags', and 'Review + create'. The 'Project Details' section asks to select a subscription and resource group. The 'Subscription' dropdown is set to 'Contoso Subscription' and the 'Resource group' dropdown is set to 'contosoRG', with a 'Create new' link. The 'Instance Details' section asks for a 'Vault name' and 'Region'. The 'Vault name' field contains 'ConstosoVMVault' with a green checkmark. The 'Region' dropdown is set to 'West Europe'. At the bottom, there are two buttons: 'Review + create' (in blue) and 'Next: Tags'.

The new vault appears on **Dashboard > All resources**, and on the main **Recovery Services vaults** page.

Set up an Azure network

When Azure VMs are created from storage after failover, they're joined to this network.

1. In the [Azure portal](#), select **Create a resource > Networking > Virtual network**. Leave Resource Manager selected as the deployment model.
2. In **Name**, enter a network name. The name must be unique within the Azure resource group. For this tutorial, use **ContosoASRnet**.
3. Specify the resource group in which to create the network. For this tutorial, use the existing resource group **contosoRG**.
4. In **Address range**, enter **10.0.0.0/24** as the range for the network. There's no subnet for this network.
5. In **Subscription**, select the subscription in which to create the network.
6. In **Location**, choose **West Europe**. The network must be in the same region as the Recovery Services vault.
7. Leave the default options of basic DDoS protection, with no service endpoint on the network.
8. Select **Create**.

Create virtual network

Name *
ContosoASRnet

Address space * ⓘ
10.1.0.0/24
10.1.0.0 - 10.1.0.255 (256 addresses)

Add an IPv6 address space ⓘ

Subscription *
Contoso Subscription

Resource group *
contosoRG Create new

Location *
(Europe) West Europe

Subnet

Name *
default

Address range * ⓘ
10.1.0.0/24
10.1.0.0 - 10.1.0.255 (256 addresses)

DDoS protection ⓘ
 Basic Standard

Service endpoints ⓘ
 Disabled Enabled

Firewall ⓘ
 Disabled Enabled

Create [Automation options](#)

The virtual network takes a few seconds to create. After it's created, you'll see it in the Azure portal dashboard.

Useful links

Learn about:

- [Azure networks](#)
- [Managed disks](#)

Next steps

[Prepare the on-premises Hyper-V infrastructure for disaster recovery to Azure](#)

Prepare on-premises Hyper-V servers for disaster recovery to Azure

11/12/2019 • 3 minutes to read • [Edit Online](#)

This article describes how to prepare your on-premises Hyper-V infrastructure when you want to set up disaster recovery of Hyper-VMs to Azure, using [Azure Site Recovery](#).

This is the second tutorial in a series that shows you how to set up disaster recovery to Azure for on-premises Hyper-V VMs. In the first tutorial, we [set up the Azure components](#) needed for Hyper-V disaster recovery.

In this tutorial you learn how to:

- Review Hyper-V requirements, and VMM requirements if your Hyper-V hosts are managed by System Center VMM.
- Prepare VMM if applicable.
- Verify internet access to Azure locations.
- Prepare VMs so that you can access them after failover to Azure.

NOTE

Tutorials show you the simplest deployment path for a scenario. They use default options where possible, and don't show all possible settings and paths. For detailed instructions, review the article in the How To section of the Site Recovery Table of Contents.

Before you start

Make sure you've prepared Azure as described in the [first tutorial in this series](#).

Review requirements and prerequisites

Make sure Hyper-V hosts and VMs comply with requirements.

1. [Verify](#) on-premises server requirements.
2. [Check the requirements](#) for Hyper-V VMs you want to replicate to Azure.
3. Check Hyper-V host [networking](#); and host and guest [storage](#) support for on-premises Hyper-V hosts.
4. Check what's supported for [Azure networking](#), [storage](#), and [compute](#), after failover.
5. Your on-premises VMs you replicate to Azure must comply with [Azure VM requirements](#).

Prepare VMM (optional)

If Hyper-V hosts are managed by VMM, you need to prepare the on-premises VMM server.

- Make sure the VMM server has at least one cloud, with one or more host groups. The Hyper-V host on which VMs are running should be located in the cloud.
- Prepare the VMM server for network mapping.

Prepare VMM for network mapping

If you're using VMM, [network mapping](#) maps between on-premises VMM VM networks, and Azure virtual networks. Mapping ensures that Azure VMs are connected to the right network when they're created after

failover.

Prepare VMM for network mapping as follows:

1. Make sure you have a [VMM logical network](#) that's associated with the cloud in which the Hyper-V hosts are located.
2. Ensure you have a [VM network](#) linked to the logical network.
3. In VMM, connect the VMs to the VM network.

Verify internet access

1. For the purposes of the tutorial, the simplest configuration is for the Hyper-V hosts and VMM server to have direct access to the internet without using a proxy.
2. Make sure that Hyper-V hosts, and the VMM server if relevant, can access the required URLs below.
3. If you're controlling access by IP address, make sure that:
 - IP address-based firewall rules can connect to [Azure Datacenter IP Ranges](#), and the HTTPS (443) port.
 - Allow IP address ranges for the Azure region of your subscription.

Required URLs

NAME	COMMERCIAL URL	GOVERNMENT URL	DESCRIPTION
Azure Active Directory	login.microsoftonline.com	login.microsoftonline.us	Used for access control and identity management by using Azure Active Directory.
Backup	*.backup.windowsazure.com	*.backup.windowsazure.us	Used for replication data transfer and coordination.
Replication	*.hypervrecoverymanager.windows.net	*.hypervrecoverymanager.windows.usgovcloudapi.net	Used for replication management operations and coordination.
Storage	*.blob.core.windows.net	*.blob.core.usgovcloudapi.net	Used for access to the storage account that stores replicated data.
Telemetry (optional)	dc.services.visualstudio.com	dc.services.visualstudio.com	Used for telemetry.
Time synchronization	time.windows.com	time.nist.gov	Used to check time synchronization between system and global time in all deployments.

Prepare to connect to Azure VMs after failover

During a failover scenario you may want to connect to your replicated on-premises network.

To connect to Windows VMs using RDP after failover, allow access as follows:

1. To access over the internet, enable RDP on the on-premises VM before failover. Make sure that TCP, and UDP rules are added for the **Public** profile, and that RDP is allowed in **Windows Firewall > Allowed Apps** for all profiles.
2. To access over site-to-site VPN, enable RDP on the on-premises machine. RDP should be allowed in the **Windows Firewall -> Allowed apps and features** for **Domain and Private** networks. Check that the

operating system's SAN policy is set to **OnlineAll**. [Learn more](#). There should be no Windows updates pending on the VM when you trigger a failover. If there are, you won't be able to sign in to the virtual machine until the update completes.

3. On the Windows Azure VM after failover, check **Boot diagnostics** to view a screenshot of the VM. If you can't connect, check that the VM is running and review these [troubleshooting tips](#).

After failover, you can access Azure VMs using the same IP address as the replicated on-premises VM, or a different IP address. [Learn more](#) about setting up IP addressing for failover.

Next steps

[Set up disaster recovery to Azure for Hyper-V VMs](#) [Set up disaster recovery to Azure for Hyper-V VMs in VMM clouds](#)

Set up disaster recovery of on-premises Hyper-V VMs to Azure

11/13/2019 • 5 minutes to read • [Edit Online](#)

The [Azure Site Recovery](#) service contributes to your disaster-recovery strategy by managing and orchestrating replication, failover, and failback of on-premises machines and Azure virtual machines (VMs).

This is the third tutorial in a series. It shows you how to set up disaster recovery of on-premises Hyper-V VMs to Azure. This tutorial applies Hyper-V VMs that are not managed by Microsoft System Center Virtual Machine Manager (VMM).

In this tutorial, you learn how to:

- Select your replication source and target.
- Set up the source replication environment, including on-premises Site Recovery components and the target replication environment.
- Create a replication policy.
- Enable replication for a VM.

NOTE

Tutorials show you the simplest deployment path for a scenario. They use default options where possible, and don't show all possible settings and paths. For detailed instructions, review the articles in the **How-to Guides** section of the [Site Recovery documentation](#).

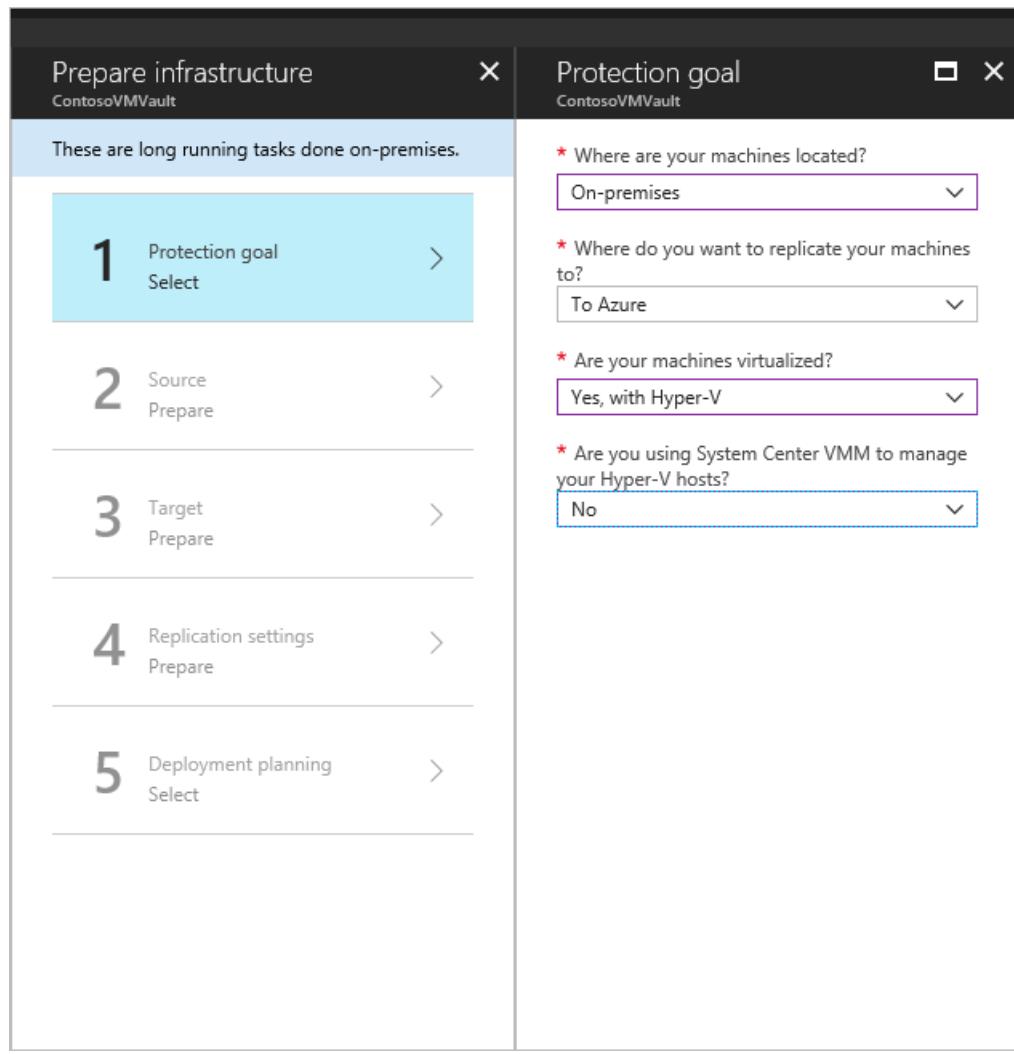
Before you begin

This is the third tutorial in a series. It assumes that you have already completed the tasks in the previous tutorials:

1. [Prepare Azure](#)
2. [Prepare on-premises Hyper-V](#)

Select a replication goal

1. In the Azure portal, go to **Recovery Services vaults** and select the vault. We prepared the vault **ContosoVMVault** in the previous tutorial.
2. In **Getting Started**, select **Site Recovery**, and then select **Prepare Infrastructure**.
3. In **Protection goal > Where are your machines located?**, select **On-premises**.
4. In **Where do you want to replicate your machines?**, select **To Azure**.
5. In **Are your machines virtualized?**, select **Yes, with Hyper-V**.
6. In **Are you using System Center VMM to manage your Hyper-V hosts?**, select **No**.
7. Select **OK**.



Confirm deployment planning

1. In **Deployment planning**, if you're planning a large deployment, download the Deployment Planner for Hyper-V from the link on the page. [Learn more](#) about Hyper-V deployment planning.
2. For this tutorial, we don't need the Deployment Planner. In **Have you completed deployment planning?**, select **I will do it later**, and then select **OK**.

The screenshot shows the Azure Recovery Services vault interface. On the left, there's a sidebar with sections for 'FOR ON-PREMISES MACHINES' (containing 'Prepare Infrastructure') and 'FOR ON-PREMISES MACHINES AND AZURE VMs' (containing 'Step 1: Replicate Application' and 'Step 2: Manage Recovery Plans'). The main area is titled 'These are long running tasks done on-premises.' and lists five steps:

- 1 Protection goal**: Hyper-V VMs to Azure. Status: ✓
- 2 Deployment planning**: Select. Status: ✓
- 3 Source**: Prepare.
- 4 Target**: Prepare.
- 5 Replication settings**: Prepare.

To the right of the steps, there's a note about network bandwidth and storage provisioning, a download link for the deployment planner, and a dropdown menu for deployment planning status.

Set up the source environment

To set up the source environment, you create a Hyper-V site and add to that site the Hyper-V hosts containing VMs that you want to replicate. Then, you download and install the Azure Site Recovery Provider and the Azure Recovery Services agent on each host, and register the Hyper-V site in the vault.

1. Under **Prepare Infrastructure**, select **Source**.
2. In **Prepare source**, select **+ Hyper-V Site**.
3. In **Create Hyper-V site**, specify the site name. We're using **ContosoHyperVSite**.

The screenshot shows the 'Create Hyper-V site' step in the wizard. The left panel shows the task list with step 3 selected ('Source Prepare'). The right panel has two sections:

- Step 1: Select Hyper-V site**: A button '+ Hyper-V Site' is highlighted with a red box. Below it is a note: '(0 sites found) Click on +Hyper-V Site in the command bar above to add a site.'
- Step 2: Ensure Hyper-V servers are added**: A note says 'Complete previous step(s)'.

A form on the right allows specifying the site name, with 'ContosoHyperVSite' entered and a green checkmark indicating it's valid.

4. After the site is created, in **Prepare source > Step 1: Select Hyper-V site**, select the site you created.

5. Select **+ Hyper-V Server**.

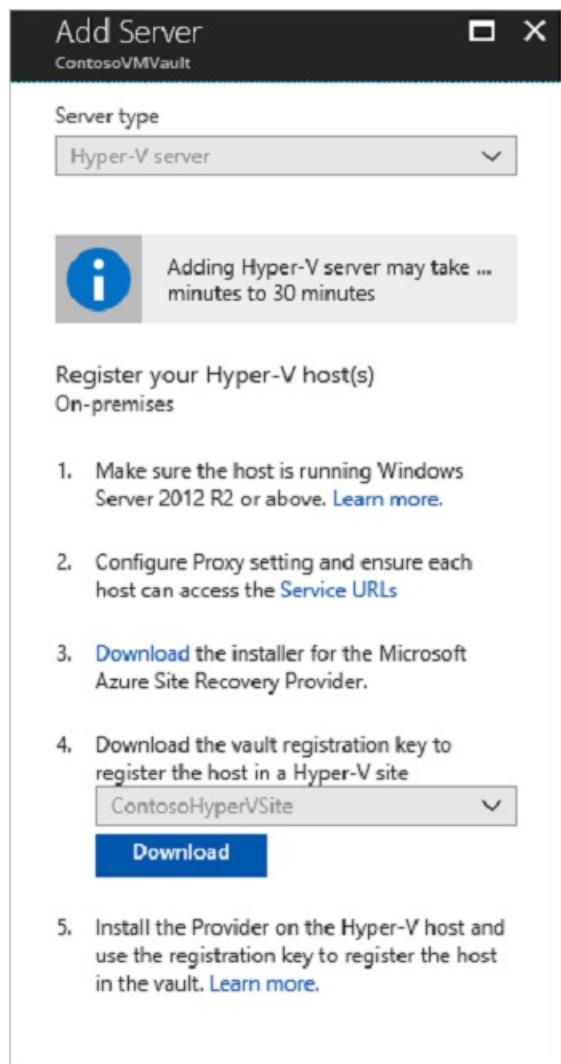
The screenshot shows the 'Prepare source > Step 1: Select Hyper-V site' configuration screen. On the left, there is a list of steps:

- 1 Protection goal: Hyper-V VMs to Azure (Completed)
- 2 Deployment planning: I will do it later (Completed)
- 3 Source: Prepare (In Progress)
- 4 Target: Prepare (Not Started)
- 5 Replication settings: Prepare (Not Started)

On the right, the 'Step 1: Select Hyper-V site' section is displayed. It includes a 'Hyper-V Site' dropdown menu where 'ContosoHyperVSite' is selected. A red box highlights the '+ Hyper-V Server' button in the top navigation bar. Below the dropdown, there is a message: '0 Found... Click on +Hyper-V server in top command bar to add a Hyper-V server to the site. This may take approximately 15 min to 30 min.'

6. Download the installer for the Microsoft Azure Site Recovery Provider.

7. Download the vault registration key. You need this key to install the Provider. The key is valid for five days after you generate it.



Install the Provider

Install the downloaded setup file (AzureSiteRecoveryProvider.exe) on each Hyper-V host that you want to add to the Hyper-V site. Setup installs the Azure Site Recovery Provider and Recovery Services agent on each Hyper-V host.

1. Run the setup file.
2. In the Azure Site Recovery Provider Setup wizard > **Microsoft Update**, opt in to use Microsoft Update to check for Provider updates.
3. In **Installation**, accept the default installation location for the Provider and agent, and select **Install**.
4. After installation, in the Microsoft Azure Site Recovery Registration Wizard > **Vault Settings**, select **Browse**, and in **Key File**, select the vault key file that you downloaded.
5. Specify the Azure Site Recovery subscription, the vault name (**ContosoVMVault**), and the Hyper-V site (**ContosoHyperVSite**) to which the Hyper-V server belongs.
6. In **Proxy Settings**, select **Connect directly to Azure Site Recovery without a proxy**.
7. In **Registration**, after the server is registered in the vault, select **Finish**.

Metadata from the Hyper-V server is retrieved by Azure Site Recovery, and the server is displayed in **Site Recovery Infrastructure > Hyper-V Hosts**. This process can take up to 30 minutes.

Install the Provider on a Hyper-V core server

If you're running a Hyper-V core server, download the setup file and follow these steps:

1. Extract the files from AzureSiteRecoveryProvider.exe to a local directory by running this command:

```
AzureSiteRecoveryProvider.exe /x:. /q
```

2. Run `.\setupdr.exe /i`. Results are logged to %Programdata%\ASRLogs\DRASetupWizard.log.

3. Register the server by running this command:

```
cd "C:\Program Files\Microsoft Azure Site Recovery Provider\DRConfigurator.exe" /r /Friendlyname "FriendlyName of the Server" /Credentials "path to where the credential file is saved"
```

Set up the target environment

Select and verify target resources:

1. Select **Prepare infrastructure > Target**.
2. Select the subscription and the resource group **ContosoRG** in which the Azure VMs will be created after failover.
3. Select the **Resource Manager**" deployment model.

Site Recovery checks that you have one or more compatible Azure storage accounts and networks.

Set up a replication policy

1. Select **Prepare infrastructure > Replication Settings > +Create and associate**.
2. In **Create and associate policy**, specify a policy name. We're using **ContosoReplicationPolicy**.
3. For this tutorial, we'll leave the default settings:
 - **Copy frequency** indicates how often delta data (after initial replication) will replicate. The default frequency is every five minutes.
 - **Recovery point retention** indicates that recovery points will be retained for two hours.
 - **App-consistent snapshot frequency** indicates that recovery points containing app-consistent snapshots will be created every hour.
 - **Initial replication start time** indicates that initial replication will start immediately.
4. After the policy is created, select **OK**. When you create a new policy, it's automatically associated with the specified Hyper-V site. In our tutorial, that's **ContosoHyperVSite**.

Create and associate policy X

IbizaAsrTest

* Name i
ContosoReplicationPolicy ✓

Source type i
Hyper-V

Target type i
Azure

Copy frequency i
5 Minutes

* Recovery point retention in hours i
2

* App-consistent snapshot frequency in hours i
1

Initial replication start time i
Immediately

Associated Hyper-V site i
ContosoHyperVSite

Enable replication

1. In **Replicate application**, select **Source**.
2. In **Source**, select the **ContosoHyperVSite** site. Then, select **OK**.
3. In **Target**, verify the target (Azure), the vault subscription, and the **Resource Manager** deployment model.
4. If you're using tutorial settings, select the **contosovmsacct1910171607** storage account created in the previous tutorial for replicated data. Also select the **ContosoASRnet** network, in which Azure VMs will be located after failover.
5. In **Virtual machines > Select**, select the VM that you want to replicate. Then, select **OK**.

You can track progress of the **Enable Protection** action in **Jobs > Site Recovery jobs**. After the **Finalize Protection** job finishes, the initial replication is complete, and the VM is ready for failover.

Next steps

[Run a disaster recovery drill](#)

Set up disaster recovery of on-premises Hyper-V VMs in VMM clouds to Azure

11/13/2019 • 5 minutes to read • [Edit Online](#)

This article describes how to enable replication for on-premises Hyper-V VMs managed by System Center Virtual Machine Manager (VMM), for disaster recovery to Azure by using the [Azure Site Recovery](#) service. If you aren't using VMM, [follow this tutorial](#) instead.

This is the third tutorial in a series that shows you how to set up disaster recovery to Azure for on-premises VMware VMs. In the previous tutorial, we [prepared the on-premises Hyper-V environment](#) for disaster recovery to Azure.

In this tutorial, you learn how to:

- Select your replication source and target.
- Set up the source replication environment, including on-premises Site Recovery components and the target replication environment.
- Set up network mapping to map between VMM VM networks and Azure virtual networks.
- Create a replication policy.
- Enable replication for a VM.

NOTE

Tutorials show you the simplest deployment path for a scenario. They use default options where possible, and don't show all possible settings and paths. For detailed instructions, review the articles in the **How-to Guides** section of the [Site Recovery documentation](#).

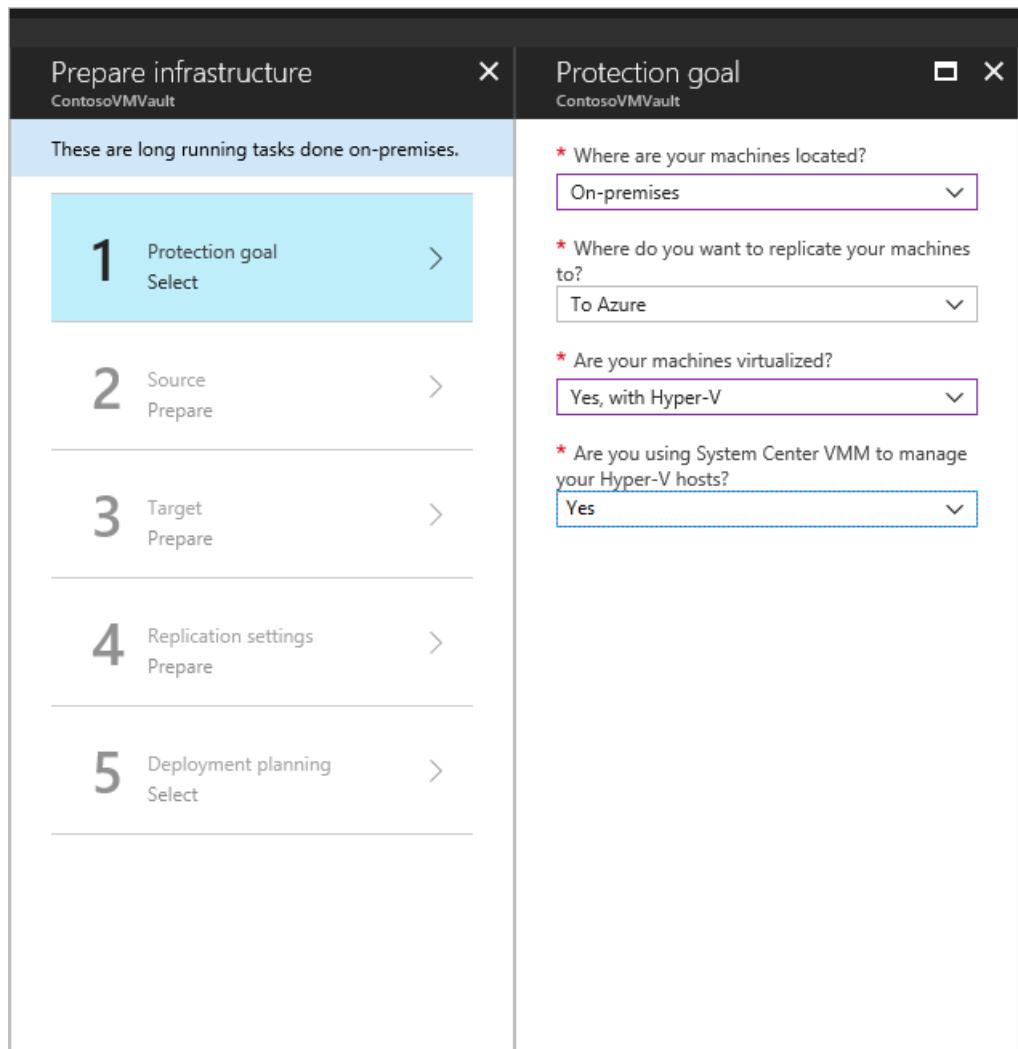
Before you begin

This is the third tutorial in a series. It assumes that you have already completed the tasks in the previous tutorials:

1. [Prepare Azure](#)
2. [Prepare on-premises Hyper-V](#)

Select a replication goal

1. In the Azure portal, go to **Recovery Services vaults** and select the vault. We prepared the vault **ContosoVMVault** in the previous tutorial.
2. In **Getting Started**, select **Site Recovery**, and then select **Prepare Infrastructure**.
3. In **Protection goal > Where are your machines located?**, select **On-premises**.
4. In **Where do you want to replicate your machines?**, select **To Azure**.
5. In **Are your machines virtualized?**, select **Yes, with Hyper-V**.
6. In **Are you using System Center VMM to manage your Hyper-V hosts?**, select **Yes**.
7. Select **OK**.



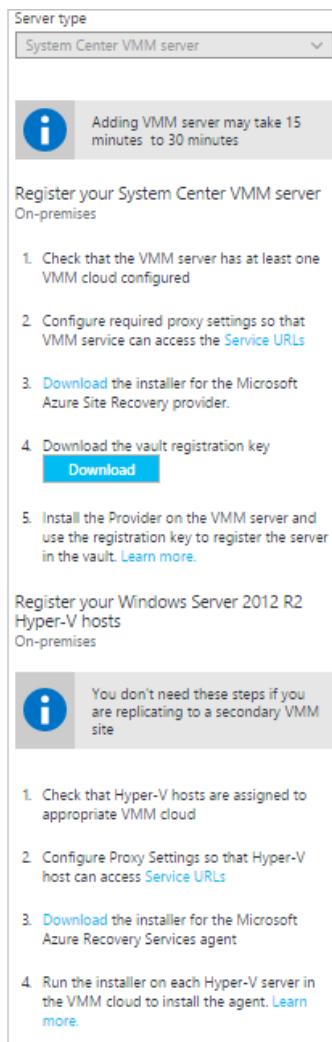
Confirm deployment planning

1. In **Deployment planning**, if you're planning a large deployment, download the Deployment Planner for Hyper-V from the link on the page. [Learn more](#) about Hyper-V deployment planning.
2. For this tutorial, we don't need the Deployment Planner. In **Have you completed deployment planning?**, select **I will do it later**, and then select **OK**.

Set up the source environment

When you set up the source environment, you install the Azure Site Recovery Provider on the VMM server and register the server in the vault. You install the Azure Recovery Services agent on each Hyper-V host.

1. In **Prepare Infrastructure**, select **Source**.
2. In **Prepare source**, select **+ VMM** to add a VMM server. In **Add Server**, check that **System Center VMM server** appears in **Server type**.
3. Download the installer for the Microsoft Azure Site Recovery Provider.
4. Download the vault registration key. You need this key when you run the Provider setup. The key is valid for five days after you generate it.
5. Download the installer for the Microsoft Azure Recovery Services agent.



Install the Provider on the VMM server

1. In the Azure Site Recovery Provider Setup wizard > **Microsoft Update**, opt in to use Microsoft Update to check for Provider updates.
2. In **Installation**, accept the default installation location for the Provider and select **Install**.
3. After installation, in the Microsoft Azure Site Recovery Registration Wizard > **Vault Settings**, select **Browse**, and in **Key file**, select the vault key file that you downloaded.
4. Specify the Azure Site Recovery subscription, and the vault name (**ContosoVMVault**). Specify a friendly name for the VMM server, to identify it in the vault.
5. In **Proxy Settings**, select **Connect directly to Azure Site Recovery without a proxy**.
6. Accept the default location for the certificate that's used to encrypt data. Encrypted data will be decrypted when you fail over.
7. In **Synchronize cloud metadata**, select **Sync cloud meta data to Site Recovery portal**. This action needs to happen only once on each server. Then, select **Register**.
8. After the server is registered in the vault, select **Finish**.

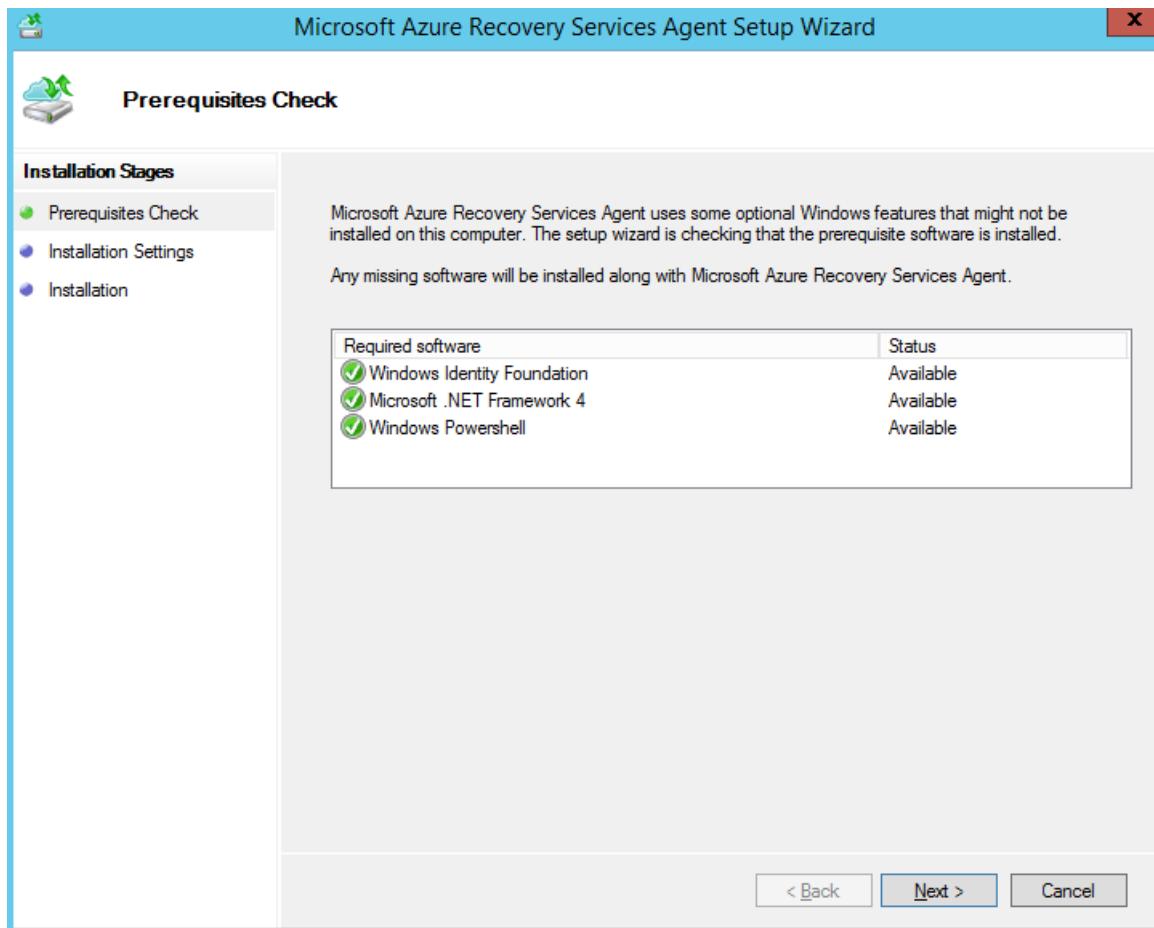
After registration finishes, metadata from the server is retrieved by Azure Site Recovery, and the VMM server is displayed in **Site Recovery Infrastructure**.

Install the Recovery Services agent on Hyper-V hosts

Install the agent on each Hyper-V host containing VMs that you want to replicate.

1. In the Microsoft Azure Recovery Services Agent Setup Wizard > **Prerequisites Check**, select **Next**. Any missing prerequisites will be installed automatically.
2. In **Installation Settings**, accept the installation location and the cache location. The cache drive needs at least 5 GB of storage. We recommend a drive with 600 GB or more of free space. Then, select **Install**.

3. In **Installation**, when installation finishes, select **Close** to finish the wizard.



Set up the target environment

1. Select **Prepare infrastructure > Target**.
2. Select the subscription and the resource group (**ContosoRG**) in which the Azure VMs will be created after failover.
3. Select the **Resource Manager** deployment model.

Site Recovery checks that you have one or more compatible Azure storage accounts and networks.

Configure network mapping

1. In **Site Recovery Infrastructure > Network mappings > Network Mapping**, select the **+Network Mapping** icon.
2. In **Add network mapping**, select the source VMM server. Select **Azure** as the target.
3. Verify the subscription and the deployment model after failover.
4. In **Source network**, select the source on-premises VM network.
5. In **Target network**, select the Azure network in which replica Azure VMs will be located when they're created after failover. Then, select **OK**.

* Source System Center VMM	* Target
CP-L2B18-X64-48.drtest.ntttest.microsoft....	Azure
* Subscription	
Contoso Subscription	
* Post-failover deployment model	
Resource Manager	
* Source network	* Target network
VSwitch_VLan	ContosoASRnet
Network type	Subnet
No isolation	default 10.0.0.0/24
Subnet	
No subnets are configured.	
Network ID	
e056827b-0d94-41bc-9631-d972e3395541	

Set up a replication policy

1. Select **Prepare infrastructure > Replication Settings > +Create and associate**.
2. In **Create and associate policy**, specify a policy name. We're using **ContosoReplicationPolicy**.
3. Leave the default settings and select **OK**.
 - **Copy frequency** indicates that, after initial replication, delta data will replicate every five minutes.
 - **Recovery point retention** indicates that each recovery point will be retained for two hours.
 - **App-consistent snapshot frequency** indicates that recovery points containing app-consistent snapshots will be created every hour.
 - **Initial replication start time** indicates that initial replication will start immediately.
 - **Encrypt data stored on Azure** is set to the default (**Off**) and indicates that at-rest data in Azure isn't encrypted.
4. After the policy is created, select **OK**. When you create a new policy, it's automatically associated with the VMM cloud.

Enable replication

1. In **Replicate application**, select **Source**.
2. In **Source**, select the VMM cloud. Then, select **OK**.
3. In **Target**, verify the target (Azure), the vault subscription, and select the **Resource Manager** model.
4. Select the **contosovmsacct1910171607** storage account and the **ContosoASRnet** Azure network.
5. In **Virtual machines > Select**, select the VM that you want to replicate. Then, select **OK**.

You can track progress of the **Enable Protection** action in **Jobs > Site Recovery jobs**. After the **Finalize Protection** job finishes, the initial replication is complete, and the VM is ready for failover.

Next steps

[Run a disaster recovery drill](#)

Run a disaster recovery drill to Azure

11/12/2019 • 4 minutes to read • [Edit Online](#)

This article describes how to run a disaster recovery drill for an on-premises machine to Azure using the [Azure Site Recovery](#) service. A drill validates your replication strategy without data loss.

This is the fourth tutorial in a series that shows you how to set up disaster recovery to Azure for on-premises machines.

In this tutorial, learn how to:

- Set up an isolated network for the test failover
- Prepare to connect to the Azure VM after failover
- Run a test failover for a single machine.

NOTE

Tutorials show you the simplest deployment path for a scenario. They use default options where possible, and don't show all possible settings and paths. If you want to learn about the disaster recovery drill steps in more detail, [review this article](#).

Before you start

Complete the previous tutorials:

1. Make sure you've [set up Azure](#) for on-premises disaster recovery of VMware VMs, Hyper-V VMs, and physical machines to Azure.
2. Prepare your on-premises [VMware](#) or [Hyper-V](#) environment for disaster recovery. If you're setting up disaster recovery for physical servers, review the [support matrix](#).
3. Set up disaster recovery for [VMware VMs](#), [Hyper-V VMs](#), or [physical machines](#).

Verify VM properties

Before you run a test failover, verify the VM properties, and make sure that the [Hyper-V VM](#), or [VMware VM](#) complies with Azure requirements.

1. In **Protected Items**, click **Replicated Items** > and the VM.
2. In the **Replicated item** pane, there's a summary of VM information, health status, and the latest available recovery points. Click **Properties** to view more details.
3. In **Compute and Network**, you can modify the Azure name, resource group, target size, availability set, and managed disk settings.
4. You can view and modify network settings, including the network/subnet in which the Azure VM will be located after failover, and the IP address that will be assigned to it.
5. In **Disk**, you can see information about the operating system and data disks on the VM.

Create a network for test failover

We recommend that for test failover, you choose a network that's isolated from the production recovery site network specific in the **Compute and Network** settings for each VM. By default, when you create an Azure virtual network, it is isolated from other networks. The test network should mimic your production network:

- The test network should have same number of subnets as your production network. Subnets should have the same names.
- The test network should use the same IP address range.
- Update the DNS of the test network with the IP address specified for the DNS VM in **Compute and Network** settings. Read [test failover considerations for Active Directory](#) for more details.

Run a test failover for a single VM

When you run a test failover, the following happens:

1. A prerequisites check runs to make sure all of the conditions required for failover are in place.
2. Failover processes the data, so that an Azure VM can be created. If you select the latest recovery point, a recovery point is created from the data.
3. An Azure VM is created using the data processed in the previous step.

Run the test failover as follows:

1. In **Settings > Replicated Items**, click the VM > **+Test Failover**.
2. Select the **Latest processed** recovery point for this tutorial. This fails over the VM to the latest available point in time. The time stamp is shown. With this option, no time is spent processing data, so it provides a low RTO (recovery time objective).
3. In **Test Failover**, select the target Azure network to which Azure VMs will be connected after failover occurs.
4. Click **OK** to begin the failover. You can track progress by clicking on the VM to open its properties. Or you can click the **Test Failover** job in vault name > **Settings > Jobs > Site Recovery jobs**.
5. After the failover finishes, the replica Azure VM appears in the Azure portal > **Virtual Machines**. Check that the VM is the appropriate size, that it's connected to the right network, and that it's running.
6. You should now be able to connect to the replicated VM in Azure.
7. To delete Azure VMs created during the test failover, click **Cleanup test failover** on the VM. In **Notes**, record and save any observations associated with the test failover.

In some scenarios, failover requires additional processing that takes around eight to ten minutes to complete. You might notice longer test failover times for VMware Linux machines, VMware VMs that don't have the DHCP service enabled, and VMware VMs that don't have the following boot drivers: storvsc, vmbus, storflt, intelide, atapi.

Connect after failover

If you want to connect to Azure VMs using RDP/SSH after failover, [prepare to connect](#). If you encounter any connectivity issues after failover, follow the [troubleshooting](#) guide.

Next steps

[Run a failover and fallback for VMware VMs](#) [Run a failover and fallback for Hyper-V VMs](#) [Run a failover and fallback for physical machines](#)

Fail over Hyper-V VMs to Azure

12/26/2019 • 2 minutes to read • [Edit Online](#)

This tutorial describes how to fail over Hyper-V VMs to Azure with [Azure Site Recovery](#). After you've failed over, you fail back to your on-premises site when it's available. In this tutorial, you learn how to:

- Verify the Hyper-V VM properties to check conform with Azure requirements.
- Fail over specific VMs to Azure.

This tutorial is the fifth tutorial in a series. It assumes that you have already completed the tasks in the previous tutorials.

1. [Prepare Azure](#)
2. [Prepare on-premises Hyper-V](#)
3. Set up disaster recovery for [Hyper-V VMs](#), or for [Hyper-V VMs managed in System Center VMM clouds](#)
4. [Run a disaster recovery drill](#)

[Learn about](#) different types of failover. If you want to fail over multiple VMs in a recovery plan, review [this article](#).

Prepare for failover

Make sure there are no snapshots on the VM, and that the on-premises VM is turned off during failback. It helps ensure data consistency during replication. Don't turn on on-premises VM during failback.

Failover and failback have three stages:

1. **Failover to Azure:** Failover Hyper-V VMs from the on-premises site to Azure.
2. **Failback to on-premises:** Failover Azure VMs to your on-premises site when the on-premises site is available. It starts synchronizing data from Azure to on-premises and on completion, it brings up the VMs on on-premises.
3. **Reverse replicate on-premises VMs:** After failed back to on-premises, reverse replicate the on-premises VMs to start replicating them to Azure.

Verify VM properties

Before failover verify the VM properties, and make sure that the VM meets with [Azure requirements](#).

In **Protected Items**, click **Replicated Items** > VM.

1. In the **Replicated item** pane, there's a summary of VM information, health status, and the latest available recovery points. Click **Properties** to view more details.
2. In **Compute and Network**, you can modify the Azure name, resource group, target size, [availability set](#), and managed disk settings.
3. You can view and modify network settings, including the network/subnet in which the Azure VM will be located after failover, and the IP address that will be assigned to it.
4. In **Disks**, you can see information about the operating system and data disks on the VM.

Fail over to Azure

1. In **Settings** > **Replicated items**, click the VM > **Failover**.

2. In **Failover**, select the **Latest** recovery point.
3. Select **Shut down machine before beginning failover**. Site Recovery attempts to do a shutdown of source VMs before triggering the failover. Failover continues even if shutdown fails. You can follow the failover progress on the **Jobs** page.
4. After you verify the failover, click **Commit**. It deletes all the available recovery points.

WARNING

Don't cancel a failover in progress: If you cancel in progress, failover stops, but the VM won't replicate again.

Connect to failed-over VM

1. If you want to connect to Azure VMs after failover by using Remote Desktop Protocol (RDP) and Secure Shell (SSH), [verify that the requirements have been met](#).
2. After failover, go to the VM and validate by [connecting](#) to it.
3. Use **Change recovery point** if you want to use a different recovery point after failover. After you commit the failover in the next step, this option will no longer be available.
4. After validation, select **Commit** to finalize the recovery point of the VM after failover.
5. After you commit, all the other available recovery points are deleted. This step completes the failover.

TIP

If you encounter any connectivity issues after failover, follow the [troubleshooting guide](#).

Next steps

After failover, reprotect the Azure VMs so that they replicate from Azure to on-premises. Then, after the VMs are reprotected and replicating to the on-premises site, fail back from Azure when you're ready.

Prepare Azure for on-premises disaster recovery to Azure

11/5/2019 • 3 minutes to read • [Edit Online](#)

This article describes how to prepare Azure resources and components so that you can set up disaster recovery of on-premises VMware VMs, Hyper-V VMs, or Windows/Linux physical servers to Azure, using the [Azure Site Recovery](#) service.

This article is the first tutorial in a series that shows you how to set up disaster recovery for on-premises VMs.

In this tutorial, you learn how to:

- Verify that the Azure account has replication permissions.
- Create a Recovery Services vault. A vault holds metadata and configuration information for VMs, and other replication components.
- Set up an Azure virtual network (VNet). When Azure VMs are created after failover, they're joined to this network.

NOTE

Tutorials show you the simplest deployment path for a scenario. They use default options where possible, and don't show all possible settings and paths. For detailed instructions, review the article in the How To section of the Site Recovery Table of Contents.

Before you start

- Review the architecture for [VMware](#), [Hyper-V](#), and [physical server](#) disaster recovery.
- Read common questions for [VMware](#) and [Hyper-V](#)

If you don't have an Azure subscription, create a [free account](#) before you begin. Then sign in to the [Azure portal](#).

Verify account permissions

If you just created your free Azure account, you're the administrator of your subscription and you have the permissions you need. If you're not the subscription administrator, work with the administrator to assign the permissions you need. To enable replication for a new virtual machine, you must have permission to:

- Create a VM in the selected resource group.
- Create a VM in the selected virtual network.
- Write to an Azure storage account.
- Write to an Azure managed disk.

To complete these tasks your account should be assigned the Virtual Machine Contributor built-in role. In addition, to manage Site Recovery operations in a vault, your account should be assigned the Site Recovery Contributor built-in role.

Create a Recovery Services vault

1. From the Azure portal menu, select **Create a resource**, and search the Marketplace for **Recovery**.
2. Select **Backup and Site Recovery** from the search results, and in the Backup and Site Recovery page, click **Create**.
3. In the **Create Recovery Services vault** page, select the **Subscription**. We're using **Contoso Subscription**.
4. In **Resource group**, select an existing resource group or create a new one. For this tutorial we're using **contosoRG**.
5. In **Vault name**, enter a friendly name to identify the vault. For this set of tutorials we're using **ContosoVMVault**.
6. In **Region**, select the region in which the vault should be located. We're using **West Europe**.
7. Select **Review + create**.

The screenshot shows the 'Create Recovery Services vault' wizard in the Microsoft Azure portal. The 'Basics' tab is active. In the 'Project Details' section, the 'Subscription' dropdown is set to 'Contoso Subscription'. Below it, the 'Resource group' dropdown is set to 'contosoRG' and has a 'Create new' link next to it. In the 'Instance Details' section, the 'Vault name' field contains 'ContosoVMVault' with a green checkmark. The 'Region' dropdown is set to 'West Europe'. At the bottom of the form, there are two buttons: 'Review + create' in blue and 'Next: Tags' in grey.

The new vault will now be listed in **Dashboard > All resources**, and on the main **Recovery Services vaults** page.

Set up an Azure network

On-premises machines are replicated to Azure managed disks. When failover occurs, Azure VMs are created from these managed disks, and joined to the Azure network you specify in this procedure.

1. In the [Azure portal](#), select **Create a resource** > **Networking** > **Virtual network**.
2. Keep **Resource Manager** selected as the deployment model.
3. In **Name**, enter a network name. The name must be unique within the Azure resource group. We're using **ContosoASRnet** in this tutorial.

4. In **Address space**, enter the virtual network's address range in CDR notation. We're using **10.1.0.0/24**.
5. In **Subscription**, select the subscription in which to create the network.
6. Specify the **Resource group** in which the network will be created. We're using the existing resource group **contosoRG**.
7. In **Location**, select the same region as that in which the Recovery Services vault was created. In our tutorial it's **West Europe**. The network must be in the same region as the vault.
8. In **Address range**, enter the range for the network. We're using **10.1.0.0/24**, and not using a subnet.
9. We're leaving the default options of basic DDoS protection, with no service endpoint, or firewall on the network.
10. Select **Create**.

Create virtual network

Name * ✓

Address space * ⓘ ✓
10.1.0.0 - 10.1.0.255 (256 addresses)

Add an IPv6 address space ⓘ

Subscription * ↗

Resource group * ↗ [Create new](#)

Location * ↗

Subnet

Name *

Address range * ⓘ ✓
10.1.0.0 - 10.1.0.255 (256 addresses)

DDoS protection ⓘ Basic Standard

Service endpoints ⓘ Disabled Enabled

Firewall ⓘ Disabled Enabled

Create [Automation options](#)

The virtual network takes a few seconds to create. After it's created, you'll see it in the Azure portal

dashboard.

Next steps

- For VMware disaster recovery, [prepare the on-premises VMware infrastructure](#).
- For Hyper-V disaster recovery, [prepare the on-premises Hyper-V servers](#).
- For physical server disaster recovery, [set up the configuration server and source environment](#)
- [Learn about Azure networks](#).
- [Learn about managed disks](#).

Migrate on-premises machines to Azure

11/12/2019 • 5 minutes to read • [Edit Online](#)

This article describes how to migrate on-premises machines to Azure, using the [Azure Site Recovery](#). Generally, Site Recovery is used to manage and orchestrate disaster recovery of on-premises machines and Azure VMs. However, it can also be used for migration. Migration uses the same steps as disaster recovery with one exception. In a migration, failing machines over from your on-premises site is the final step. Unlike disaster recovery, you can't fail back to on-premises in a migration scenario.

This tutorial shows you how to migrate on-premises VMs and physical servers to Azure. You learn how to:

- Set up the source and target environment for migration
- Set up a replication policy
- Enable replication
- Run a test migration to make sure everything's working as expected
- Run a one-time failover to Azure

TIP

You can now migrate on-premises servers to Azure using the Azure Migrate service. [Learn more](#)

Before you start

Note that devices exported by paravirtualized drivers aren't supported.

Prepare Azure and on-premises

1. Prepare Azure as described in [this article](#). Although this article describes preparation steps for disaster recovery, the steps are also valid for migration.
2. Prepare on-premises [VMware](#) or [Hyper-V](#) servers. If you're migrating physical machines, you don't need to prepare anything. Just verify the [support matrix](#).

Select a protection goal

Select what you want to replicate, and where you want to replicate to.

1. Click **Recovery Services vaults** > vault.
2. In the Resource Menu, click **Site Recovery** > **Prepare Infrastructure** > **Protection goal**.
3. In **Protection goal**, select what you want to migrate.
 - **VMware**: Select **To Azure** > **Yes, with VMWare vSphere Hypervisor**.
 - **Physical machine**: Select **To Azure** > **Not virtualized/Other**.
 - **Hyper-V**: Select **To Azure** > **Yes, with Hyper-V**. If Hyper-V VMs are managed by VMM, select **Yes**.

Set up the source environment

SCENARIO

DETAILS

SCENARIO	DETAILS
VMware	Set up the source environment , and set up the configuration server .
Physical machine	Set up the source environment and configuration server.
Hyper-V	<p>Set up the source environment</p> <p>Set up the source environment for Hyper-V deployed with System Center VMM.</p>

Set up the target environment

Select and verify target resources.

1. Click **Prepare infrastructure > Target**, and select the Azure subscription you want to use.
2. Specify the Resource Manager deployment model.
3. Site Recovery checks the Azure resources.
 - If you're migrating VMware VMs or physical servers, Site Recovery verifies you have an Azure network in which the Azure VMs will be located when they're created after failover.
 - If you're migrating Hyper-V VMs, Site Recovery verifies you have a compatible Azure storage account and network.
4. If you're migrating Hyper-V VMs managed by System Center VMM, set up [network mapping](#).

Set up a replication policy

SCENARIO	DETAILS
VMware	Set up a replication policy for VMware VMs.
Physical machine	Set up a replication policy for physical machines.
Hyper-V	<p>Set up a replication policy</p> <p>Set up a replication policy for Hyper-V deployed with System Center VMM.</p>

Enable replication

SCENARIO	DETAILS
VMware	Enable replication for VMware VMs.
Physical machine	Enable replication for physical machines.
Hyper-V	<p>Enable replication</p> <p>Enable replication for Hyper-V deployed with System Center VMM.</p>

Run a test migration

Run a [test failover](#) to Azure, to make sure everything's working as expected.

Migrate to Azure

Run a failover for the machines you want to migrate.

1. In **Settings > Replicated items** click the machine > **Failover**.
2. In **Failover** select a **Recovery Point** to fail over to. Select the latest recovery point.
3. The encryption key setting isn't relevant for this scenario.
4. Select **Shutdown machine before beginning failover**. Site Recovery will attempt to shutdown virtual machines before triggering the failover. Failover continues even if shutdown fails. You can follow the failover progress on the **Jobs** page.
5. Check that the Azure VM appears in Azure as expected.
6. In **Replicated items**, right-click the VM > **Complete Migration**. This does the following:
 - Finishes the migration process, stops replication for the on-premises VM, and stops Site Recovery billing for the VM.
 - This step cleans up the replication data. It doesn't delete the migrated VMs.

The screenshot shows the 'Replicated items' blade in the Azure portal. At the top, there are buttons for Refresh, Replicate, and Columns. Below that, a message says 'Last refreshed at: 10/13/2016, 2:59:17 PM' and 'Finished loading data from service.' There is a 'Filter items...' search bar. The main table lists five VMs:

NAME	HEALTH	STATUS	ACTIVE LOCATION	REPLICATION POLICY
AWSServer2012	OK	Unplanned failover comp...	Microsoft Azure	AWSReplicationPolicy
AWSWordPressRedHat	OK	Protected	AWSGATEWAY	AWSReplicationPolicy
FabrikamMarketing	OK	Unplanned failover comp...	Microsoft Azure	ContosoReplicationPolicy
FabrikamFinance	OK	Protected	CONTOSOGATEWAY	ContosoReplicationPolicy
▶ ContosoReplicationGr...	-	-	-	-

A context menu is open over the 'FabrikamFinance' row, listing options: Pin to dashboard, Unplanned Failover, Test Failover, Change PIT, Commit, Complete Migration (which is highlighted with a red box), Re-protect, Resynchronize, Error Details, and Delete.

WARNING

Don't cancel a failover in progress: VM replication is stopped before failover starts. If you cancel a failover in progress, failover stops, but the VM won't replicate again.

In some scenarios, failover requires additional processing that takes around eight to ten minutes to complete. You might notice longer test failover times for physical servers, VMware Linux machines, VMware VMs that don't have the DHCP service enabled, and VMware VMs that don't have the following boot drivers: storvsc, vmbus, storflt, intelide, atapi.

After migration

After machines are migrated to Azure, there are a number of steps you should complete.

Some steps can be automated as part of the migration process using the in-built automation scripts capability in [recovery plans](#)

Post-migration steps in Azure

- Perform any post-migration app tweaks, such as updating database connection strings, and web server configurations.
- Perform final application and migration acceptance testing on the migrated application now running in Azure.
- The [Azure VM agent](#) manages VM interaction with the Azure Fabric Controller. It's required for some Azure services, such as Azure Backup, Site Recovery, and Azure Security.
 - If you're migrating VMware machines and physical servers, the Mobility Service installer installs available Azure VM agent on Windows machines. On Linux VMs, we recommend that you install the agent after failover.
 - If you're migrating Azure VMs to a secondary region, the Azure VM agent must be provisioned on the VM before the migration.
 - If you're migrating Hyper-V VMs to Azure, install the Azure VM agent on the Azure VM after the migration.
- Manually remove any Site Recovery provider/agent from the VM. If you migrate VMware VMs or physical servers, uninstall the Mobility service from the VM.
- For increased resilience:
 - Keep data secure by backing up Azure VMs using the Azure Backup service. [Learn more](#).
 - Keep workloads running and continuously available by replicating Azure VMs to a secondary region with Site Recovery. [Learn more](#).
- For increased security:
 - Lock down and limit inbound traffic access with Azure Security Center [Just in time administration](#)
 - Restrict network traffic to management endpoints with [Network Security Groups](#).
 - Deploy [Azure Disk Encryption](#) to help secure disks, and keep data safe from theft and unauthorized access.
 - Read more about [securing IaaS resources](#), and visit the [Azure Security Center](#).
- For monitoring and management:
 - Consider deploying [Azure Cost Management](#) to monitor resource usage and spending.

Post-migration steps on-premises

- Move app traffic over to the app running on the migrated Azure VM instance.
- Remove the on-premises VMs from your local VM inventory.
- Remove the on-premises VMs from local backups.
- Update any internal documentation to show the new location and IP address of the Azure VMs.

Next steps

In this tutorial you migrated on-premises VMs to Azure VMs. Now

[Set up disaster recovery](#) to a secondary Azure region for the Azure VMs.

Migrate servers running Windows Server 2008 to Azure

11/12/2019 • 6 minutes to read • [Edit Online](#)

This tutorial shows you how to migrate on-premises servers running Windows Server 2008 or 2008 R2 to Azure using Azure Site Recovery. In this tutorial, you learn how to:

- Prepare your on-premises environment for migration
- Set up the target environment
- Set up a replication policy
- Enable replication
- Run a test migration to make sure everything's working as expected
- Failover to Azure and complete the migration

The limitations and known issues section, lists some of limitations and workarounds for known issues that you may encounter while migrating Windows Server 2008 machines to Azure.

NOTE

You can now migrate from on-premises to Azure using the Azure Migrate service. [Learn more](#).

Supported Operating Systems and environments

OPERATING SYSTEM	ON-PREMISES ENVIRONMENT
Windows Server 2008 SP2 - 32 bit and 64 bit(IA-32 and x86-64) - Standard - Enterprise - Datacenter	VMware VMs, Hyper-V VMs, and Physical Servers
Windows Server 2008 R2 SP1 - 64 bit - Standard - Enterprise - Datacenter	VMware VMs, Hyper-V VMs, and Physical Servers

WARNING

- Migration of servers running Server Core is not supported.
- Ensure that you have the latest service pack and Windows updates installed before migrating.

Prerequisites

Before you start, it's helpful to review the Azure Site Recovery architecture for [VMware and Physical server migration](#) or [Hyper-V virtual machine migration](#)

To migrate Hyper-V virtual machines running Windows Server 2008 or Windows Server 2008 R2, follow the steps in the [migrate on-premises machines to Azure](#) tutorial.

The rest of this tutorial shows you how you can migrate on-premises VMware virtual machines and Physical servers running Windows Server 2008 or 2008 R2.

TIP

Looking for an agentless way to migrate VMware VMs to Azure? [Click here](#)

Limitations and known issues

- The Configuration Server, additional process servers, and mobility service used to migrate Windows Server 2008 SP2 servers should be running version 9.19.0.0 or later of the Azure Site Recovery software.
- Application consistent recovery points and the multi-VM consistency feature are not supported for replication of servers running Windows Server 2008 SP2. Windows Server 2008 SP2 servers should be migrated to a crash consistent recovery point. Crash consistent recovery points are generated every 5 minutes by default. Using a replication policy with a configured application consistent snapshot frequency will cause replication health to turn critical due to the lack of application consistent recovery points. To avoid false positives, set the application-consistent snapshot frequency in the replication policy to "Off".
- The servers being migrated should have .NET Framework 3.5 Service Pack 1 for the mobility service to work.
- If your server has dynamic disks, you may notice in certain configurations, that these disks on the failed over server are marked offline or shown as foreign disks. You may also notice that the mirrored set status for mirrored volumes across dynamic disks is marked "Failed redundancy". You can fix this issue from diskmgmt.msc by manually importing these disks and reactivating them.
- The servers being migrated should have the vmstorfl.sys driver. Failover may fail if the driver is not present in the server being migrated.

TIP

Check if the driver is present at "C:\Windows\system32\drivers\vmstorfl.sys" . If the driver is not found, you can workaround the issue by creating a dummy file in place.

Open command prompt (run > cmd) and run the following: "copy nul c:\Windows\system32\drivers\vmstorfl.sys"

- You may be unable to RDP to Windows Server 2008 SP2 servers running the 32-bit operating system immediately after they are failed over or test failed over to Azure. Restart the failed over virtual machine from the Azure portal and try connecting again. If you are still unable to connect, check if the server is configured to allow remote desktop connections, and ensure that there are no firewall rules or network security groups blocking the connection.

TIP

A test failover is highly recommended before migrating servers. Ensure that you've performed at least one successful test failover on each server that you are migrating. As part of the test failover, connect to the test failed over machine and ensure things work as expected.

The test failover operation is non-disruptive and helps you test migrations by creating virtual machines in an isolated network of your choice. Unlike the failover operation, during the test failover operation, data replication continues to progress. You can perform as many test failovers as you like before you are ready to migrate.

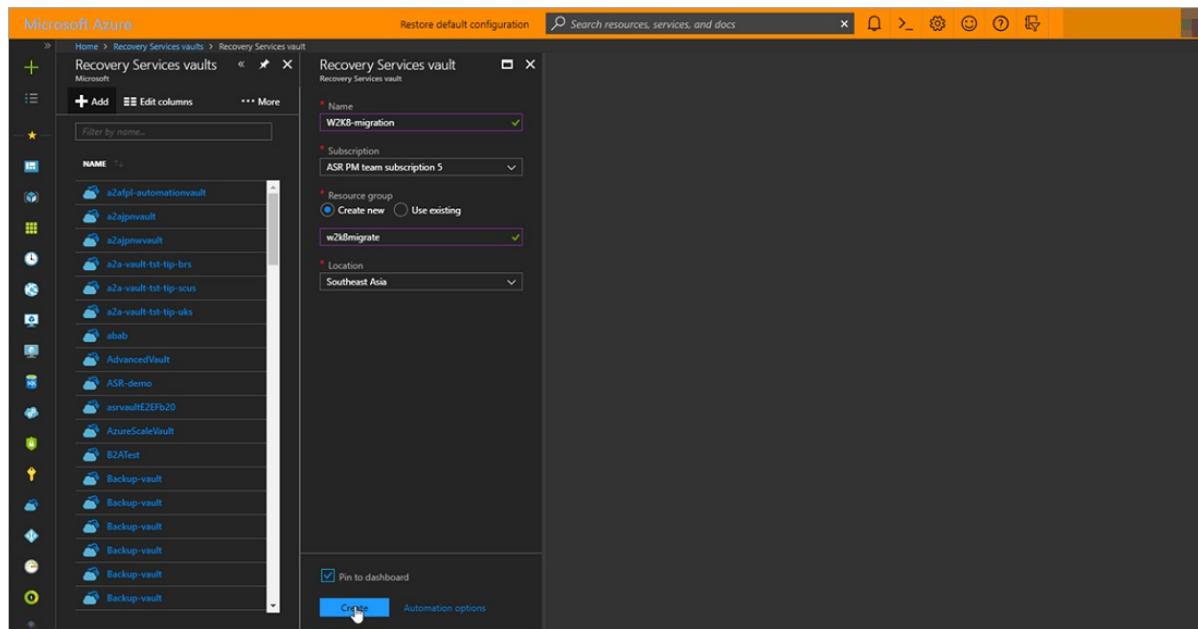
Getting started

Perform the following tasks to prepare the Azure subscription and on-premises VMware/Physical environment:

1. [Prepare Azure](#)
2. Prepare on-premises [VMware](#)

Create a Recovery Services vault

1. Sign in to the [Azure portal](#) > **Recovery Services**.
2. Click **Create a resource** > **Management Tools** > **Backup and Site Recovery**.
3. In **Name**, specify the friendly name **W2K8-migration**. If you have more than one subscription, select the appropriate one.
4. Create a resource group **w2k8migrate**.
5. Specify an Azure region. To check supported regions, see geographic availability in [Azure Site Recovery Pricing Details](#).
6. To quickly access the vault from the dashboard, click **Pin to dashboard** and then click **Create**.



The new vault is added to the **Dashboard** under **All resources**, and on the main **Recovery Services vaults** page.

Prepare your on-premises environment for migration

- To migrate Windows Server 2008 virtual machines running on VMware, [setup the on-premises Configuration Server on VMware](#).
- If the Configuration Server cannot be setup as a VMware virtual machine, [setup the Configuration Server on an on-premises physical server or virtual machine](#).

Set up the target environment

Select and verify target resources.

1. Click **Prepare infrastructure** > **Target**, and select the Azure subscription you want to use.
2. Specify the Resource Manager deployment model.
3. Site Recovery checks that you have one or more compatible Azure storage accounts and networks.

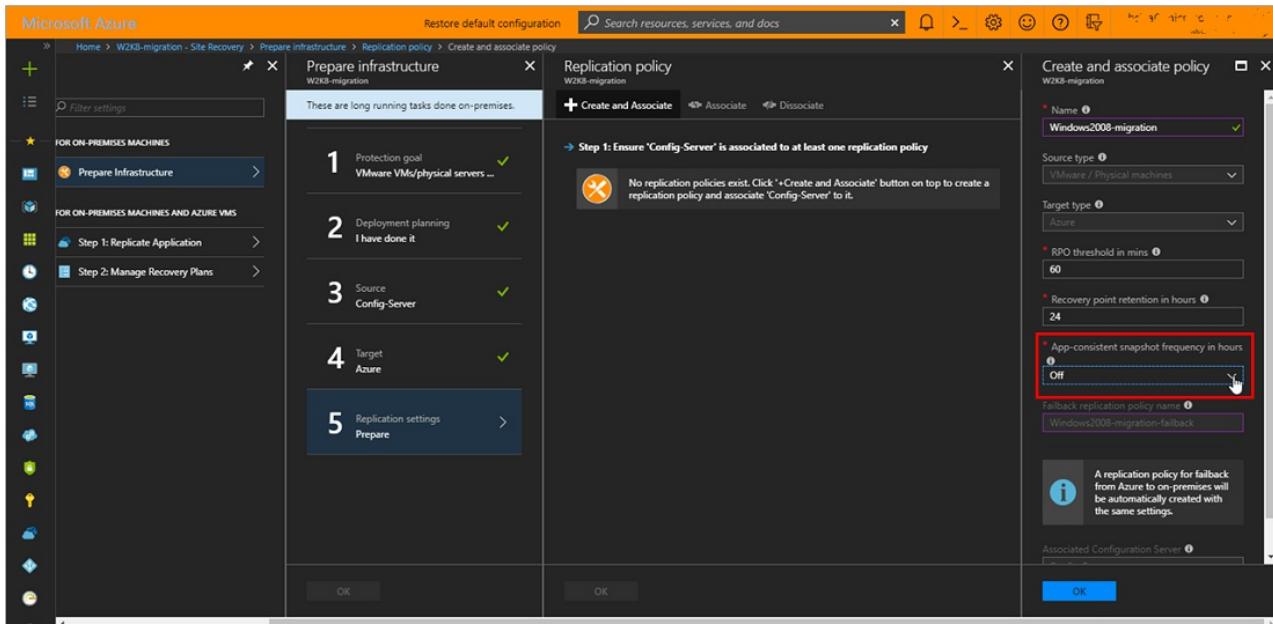
Set up a replication policy

1. To create a new replication policy, click **Site Recovery infrastructure > Replication Policies > +Replication Policy**.
2. In **Create replication policy**, specify a policy name.
3. In **RPO threshold**, specify the recovery point objective (RPO) limit. An alert is generated if the replication RPO exceeds this limit.
4. In **Recovery point retention**, specify how long (in hours) the retention window is for each recovery point. Replicated servers can be recovered to any point in this window. Up to 24 hours retention is supported for machines replicated to premium storage, and 72 hours for standard storage.
5. In **App-consistent snapshot frequency**, specify **Off**. Click **OK** to create the policy.

The policy is automatically associated with the configuration server.

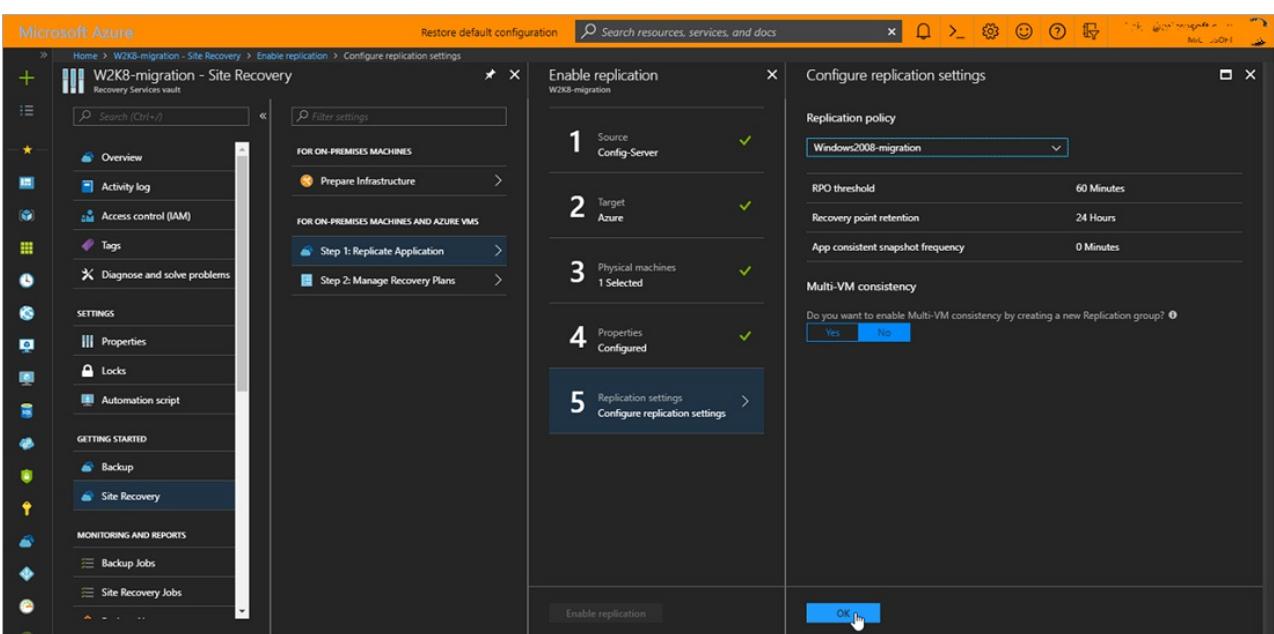
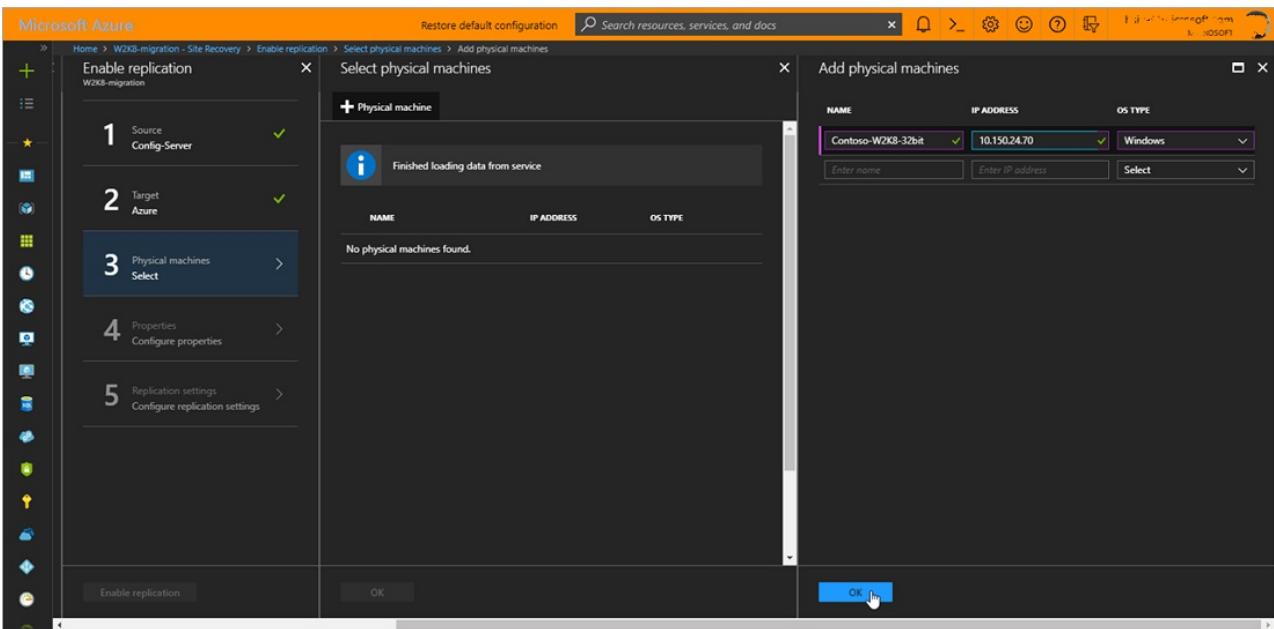
WARNING

Ensure that you specify **OFF** in the App-consistent snapshot frequency setting of the replication policy. Only crash-consistent recovery points are supported while replicating servers running Windows Server 2008. Specifying any other value for the App-consistent snapshot frequency will result in false alerts by turning replication health of the server critical due to lack of App-consistent recovery points.



Enable replication

Enable replication for the Windows Server 2008 SP2 / Windows Server 2008 R2 SP1 server to be migrated.



Run a test migration

You can perform a test failover of replicating servers after initial replication completes and the server status turns to **Protected**.

Run a [test failover](#) to Azure, to make sure everything's working as expected.

The screenshot shows the Microsoft Azure Site Recovery service vault interface. On the left, there's a navigation pane with options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Properties, Locks, Automation script, Backup, Site Recovery, Backup Jobs, Site Recovery Jobs, Backup Alerts, and Site Recovery Events. The main area displays a table with columns: NAME, REPLICATION HEALTH, STATUS, ACTIVE LOCATION, and RPO. A single row is shown for 'Contoso-W2K8-32bit' with 'Healthy' replication health, 'Protected' status, 'Config-Server' active location, and 'RPO' set to 'Test Failover'. A context menu is open over the 'RPO' cell, listing options: Pin to dashboard, Failover, Test Failover (which is highlighted with a red box), Cleanup test failover, Change recovery point, Commit, Complete Migration, Re-protect, Resynchronize, Error Details, and Disable Replication.

Migrate to Azure

Run a failover for the machines you want to migrate.

1. In **Settings > Replicated items** click the machine > **Failover**.
2. In **Failover** select a **Recovery Point** to fail over to. Select the latest recovery point.
3. Select **Shutdown machine before beginning failover**. Site Recovery will attempt to shut down the server before triggering the failover. Failover continues even if shutdown fails. You can follow the failover progress on the **Jobs** page.
4. Check that the Azure VM appears in Azure as expected.
5. In **Replicated items**, right-click the server > **Complete Migration**. This does the following:
 - Finishes the migration process, stops replication for the server, and stops Site Recovery billing for the server.
 - This step cleans up the replication data. It doesn't delete the migrated VMs.

This screenshot is similar to the one above but shows a different state. The replicated item 'Contoso-W2K8-32bit' now has 'Failover completed' in the 'STATUS' column and 'Microsoft Azure' in the 'ACTIVE LOCATION' column. The context menu for the 'RPO' cell still includes 'Test Failover' and 'Complete Migration', with 'Complete Migration' highlighted by a red box.

WARNING

Don't cancel a failover in progress: Server replication is stopped before failover starts. If you cancel a failover in progress, failover stops, but the server won't continue to replicate.

Migrate Amazon Web Services (AWS) VMs to Azure

10/22/2019 • 10 minutes to read • [Edit Online](#)

This tutorial teaches you how to migrate Amazon Web Services (AWS) virtual machines (VMs) to Azure VMs by using Azure Site Recovery. When you migrate AWS EC2 instances to Azure, the VMs are treated like physical, on-premises computers. In this tutorial, you learn how to:

- Verify prerequisites
- Prepare Azure resources
- Prepare AWS EC2 instances for migration
- Deploy a configuration server
- Enable replication for VMs
- Test the failover to make sure everything's working
- Run a onetime failover to Azure

If you don't have an Azure subscription, create a [free account](#) before you begin.

NOTE

You can now use the Azure Migrate service to migrate AWS instances to Azure. [Learn more.](#)

Prerequisites

- Ensure that the VMs that you want to migrate are running a supported OS version. Supported versions include:
 - Windows Server 2016
 - Windows Server 2012 R2
 - Windows Server 2012
 - 64-bit version of Windows Server 2008 R2 SP1 or later
 - Red Hat Enterprise Linux 6.4 to 6.10, 7.1 to 7.6 (HVM virtualized instances only) (*Instances running RedHat PV drivers aren't supported.*)
 - CentOS 6.4 to 6.10, 7.1 to 7.6 (HVM virtualized instances only)
- The Mobility service must be installed on each VM that you want to replicate.

IMPORTANT

Site Recovery installs this service automatically when you enable replication for the VM. For automatic installation, you must prepare an account on the EC2 instances that Site Recovery will use to access the VM. You can use a domain or local account.

- For Linux VMs, the account should be root on the source Linux server.
- For Windows VMs, if you're not using a domain account, disable Remote User Access control on the local machine:

In the registry, under

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System, add the DWORD entry **LocalAccountTokenFilterPolicy** and set the value to **1**.

- A separate EC2 instance that you can use as the Site Recovery configuration server. This instance must be running Windows Server 2012 R2.

Prepare Azure resources

You must have a few resources ready in Azure for the migrated EC2 instances to use. These include a storage account, a vault, and a virtual network.

Create a storage account

Images of replicated machines are held in Azure Storage. Azure VMs are created from storage when you fail over from on-premises to Azure.

1. In the [Azure portal](#), in the left menu, select **Create a resource > Storage > Storage account**.
2. Enter a name for your storage account. In these tutorials, we use the name **awsmigrated2017**. The name must:
 - Be unique in Azure
 - Be between 3 and 24 characters
 - Contain only numbers and lowercase letters
3. Leave the defaults for **Deployment model**, **Account kind**, **Performance**, and **Secure transfer required**.
4. For **Replication**, select the default **RA-GRS**.
5. Select the subscription that you want to use for this tutorial.
6. For **Resource group**, select **Create new**. In this example, we use **migrationRG** for the resource group name.
7. For **Location**, select **West Europe**.
8. Select **Create** to create the storage account.

Create a vault

1. In the [Azure portal](#), select **All services**. Search for and then select **Recovery Services vaults**.
2. On the Azure Recovery Services vaults page, select **Add**.
3. For **Name**, enter **myVault**.
4. For **Subscription**, select the subscription that you want to use.
5. For **Resource Group**, select **Use existing**, and then select **migrationRG**.
6. For **Location**, select **West Europe**.
7. Select **Pin to dashboard** to be able to quickly access the new vault from the dashboard.
8. When you're done, select **Create**.

To see the new vault, go to **Dashboard > All resources**. The new vault also appears on the main **Recovery Services vaults** page.

Set up an Azure network

When Azure VMs are created after the migration (failover), they're joined to this Azure network.

1. In the [Azure portal](#), select **Create a resource > Networking > Virtual network**.
2. For **Name**, enter **myMigrationNetwork**.
3. Leave the default value for **Address space** (must enter value).
4. For **Subscription**, select the subscription that you want to use.
5. For **Resource group**, select **Use existing**, and then select **migrationRG**.
6. For **Location**, select **West Europe**.
7. Under **Subnet**, leave the default values for **Name** and **IP range (must enter value)**.
8. Add instructions for DDoS protection settings.
9. Leave the **Service Endpoints** option disabled.
10. Add instructions for Firewall settings.
11. When you're done, select **Create**.

Prepare the infrastructure

On your vault page in the Azure portal, in the **Getting Started** section, select **Site Recovery**, and then select **Prepare Infrastructure**. Complete the following steps.

1: Protection goal

On the **Protection Goal** page, select the following values:

Where are your machines located?	Select On-premises .
Where do you want to replicate your machines?	Select To Azure .
Are you performing a migration?	Select Yes , and then check the box next to I understand, but I would like to continue with Azure Site Recovery .
Are your machines virtualized?	Select Not virtualized / Other .

When you're done, select **OK** to move to the next section.

2: Select deployment planning

In **Have you completed deployment planning**, select **I will do it later**, and then select **OK**.

3: Prepare source

On the **Prepare source** page, select **+ Configuration Server**.

1. Use an EC2 instance that's running Windows Server 2012 R2 to create a configuration server and register it with your recovery vault.
2. Configure the proxy on the EC2 instance VM you're using as the configuration server so that it can access the [service URLs](#).
3. Download [Microsoft Azure Site Recovery Unified Setup](#). You can download it to your local machine and then copy it to the VM you're using as the configuration server.
4. Select the **Download** button to download the vault registration key. Copy the downloaded file to the VM you're using as the configuration server.
5. On the VM, right-click the installer you downloaded for Microsoft Azure Site Recovery Unified Setup, and then select **Run as administrator**.
 - a. Under **Before You Begin**, select **Install the configuration server and process server**, and then select **Next**.
 - b. In **Third-Party Software License**, select **I accept the third-party license agreement**, and then select **Next**.
 - c. In **Registration**, select **Browse**, and then go to where you put the vault registration key file. Select **Next**.
 - d. In **Internet Settings**, select **Connect to Azure Site Recovery without a proxy server**, and then select **Next**.
 - e. The **Prerequisites Check** page runs checks for several items. When it's finished, select **Next**.
 - f. In **MySQL Configuration**, provide the required passwords, and then select **Next**.
 - g. In **Environment Details**, select **No**. You don't need to protect VMware machines. Then, select **Next**.
 - h. In **Install Location**, select **Next** to accept the default.
 - i. In **Network Selection**, select **Next** to accept the default.
 - j. In **Summary**, select **Install**.

- k. **Installation Progress** shows you information about the installation process. When it's finished, select **Finish**. A window displays a message about a reboot. Select **OK**. Next, a window displays a message about the configuration server connection passphrase. Copy the passphrase to your clipboard and save it somewhere safe.
6. On the VM, run `cspconfigtool.exe` to create one or more management accounts on the configuration server. Make sure that the management accounts have administrator permissions on the EC2 instances that you want to migrate.

When you're done setting up the configuration server, go back to the portal and select the server that you created for **Configuration Server**. Select **OK** to go to 3: Prepare target.

4: Prepare target

In this section, you enter information about the resources that you created in [Prepare Azure resources](#) earlier in this tutorial.

1. In **Subscription**, select the Azure subscription that you used for the [Prepare Azure](#) tutorial.
2. Select **Resource Manager** as the deployment model.
3. Site Recovery verifies that you have one or more compatible Azure storage account and network. These should be the resources that you created in [Prepare Azure resources](#) earlier in this tutorial.
4. When you're done, select **OK**.

5: Prepare replication settings

Before you can enable replication, you must create a replication policy.

1. Select **Create and Associate**.
2. In **Name**, enter **myReplicationPolicy**.
3. Leave the rest of the default settings, and then select **OK** to create the policy. The new policy is automatically associated with the configuration server.

When you're finished with all five sections under **Prepare Infrastructure**, select **OK**.

Enable replication

Enable replication for each VM that you want to migrate. When replication is enabled, Site Recovery automatically installs the Mobility service.

1. Go to the [Azure portal](#).
2. On the page for your vault, under **Getting Started**, select **Site Recovery**.
3. Under **For on-premises machines and Azure VMs**, select **Step 1: Replicate application**. Complete the wizard pages with the following information. Select **OK** on each page when you're done:
 - 1: Configure source

Source:	Select On Premises .
Source location:	Enter the name of your configuration server EC2 instance.
Machine type:	Select Physical machines .
Process server:	Select the configuration server from the drop-down list.

- 2: Configure target

Target:	Leave the default.
Subscription:	Select the subscription that you have been using.
Post-failover resource group:	Use the resource group you created in Prepare Azure resources .
Post-failover deployment model:	Select Resource Manager .
Storage account:	Select the storage account that you created in Prepare Azure resources .
Azure network:	Select Configure now for selected machines .
Post-failover Azure network:	Choose the network you created in Prepare Azure resources .
Subnet:	Select the default in the drop-down list.

- 3: Select physical machines

Select **Physical machine**, and then enter the values for **Name**, **IP Address**, and **OS Type** of the EC2 instance that you want to migrate. Select **OK**.

- 4: Configure properties

Select the account that you created on the configuration server, and then select **OK**.

- 5: Configure replication settings

Make sure that the replication policy selected in the drop-down list is **myReplicationPolicy**, and then select **OK**.

4. When the wizard is finished, select **Enable replication**.

To track the progress of the **Enable Protection** job, go to **Monitoring and reports > Jobs > Site Recovery Jobs**. After the **Finalize Protection** job runs, the machine is ready for failover.

When you enable replication for a VM, changes can take 15 minutes or longer to take effect and appear in the portal.

Run a test failover

When you run a test failover, the following events occur:

- A prerequisites check runs to make sure that all the conditions required for failover are in place.
- Failover processes the data so that an Azure VM can be created. If you select the latest recovery point, a recovery point is created from the data.
- An Azure VM is created by using the data processed in the preceding step.

In the portal, run the test failover:

1. On the page for your vault, go to **Protected items > Replicated Items**. Select the VM, and then select **Test Failover**.

2. Select a recovery point to use for the failover:

- **Latest processed:** Fails over the VM to the latest recovery point that was processed by Site Recovery. The time stamp is shown. With this option, no time is spent processing data, so it provides a low recovery time objective (RTO).
- **Latest app-consistent:** This option fails over all VMs to the latest app-consistent recovery point. The time stamp is shown.
- **Custom:** Select any recovery point.

3. In **Test Failover**, select the target Azure network to which Azure VMs will be connected after failover occurs.

This should be the network you created in [Prepare Azure resources](#).

4. Select **OK** to begin the failover. To track progress, select the VM to view its properties. Or you can select the **Test Failover** job on the page for your vault. To do this, select **Monitoring and reports > Jobs > Site Recovery jobs**.

5. When the failover finishes, the replica Azure VM appears in the Azure portal. To view the VM, select **Virtual Machines**. Ensure that the VM is the appropriate size, that it's connected to the right network, and that it's running.

6. You should now be able to connect to the replicated VM in Azure.

7. To delete Azure VMs that were created during the test failover, select **Cleanup test failover** in the recovery plan. In **Notes**, record and save any observations associated with the test failover.

In some scenarios, failover requires additional processing. Processing takes 8 to 10 minutes to finish.

Migrate to Azure

Run an actual failover for the EC2 instances to migrate them to Azure VMs:

1. In **Protected items > Replicated items**, select the AWS instances, and then select **Failover**.
2. In **Failover**, select a **Recovery Point** to failover to. Select the latest recovery point, and start the failover. You can follow the failover progress on the **Jobs** page.
3. Ensure that the VM appears in **Replicated items**.
4. Right-click each VM, and then select **Complete Migration**. This does the following:
 - This finishes the migration process, stops replication for the AWS VM, and stops Site Recovery billing for the VM.
 - This step cleans up the replication data. It doesn't delete the migrated VMs.

NAME	HEALTH	STATUS	ACTIVE LOCATION	REPLICATION POLICY
AWSServer2012	OK	Unplanned failover comp...	Microsoft Azure	AWSReplicationPolicy
AWSWordpressRedHat	OK	Protected	AWSGATEWAY	AWSReplicationPolicy
FabrikamMarketing	OK	Unplanned failover comp...	Microsoft Azure	ContosoReplicationPolicy
FabrikamFinance	OK	Protected	CONTOSOGATEWAY	ContosoReplicationPolicy
▶ ContosoReplicationGr...	-	-	-	-

WARNING

Don't cancel a failover that is in progress. Before failover is started, VM replication is stopped. If you cancel a failover that is in progress, failover stops, but the VM won't replicate again.

Next steps

In this article, you learned how to migrate AWS EC2 instances to Azure VMs. To learn more about Azure VMs, continue to the tutorials for Windows VMs.

[Azure Windows virtual machine tutorials](#)

General questions about Azure Site Recovery

1/24/2020 • 10 minutes to read • [Edit Online](#)

This article summarizes frequently asked questions about Azure Site Recovery. For specific scenarios review these articles

- [Questions about Azure VM disaster recovery to Azure](#)
- [Questions about VMware VM disaster recovery to Azure](#)
- [Questions about Hyper-V VM disaster recovery to Azure](#)

General

What does Site Recovery do?

Site Recovery contributes to your business continuity and disaster recovery (BCDR) strategy, by orchestrating and automating replication of Azure VMs between regions, on-premises virtual machines and physical servers to Azure, and on-premises machines to a secondary datacenter. [Learn more.](#)

Can I protect a virtual machine that has a Docker disk?

No, this is an unsupported scenario.

Service providers

I'm a service provider. Does Site Recovery work for dedicated and shared infrastructure models?

Yes, Site Recovery supports both dedicated and shared infrastructure models.

For a service provider, is the identity of my tenant shared with the Site Recovery service?

No. Tenant identity remains anonymous. Your tenants don't need access to the Site Recovery portal. Only the service provider administrator interacts with the portal.

Will tenant application data ever go to Azure?

When replicating between service provider-owned sites, application data never goes to Azure. Data is encrypted in-transit, and replicated directly between the service provider sites.

If you're replicating to Azure, application data is sent to Azure storage but not to the Site Recovery service. Data is encrypted in-transit, and remains encrypted in Azure.

Will my tenants receive a bill for any Azure services?

No. Azure's billing relationship is directly with the service provider. Service providers are responsible for generating specific bills for their tenants.

If I'm replicating to Azure, do we need to run virtual machines in Azure at all times?

No. Data is replicated to Azure storage in your subscription. When you perform a test failover (DR drill) or an actual failover, Site Recovery automatically creates virtual machines in your subscription.

Do you ensure tenant-level isolation when I replicate to Azure?

Yes.

What platforms do you currently support?

We support Azure Pack, Cloud Platform System, and System Center based (2012 and higher) deployments. [Learn more](#) about Azure Pack and Site Recovery integration.

Do you support single Azure Pack and single VMM server deployments?

Yes, you can replicate Hyper-V virtual machines to Azure, or between service provider sites. Note that if you replicate between service provider sites, Azure runbook integration isn't available.

Pricing

Where can I find pricing information?

Review [Site Recovery pricing](#) details.

How can I calculate approximate charges during the use of Site Recovery?

You can use the [pricing calculator](#) to estimate costs while using Site Recovery.

For detailed estimate on costs, run the deployment planner tool for [VMware](#) or [Hyper-V](#), and use the [cost estimation report](#).

Managed disks are now used to replicate VMware VMs and physical servers. Do I incur additional charges for the cache storage account with managed disks?

No, there are no additional charges for cache. When you replicate to standard storage account, this cache storage is part of the same target storage account.

I have been an Azure Site Recovery user for over a month. Do I still get the first 31 days free for every protected instance?

Yes. Every protected instance incurs no Azure Site Recovery charges for the first 31 days. For example, if you have been protecting 10 instances for the last 6 months and you connect an 11th instance to Azure Site Recovery, there are no charges for the 11th instance for the first 31 days. The first 10 instances continue to incur Azure Site Recovery charges since they've been protected for more than 31 days.

During the first 31 days, will I incur any other Azure charges?

Yes, even though Site Recovery is free during the first 31 days of a protected instance, you might incur charges for Azure Storage, storage transactions, and data transfer. A recovered virtual machine might also incur Azure compute charges.

Is there a cost associated to perform disaster recovery drills/test failover?

There is no separate cost for DR drill. There will be compute charges after the VM is created after the test failover.

Security

Is replication data sent to the Site Recovery service?

No, Site Recovery doesn't intercept replicated data, and doesn't have any information about what's running on your virtual machines or physical servers. Replication data is exchanged between on-premises Hyper-V hosts, VMware hypervisors, or physical servers and Azure storage or your secondary site. Site Recovery has no ability to intercept that data. Only the metadata needed to orchestrate replication and failover is sent to the Site Recovery service.

Site Recovery is ISO 27001:2013, 27018, HIPAA, DPA certified, and is in the process of SOC2 and FedRAMP JAB assessments.

For compliance reasons, even our on-premises metadata must remain within the same geographic region. Can Site Recovery help us?

Yes. When you create a Site Recovery vault in a region, we ensure that all metadata that we need to enable and orchestrate replication and failover remains within that region's geographic boundary.

Does Site Recovery encrypt replication?

For virtual machines and physical servers, replicating between on-premises sites encryption-in-transit is supported. For virtual machines and physical servers replicating to Azure, both encryption-in-transit and [encryption-at-rest \(in Azure\)](#) are supported.

How can I enforce TLS 1.2 on all on-premises Azure Site Recovery components?

Mobility agents installed on the replicated items communicate to Process Server only on TLS 1.2. However, communication from Configuration Server to Azure and from Process Server to Azure could be on TLS 1.1 or 1.0. Please follow the [guidance](#) to enforce TLS 1.2 on all Configuration Servers and Process Servers set up by you.

Disaster recovery

What can Site Recovery protect?

- **Azure VMs:** Site Recovery can replicate any workload running on a supported Azure VM
- **Hyper-V virtual machines:** Site Recovery can protect any workload running on a Hyper-V VM.
- **Physical servers:** Site Recovery can protect physical servers running Windows or Linux.
- **VMware virtual machines:** Site Recovery can protect any workload running in a VMware VM.

What workloads can I protect with Site Recovery?

You can use Site Recovery to protect most workloads running on a supported VM or physical server. Site Recovery provides support for application-aware replication, so that apps can be recovered to an intelligent state. It integrates with Microsoft applications such as SharePoint, Exchange, Dynamics, SQL Server and Active Directory, and works closely with leading vendors, including Oracle, SAP, IBM and Red Hat. [Learn more](#) about workload protection.

Can I manage disaster recovery for my branch offices with Site Recovery?

Yes. When you use Site Recovery to orchestrate replication and failover in your branch offices, you'll get a unified orchestration and view of all your branch office workloads in a central location. You can easily run failovers and administer disaster recovery of all branches from your head office, without visiting the branches.

Is disaster recovery supported for Azure VMs?

Yes, Site Recovery supports disaster for Azure VMs between Azure regions. [Review common questions](#) about Azure VM disaster recovery.

Is disaster recovery supported for VMware VMs?

Yes, Site Recovery supports disaster recovery of on-premises VMware VMs. [Review common questions](#) for disaster recovery of VMware VMs.

Is disaster recovery supported for Hyper-V VMs?

Yes, Site Recovery supports disaster recovery of on-premises Hyper-V VMs. [Review common questions](#) for disaster recovery of Hyper-V VMs.

Is disaster recovery supported for physical servers?

Yes, Site Recovery supports disaster recovery of on-premises physical servers running Windows and Linux to Azure or to a secondary site. Learn about requirements for disaster recovery to [Azure](#), and to [a secondary site](#). Note that physical servers will run as VMs in Azure after failover. Failback from Azure to an on-premises physical server isn't currently supported. You can only fail back to a VMware virtual machine.

Replication

Can I replicate over a site-to-site VPN to Azure?

Azure Site Recovery replicates data to an Azure storage account or managed disks, over a public endpoint. Replication isn't over a site-to-site VPN.

Why can't I replicate over VPN?

When you replicate to Azure, replication traffic reaches the public endpoints of an Azure Storage. Thus you can only replicate over the public internet or via ExpressRoute (Microsoft peering or an existing public peering).

Can I use Riverbed SteelHeads for replication?

Our partner, Riverbed, provides detailed guidance on working with Azure Site Recovery. Review their [solution guide](#).

Can I use ExpressRoute to replicate virtual machines to Azure?

Yes, [ExpressRoute can be used](#) to replicate on-premises virtual machines to Azure.

- Azure Site Recovery replicates data to an Azure Storage over a public endpoint. You need to set up [Microsoft peering](#) or use an existing [public peering](#) (deprecated for new circuits) to use ExpressRoute for Site Recovery replication.
- Microsoft peering is the recommended routing domain for replication.
- Replication is not supported over private peering.
- If you're protecting VMware machines or physical machines, ensure that the [Networking Requirements](#) for Configuration Server are also met. Connectivity to specific URLs is required by Configuration Server for orchestration of Site Recovery replication. ExpressRoute cannot be used for this connectivity.
- After the virtual machines have been failed over to an Azure virtual network you can access them using the [private peering](#) setup with the Azure virtual network.

If I replicate to Azure, what kind of storage account or managed disk do I need?

You need an LRS or GRS storage. We recommend GRS so that data is resilient if a regional outage occurs, or if the primary region can't be recovered. The account must be in the same region as the Recovery Services vault.

Premium storage is supported for VMware VM, Hyper-V VM, and physical server replication, when you deploy Site Recovery in the Azure portal. Managed disks only support LRS.

How often can I replicate data?

- **Hyper-V:** Hyper-V VMs can be replicated every 30 seconds (except for premium storage), five minutes or 15 minutes.
- **Azure VMs, VMware VMs, physical servers:** A replication frequency isn't relevant here. Replication is continuous.

Can I extend replication from existing recovery site to another tertiary site?

Extended or chained replication isn't supported. Request this feature in [feedback forum](#).

Can I do an offline replication the first time I replicate to Azure?

This isn't supported. Request this feature in the [feedback forum](#).

Can I exclude specific disks from replication?

This is supported when you're replicating VMware VMs and Hyper-V VMs to Azure, using the Azure portal.

Can I replicate virtual machines with dynamic disks?

Dynamic disks are supported when replicating Hyper-V virtual machines, and when replicating VMware VMs and physical machines to Azure. The operating system disk must be a basic disk.

Can I throttle bandwidth allotted for replication traffic?

Yes. You can read more about throttling bandwidth in these articles:

- [Capacity planning for replicating VMware VMs and physical servers](#)
- [Capacity planning for replicating Hyper-V VMs to Azure](#)

Failover

If I'm failing over to Azure, how do I access the Azure VMs after failover?

You can access the Azure VMs over a secure Internet connection, over a site-to-site VPN, or over Azure ExpressRoute. You need to prepare a number of things in order to connect. [Learn more](#).

If I fail over to Azure how does Azure make sure my data is resilient?

Azure is designed for resilience. Site Recovery is already engineered for failover to a secondary Azure datacenter, in accordance with the Azure SLA. If this happens, we make sure your metadata and vaults remain within the same geographic region that you chose for your vault.

If I'm replicating between two datacenters what happens if my primary datacenter experiences an unexpected outage?

You can trigger an unplanned failover from the secondary site. Site Recovery doesn't need connectivity from the primary site to perform the failover.

Is failover automatic?

Failover isn't automatic. You initiate failovers with single click in the portal, or you can use [Site Recovery PowerShell](#) to trigger a failover. Failing back is a simple action in the Site Recovery portal.

To automate you could use on-premises Orchestrator or Operations Manager to detect a virtual machine failure, and then trigger the failover using the SDK.

- [Read more](#) about recovery plans.
- [Read more](#) about failover.
- [Read more](#) about failing back VMware VMs and physical servers

If my on-premises host is not responding or crashed, can I fail back to a different host?

Yes, you can use the alternate location recovery to failback to a different host from Azure.

- [For VMware virtual machines](#)
- [For Hyper-V virtual machines](#)

Automation

Can I automate Site Recovery scenarios with an SDK?

Yes. You can automate Site Recovery workflows using the Rest API, PowerShell, or the Azure SDK. Currently supported scenarios for deploying Site Recovery using PowerShell:

- [Replicate Hyper-V VMs in VMMs clouds to Azure PowerShell Resource Manager](#)
- [Replicate Hyper-V VMs without VMM to Azure PowerShell Resource Manager](#)
- [Replicate VMware to Azure with PowerShell Resource Manager](#)

Component/provider upgrade

Where can I find the release notes/update rollups of Site Recovery upgrades

[Learn](#) about new updates, and [get rollup information](#).

Next steps

- Read the [Site Recovery overview](#)

Azure to Azure disaster recovery architecture

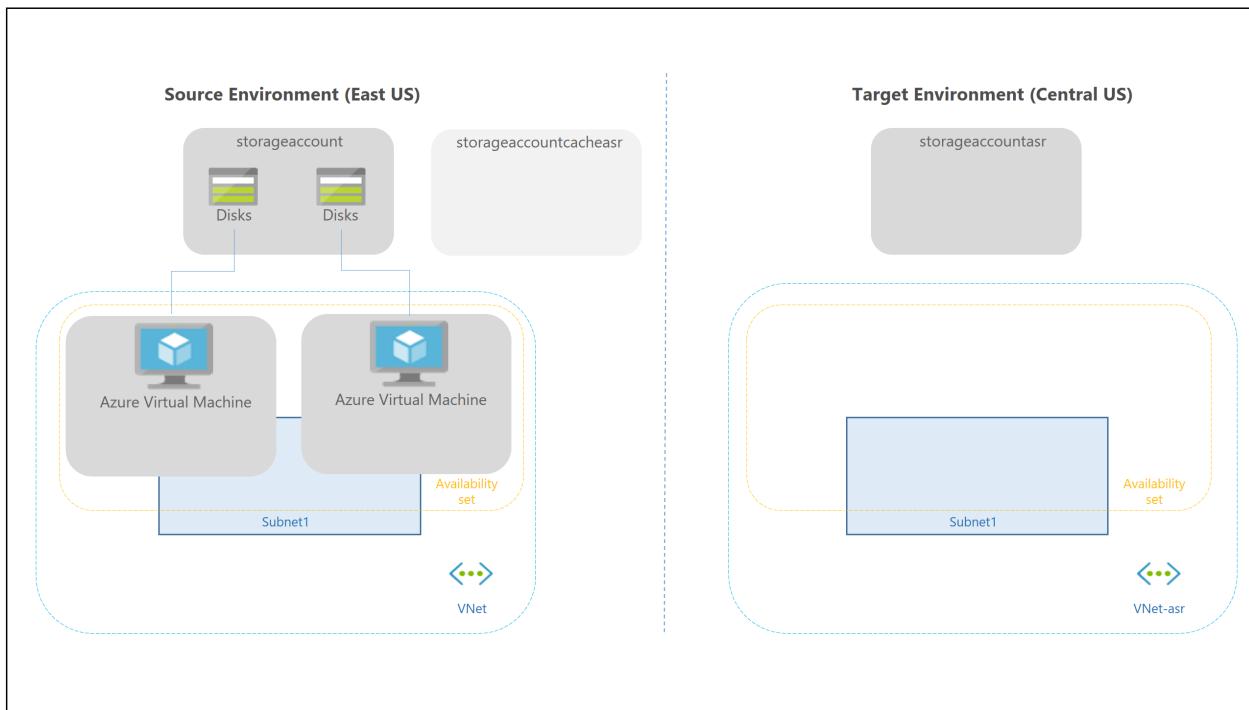
1/24/2020 • 8 minutes to read • [Edit Online](#)

This article describes the architecture, components, and processes used when you deploy disaster recovery for Azure virtual machines (VMs) using the [Azure Site Recovery](#) service. With disaster recovery set up, Azure VMs continuously replicate from to a different target region. If an outage occurs, you can fail over VMs to the secondary region, and access them from there. When everything's running normally again, you can fail back and continue working in the primary location.

Architectural components

The components involved in disaster recovery for Azure VMs are summarized in the following table.

COMPONENT	REQUIREMENTS
VMs in source region	One or more Azure VMs in a supported source region . VMs can be running any supported operating system .
Source VM storage	Azure VMs can be managed, or have non-managed disks spread across storage accounts. Learn about supported Azure storage.
Source VM networks	VMs can be located in one or more subnets in a virtual network (VNet) in the source region. Learn more about networking requirements.
Cache storage account	You need a cache storage account in the source network. During replication, VM changes are stored in the cache before being sent to target storage. Cache storage accounts must be Standard. Using a cache ensures minimal impact on production applications that are running on a VM. Learn more about cache storage requirements.
Target resources	Target resources are used during replication, and when a failover occurs. Site Recovery can set up target resource by default, or you can create/customize them. In the target region, check that you're able to create VMs, and that your subscription has enough resources to support VM sizes that will be needed in the target region.



Target resources

When you enable replication for a VM, Site Recovery gives you the option of creating target resources automatically.

TARGET RESOURCE	DEFAULT SETTING
Target subscription	Same as the source subscription.
Target resource group	<p>The resource group to which VMs belong after failover.</p> <p>It can be in any Azure region except the source region.</p> <p>Site Recovery creates a new resource group in the target region, with an "asr" suffix.</p>
Target VNet	<p>The virtual network (VNet) in which replicated VMs are located after failover. A network mapping is created between source and target virtual networks, and vice versa.</p> <p>Site Recovery creates a new VNet and subnet, with the "asr" suffix.</p>
Target storage account	<p>If the VM doesn't use a managed disk, this is the storage account to which data is replicated.</p> <p>Site Recovery creates a new storage account in the target region, to mirror the source storage account.</p>
Replica managed disks	<p>If the VM uses a managed disk, this is the managed disks to which data is replicated.</p> <p>Site Recovery creates replica managed disks in the storage region to mirror the source.</p>

TARGET RESOURCE	DEFAULT SETTING
Target availability sets	Availability set in which replicating VMs are located after failover. Site Recovery creates an availability set in the target region with the suffix "asr", for VMs that are located in an availability set in the source location. If an availability set exists, it's used and a new one isn't created.
Target availability zones	If the target region supports availability zones, Site Recovery assigns the same zone number as that used in the source region.

Managing target resources

You can manage target resources as follows:

- You can modify target settings as you enable replication.
- You can modify target settings after replication is already working. The exception is the availability type (single instance, set or zone). To change this setting you need to disable replication, modify the setting, and then reenable.

Replication policy

When you enable Azure VM replication, by default Site Recovery creates a new replication policy with the default settings summarized in the table.

POLICY SETTING	DETAILS	DEFAULT
Recovery point retention	Specifies how long Site Recovery keeps recovery points	24 hours
App-consistent snapshot frequency	How often Site Recovery takes an app-consistent snapshot.	Every four hours

Managing replication policies

You can manage and modify the default replication policies settings as follows:

- You can modify the settings as you enable replication.
- You can create a replication policy at any time, and then apply it when you enable replication.

Multi-VM consistency

If you want VMs to replicate together, and have shared crash-consistent and app-consistent recovery points at failover, you can gather them together into a replication group. Multi-VM consistency impacts workload performance, and should only be used for VMs running workloads that need consistency across all machines.

Snapshots and recovery points

Recovery points are created from snapshots of VM disks taken at a specific point in time. When you fail over a VM, you use a recovery point to restore the VM in the target location.

When failing over, we generally want to ensure that the VM starts with no corruption or data loss, and that the VM data is consistent for the operating system, and for apps that run on the VM. This depends on the type of snapshots taken.

Site Recovery takes snapshots as follows:

1. Site Recovery takes crash-consistent snapshots of data by default, and app-consistent snapshots if you specify a frequency for them.
2. Recovery points are created from the snapshots, and stored in accordance with retention settings in the replication policy.

Consistency

The following table explains different types of consistency.

Crash-consistent

Description	Details	Recommendation
<p>A crash consistent snapshot captures data that was on the disk when the snapshot was taken. It doesn't include anything in memory.</p> <p>It contains the equivalent of the on-disk data that would be present if the VM crashed or the power cord was pulled from the server at the instant that the snapshot was taken.</p> <p>A crash-consistent doesn't guarantee data consistency for the operating system, or for apps on the VM.</p>	<p>Site Recovery creates crash-consistent recovery points every five minutes by default. This setting can't be modified.</p>	<p>Today, most apps can recover well from crash-consistent points.</p> <p>Crash-consistent recovery points are usually sufficient for the replication of operating systems, and apps such as DHCP servers and print servers.</p>

App-consistent

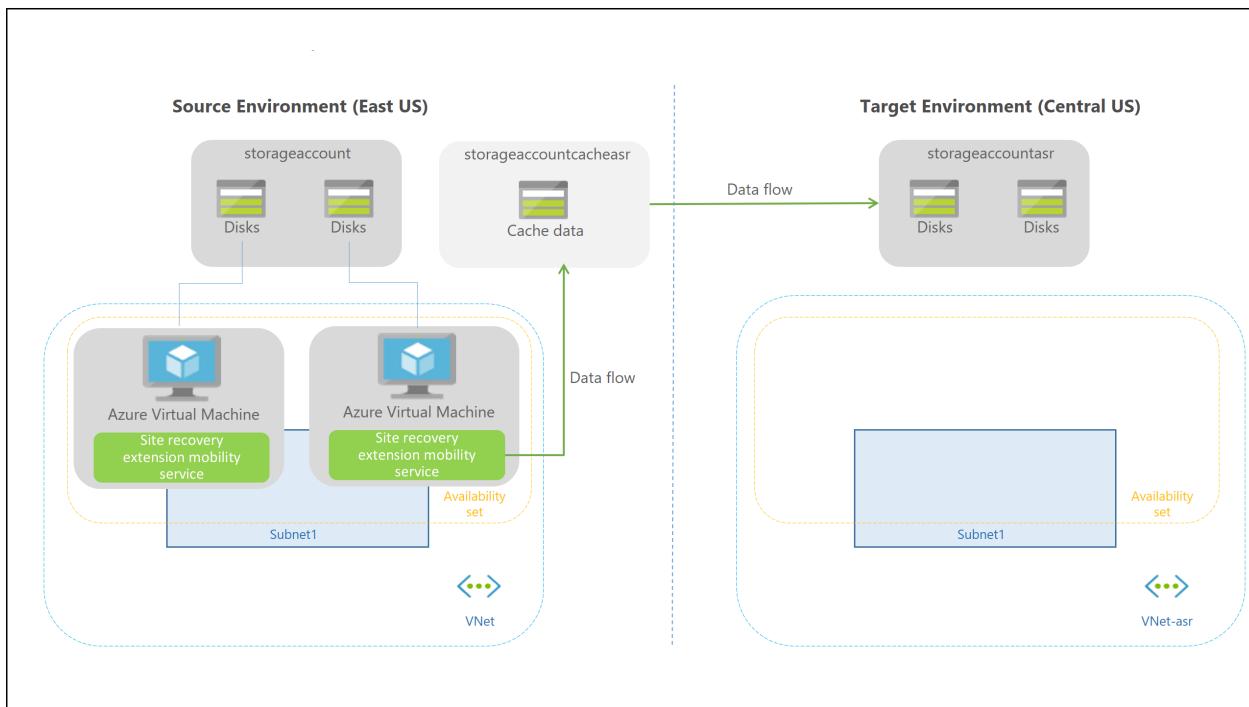
Description	Details	Recommendation
<p>App-consistent recovery points are created from app-consistent snapshots.</p> <p>An app-consistent snapshot contain all the information in a crash-consistent snapshot, plus all the data in memory and transactions in progress.</p>	<p>App-consistent snapshots use the Volume Shadow Copy Service (VSS):</p> <ol style="list-style-type: none"> 1) When a snapshot is initiated, VSS perform a copy-on-write (COW) operation on the volume. 2) Before it performs the COW, VSS informs every app on the machine that it needs to flush its memory-resident data to disk. 3) VSS then allows the backup/disaster recovery app (in this case Site Recovery) to read the snapshot data and proceed. 	<p>App-consistent snapshots are taken in accordance with the frequency you specify. This frequency should always be less than you set for retaining recovery points. For example, if you retain recovery points using the default setting of 24 hours, you should set the frequency at less than 24 hours.</p> <p>They're more complex and take longer to complete than crash-consistent snapshots.</p> <p>They affect the performance of apps running on a VM enabled for replication.</p>

Replication process

When you enable replication for an Azure VM, the following happens:

1. The Site Recovery Mobility service extension is automatically installed on the VM.
2. The extension registers the VM with Site Recovery.
3. Continuous replication begins for the VM. Disk writes are immediately transferred to the cache storage account in the source location.
4. Site Recovery processes the data in the cache, and sends it to the target storage account, or to the replica managed disks.
5. After the data is processed, crash-consistent recovery points are generated every five minutes. App-consistent

recovery points are generated according to the setting specified in the replication policy.



Replication process

Connectivity requirements

The Azure VMs you replicate need outbound connectivity. Site Recovery never needs inbound connectivity to the VM.

Outbound connectivity (URLs)

If outbound access for VMs is controlled with URLs, allow these URLs.

URL	DETAILS
*.blob.core.windows.net	Allows data to be written from the VM to the cache storage account in the source region.
login.microsoftonline.com	Provides authorization and authentication to Site Recovery service URLs.
*.hypervrecoverymanager.windowsazure.com	Allows the VM to communicate with the Site Recovery service.
*.servicebus.windows.net	Allows the VM to write Site Recovery monitoring and diagnostics data.

Outbound connectivity for IP address ranges

To control outbound connectivity for VMs using IP addresses, allow these addresses. Please note that details of network connectivity requirements can be found in [networking white paper](#)

Source region rules

RULE	DETAILS	SERVICE TAG
Allow HTTPS outbound: port 443	Allow ranges that correspond to storage accounts in the source region	Storage.<region-name>

RULE	DETAILS	SERVICE TAG
Allow HTTPS outbound: port 443	Allow ranges that correspond to Azure Active Directory (Azure AD)	AzureActiveDirectory
Allow HTTPS outbound: port 443	Allow ranges that correspond to Events Hub in the target region.	EventsHub.<region-name>
Allow HTTPS outbound: port 443	Allow ranges that correspond to Azure Site Recovery	AzureSiteRecovery

Target region rules

RULE	DETAILS	SERVICE TAG
Allow HTTPS outbound: port 443	Allow ranges that correspond to storage accounts in the target region	Storage.<region-name>
Allow HTTPS outbound: port 443	Allow ranges that correspond to Azure AD	AzureActiveDirectory
Allow HTTPS outbound: port 443	Allow ranges that correspond to Events Hub in the source region.	EventsHub.<region-name>
Allow HTTPS outbound: port 443	Allow ranges that correspond to Azure Site Recovery	AzureSiteRecovery

Control access with NSG rules

If you control VM connectivity by filtering network traffic to and from Azure networks/subnets using [NSG rules](#), note the following requirements:

- NSG rules for the source Azure region should allow outbound access for replication traffic.
- We recommend you create rules in a test environment before you put them into production.
- Use [service tags](#) instead of allowing individual IP addresses.
 - Service tags represent a group of IP address prefixes gathered together to minimize complexity when creating security rules.
 - Microsoft automatically updates service tags over time.

Learn more about [outbound connectivity](#) for Site Recovery, and [controlling connectivity with NSGs](#).

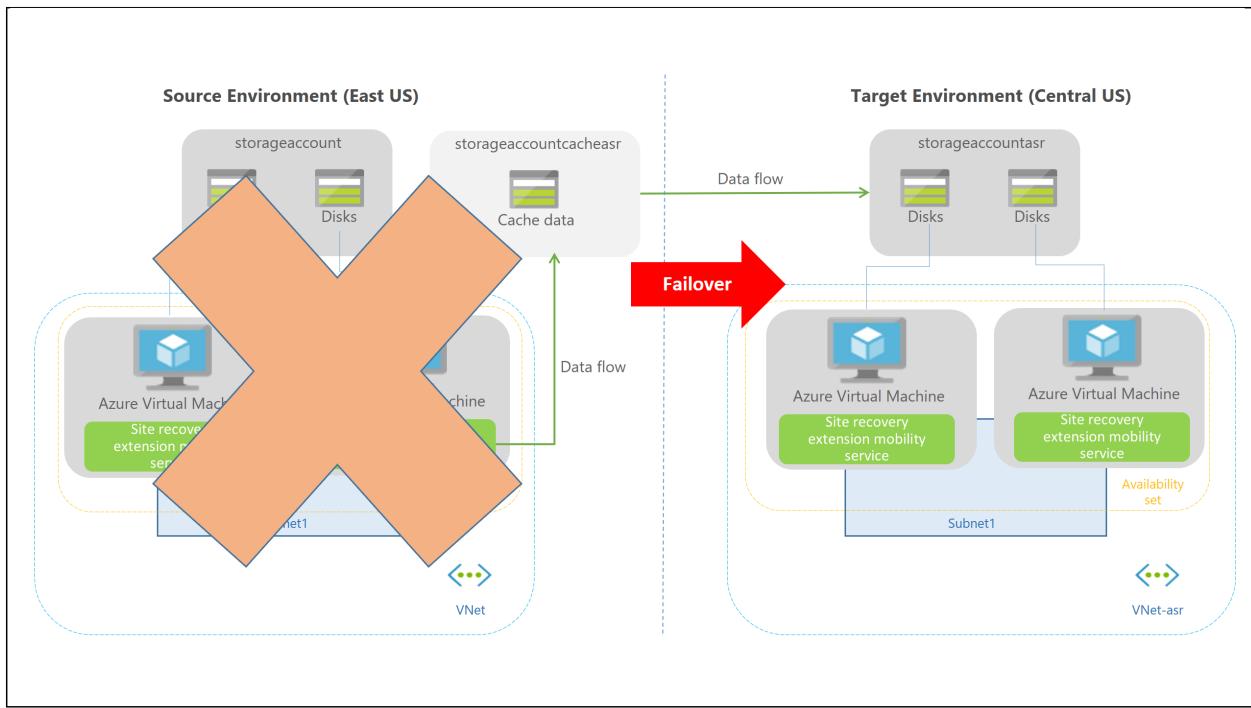
Connectivity for multi-VM consistency

If you enable multi-VM consistency, machines in the replication group communicate with each other over port 20004.

- Ensure that there is no firewall appliance blocking the internal communication between the VMs over port 20004.
- If you want Linux VMs to be part of a replication group, ensure the outbound traffic on port 20004 is manually opened as per the guidance of the specific Linux version.

Failover process

When you initiate a failover, the VMs are created in the target resource group, target virtual network, target subnet, and in the target availability set. During a failover, you can use any recovery point.



Next steps

[Quickly replicate](#) an Azure VM to a secondary region.

Common questions: Azure-to-Azure disaster recovery

2/12/2020 • 14 minutes to read • [Edit Online](#)

This article answers common questions about disaster recovery of Azure VMs to another Azure region for when you use [Azure Site Recovery](#).

General

How is Site Recovery priced?

Review [Azure Site Recovery pricing for VMs](#).

How does the free tier for Azure Site Recovery work?

Every instance that is protected with Azure Site Recovery is free for the first 31 days of protection. After that period, protection for each instance is at the rates in [Azure Site Recovery pricing for Azure Virtual Machines](#).

During the first 31 days, will I incur any other Azure charges?

Yes. Even though Azure Site Recovery is free during the first 31 days of a protected instance, you might incur charges for Azure Storage, storage transactions, and data transfers. A recovered Virtual Machine might also incur Azure compute charges. Get complete details on pricing at [Azure Site Recovery pricing](#).

What are the best practices for Azure Virtual Machines disaster recovery?

1. [Understand Azure-to-Azure architecture](#)
2. [Review the supported and not-supported configurations](#)
3. [Set up disaster recovery for Azure VMs](#)
4. [Run a test failover](#)
5. [Fail over and fail back to the primary region](#)

How is capacity ensured in the target region?

The Site Recovery team and Azure capacity management team plan for sufficient infrastructure capacity. When you start a failover, the teams also help ensure VM instances that are protected by Site Recovery will deploy to the target region.

Replication

Can I replicate VMs enabled through Azure disk encryption?

Yes. Site Recovery supports disaster recovery of VMs that have Azure Disk Encryption enabled. When you enable replication, Azure copies all the required disk encryption keys and secrets from the source region to the target region in the user context. If you don't have the appropriate permissions, your security administrator can use a script to copy the keys and secrets.

- Site Recovery supports Azure Disk Encryption for Azure VMs that are running Windows.
- Site Recovery supports Azure Disk Encryption version 0.1, which has a schema that requires Azure Active Directory (Azure AD). Site Recovery also supports version 1.1, which doesn't require Azure AD. [Learn more about the extension schemata for Azure disk encryption](#).
 - For Azure Disk Encryption version 1.1, you have to use the Windows VMs with managed disks.
 - [Learn more](#) about enabling replication for encrypted VMs.

Can I replicate VMs to another subscription?

Yes, you can replicate Azure VMs to a different subscription within the same Azure AD tenant.

Configure disaster recovery [across subscriptions](#) by selecting another subscription at the time of replication.

Can I replicate zone-pinned Azure VMs to another region?

Yes, you can [replicate zone-pinned VMs](#) to another region.

Can I exclude disks?

Yes, you can exclude disks at the time of protection by using PowerShell. For more information, see [how to exclude disks from replication](#).

Can I add new disks to replicated VMs and enable replication for them?

Yes, adding new disks to replicated VMs and enabling replication for them is supported for Azure VMs with managed disks. When you add a new disk to an Azure VM that's enabled for replication, replication health for the VM shows a warning. That warning states that one or more disks on the VM are available for protection. You can enable replication for added disks.

- If you enable protection for the added disks, the warning will disappear after the initial replication.
- If you don't enable replication for the disk, you can dismiss the warning.
- If you fail over a VM that has an added disk and replication enabled, there are replication points. The replication points will show the disks that are available for recovery.

For example, let's say a VM has a single disk and you add a new one. There might be a replication point that was created before you added the disk. This replication point will show that it consists of "1 of 2 disks."

Site Recovery doesn't support "hot remove" of a disk from a replicated VM. If you remove a VM disk, you need to disable and then re-enable replication for the VM.

How often can I replicate to Azure?

Replication is continuous when you're replicating Azure VMs to another Azure region. For more information, see the [Azure-to-Azure replication architecture](#).

Can I replicate virtual machines within a region? I need this functionality to migrate VMs.

You can't use an Azure-to-Azure disk recovery solution to replicate VMs within a region.

Can I replicate VM instances to any Azure region?

By using Site Recovery, you can replicate and recover VMs between any two regions within the same geographic cluster. Geographic clusters are defined with data latency and sovereignty in mind. For more information, see the Site Recovery [region support matrix](#).

Does Site Recovery require internet connectivity?

No, Site Recovery doesn't require internet connectivity. But it does require access to Site Recovery URLs and IP ranges, as mentioned in [networking in Azure VM disaster recovery](#).

Can I replicate an application that has a separate resource group for separate tiers?

Yes, you can replicate the application and keep the disaster recovery configuration in a separate resource group too.

For example, if your application has each tier's application, database, and web in a separate resource group, then you have to select the [replication wizard](#) three times to protect all the tiers. Site Recovery will replicate these three tiers into three different resource groups.

Replication policy

What is a replication policy?

A replication policy defines the settings for the retention history of recovery points. The policy also defines the frequency of app-consistent snapshots. By default, Azure Site Recovery creates a new replication policy with default settings of:

- 24 hours for the retention history of recovery points.
- 60 minutes for the frequency of app-consistent snapshots.

[Learn more about replication settings.](#)

What is a crash-consistent recovery point?

A crash-consistent recovery point has the on-disk data as if you pulled the power cord from the server during the snapshot. The crash-consistent recovery point doesn't include anything that was in memory when the snapshot was taken.

Today, most applications can recover well from crash-consistent snapshots. A crash-consistent recovery point is usually enough for no-database operating systems and applications like file servers, DHCP servers, and print servers.

What is the frequency of crash-consistent recovery point generation?

Site Recovery creates a crash-consistent recovery point every 5 minutes.

What is an application-consistent recovery point?

Application-consistent recovery points are created from application-consistent snapshots. Application-consistent recovery points capture the same data as crash-consistent snapshots while also capturing data in memory and all transactions in process.

Because of their extra content, application-consistent snapshots are the most involved and take the longest. We recommend application-consistent recovery points for database operating systems and applications such as SQL Server.

What is the impact of application-consistent recovery points on application performance?

Application-consistent recovery points capture all the data in memory and in process. Because recovery points capture that data, they require framework like Volume Shadow Copy Service on Windows to quiesce the application. If the capturing process is frequent, it can affect performance when the workload is already busy. We don't recommend that you use low frequency for app-consistent recovery points for non-database workloads. Even for database workload, 1 hour is enough.

What is the minimum frequency of application-consistent recovery point generation?

Site Recovery can create an application-consistent recovery point with a minimum frequency of 1 hour.

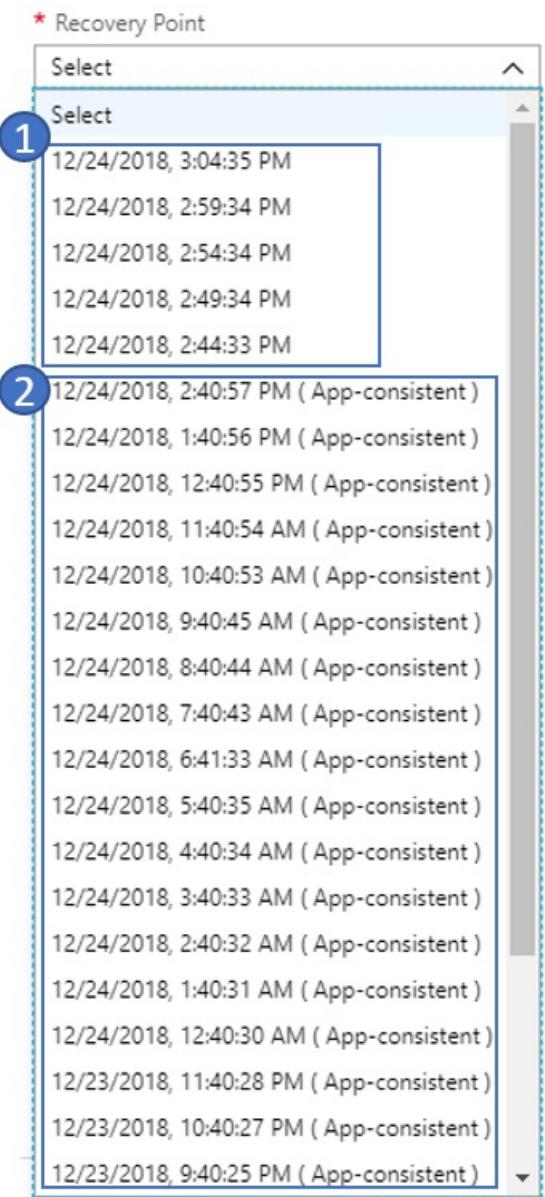
How are recovery points generated and saved?

To understand how Site Recovery generates recovery points, let's see an example of a replication policy. This replication policy has a recovery point with a 24-hour retention window and an app-consistent frequency snapshot of 1 hour.

Site Recovery creates a crash-consistent recovery point every 5 minutes. You can't change this frequency. For the last hour, you can choose from 12 crash-consistent points and 1 app-consistent point. As time progresses, Site Recovery prunes all the recovery points beyond the last hour and saves only 1 recovery point per hour.

The following screenshot illustrates the example. In the screenshot:

- Within the past hour, there are recovery points with a frequency of 5 minutes.
- Beyond the past hour, Site Recovery keeps only 1 recovery point.



How far back can I recover?

The oldest recovery point that you can use is 72 hours.

I have a replication policy of 24 hours. What will happen if a problem prevents Site Recovery from generating recovery points for more than 24 hours? Will my previous recovery points be lost?

No, Site Recovery will keep all your previous recovery points. Depending on the recovery points' retention window, Site Recovery replaces the oldest point only if it generates new points. Because of the problem, Site Recovery can't generate any new recovery points. Until there are new recovery points, all the old points will remain after you reach the window of retention.

After replication is enabled on a VM, how do I change the replication policy?

Go to **Site Recovery Vault > Site Recovery Infrastructure > Replication policies**. Select the policy that you want to edit, and save the changes. Any change will apply to all the existing replications too.

Are all the recovery points a complete copy of the VM or a differential?

The first recovery point that's generated has the complete copy. Any successive recovery points have delta changes.

Does increasing the retention period of recovery points increase the storage cost?

Yes, if you increase the retention period from 24 hours to 72 hours, Site Recovery will save the recovery points for an additional 48 hours. The added time will incur storage charges. For example, a single recovery point might have

delta changes of 10 GB with a per-GB cost of \$0.16 per month. Additional charges would be $\$1.60 \times 48$ per month.

Multi-VM consistency

What is multi-VM consistency?

Multi-VM consistency ensures that the recovery point is consistent across all the replicated virtual machines.

Site Recovery provides a **Multi-VM consistency** option, which creates a replication group of all the machines.

When you fail over the virtual machines, they'll have shared crash-consistent and app-consistent recovery points.

Go through the tutorial to [enable multi-VM consistency](#).

Can I fail over a single virtual machine within a multi-VM consistency replication group?

When you select the **Multi-VM consistency** option, you're stating that the application has a dependency on all the virtual machines within a group. Single virtual machine failover isn't allowed.

How many virtual machines can I replicate as a part of a multi-VM consistency replication group?

You can replicate 16 virtual machines together in a replication group.

When should I enable multi-VM consistency?

Because multi-VM consistency is CPU intensive, enabling it can affect workload performance. Use multi-VM consistency only if machines are running the same workload and you need consistency across multiple machines. For example, if you have two SQL Server instances and two web servers in an application, you should have multi-VM consistency for the SQL Server instances only.

Failover

How is capacity ensured in the target region for Azure VMs?

The Site Recovery team and Azure capacity management team plan for sufficient infrastructure capacity. When you start a failover, the teams also help ensure VM instances that are protected by Site Recovery will deploy to the target region.

Is failover automatic?

Failover isn't automatic. You can start failovers with a single click in the portal, or you can use [PowerShell](#) to trigger a failover.

Can I keep a public IP address after a failover?

You can't keep the public IP address of the production application after a failover.

When you bring up a workload as part of the failover process, you need to assign an Azure public IP resource to the workload. The Azure public IP resource has to be available in the target region. You can assign the Azure public IP resource manually, or you can automate it with a recovery plan. Learn how to [set up public IP addresses after failover](#).

Can I keep a private IP address during a failover?

Yes, you can keep a private IP address. By default, when you enable disaster recovery for Azure VMs, Site Recovery creates target resources based on source resource settings. For Azure Virtual Machines configured with static IP addresses, Site Recovery tries to provision the same IP address for the target VM if it's not in use. Learn about [keeping IP addresses during failover](#).

After a failover, why is the server assigned a new IP address?

Site Recovery tries to provide the IP address at the time of failover. If another virtual machine is taking that address, Site Recovery sets the next available IP address as the target.

Learn more about [setting up network mapping and IP addressing for virtual networks](#).

What are Latest (lowest RPO) recovery points?

The **Latest (lowest RPO)** option first processes all the data that has been sent to the Site Recovery. After the service processes the data, it creates a recovery point for each VM before failing over to the VM. This option provides the lowest recovery point objective (RPO). The VM created after failover has all the data replicated to Site Recovery from when the failover was triggered.

Do Latest (lowest RPO) recovery points have an impact on failover RTO?

Yes. Site Recovery processes all pending data before failing over, so this option has a higher recovery time objective (RTO) compared to other options.

What does the Latest processed option in recovery points mean?

The **Latest processed** option fails over all VMs in the plan to the latest recovery point that Site Recovery processed. To see the latest recovery point for a specific VM, check **Latest Recovery Points** in the VM settings. This option provides a low RTO, because no time is spent processing unprocessed data.

What happens if my primary region experiences an unexpected outage?

You can trigger a failover after the outage. Site Recovery doesn't need connectivity from the primary region to do the failover.

What is an RTO of a VM failover?

Site Recovery has an [RTO SLA of 2 hours](#). However, most of the time, Site Recovery fails over virtual machines within minutes. You can calculate the RTO by going to the failover jobs, which show the time it took to bring up the VM. For Recovery plan RTO, refer to the next section.

Recovery plans

What is a recovery plan?

A recovery plan in Site Recovery orchestrates the failover recovery of VMs. It helps make the recovery consistently accurate, repeatable, and automated. A recovery plan addresses the following needs:

- Defining a group of virtual machines that fail over together
- Defining the dependencies between virtual machines so that the application comes up accurately
- Automating the recovery along with custom manual actions to achieve tasks other than the failover of virtual machines

Learn more [about creating recovery plans](#).

How is sequencing achieved in a recovery plan?

In a recovery plan, you can create multiple groups to achieve sequencing. Every group fails over at one time. Virtual machines that are part of the same group fail over together, followed by another group. To learn how to model an application by using a recovery plan, see [About recovery plans](#).

How can I find the RTO of a recovery plan?

To check the RTO of a recovery plan, do a test failover for the recovery plan and go to **Site Recovery jobs**. In the following example, see the job **SAPTestRecoveryPlan**. The job took 8 minutes and 59 seconds to fail over all the virtual machines and do specified actions.

Site Recovery jobs

SAPSQLvaul

 Filter  Export jobs

 Filter items...

NAME	STATUS	TYPE	ITEM	START TIME	DURATION
Test failover cleanup	 Successful	Recovery plan	SAPTestRecoveryPlan	12/11/2018, 4:25:37 PM	00:05:57
Test failover	 Successful	Recovery plan	SAPTestRecoveryPlan	12/11/2018, 3:41:50 PM	00:08:16
Test failover cleanup	 Successful	Recovery plan	SAPTestRecoveryPlan	12/11/2018, 3:08:40 PM	00:05:03
Test failover	 Successful	Recovery plan	SAPTestRecoveryPlan	12/11/2018, 2:40:47 PM	00:08:59
Test failover cleanup	 Successful	Recovery plan	SAPTestRecoveryPlan	12/10/2018, 2:11:21 PM	00:02:50
Test failover	 Successful	Recovery plan	SAPTestRecoveryPlan	12/10/2018, 11:22:19 AM	00:08:41

Can I add automation runbooks to the recovery plan?

Yes, you can integrate Azure Automation runbooks into your recovery plan. Learn more about [adding Azure Automation runbooks](#).

Reprotection and fallback

I failed over from the primary region to a disaster recovery region. Are VMs in a DR region protected automatically?

No. When you [fail over](#) Azure VMs from one region to another, the VMs start up in the DR region in an unprotected state. To fail back the VMs to the primary region, you need to [reprotect](#) the VMs in the secondary region.

At the time of reprotection, does Site Recovery replicate complete data from the secondary region to the primary region?

It depends on the situation. If the source region VM exists, then only changes between the source disk and the target disk are synchronized. Site Recovery computes the differentials by comparing the disks, and then it transfers the data. This process usually takes a few hours. For more information about what happens during reprotection, see [Reprotect failed over Azure VM instances to the primary region](#).

How much time does it take to fail back?

After reprotection, fallback takes about the same amount of time it takes to fail over from the primary region to a secondary region.

Capacity

How is capacity ensured in the target region for Azure VMs?

The Site Recovery team and Azure capacity management team plan for sufficient infrastructure capacity. When you start a failover, the teams also help ensure VM instances that are protected by Site Recovery will deploy to the target region.

Does Site Recovery work with reserved instances?

Yes, you can purchase [reserved Azure VMs](#) in the disaster recovery region, and Site Recovery failover operations will use them. No additional configuration is needed.

Security

Is replication data sent to the Site Recovery service?

No, Site Recovery doesn't intercept replicated data, and it doesn't have any information about what's running on your VMs. Only the metadata needed to orchestrate replication and failover is sent to the Site Recovery service.

Site Recovery is ISO 27001:2013, 27018, HIPAA, and DPA certified. The service is undergoing SOC2 and FedRAMP JAB assessments.

Does Site Recovery encrypt replication?

Yes, both encryption in transit and [encryption at rest in Azure](#) are supported.

Next steps

- [Review Azure-to-Azure support requirements.](#)
- [Set up Azure-to-Azure replication.](#)
- If you have questions after reading this article, post them on the [Azure Recovery Services forum](#).

Support matrix for Azure VM disaster recovery between Azure regions

2/18/2020 • 15 minutes to read • [Edit Online](#)

This article summarizes support and prerequisites for disaster recovery of Azure VMs from one Azure region to another, using the [Azure Site Recovery](#) service.

Deployment method support

DEPLOYMENT	SUPPORT
Azure portal	Supported.
PowerShell	Supported. Learn more
REST API	Supported.
CLI	Not currently supported

Resource support

RESOURCE ACTION	DETAILS
Move vaults across resource groups	Not supported
Move compute/storage/network resources across resource groups	Not supported. If you move a VM or associated components such as storage/network after the VM is replicating, you need to disable and then re-enable replication for the VM.
Replicate Azure VMs from one subscription to another for disaster recovery	Supported within the same Azure Active Directory tenant.
Migrate VMs across regions within supported geographical clusters (within and across subscriptions)	Supported within the same Azure Active Directory tenant.
Migrate VMs within the same region	Not supported.

Region support

You can replicate and recover VMs between any two regions within the same geographic cluster. Geographic clusters are defined keeping data latency and sovereignty in mind.

GEOGRAPHIC CLUSTER	AZURE REGIONS

GEOGRAPHIC CLUSTER	AZURE REGIONS
America	Canada East, Canada Central, South Central US, West Central US, East US, East US 2, West US, West US 2, Central US, North Central US
Europe	UK West, UK South, North Europe, West Europe, France Central, France South, South Africa West, South Africa North, Norway East, Norway West
Asia	South India, Central India, West India, Southeast Asia, East Asia, Japan East, Japan West, Korea Central, Korea South, UAE Central, UAE North
Australia	Australia East, Australia Southeast, Australia Central, Australia Central 2
Azure Government	US GOV Virginia, US GOV Iowa, US GOV Arizona, US GOV Texas, US DOD East, US DOD Central
Germany	Germany Central, Germany Northeast
China	China East, China North, China North2, China East2
Restricted Regions reserved for in-country disaster recovery	Germany North reserved for Germany West Central, Switzerland West reserved for Switzerland North, France South reserved for France Central customers

NOTE

- For **Brazil South**, you can replicate and fail over to these regions: South Central US, West Central US, East US, East US 2, West US, West US 2, and North Central US.
- Brazil South can only be used as a source region from which VMs can replicate using Site Recovery. It can't act as a target region. This is because of latency issues due to geographical distances. Note that if you fail over from Brazil South as a source region to a target, fallback to Brazil South from the target region is supported.
- You can work within regions for which you have appropriate access.
- If the region in which you want to create a vault doesn't show, make sure your subscription has access to create resources in that region.
- If you can't see a region within a geographic cluster when you enable replication, make sure your subscription has permissions to create VMs in that region.

Cache storage

This table summarizes support for the cache storage account used by Site Recovery during replication.

SETTING	SUPPORT	DETAILS
General purpose V2 storage accounts (Hot and Cool tier)	Supported	Usage of GPv2 is not recommended because transaction costs for V2 are substantially higher than V1 storage accounts.
Premium storage	Not supported	Standard storage accounts are used for cache storage, to help optimize costs.

SETTING	SUPPORT	DETAILS
Azure Storage firewalls for virtual networks	Supported	If you are using firewall enabled cache storage account or target storage account, ensure you ' Allow trusted Microsoft services '. Also, ensure that you allow access to at least one subnet of source Vnet.

Replicated machine operating systems

Site Recovery supports replication of Azure VMs running the operating systems listed in this section.

Windows

OPERATING SYSTEM	DETAILS
Windows Server 2019	Supported for Server Core, Server with Desktop Experience.
Windows Server 2016	Supported Server Core, Server with Desktop Experience.
Windows Server 2012 R2	Supported.
Windows Server 2012	Supported.
Windows Server 2008 R2 with SP1/SP2	Supported. From version 9.30 of the Mobility service extension for Azure VMs, you need to install a Windows servicing stack update (SSU) and SHA-2 update on machines running Windows Server 2008 R2 SP1/SP2. SHA-1 isn't supported from September 2019, and if SHA-2 code signing isn't enabled the agent extension won't install/upgrade as expected. Learn more about SHA-2 upgrade and requirements .
Windows 10 (x64)	Supported.
Windows 8.1 (x64)	Supported.
Windows 8 (x64)	Supported.
Windows 7 (x64) with SP1 onwards	From version 9.30 of the Mobility service extension for Azure VMs, you need to install a Windows servicing stack update (SSU) and SHA-2 update on machines running Windows 7 with SP1. SHA-1 isn't supported from September 2019, and if SHA-2 code signing isn't enabled the agent extension won't install/upgrade as expected.. Learn more about SHA-2 upgrade and requirements .

Linux

OPERATING SYSTEM	DETAILS
Red Hat Enterprise Linux	6.7, 6.8, 6.9, 6.10, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7 , 8.0 , 8.1
CentOS	6.5, 6.6, 6.7, 6.8, 6.9, 6.10, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 8.0, 8.1

OPERATING SYSTEM	DETAILS
Ubuntu 14.04 LTS Server	Supported kernel versions
Ubuntu 16.04 LTS Server	Supported kernel version Ubuntu servers using password-based authentication and sign in, and the cloud-init package to configure cloud VMs, might have password-based sign in disabled on failover (depending on the cloudinit configuration). Password-based sign in can be re-enabled on the virtual machine by resetting the password from the Support > Troubleshooting > Settings menu (of the failed over VM in the Azure portal).
Ubuntu 18.04 LTS Server	Supported kernel version
Debian 7	Supported kernel versions
Debian 8	Supported kernel versions
SUSE Linux Enterprise Server 12	SP1, SP2, SP3, SP4. (Supported kernel versions)
SUSE Linux Enterprise Server 15	15 and 15 SP1. (Supported kernel versions)
SUSE Linux Enterprise Server 11	SP3 Upgrade of replicating machines from SP3 to SP4 isn't supported. If a replicated machine has been upgraded, you need to disable replication and re-enable replication after the upgrade.
SUSE Linux Enterprise Server 11	SP4
Oracle Linux	6.4, 6.5, 6.6, 6.7, 6.8, 6.9, 6.10, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7 Running the Red Hat compatible kernel or Unbreakable Enterprise Kernel Release 3, 4 & 5 (UEK3, UEK4, UEK5)

Supported Ubuntu kernel versions for Azure virtual machines

RELEASE	MOBILITY SERVICE VERSION	KERNEL VERSION
14.04 LTS	9.32	3.13.0-24-generic to 3.13.0-170-generic, 3.16.0-25-generic to 3.16.0-77-generic, 3.19.0-18-generic to 3.19.0-80-generic, 4.2.0-18-generic to 4.2.0-42-generic, 4.4.0-21-generic to 4.4.0-148-generic, 4.15.0-1023-azure to 4.15.0-1045-azure

RELEASE	MOBILITY SERVICE VERSION	KERNEL VERSION
14.04 LTS	9.31	3.13.0-24-generic to 3.13.0-170-generic, 3.16.0-25-generic to 3.16.0-77-generic, 3.19.0-18-generic to 3.19.0-80-generic, 4.2.0-18-generic to 4.2.0-42-generic, 4.4.0-21-generic to 4.4.0-148-generic, 4.15.0-1023-azure to 4.15.0-1045-azure
14.04 LTS	9.30	3.13.0-24-generic to 3.13.0-170-generic, 3.16.0-25-generic to 3.16.0-77-generic, 3.19.0-18-generic to 3.19.0-80-generic, 4.2.0-18-generic to 4.2.0-42-generic, 4.4.0-21-generic to 4.4.0-148-generic, 4.15.0-1023-azure to 4.15.0-1045-azure
14.04 LTS	9.29	3.13.0-24-generic to 3.13.0-170-generic, 3.16.0-25-generic to 3.16.0-77-generic, 3.19.0-18-generic to 3.19.0-80-generic, 4.2.0-18-generic to 4.2.0-42-generic, 4.4.0-21-generic to 4.4.0-148-generic, 4.15.0-1023-azure to 4.15.0-1045-azure
16.04 LTS	9.32	4.4.0-21-generic to 4.4.0-171-generic, 4.8.0-34-generic to 4.8.0-58-generic, 4.10.0-14-generic to 4.10.0-42-generic, 4.11.0-13-generic to 4.11.0-14-generic, 4.13.0-16-generic to 4.13.0-45-generic, 4.15.0-13-generic to 4.15.0-74-generic 4.11.0-1009-azure to 4.11.0-1016-azure, 4.13.0-1005-azure to 4.13.0-1018-azure 4.15.0-1012-azure to 4.15.0-1066-azure

RELEASE	MOBILITY SERVICE VERSION	KERNEL VERSION
16.04 LTS	9.31	4.4.0-21-generic to 4.4.0-170-generic, 4.8.0-34-generic to 4.8.0-58-generic, 4.10.0-14-generic to 4.10.0-42-generic, 4.11.0-13-generic to 4.11.0-14-generic, 4.13.0-16-generic to 4.13.0-45-generic, 4.15.0-13-generic to 4.15.0-72-generic 4.11.0-1009-azure to 4.11.0-1016-azure, 4.13.0-1005-azure to 4.13.0-1018-azure 4.15.0-1012-azure to 4.15.0-1063-azure
16.04 LTS	9.30	4.4.0-21-generic to 4.4.0-166-generic, 4.8.0-34-generic to 4.8.0-58-generic, 4.10.0-14-generic to 4.10.0-42-generic, 4.11.0-13-generic to 4.11.0-14-generic, 4.13.0-16-generic to 4.13.0-45-generic, 4.15.0-13-generic to 4.15.0-66-generic 4.11.0-1009-azure to 4.11.0-1016-azure, 4.13.0-1005-azure to 4.13.0-1018-azure 4.15.0-1012-azure to 4.15.0-1061-azure
16.04 LTS	9.29	4.4.0-21-generic to 4.4.0-164-generic, 4.8.0-34-generic to 4.8.0-58-generic, 4.10.0-14-generic to 4.10.0-42-generic, 4.11.0-13-generic to 4.11.0-14-generic, 4.13.0-16-generic to 4.13.0-45-generic, 4.15.0-13-generic to 4.15.0-64-generic 4.11.0-1009-azure to 4.11.0-1016-azure, 4.13.0-1005-azure to 4.13.0-1018-azure 4.15.0-1012-azure to 4.15.0-1059-azure
18.04 LTS	9.32	4.15.0-20-generic to 4.15.0-74-generic 4.18.0-13-generic to 4.18.0-25-generic 5.0.0-15-generic to 5.0.0-37-generic 5.3.0-19-generic to 5.3.0-24-generic 4.15.0-1009-azure to 4.15.0-1037-azure 4.18.0-1006-azure to 4.18.0-1025-azure 5.0.0-1012-azure to 5.0.0-1028-azure 5.3.0-1007-azure to 5.3.0-1009-azure

RELEASE	MOBILITY SERVICE VERSION	KERNEL VERSION
18.04 LTS	9.31	4.15.0-20-generic to 4.15.0-72-generic 4.18.0-13-generic to 4.18.0-25-generic 5.0.0-15-generic to 5.0.0-37-generic 5.3.0-19-generic to 5.3.0-24-generic 4.15.0-1009-azure to 4.15.0-1037-azure 4.18.0-1006-azure to 4.18.0-1025-azure 5.0.0-1012-azure to 5.0.0-1025-azure 5.3.0-1007-azure
18.04 LTS	9.30	4.15.0-20-generic to 4.15.0-66-generic 4.18.0-13-generic to 4.18.0-25-generic 5.0.0-15-generic to 5.0.0-32-generic 4.15.0-1009-azure to 4.15.0-1037-azure 4.18.0-1006-azure to 4.18.0-1025-azure 5.0.0-1012-azure to 5.0.0-1023-azure
18.04 LTS	9.29	4.15.0-20-generic to 4.15.0-64-generic 4.18.0-13-generic to 4.18.0-25-generic 5.0.0-15-generic to 5.0.0-29-generic 4.15.0-1009-azure to 4.15.0-1037-azure 4.18.0-1006-azure to 4.18.0-1025-azure 5.0.0-1012-azure to 5.0.0-1020-azure

Supported Debian kernel versions for Azure virtual machines

RELEASE	MOBILITY SERVICE VERSION	KERNEL VERSION
Debian 7	9.28,9.29,9.30,9.31	3.2.0-4-amd64 to 3.2.0-6-amd64, 3.16.0-0.bpo.4-amd64
Debian 8	9.29,9.30,9.31	3.16.0-4-amd64 to 3.16.0-10-amd64, 4.9.0-0.bpo.4-amd64 to 4.9.0-0.bpo.11-amd64
Debian 8	9.28	3.16.0-4-amd64 to 3.16.0-10-amd64, 4.9.0-0.bpo.4-amd64 to 4.9.0-0.bpo.9-amd64

Supported SUSE Linux Enterprise Server 12 kernel versions for Azure virtual machines

RELEASE	MOBILITY SERVICE VERSION	KERNEL VERSION
SUSE Linux Enterprise Server 12 (SP1,SP2,SP3,SP4)	9.32	All stock SUSE 12 SP1,SP2,SP3,SP4 kernels are supported. 4.4.138-4.7-azure to 4.4.180-4.31-azure, 4.12.14-6.3-azure to 4.12.14-6.34-azure

RELEASE	MOBILITY SERVICE VERSION	KERNEL VERSION
SUSE Linux Enterprise Server 12 (SP1,SP2,SP3,SP4)	9.31	All stock SUSE 12 SP1,SP2,SP3,SP4 kernels are supported. 4.4.138-4.7-azure to 4.4.180-4.31-azure, 4.12.14-6.3-azure to 4.12.14-6.29-azure
SUSE Linux Enterprise Server 12 (SP1,SP2,SP3,SP4)	9.30	All stock SUSE 12 SP1,SP2,SP3,SP4 kernels are supported. 4.4.138-4.7-azure to 4.4.180-4.31-azure, 4.12.14-6.3-azure to 4.12.14-6.29-azure
SUSE Linux Enterprise Server 12 (SP1,SP2,SP3,SP4)	9.29	All stock SUSE 12 SP1,SP2,SP3,SP4 kernels are supported. 4.4.138-4.7-azure to 4.4.180-4.31-azure, 4.12.14-6.3-azure to 4.12.14-6.23-azure

Supported SUSE Linux Enterprise Server 15 kernel versions for Azure virtual machines

RELEASE	MOBILITY SERVICE VERSION	KERNEL VERSION
SUSE Linux Enterprise Server 15 and 15 SP1	9.32	All stock SUSE 15 and 15 kernels are supported. 4.12.14-5.5-azure to 4.12.14-8.22-azure

Replicated machines - Linux file system/guest storage

- File systems: ext3, ext4, ReiserFS (Suse Linux Enterprise Server only), XFS, BTRFS
- Volume manager: LVM2
- Multipath software: Device Mapper

Replicated machines - compute settings

SETTING	SUPPORT	DETAILS
Size	Any Azure VM size with at least 2 CPU cores and 1-GB RAM	Verify Azure virtual machine sizes .
Availability sets	Supported	If you enable replication for an Azure VM with the default options, an availability set is created automatically, based on the source region settings. You can modify these settings.
Availability zones	Supported	
Hybrid Use Benefit (HUB)	Supported	If the source VM has a HUB license enabled, a test failover or failed over VM also uses the HUB license.

Setting	Support	Details
Virtual machine scale sets	Not supported	
Azure gallery images - Microsoft published	Supported	Supported if the VM runs on a supported operating system.
Azure Gallery images - Third party published	Supported	Supported if the VM runs on a supported operating system.
Custom images - Third party published	Supported	Supported if the VM runs on a supported operating system.
VMs migrated using Site Recovery	Supported	If a VMware VM or physical machine was migrated to Azure using Site Recovery, you need to uninstall the older version of Mobility service running on the machine, and restart the machine before replicating it to another Azure region.
RBAC policies	Not supported	Role based Access control (RBAC) policies on VMs are not replicated to the failover VM in target region.
Extensions	Not supported	Extensions are not replicated to the failover VM in target region. It needs to be installed manually after failover.

Replicated machines - disk actions

Action	Details
Resize disk on replicated VM	Supported on the source VM before failover. No need to disable/re-enable replication. If you change the source VM after failover, the changes aren't captured. If you change the disk size on the Azure VM after failover, changes aren't captured by Site Recovery, and fallback will be to the original VM size.
Add a disk to a replicated VM	Supported

Replicated machines - storage

This table summarized support for the Azure VM OS disk, data disk, and temporary disk.

- It's important to observe the VM disk limits and targets for [Linux](#) and [Windows](#) VMs to avoid any performance issues.
- If you deploy with the default settings, Site Recovery automatically creates disks and storage accounts based on the source settings.
- If you customize, ensure you follow the guidelines.

Component	Support	Details
OS disk maximum size	2048 GB	Learn more about VM disks.
Temporary disk	Not supported	The temporary disk is always excluded from replication. Don't store any persistent data on the temporary disk. Learn more .
Data disk maximum size	8192 GB for managed disks 4095 GB for unmanaged disks	
Data disk minimum size	No restriction for unmanaged disks. 2 GB for managed disks	
Data disk maximum number	Up to 64, in accordance with support for a specific Azure VM size	Learn more about VM sizes.
Data disk change rate	Maximum of 10 MBps per disk for premium storage. Maximum of 2 MBps per disk for Standard storage.	If the average data change rate on the disk is continuously higher than the maximum, replication won't catch up. However, if the maximum is exceeded sporadically, replication can catch up, but you might see slightly delayed recovery points.
Data disk - standard storage account	Supported	
Data disk - premium storage account	Supported	If a VM has disks spread across premium and standard storage accounts, you can select a different target storage account for each disk, to ensure you have the same storage configuration in the target region.
Managed disk - standard	Supported in Azure regions in which Azure Site Recovery is supported.	
Managed disk - premium	Supported in Azure regions in which Azure Site Recovery is supported.	
Standard SSD	Supported	
Redundancy	LRS and GRS are supported. ZRS isn't supported.	
Cool and hot storage	Not supported	VM disks aren't supported on cool and hot storage
Storage Spaces	Supported	
Encryption at rest (SSE)	Supported	SSE is the default setting on storage accounts.

COMPONENT	SUPPORT	DETAILS
Encryption at rest (CMK)	Supported	Both Software and HSM keys are supported for managed disks
Azure Disk Encryption (ADE) for Windows OS	Supported for VMs with managed disks. VMs using unmanaged disks are not supported	
Azure Disk Encryption (ADE) for Linux OS	Supported	
Hot add	Supported	Enabling replication for a data disk that you add to a replicated Azure VM is supported for VMs that use managed disks.
Hot remove disk	Not supported	If you remove data disk on the VM, you need to disable replication and enable replication again for the VM.
Exclude disk	Support. You must use Powershell to configure.	Temporary disks are excluded by default.
Storage Spaces Direct	Supported for crash consistent recovery points. Application consistent recovery points are not supported.	
Scale-out File Server	Supported for crash consistent recovery points. Application consistent recovery points are not supported.	
LRS	Supported	
GRS	Supported	
RA-GRS	Supported	
ZRS	Not supported	
Cool and Hot Storage	Not supported	Virtual machine disks are not supported on cool and hot storage
Azure Storage firewalls for virtual networks	Supported	If restrict virtual network access to storage accounts, enable Allow trusted Microsoft services .
General purpose V2 storage accounts (Both Hot and Cool tier)	Supported	Transaction costs increase substantially compared to General purpose V1 storage accounts
Generation 2 (UEFI boot)	Supported	

IMPORTANT

To avoid performance issues, make sure that you follow VM disk scalability and performance targets for [Linux](#) or [Windows](#) VMs. If you use default settings, Site Recovery creates the required disks and storage accounts, based on the source configuration. If you customize and select your own settings, follow the disk scalability and performance targets for your source VMs.

Limits and data change rates

The following table summarizes Site Recovery limits.

- These limits are based on our tests, but obviously don't cover all possible application I/O combinations.
- Actual results can vary based on your app I/O mix.
- There are two limits to consider, per disk data churn and per virtual machine data churn.

STORAGE TARGET	AVERAGE SOURCE DISK I/O	AVERAGE SOURCE DISK DATA CHURN	TOTAL SOURCE DISK DATA CHURN PER DAY
Standard storage	8 KB	2 MB/s	168 GB per disk
Premium P10 or P15 disk	8 KB	2 MB/s	168 GB per disk
Premium P10 or P15 disk	16 KB	4 MB/s	336 GB per disk
Premium P10 or P15 disk	32 KB or greater	8 MB/s	672 GB per disk
Premium P20 or P30 or P40 or P50 disk	8 KB	5 MB/s	421 GB per disk
Premium P20 or P30 or P40 or P50 disk	16 KB or greater	20 MB/s	1684 GB per disk

Replicated machines - networking

SETTING	SUPPORT	DETAILS
NIC	Maximum number supported for a specific Azure VM size	NICs are created when the VM is created during failover. The number of NICs on the failover VM depends on the number of NICs on the source VM when replication was enabled. If you add or remove a NIC after enabling replication, it doesn't impact the number of NICs on the replicated VM after failover. Also note that the order of NICs after failover is not guaranteed to be the same as the original order.
Internet Load Balancer	Supported	Associate the preconfigured load balancer using an Azure Automation script in a recovery plan.

Setting	Support	Details
Internal Load balancer	Supported	Associate the preconfigured load balancer using an Azure Automation script in a recovery plan.
Public IP address	Supported	Associate an existing public IP address with the NIC. Or, create a public IP address and associate it with the NIC using an Azure Automation script in a recovery plan.
NSG on NIC	Supported	Associate the NSG with the NIC using an Azure Automation script in a recovery plan.
NSG on subnet	Supported	Associate the NSG with the subnet using an Azure Automation script in a recovery plan.
Reserved (static) IP address	Supported	<p>If the NIC on the source VM has a static IP address, and the target subnet has the same IP address available, it's assigned to the failed over VM.</p> <p>If the target subnet doesn't have the same IP address available, one of the available IP addresses in the subnet is reserved for the VM.</p> <p>You can also specify a fixed IP address and subnet in Replicated items > Settings > Compute and Network > Network interfaces.</p>
Dynamic IP address	Supported	<p>If the NIC on the source has dynamic IP addressing, the NIC on the failed over VM is also dynamic by default.</p> <p>You can modify this to a fixed IP address if required.</p>
Multiple IP addresses	Not supported	When you fail over a VM that has a NIC with multiple IP addresses, only the primary IP address of the NIC in the source region is kept. To assign multiple IP addresses, you can add VMs to a recovery plan and attach a script to assign additional IP addresses to the plan, or you can make the change manually or with a script after failover.
Traffic Manager	Supported	You can preconfigure Traffic Manager so that traffic is routed to the endpoint in the source region on a regular basis, and to the endpoint in the target region in case of failover.
Azure DNS	Supported	

Setting	Support	Details
Custom DNS	Supported	
Unauthenticated proxy	Supported	Learn more
Authenticated Proxy	Not supported	If the VM is using an authenticated proxy for outbound connectivity, it cannot be replicated using Azure Site Recovery.
VPN site-to-site connection to on-premises (with or without ExpressRoute)	Supported	Ensure that the UDRs and NSGs are configured in such a way that the Site Recovery traffic is not routed to on-premises. Learn more
VNET to VNET connection	Supported	Learn more
Virtual Network Service Endpoints	Supported	If you are restricting the virtual network access to storage accounts, ensure that the trusted Microsoft services are allowed access to the storage account.
Accelerated networking	Supported	Accelerated networking must be enabled on source VM. Learn more .

Next steps

- Read [networking guidance](#) for replicating Azure VMs.
- Deploy disaster recovery by [replicating Azure VMs](#).

Support for using Site Recovery with Azure Backup

10/15/2019 • 2 minutes to read • [Edit Online](#)

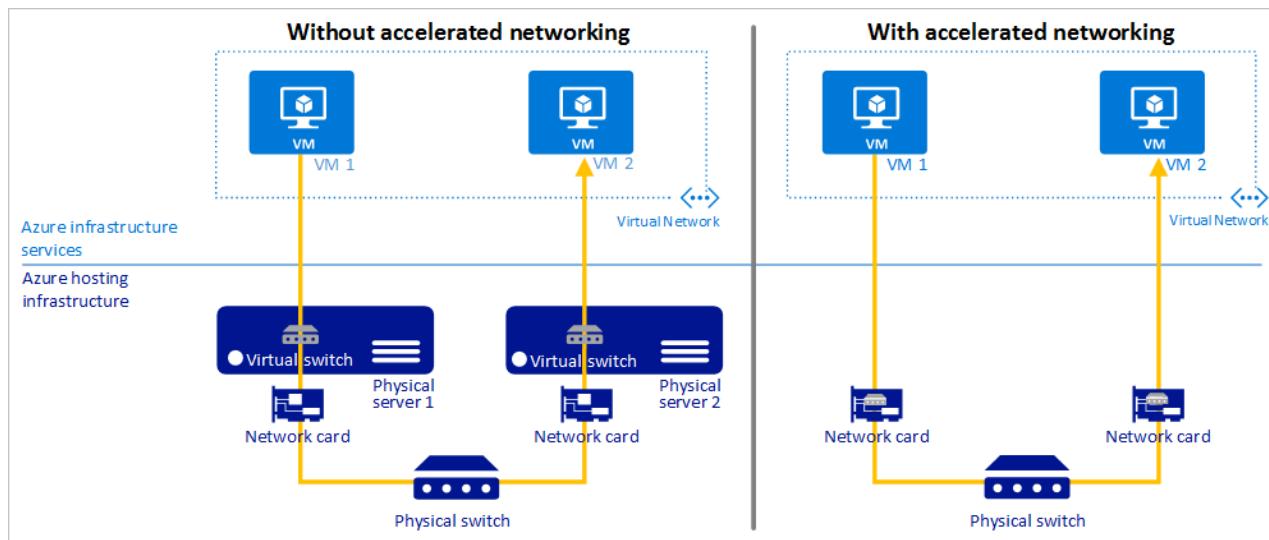
This article summarizes support for using the [Site Recovery service](#) together with the [Azure Backup service](#).

ACTION	SITE RECOVERY SUPPORT	DETAILS
Deploy services together	Supported	Services are interoperable and can be configured together.
File backup/restore	Supported	When backup and replication are enabled for a VM and backups are taken, there's no issue in restoring files on the source-side VMs, or group of VMs. Replication continues as usual with no change in replication health.
Disk restore	No current support	If you restore a backed up disk, you need to disable and re-enable replication for the VM again.
VM restore	No current support	If you restore a VM or group of VMs, you need to disable and re-enable replication for the VM.

Accelerated Networking with Azure virtual machine disaster recovery

11/5/2019 • 3 minutes to read • [Edit Online](#)

Accelerated Networking enables single root I/O virtualization (SR-IOV) to a VM, greatly improving its networking performance. This high-performance path bypasses the host from the datapath, reducing latency, jitter, and CPU utilization, for use with the most demanding network workloads on supported VM types. The following picture shows communication between two VMs with and without accelerated networking:



Azure Site Recovery enables you to utilize the benefits of Accelerated Networking, for Azure virtual machines that are failed over to a different Azure region. This article describes how you can enable Accelerated Networking for Azure virtual machines replicated with Azure Site Recovery.

Prerequisites

Before you begin, ensure that you understand:

- Azure virtual machine [replication architecture](#)
- [Setting up replication](#) for Azure virtual machines
- [Failing over](#) Azure virtual machines

Accelerated Networking with Windows VMs

Azure Site Recovery supports enabling Accelerated Networking for replicated virtual machines only if the source virtual machine has Accelerated Networking enabled. If your source virtual machine does not have Accelerated Networking enabled, you can learn how to enable Accelerated Networking for Windows virtual machines [here](#).

Supported operating systems

The following distributions are supported out of the box from the Azure Gallery:

- **Windows Server 2016 Datacenter**
- **Windows Server 2012 R2 Datacenter**

Supported VM instances

Accelerated Networking is supported on most general purpose and compute-optimized instance sizes with 2 or

more vCPUs. These supported series are: D/DSv2 and F/Fs

On instances that support hyperthreading, Accelerated Networking is supported on VM instances with 4 or more vCPUs. Supported series are: D/DSv3, E/ESv3, Fsv2, and Ms/Mms

For more information on VM instances, see [Windows VM sizes](#).

Accelerated Networking with Linux VMs

Azure Site Recovery supports enabling Accelerated Networking for replicated virtual machines only if the source virtual machine has Accelerated Networking enabled. If your source virtual machine does not have Accelerated Networking enabled, you can learn how to enable Accelerated Networking for Linux virtual machines [here](#).

Supported operating systems

The following distributions are supported out of the box from the Azure Gallery:

- **Ubuntu 16.04**
- **SLES 12 SP3**
- **RHEL 7.4**
- **CentOS 7.4**
- **CoreOS Linux**
- **Debian "Stretch" with backports kernel**
- **Oracle Linux 7.4**

Supported VM instances

Accelerated Networking is supported on most general purpose and compute-optimized instance sizes with 2 or more vCPUs. These supported series are: D/DSv2 and F/Fs

On instances that support hyperthreading, Accelerated Networking is supported on VM instances with 4 or more vCPUs. Supported series are: D/DSv3, E/ESv3, Fsv2, and Ms/Mms.

For more information on VM instances, see [Linux VM sizes](#).

Enabling Accelerated Networking for replicated VMs

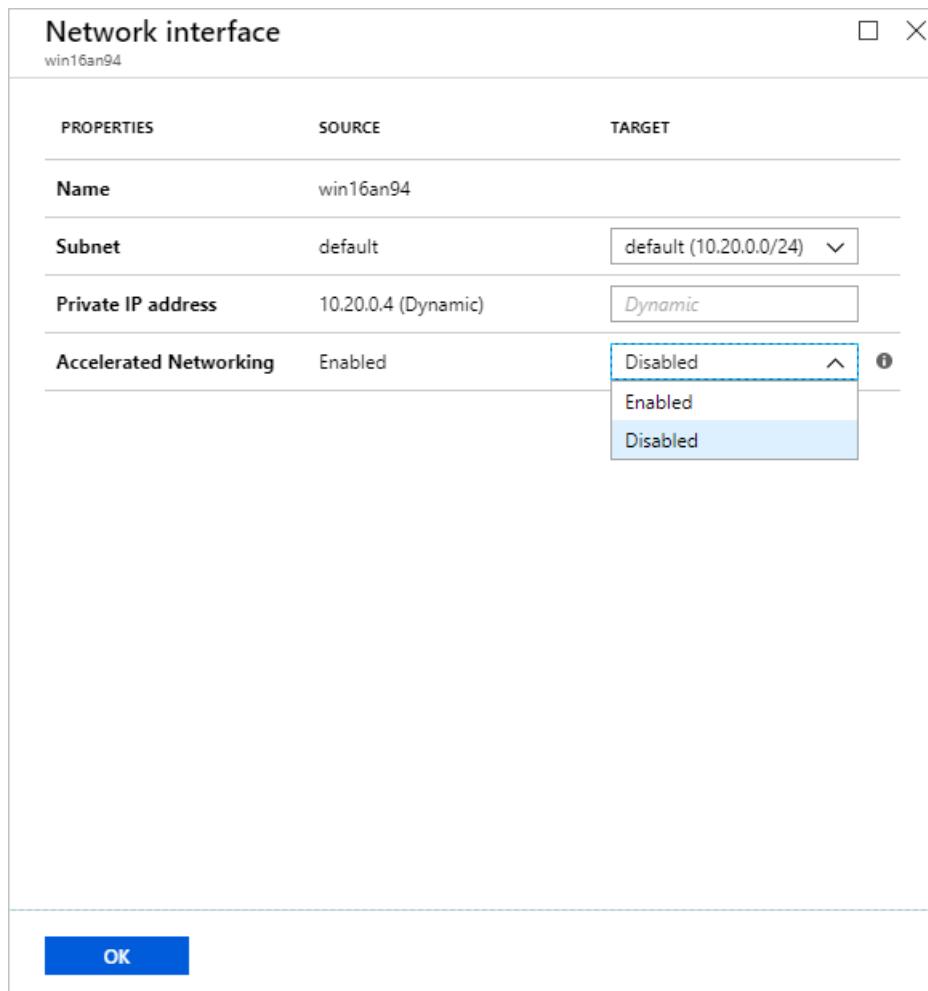
When you [enable replication](#) for Azure virtual machines, Site Recovery will automatically detect whether the virtual machine network interfaces have Accelerated Networking enabled. If Accelerated Networking is already enabled, Site Recovery will automatically configure Accelerated Networking on the network interfaces of the replicated virtual machine.

The status of Accelerated Networking can be verified under the **Network interfaces** section of the **Compute and Network** settings for the replicated virtual machine.

SOURCE NIC NAME	SOURCE SUBNET	TARGET SUBNET	SOURCE IP	TARGET IP	ACCELERATED NETWORKING
win16an94	default	default	10.20.0.4 (Dynamic)	DHCP assigned	Enabled

If you have enabled Accelerated Networking on the source virtual machine after enabling replication, you can enable Accelerated Networking for the replicated virtual machine's network interfaces by the following process:

1. Open **Compute and Network** settings for the replicated virtual machine
2. Click on the name of the network interface under the **Network interfaces** section
3. Select **Enabled** from the dropdown for Accelerated Networking under the **Target** column



The above process should also be followed for existing replicated virtual machines, that did not previously have Accelerated Networking enabled automatically by Site Recovery.

Next steps

- Learn more about [benefits of Accelerated Networking](#).
- Learn more about limitations and constraints of Accelerated Networking for [Windows virtual machines](#) and [Linux virtual machines](#).
- Learn more about [recovery plans](#) to automate application failover.

Integrate ExpressRoute with disaster recovery for Azure VMs

11/12/2019 • 9 minutes to read • [Edit Online](#)

This article describes how to integrate Azure ExpressRoute with [Azure Site Recovery](#), when you set up disaster recovery for Azure VMs to a secondary Azure region.

Site Recovery enables disaster recovery of Azure VMs by replicating Azure VM data to Azure.

- If Azure VMs use [Azure managed disks](#), VM data is replicated to an replicated managed disk in the secondary region.
- If Azure VMs don't use managed disks, VM data is replicated to an Azure storage account.
- Replication endpoints are public, but replication traffic for Azure VMs doesn't cross the internet.

ExpressRoute enables you to extend on-premises networks into the Microsoft Azure cloud over a private connection, facilitated by a connectivity provider. If you have ExpressRoute configured, it integrates with Site Recovery as follows:

- **During replication between Azure regions:** Replication traffic for Azure VM disaster recovery is within Azure only, and ExpressRoute isn't needed or used for replication. However, if you're connecting from an on-premises site to the Azure VMs in the primary Azure site, there are a number of issues to be aware of when you're setting up disaster recovery for those Azure VMs.
- **Failover between Azure regions:** When outages occur, you fail over Azure VMs from the primary to secondary Azure region. After failing over to a secondary region, there are a number of steps to take in order to access the Azure VMs in the secondary region using ExpressRoute.

Before you begin

Before you begin, make sure you understand the following concepts:

- ExpressRoute [circuits](#)
- ExpressRoute [routing domains](#)
- ExpressRoute [locations](#).
- Azure VM [replication architecture](#)
- How to [set up replication](#) for Azure VMs.
- How to [fail over](#) Azure VMs.

General recommendations

For best practice, and to ensure efficient Recovery Time Objectives (RTOs) for disaster recovery, we recommend you do the following when you set up Site Recovery to integrate with ExpressRoute:

- Provision networking components before failover to a secondary region:
 - When you enable replication for Azure VMs, Site Recovery can automatically deploy networking resources such as networks, subnets, and gateways in the target Azure region, based on source network settings.
 - Site Recovery can't automatically set up networking resources such as VNet gateways.
 - We recommend you provision these additional networking resources before failover. A small downtime is associated with this deployment, and it can impact the overall recovery time, if you didn't account for it

during deployment planning.

- Run regular disaster recovery drills:
 - A drill validates your replication strategy without data loss or downtime, and doesn't affect your production environment. It helps avoid last-minute configuration issues that can adversely impact RTO.
 - When you run a test failover for the drill, we recommend that you use a separate Azure VM network, instead of the default network that's set up when you enable replication.
- Use different IP address spaces if you have a single ExpressRoute circuit.
 - We recommend that you use a different IP address space for the target virtual network. This avoids issues when establishing connections during regional outages.
 - If you can't use a separate address space, be sure to run the disaster recovery drill test failover on a separate test network with different IP addresses. You can't connect two VNets with overlapping IP address space to the same ExpressRoute circuit.

Replicate Azure VMs when using ExpressRoute

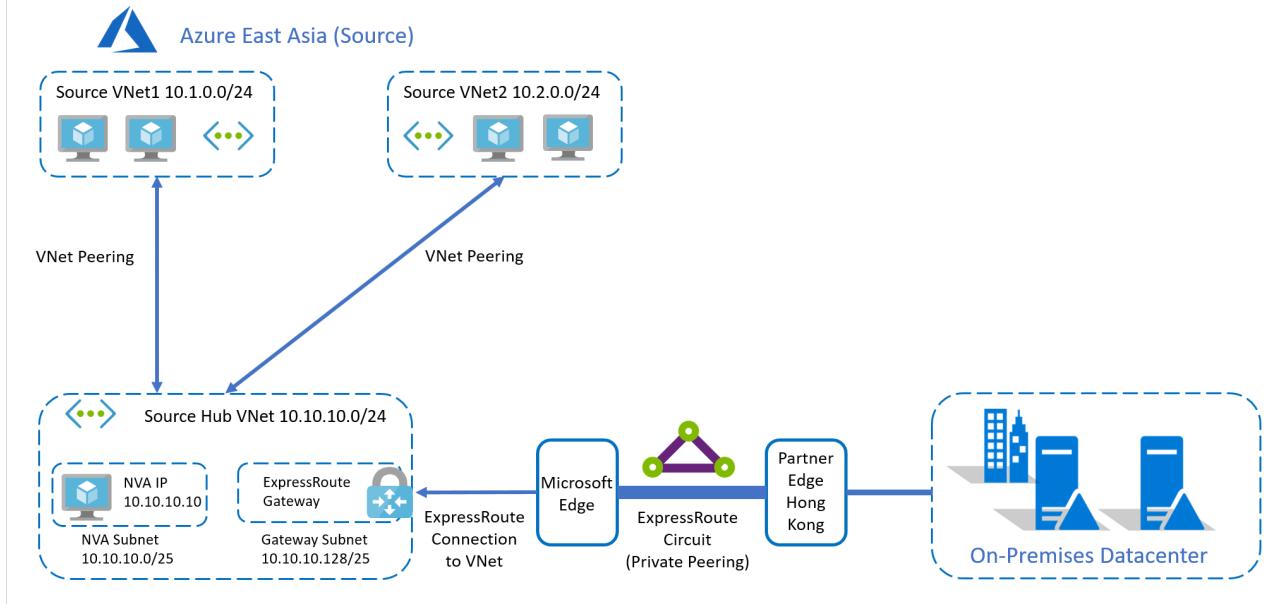
If you want to set up replication for Azure VMs in a primary site, and you're connecting to these VMs from your on-premises site over ExpressRoute, here's what you need to do:

1. [Enable replication](#) for each Azure VM.
2. Optionally let Site Recovery set up networking:
 - When you configure and enable replication, Site Recovery sets up networks, subnets, and gateway subnets in the target Azure region, to match those in the source region. Site Recovery also maps between the source and target virtual networks.
 - If you don't want Site Recovery to do this automatically, create the target-side network resources before you enable replication.
3. Create other networking elements:
 - Site Recovery doesn't create route tables, VNet gateways, VNet gateway connections, VNet peering, or other networking resources and connections in the secondary region.
 - You need to create these additional networking elements in the secondary region, any time before running a failover from the primary region.
 - You can use [recovery plans](#) and automation scripts to set up and connect these networking resources.
4. If you have a network virtual appliance (NVA) deployed to control the flow of network traffic, note that:
 - Azure's default system route for Azure VM replication is 0.0.0.0/0.
 - Typically, NVA deployments also define a default route (0.0.0.0/0) that forces outbound Internet traffic to flow through the NVA. The default route is used when no other specific route configuration can be found.
 - If this is the case, the NVA might be overloaded if all replication traffic passes through the NVA.
 - The same limitation also applies when using default routes for routing all Azure VM traffic to on-premises deployments.
 - In this scenario, we recommend that you [create a network service endpoint](#) in your virtual network for the Microsoft.Storage service, so that the replication traffic doesn't leave Azure boundary.

Replication example

Typically enterprise deployments have workloads split across multiple Azure VNets, with a central connectivity hub for external connectivity to the internet and to on-premises sites. A hub and spoke topology is typically used together with ExpressRoute.

On-premises to Azure connectivity – Before failover



- **Region.** Apps are deployed in the Azure East Asia region.
- **Spoke vNets.** Apps are deployed in two spoke vNets:
 - **Source vNet1:** 10.1.0.0/24.
 - **Source vNet2:** 10.2.0.0/24.
 - Each spoke virtual network is connected to **Hub vNet**.
- **Hub vNet.** There's a hub vNet **Source Hub vNet:** 10.10.10.0/24.
 - This hub vNet acts as the gatekeeper.
 - All communications across subnets go through this hub.
 - **Hub vNet subnets.** The hub vNet has two subnets:
 - **NVA subnet:** 10.10.10.0/25. This subnet contains an NVA (10.10.10.10).
 - **Gateway subnet:** 10.10.10.128/25. This subnet contains an ExpressRoute gateway connected to an ExpressRoute connection that routes to the on-premises site via a private peering routing domain.
- The on-premises datacenter has an ExpressRoute circuit connection through a partner edge in Hong Kong.
- All routing is controlled through Azure route tables (UDR).
- All outbound traffic between vNets, or to the on-premises datacenter is routed through the NVA.

Hub and spoke peering settings

Spoke to hub

DIRECTION	SETTING	STATE
Spoke to hub	Allow virtual network address	Enabled
Spoke to hub	Allow forwarded traffic	Enabled
Spoke to hub	Allow gateway transit	Disabled
Spoke to hub	Use remote gateways	Enabled

Configuration

Allow virtual network access [?](#)

Disabled Enabled

Allow forwarded traffic [?](#)

Allow gateway transit [?](#)

Use remote gateways [?](#)

Hub to spoke

DIRECTION	SETTING	STATE
Hub to spoke	Allow virtual network address	Enabled
Hub to spoke	Allow forwarded traffic	Enabled
Hub to spoke	Allow gateway transit	Enabled
Hub to spoke	Use remove gateways	Disabled

Configuration

Allow virtual network access [?](#)

Disabled Enabled

Allow forwarded traffic [?](#)

Allow gateway transit [?](#)

Use remote gateways [?](#)

Example steps

In our example, the following should happen when enabling replication for Azure VMs in the source network:

1. You [enable replication](#) for a VM.
2. Site Recovery will create replica vNets, subnets, and gateway subnets in the target region.
3. Site Recovery creates mappings between the source networks and the replica target networks it creates.
4. You manually create virtual network gateways, virtual network gateway connections, virtual network peering, or any other networking resources or connections.

Fail over Azure VMs when using ExpressRoute

After you fail Azure VMs over to the target Azure region using Site Recovery, you can access them using ExpressRoute [private peering](#).

- You need to connect ExpressRoute to the target vNet with a new connection. The existing ExpressRoute connection isn't automatically transferred.
- The way in which you set up your ExpressRoute connection to the target vNet depends on your ExpressRoute topology.

Access with two circuits

Two circuits with two peering locations

This configuration helps protects ExpressRoute circuits against regional disaster. If your primary peering location goes down, connections can continue from the other location.

- The circuit connected to the production environment is usually the primary. The secondary circuit typically has lower bandwidth, which can be increased if a disaster occurs.
- After failover, you can establish connections from the secondary ExpressRoute circuit to the target vNet. Alternatively, you can have connections set up and ready in case of disaster, to reduce overall recovery time.
- With simultaneous connections to both primary and target vNets, make sure that your on-premises routing only uses the secondary circuit and connection after failover.
- The source and target vNets can receive new IP addresses, or keep the same ones, after failover. In both cases, the secondary connections can be established prior to failover.

Two circuits with single peering location

This configuration helps protect against failure of the primary ExpressRoute circuit, but not if the single ExpressRoute peering location goes down, impacting both circuits.

- You can have simultaneous connections from the on-premises datacenter to source vNET with the primary circuit, and to the target vNet with the secondary circuit.
- With simultaneous connections to primary and target, make sure that on-premises routing only uses the secondary circuit and connection after failover.
- You can't connect both circuits to the same vNet when circuits are created at the same peering location.

Access with a single circuit

In this configuration there's only one Expressroute circuit. Although the circuit has a redundant connection in case one goes down, a single route circuit will not provide resilience if your peering region goes down. Note that:

- You can replicate Azure VMs to any Azure region in the [same geographic location](#). If the target Azure region isn't in the same location as the source, you need to enable ExpressRoute Premium if you're using a single ExpressRoute circuit. Learn about [ExpressRoute locations](#) and [ExpressRoute pricing](#).
- You can't connect source and target vNets simultaneously to the circuit if the same IP address space is used on the target region. In this scenario:
 - Disconnect the source side connection, and then establish the target side connection. This connection change can be scripted as part of a Site Recovery recovery plan. Note that:
 - In a regional failure, if the primary region is inaccessible, the disconnect operation could fail. This could impact connection creation to the target region.
 - If you created the connection in the target region, and primary region recovers later, you might experience packet drops if two simultaneous connections attempt to connect to the same address space.
 - To prevent this, terminate the primary connection immediately.
 - After VM failback to the primary region, the primary connection can again be established, after you disconnect the secondary connection.
- If a different address spaces is used on the target vNet, you can simultaneously connect to the source and target vNets from the same ExpressRoute circuit.

Failover example

In our example, we're using the following topology:

- Two different ExpressRoute circuits in two different peering locations.
- Retain private IP addresses for the Azure VMs after failover.
- The target recovery region is Azure SouthEast Asia.
- A secondary ExpressRoute circuit connection is established through a partner edge in Singapore.

For a simple topology that uses a single ExpressRoute circuit, with same IP address after failover, [review this article](#).

Example steps

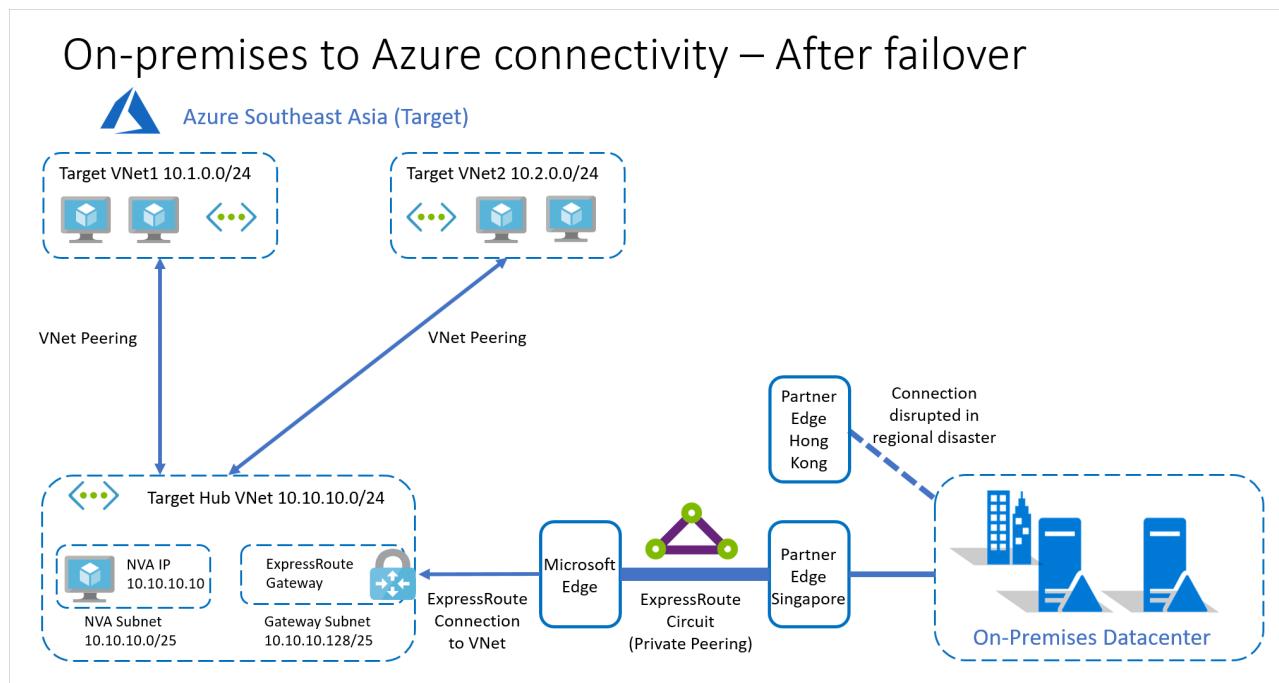
To automate recovery in this example, here's what you need to do:

1. Follow the steps to set up replication.
2. [Fail over the Azure VMs](#), with these additional steps during or after the failover.
 - a. Create the Azure ExpressRoute Gateway in the target region hub VNet. This is needed to connect the target hub vNet to the ExpressRoute circuit.
 - b. Create the connection from the target hub vNet to the target ExpressRoute circuit.
 - c. Set up the VNet peerings between the target region's hub and spoke virtual networks. The peering properties on the target region will be the same as those on the source region.
 - d. Set up the UDRs in the hub VNet, and the two spoke VNets.
 - The properties of the target side UDRs are the same as those on the source side when using the same IP addresses.
 - With different target IP addresses, the UDRs should be modified accordingly.

The above steps can be scripted as part of a [recovery plan](#). Depending on the application connectivity and recovery time requirements, the above steps can also be completed prior to starting the failover.

After recovery

After recovering the VMs and completing connectivity, the recovery environment is as follows.



Next steps

Learn more about using [recovery plans](#) to automate app failover.

Moving Azure VMs to another Azure region

12/26/2019 • 3 minutes to read • [Edit Online](#)

This article provides an overview of the reasons and steps involved in moving Azure VMs to another Azure region using [Azure Site Recovery](#).

Reasons to move Azure VMs

You might move VMs for the following reasons:

- You already deployed in one region, and a new region support was added which is closer to the end users of your application or service. In this scenario, you'd want to move your VMs as is to the new region to reduce latency. Use the same approach if you want to consolidate subscriptions or if there are governance or organization rules that require you to move.
- Your VM was deployed as a single-instance VM or as part of an availability set. If you want to increase the availability SLAs, you can move your VMs into an Availability Zone.

Steps to move Azure VMs

Moving VMs involves the following steps:

1. Verify prerequisites.
2. Prepare the source VMs.
3. Prepare the target region.
4. Copy data to the target region. Use Azure Site Recovery replication technology to copy data from the source VM to the target region.
5. Test the configuration. After the replication is complete, test the configuration by performing a test failover to a non-production network.
6. Perform the move.
7. Discard the resources in the source region.

NOTE

Details about these steps are provided in the following sections.

IMPORTANT

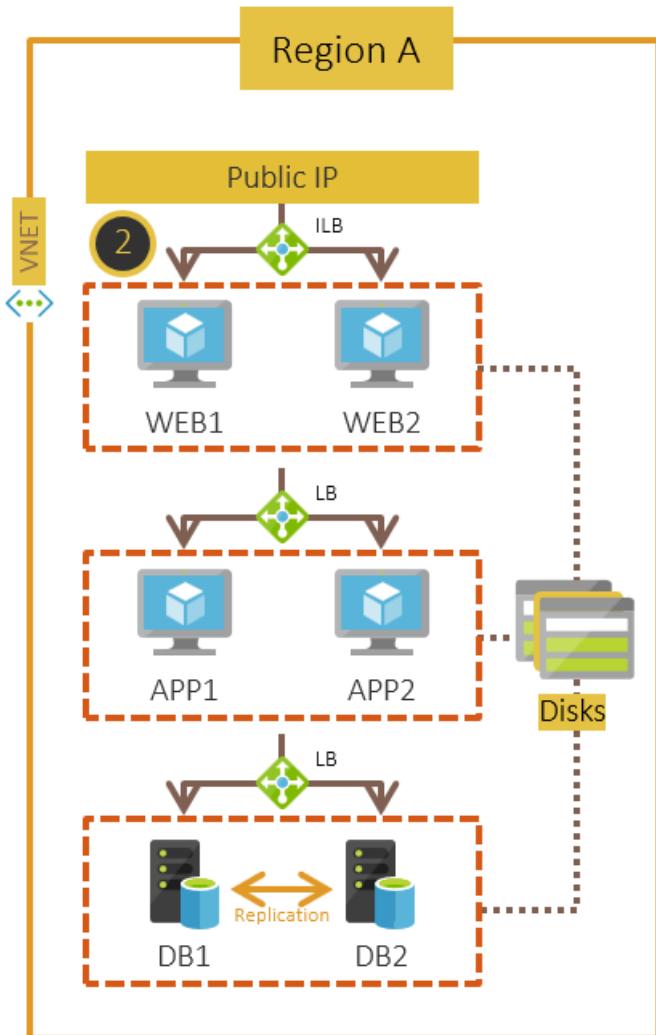
Currently, Azure Site Recovery supports moving VMs from one region to another but doesn't support moving within a region.

Typical architectures for a multi-tier deployment

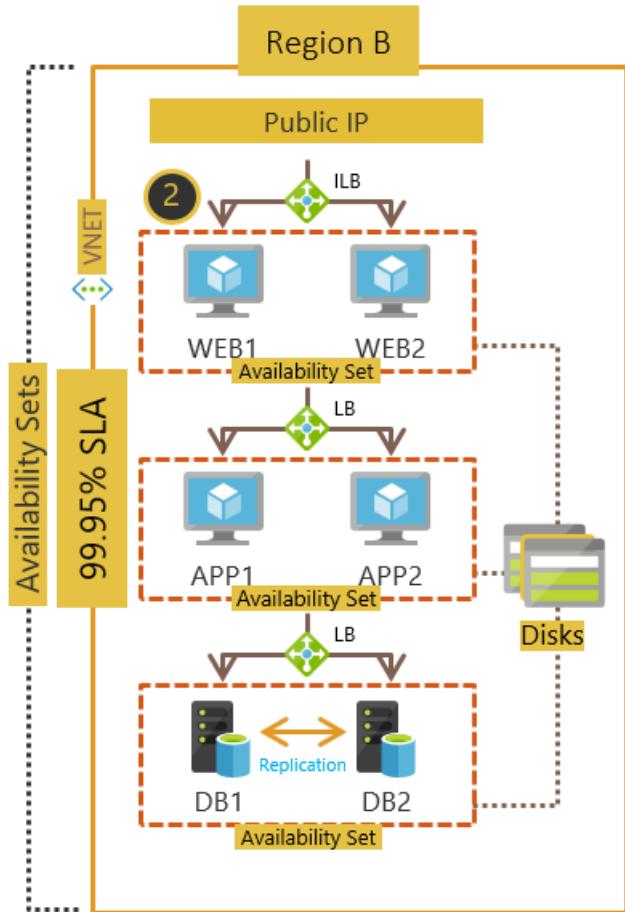
This section describes the most common deployment architectures for a multi-tier application in Azure. The example is a three-tiered application with a public IP. Each of the tiers (web, application, and database) has two VMs each, and they are connected by an Azure load balancer to the other tiers. The database tier has SQL Server Always On replication between the VMs for high availability.

- **Single-instance VMs deployed across various tiers:** Each VM in a tier is configured as a single-instance

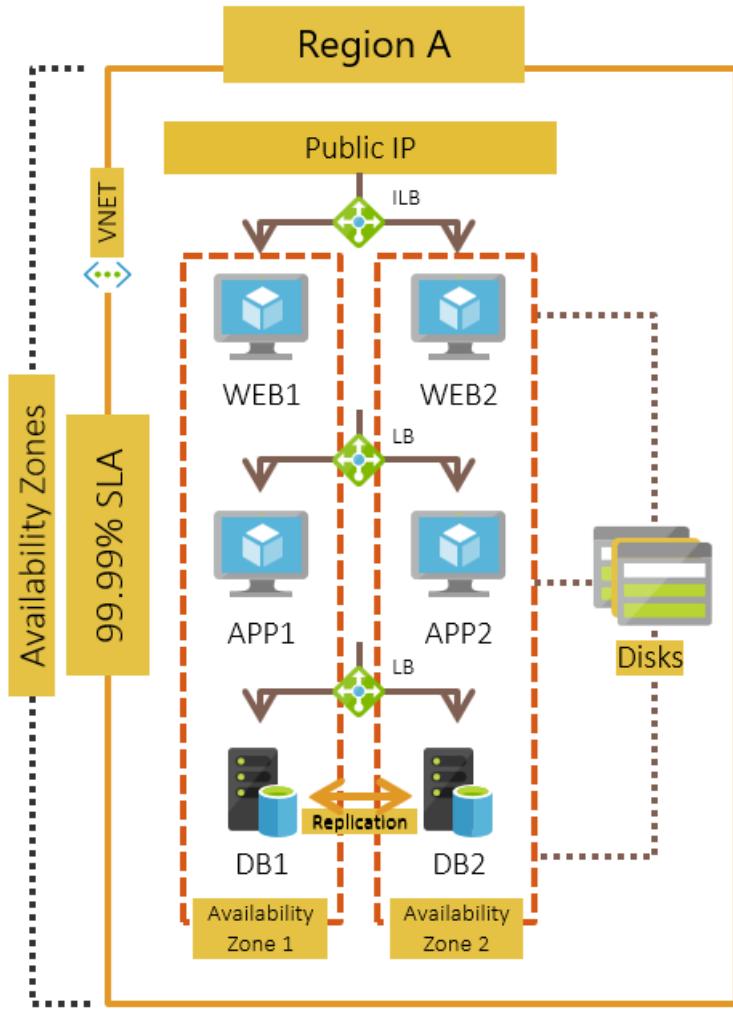
VM and is connected by load balancers to the other tiers. This configuration is the simplest to adopt.



- **VMs in each tier deployed across availability sets:** Each VM in a tier is configured in an availability set. [Availability sets](#) ensure that the VMs you deploy on Azure are distributed across multiple isolated hardware nodes in a cluster. This ensures that if a hardware or software failure within Azure happens, only a subset of your VMs are affected, and your overall solution remains available and operational.



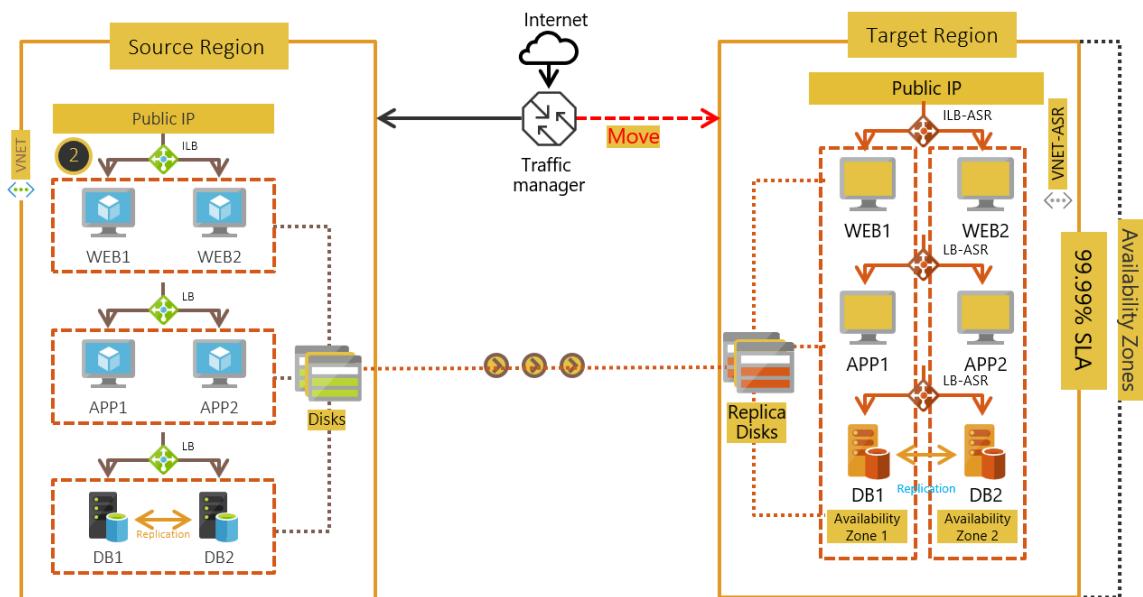
- **VMs in each tier deployed across Availability Zones:** Each VM in a tier is configured across [Availability Zones](#). An Availability Zone in an Azure region is a combination of a fault domain and an update domain. For example, if you create three or more VMs across three zones in an Azure region, your VMs are effectively distributed across three fault domains and three update domains. The Azure platform recognizes this distribution across update domains to make sure that VMs in different zones are not updated at the same time.



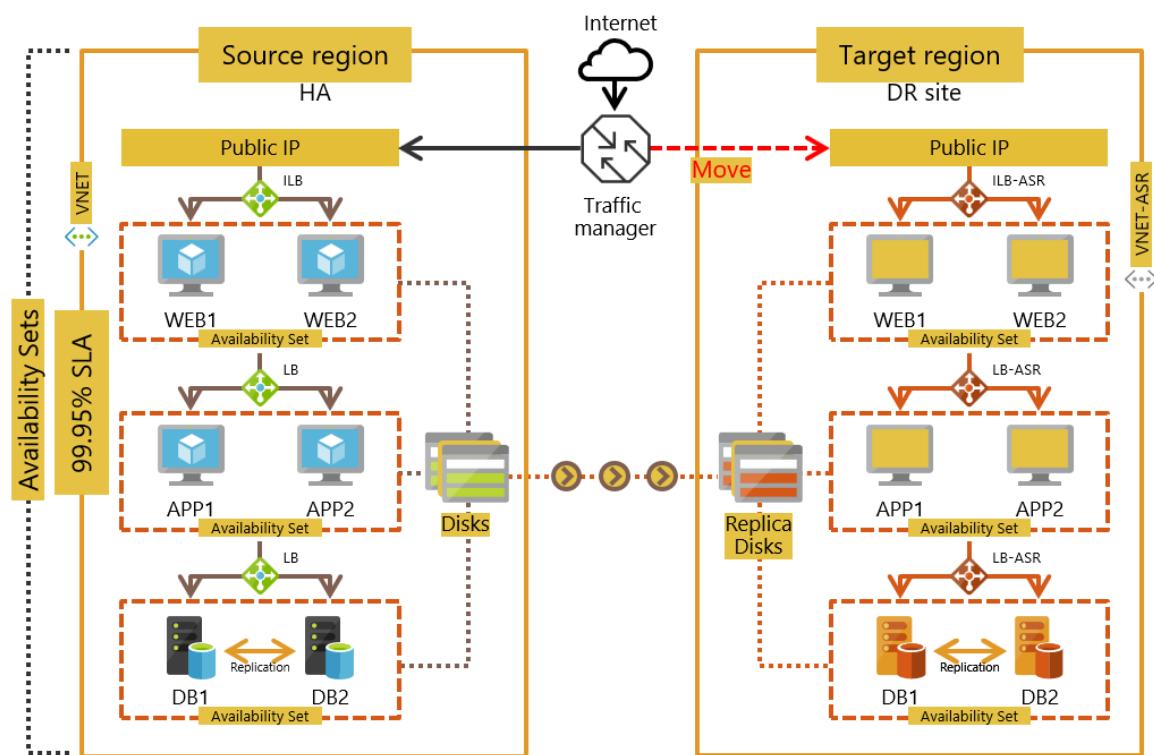
Move VMs as is to a target region

Based on the [architectures](#) mentioned earlier, here's what the deployments will look like after you perform the move as is to the target region.

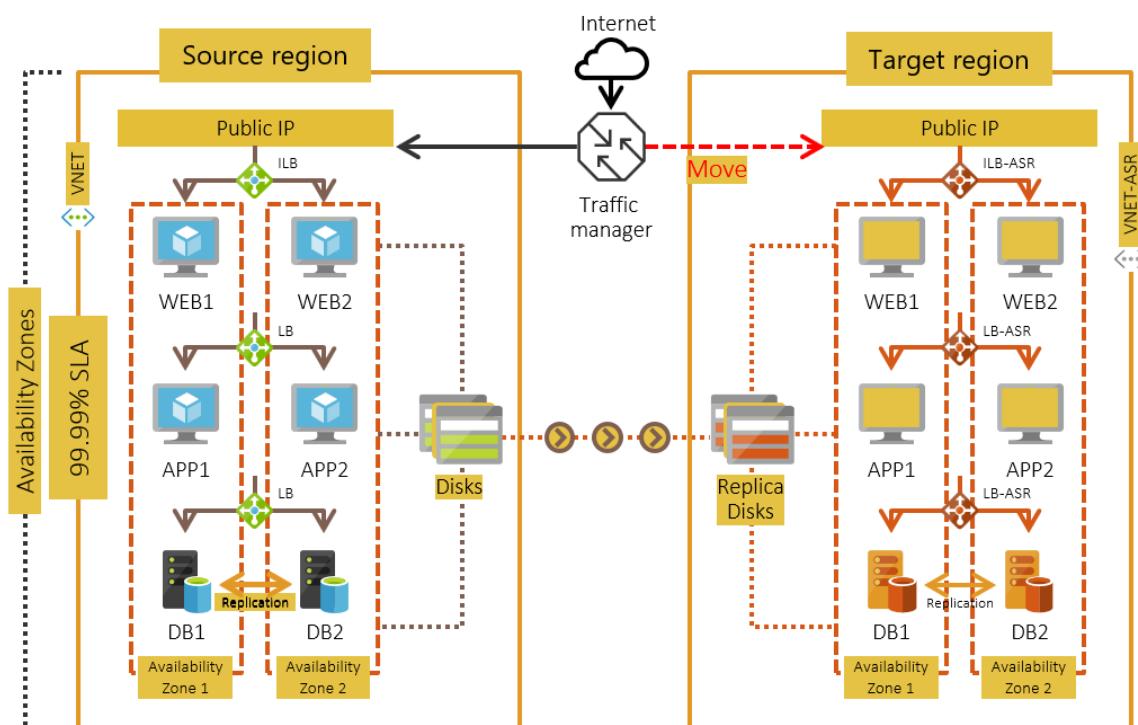
- Single-instance VMs deployed across various tiers



- VMs in each tier deployed across availability sets

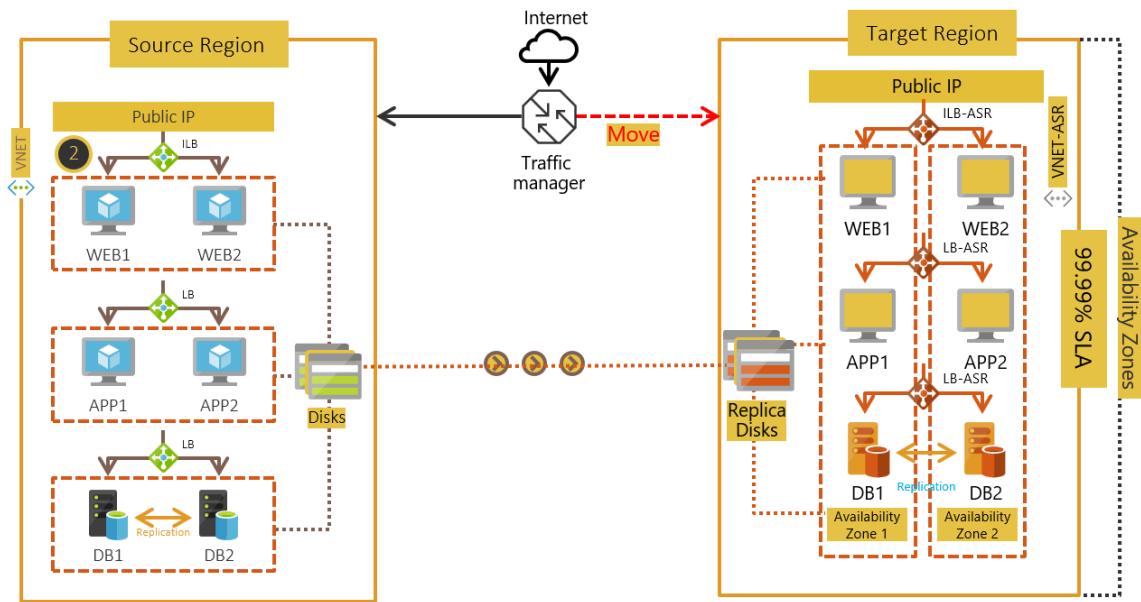


- VMs in each tier deployed across Availability Zones

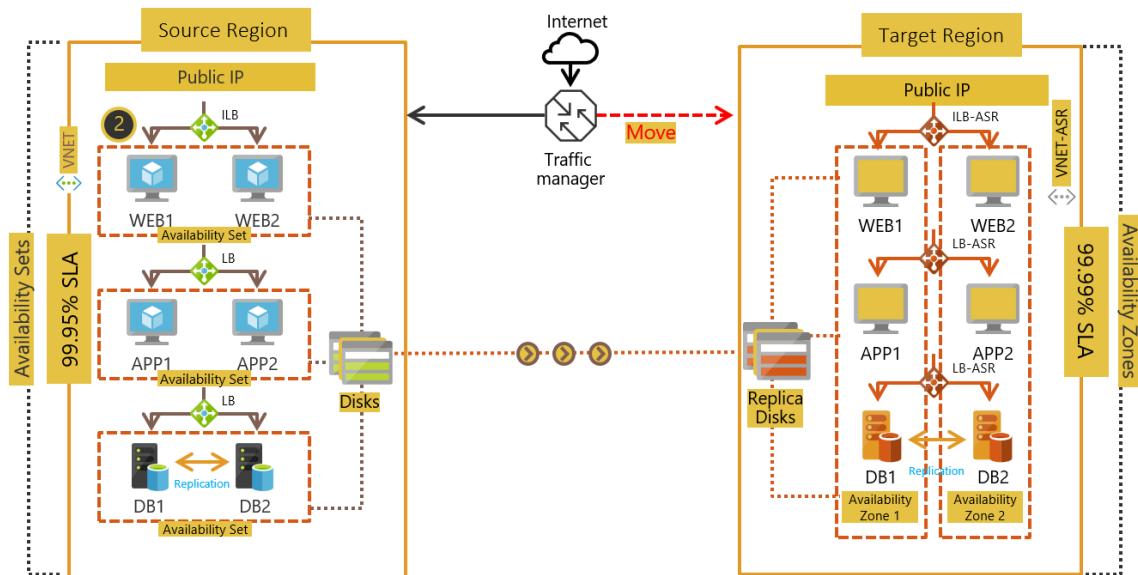


Move VMs to increase availability

- Single-instance VMs deployed across various tiers



- VMs in each tier deployed across availability sets:** You can configure your VMs in an availability set into separate Availability Zones when you enable replication for your VM by using Azure Site Recovery. The SLA for availability will be 99.99% after you complete the move operation.



Next steps

- Move Azure VMs to another region
- Move Azure VMs into Availability Zones

About disaster recovery of VMware VMs to Azure

11/12/2019 • 6 minutes to read • [Edit Online](#)

This article provides an overview of disaster recovery for on-premises VMware VMs to Azure using the [Azure Site Recovery](#) service.

What is BCDR?

A business continuity and disaster recovery (BCDR) strategy helps keep your business up and running. During planned downtime and unexpected outages, BCDR keeps data safe and available, and ensures that apps continue running. In addition to platform BCDR features such as regional pairing, and high availability storage, Azure provides Recovery Services as an integral part of your BCDR solution. Recovery services include:

- [Azure Backup](#) backs up your on-premises and Azure VM data. You can back up a file and folders, specific workloads, or an entire VM.
- [Azure Site Recovery](#) provides resilience and disaster recovery for apps and workloads running on on-premises machines, or Azure IaaS VMs. Site Recovery orchestrates replication, and handles failover to Azure when outages occur. It also handles recovery from Azure to your primary site.

How does Site Recovery do disaster recovery?

1. After preparing Azure and your on-premises site, you set up and enable replication for your on-premises machines.
2. Site Recovery orchestrates initial replication of the machine, in accordance with your policy settings.
3. After the initial replication, Site Recovery replicates delta changes to Azure.
4. When everything's replicating as expected, you run a disaster recovery drill.
 - The drill helps ensure that failover will work as expected when a real need arises.
 - The drill performs a test failover without impacting your production environment.
5. If an outage occurs, you run a full failover to Azure. You can fail over a single machine, or you can create a recovery plan that fails over multiple machines at the same time.
6. On failover, Azure VMs are created from the VM data in Managed disks or storage accounts. Users can continue accessing apps and workloads from the Azure VM
7. When your on-premises site is available again, you fail back from Azure.
8. After you fail back and are working from your primary site once more, you start replicating on-premises VMs to Azure again.

How do I know if my environment is suitable for disaster recovery to Azure?

Site Recovery can replicate any workload running on a supported VMware VM or physical server. Here are the things you need to check in your environment:

- If you're replicating VMware VMs, are you running the right versions of VMware virtualization servers? [Check here](#).
- Are the machines you want to replicate running a supported operating system? [Check here](#).
- For Linux disaster recovery, are machines running a supported file system/guest storage? [Check here](#).
- Do the machines you want to replicate comply with Azure requirements? [Check here](#).
- Is your network configuration supported? [Check here](#).

- Is your storage configuration supported? [Check here.](#)

What do I need to set up in Azure before I start?

In Azure you need to prepare the following:

1. Verify that your Azure account has permissions to create VMs in Azure.
2. Create an Azure network that Azure VMs will join when they're created from storage accounts or managed disks after failover.
3. Set up an Azure Recovery Services vault for Site Recovery. The vault resides in the Azure portal, and is used to deploy, configure, orchestrate, monitor, and troubleshoot your Site Recovery deployment.

Need more help?

Learn how to set up Azure by [verifying your account](#), creating a [network](#), and [setting up a vault](#).

What do I need to set up on-premises before I start?

On-premises here's what you need to do:

1. You need to set up a couple of accounts:
 - If you're replicating VMware VMs, an account is needed for Site Recovery to access vCenter Server or vSphere ESXi hosts to automatically discover VMs.
 - An account is needed to install the Site Recovery Mobility service agent on each physical machine or VM you want to replicate.
2. You need to check the compatibility of your VMware infrastructure if you didn't previously do that.
3. Ensure that you can connect to Azure VMs after a failover. You set up RDP on on-premises Windows machines, or SSH on Linux machines.

Need more help?

- Prepare accounts for [automatic discovery](#) and for [installation of the Mobility service](#).
- [Verify](#) that your VMware settings are compatible.
- [Prepare](#) so that you connect in Azure after failover.
- If you want more in-depth help about setting up IP addressing for Azure VMs after failover, [read this article](#).

How do I set up disaster recovery?

After you have your Azure and on-premises infrastructure in place, you can set up disaster recovery.

1. To understand the components that you'll need to deploy, review the [VMware to Azure architecture](#), and the [physical to Azure architecture](#). There are a number of components, so it's important to understand how they all fit together.
2. **Source environment:** As a first step in deployment, you set up your replication source environment. You specify what you want to replicate, and where you want to replicate to.
3. **Configuration server:** You need to set up a configuration server in your on-premises source environment:
 - The configuration server is a single on-premises machine. For VMware disaster recovery, we recommend that you deploy it as a VMware VM that can be deployed from a downloadable OVF template.
 - The configuration server coordinates communications between on-premises and Azure
 - A couple of other components run on the configuration server machine.
 - The process server receives, optimizes, and sends replication data to cache storage account in Azure. It also handles automatic installation of the Mobility service on machines you want to

replicate, and performs automatic discovery of VMs on VMware servers.

- The master target server handles replication data during failback from Azure.
 - Set up includes registering the configuration server in the vault, downloading MySQL Server and VMware PowerCLI, and specifying the accounts created for automatic discovery and Mobility service installation.
4. **Target environment:** You set up your target Azure environment by specifying your Azure subscription and network settings.
5. **Replication policy:** You specify how replication should occur. Settings include how often recovery points are created and stored, and whether app-consistent snapshots should be created.
6. **Enable replication.** You enable replication for on-premises machines. If you created an account to install the Mobility service, then it will be installed when you enable replication for a machine.

Need more help?

- For a quick walkthrough of these steps, you can try out our [VMware tutorial](#), and [physical server walkthrough](#).
- [Learn more](#) about setting up your source environment.
- [Learn about](#) configuration server requirements, and setting up the configuration server with an OVF template for VMware replication. If for some reason you can't use a template, or you're replicating physical servers, [use these instructions](#).
- [Learn more](#) about target settings.
- [Get more information](#) about setting up a replication policy.
- [Learn](#) how to enable replication, and [exclude](#) disks from replication.

Something went wrong, how do I troubleshoot?

- As a first step, try [monitoring your deployment](#) to verify the status of replicated items, jobs, and infrastructure issues, and identify any errors.
- If you're unable to complete the initial replication, or ongoing replication isn't working as expected, [review this article](#) for common errors and troubleshooting tips.
- If you're having issues with the automatic installation of the Mobility service on machines you want to replicate, review common errors in [this article](#).
- If failover isn't working as expected, check common errors in [this article](#).
- If failback isn't working, check whether your issue appears in [this article](#).

Next steps

With replication now in place, you should [run a disaster recovery drill](#) to ensure that failover works as expected.

Common questions about VMware to Azure replication

1/23/2020 • 13 minutes to read • [Edit Online](#)

This article answers common questions that might come up when you deploy disaster recovery of on-premises VMware virtual machines (VMs) to Azure.

General

What do I need for VMware VM disaster recovery?

[Learn about the components involved](#) in disaster recovery of VMware VMs.

Can I use Site Recovery to migrate VMware VMs to Azure?

Yes. In addition to using Site Recovery to set up full disaster recovery for VMware VMs, you can also use Site Recovery to migrate on-premises VMware VMs to Azure. In this scenario, you replicate on-premises VMware VMs to Azure Storage. Then, you fail over from on-premises to Azure. After failover, your apps and workloads are available and running on Azure VMs. The process is like setting up full disaster recovery, except that in a migration you can't fail back from Azure.

Does my Azure account need permissions to create VMs?

If you're a subscription administrator, you have the replication permissions you need. If you're not an administrator, you need permissions to take these actions:

- Create an Azure VM in the resource group and virtual network you that you specify when you configure Site Recovery.
- Write to the selected storage account or managed disk based on your configuration.

[Learn more](#) about required permissions.

What applications can I replicate?

You can replicate any app or workload running on a VMware VM that meets the [replication requirements](#).

- Site Recovery supports application-aware replication, so that apps can be failed over and failed back to an intelligent state.
- Site Recovery integrates with Microsoft applications such as SharePoint, Exchange, Dynamics, SQL Server, and Active Directory. It also works closely with leading vendors, including Oracle, SAP, IBM, and Red Hat.

[Learn more](#) about workload protection.

Can I use a guest OS server license on Azure?

Yes, Microsoft Software Assurance customers can use [Azure Hybrid Benefit](#) to save on licensing costs for Windows Server machines that are migrated to Azure, or to use Azure for disaster recovery.

Security

What access to VMware servers does Site Recovery need?

Site Recovery needs access to VMware servers to:

- Set up a VMware VM running the Site Recovery configuration server.
- Automatically discover VMs for replication.

What access to VMware VMs does Site Recovery need?

- To replicate, a VMware VM must have the Site Recovery Mobility service installed and running. You can deploy the tool manually, or you can specify that Site Recovery do a push installation of the service when you enable replication for a VM.
- During replication, VMs communicate with Site Recovery as follows:
 - VMs communicate with the configuration server on HTTPS port 443 for replication management.
 - VMs send replication data to the process server on HTTPS port 9443. (This setting can be modified.)
 - If you enable multi-VM consistency, VMs communicate with each other over port 20004.

Is replication data sent to Site Recovery?

No, Site Recovery doesn't intercept replicated data and doesn't have any information about what's running on your VMs. Replication data is exchanged between VMware hypervisors and Azure Storage. Site Recovery has no ability to intercept that data. Only the metadata needed to orchestrate replication and failover is sent to the Site Recovery service.

Site Recovery is certified for ISO 27001:2013 and 27018, HIPAA, and DPA. It's in the process of SOC2 and FedRAMP JAB assessments.

Pricing

How do I calculate approximate charges for VMware disaster recovery?

Use the [pricing calculator](#) to estimate costs while using Site Recovery.

For a detailed estimate of costs, run the deployment planner tool for [VMware](#) and use the [cost estimation report](#).

Is there any difference in cost between replicating to storage or directly to managed disks?

Managed disks are charged slightly differently from storage accounts. [Learn more](#) about managed-disk pricing.

Is there any difference in cost when replicating to General Purpose v2 storage account?

You will typically see an increase in the transactions cost incurred on GPv2 storage accounts since Azure Site Recovery is transactions heavy. [Read more](#) to estimate the change.

Mobility service

Where can I find the Mobility service installers?

The installers are in the %ProgramData%\ASR\home\svsystems\pushinstallsvc\repository folder on the configuration server.

How do I install the Mobility service?

On each VM that you want to replicate, install the service by one of several methods:

- [Push installation](#)
- [Manual installation](#) from the UI or PowerShell
- Deployment by using a deployment tool such as [Configuration Manager](#)

Managed disks

Where does Site Recovery replicate data to?

Site Recovery replicates on-premises VMware VMs and physical servers to managed disks in Azure.

- The Site Recovery process server writes replication logs to a cache storage account in the target region.
- These logs are used to create recovery points on Azure-managed disks that have prefix of **asrseeddisk**.

- When failover occurs, the recovery point you select is used to create a new target managed disk. This managed disk is attached to the VM in Azure.
- VMs that were previously replicated to a storage account (before March 2019) aren't affected.

Can I replicate new machines to storage accounts?

No. Beginning in March 2019, in the Azure portal, you can replicate only to Azure managed disks.

Replication of new VMs to a storage account is available only by using PowerShell or the REST API (version 2018-01-10 or 2016-08-10).

What are the benefits of replicating to managed disks?

[Learn how](#) Site Recovery simplifies disaster recovery with managed disks.

Can I change the managed-disk type after a machine is protected?

Yes, you can easily [change the type of managed disk](#) for ongoing replications. Before changing the type, ensure that no shared access signature URL is generated on the managed disk:

1. Go to the **Managed Disk** resource on the Azure portal and check whether you have a shared access signature URL banner on the **Overview** blade.
2. If the banner is present, select it to cancel the ongoing export.
3. Change the type of the disk within the next few minutes. If you change the managed-disk type, wait for fresh recovery points to be generated by Azure Site Recovery.
4. Use the new recovery points for any test failover or failover in the future.

Can I switch replication from managed disks to unmanaged disks?

No. Switching from managed to unmanaged isn't supported.

Replication

What are the replicated VM requirements?

[Learn more](#) about support requirements for VMware VMs and physical servers.

How often can I replicate to Azure?

Replication is continuous when replicating VMware VMs to Azure.

Can I extend replication?

Extended or chained replication isn't supported. Request this feature in the [feedback forum](#).

Can I do an offline initial replication?

Offline replication isn't supported. Request this feature in the [feedback forum](#).

What is `asrseeddisk`?

For every source disk, data is replicated to a managed disk in Azure. This disk has the prefix of **asrseeddisk**. It stores the copy of the source disk and all the recovery point snapshots.

Can I exclude disks from replication?

Yes, you can exclude disks.

Can I replicate VMs that have dynamic disks?

Dynamic disks can be replicated. The operating system disk must be a basic disk.

If I use replication groups for multi-VM consistency, can I add a new VM to an existing replication group?

Yes, you can add new VMs to an existing replication group when you enable replication for them. However:

- You can't add a VM to an existing replication group after replication has begun.

- You can't create a replication group for existing VMs.

Can I modify VMs that are replicating by adding or resizing disks?

For VMware replication to Azure, you can modify disk size of source VMs. If you want to add new disks, you must add the disk and reenable protection for the VM.

Can I migrate on-premises machines to a new vCenter Server without impacting ongoing replication?

No. A change of VMware Vcenter or migration will impact ongoing replication. Set up Site Recovery with the new vCenter Server and enable replication for machines again.

Can I replicate to a cache or target storage account that has a virtual network (with Azure Firewalls) configured on it?

No, Site Recovery doesn't support replication to Azure Storage on virtual networks.

Component upgrade

My version of the Mobility services agent or configuration server is old, and my upgrade failed. What do I do?

Site Recovery follows the N-4 support model. [Learn more](#) about how to upgrade from very old versions.

Where can I find the release notes and update rollups for Azure Site Recovery?

[Learn about new updates](#), and [get rollup information](#).

Where can I find upgrade information for disaster recovery to Azure?

[Learn about upgrading](#).

Do I need to reboot source machines for each upgrade?

A reboot is recommended but not mandatory for each upgrade. [Learn more](#).

Configuration server

What does the configuration server do?

The configuration server runs the on-premises Site Recovery components, including:

- The configuration server itself. The server coordinates communications between on-premises components and Azure, and manages data replication.
- The process server, which acts as a replication gateway. This server:
 1. Receives replication data.
 2. Optimizes the data with caching, compression, and encryption.
 3. Sends the data to Azure Storage. The process server also does a push install of the Mobility Service on VMs and performs automatic discovery of on-premises VMware VMs.
- The master target server, which handles replication data during failback from Azure.

[Learn more](#) about the configuration server components and processes.

Where do I set up the configuration server?

You need a single, highly available, on-premises VMware VM for the configuration server. For physical server disaster recovery, install the configuration server on a physical machine.

What do I need for the configuration server?

Review the [prerequisites](#).

Can I manually set up the configuration server instead of using a template?

We recommend that you [create the configuration server VM](#) by using the latest version of the Open Virtualization

Format (OVF) template. If you can't use the template (for example, if you don't have access to the VMware server), [download](#) the setup file from the portal and set up the configuration server.

Can a configuration server replicate to more than one region?

No. To replicate to more than one region, you need a configuration server in each region.

Can I host a configuration server in Azure?

Although it's possible, the Azure VM running the configuration server would need to communicate with your on-premises VMware infrastructure and VMs. This communication adds latency and impacts ongoing replication.

How do I update the configuration server?

[Learn](#) how to update the configuration server.

- You can find the latest update information on the [Azure updates page](#).
- You can download the latest version from the portal. Or, you can download the latest version of the configuration server directly from the [Microsoft Download Center](#).
- If your version is more than four versions older than the current version, see the [support statement](#) for upgrade guidance.

Should I back up the configuration server?

We recommend taking regular scheduled backups of the configuration server.

- For successful failback, the VM being failed back must exist in the configuration server database.
- The configuration server must be running and in a connected state.
- [Learn more](#) about common configuration server management tasks.

When I'm setting up the configuration server, can I download and install MySQL manually?

Yes. Download MySQL and place it in the C:\Temp\ASRSetup folder. Then, install it manually. When you set up the configuration server VM and accept the terms, MySQL will be listed as **Already installed** in **Download and install**.

Can I avoid downloading MySQL but let Site Recovery install it?

Yes. Download the MySQL installer and place it in the C:\Temp\ASRSetup folder. When you set up the configuration server VM, accept the terms and select **Download and install**. The portal will use the installer that you added to install MySQL.

Can I use the configuration server VM for anything else?

No. Use the VM only for the configuration server.

Can I clone a configuration server and use it for orchestration?

No. Set up a fresh configuration server to avoid registration issues.

Can I change the vault in which the configuration server is registered?

No. After a vault is associated with the configuration server, it can't be changed. [Learn](#) about registering a configuration server with a different vault.

Can I use the same configuration server for disaster recovery of both VMware VMs and physical servers?

Yes, but note that physical machine can be failed back only to a VMware VM.

Where can I download the passphrase for the configuration server?

[Learn](#) how to download the passphrase.

Where can I download vault registration keys?

In the Recovery Services vault, select **Configuration Servers** in **Site Recovery Infrastructure > Manage**. Then, in **Servers**, select **Download registration key** to download the vault credentials file.

Can a single configuration server be used to protect multiple vCenter instances?

Yes, a single configuration server can protect VMs across multiple vCenters. There is no limit on how many vCenter instances can be added to the configuration server, however the limits for how many VMs a single configuration server can protect do apply.

Can a single configuration server protect multiple clusters within vCenter?

Yes, Azure Site Recovery can protect VMs across different clusters.

Process server

Why am I unable to select the process server when I enable replication?

Updates in versions 9.24 and later now display the [health of the process server when you enable replication](#). This feature helps to avoid process-server throttling and to minimize the use of unhealthy process servers.

How do I update the process server to version 9.24 or later for accurate health information?

Beginning with [version 9.24](#), more alerts have been added to indicate the health of the process server. [Update your Site Recovery components to version 9.24 or later](#) so that all alerts are generated.

Failover and failback

Can I use the on-premises process server for failback?

We strongly recommend creating a process server in Azure for failback purposes, to avoid data transfer latencies. Additionally, in case you separated the source VMs network with the Azure facing network in the configuration server, it's essential to use the process server created in Azure for failback.

Can I keep the IP address on failover?

Yes, you can keep the IP address on failover. Ensure that you specify the target IP address in the **Compute and Network** settings for the VM before failover. Also, shut down machines at the time of failover to avoid IP address conflicts during failback.

Can I change the target VM size or VM type before failover?

Yes, you can change the type or size of the VM at any time before failover. In the portal, use the **Compute and Network** settings for the replicated VM.

How far back can I recover?

For VMware to Azure, the oldest recovery point you can use is 72 hours.

How do I access Azure VMs after failover?

After failover, you can access Azure VMs over a secure internet connection, over a site-to-site VPN, or over Azure ExpressRoute. To connect, you must prepare several things. [Learn more](#).

Is failed-over data resilient?

Azure is designed for resilience. Site Recovery is engineered for failover to a secondary Azure datacenter, as required by the Azure service-level agreement (SLA). When failover occurs, we make sure your metadata and vaults remain in the same geographic region that you chose for your vault.

Is failover automatic?

[Failover](#) isn't automatic. You start a failover by making a single selection in the portal, or you can use [PowerShell](#) to trigger a failover.

Can I fail back to a different location?

Yes. If you failed over to Azure, you can fail back to a different location if the original one isn't available. [Learn more](#).

Why do I need a VPN or ExpressRoute with private peering to fail back?

When you fail back from Azure, data from Azure is copied back to your on-premises VM, and private access is required.

Automation and scripting

Can I set up replication with scripting?

Yes. You can automate Site Recovery workflows by using the Rest API, PowerShell, or the Azure SDK. [Learn more](#).

Performance and capacity

Can I throttle replication bandwidth?

Yes. [Learn more](#).

Next steps

- [Review](#) support requirements.
- [Set up](#) VMware to Azure replication.

Support matrix for disaster recovery of VMware VMs and physical servers to Azure

2/18/2020 • 15 minutes to read • [Edit Online](#)

This article summarizes supported components and settings for disaster recovery of VMware VMs and physical servers to Azure using [Azure Site Recovery](#).

- [Learn more](#) about VMware VM/physical server disaster recovery architecture.
- Follow our [tutorials](#) to try out disaster recovery.

Deployment scenarios

SCENARIO	DETAILS
Disaster recovery of VMware VMs	Replication of on-premises VMware VMs to Azure. You can deploy this scenario in the Azure portal or by using PowerShell .
Disaster recovery of physical servers	Replication of on-premises Windows/Linux physical servers to Azure. You can deploy this scenario in the Azure portal.

On-premises virtualization servers

SERVER	REQUIREMENTS	DETAILS
vCenter Server	Version 6.7, 6.5, 6.0, or 5.5	We recommend that you use a vCenter server in your disaster recovery deployment.
vSphere hosts	Version 6.7, 6.5, 6.0, or 5.5	We recommend that vSphere hosts and vCenter servers are located in the same network as the process server. By default the process server runs on the configuration server. Learn more .

Site Recovery configuration server

The configuration server is an on-premises machine that runs Site Recovery components, including the configuration server, process server, and master target server.

- For VMware VMs you set the configuration server by downloading an OVF template to create a VMware VM.
- For physical servers, you set up the configuration server machine manually.

COMPONENT	REQUIREMENTS
CPU cores	8
RAM	16 GB

COMPONENT	REQUIREMENTS
Number of disks	3 disks Disks include the OS disk, process server cache disk, and retention drive for failback.
Disk free space	600 GB of space for the process server cache.
Disk free space	600 GB of space for the retention drive.
Operating system	Windows Server 2012 R2, or Windows Server 2016 with Desktop experience If you plan to use the in-built Master Target of this appliance for failback, ensure that the OS version is same or higher than the replicated items.
Operating system locale	English (en-us)
PowerCLI	Not needed for configuration server version 9.14 or later.
Windows Server roles	Don't enable Active Directory Domain Services; Internet Information Services (IIS) or Hyper-V.
Group policies	- Prevent access to the command prompt. - Prevent access to registry editing tools. - Trust logic for file attachments. - Turn on Script Execution. - Learn more
IIS	Make sure you: - Don't have a preexisting default website - Enable anonymous authentication - Enable FastCGI setting - Don't have preexisting website/app listening on port 443
NIC type	VMXNET3 (when deployed as a VMware VM)
IP address type	Static
Ports	443 used for control channel orchestration 9443 for data transport

Replicated machines

Site Recovery supports replication of any workload running on a supported machine.

NOTE

The following table lists the support for machines with BIOS boot. Please refer to [Storage](#) section for support on UEFI based machines.

COMPONENT	DETAILS
Machine settings	Machines that replicate to Azure must meet Azure requirements .
Machine workload	Site Recovery supports replication of any workload running on a supported machine. Learn more .
Windows Server 2019	Supported from Update rollup 34 (version 9.22 of the Mobility service) onwards.
Windows Server 2016 64-bit	Supported for Server Core, Server with Desktop Experience.
Windows Server 2012 R2 / Windows Server 2012	Supported.
Windows Server 2008 R2 with SP1 onwards.	Supported. From version 9.30 of the Mobility service agent, you need servicing stack update (SSU) and SHA-2 update installed on machines running Windows 2008 R2 with SP1 or later. SHA-1 isn't supported from September 2019, and if SHA-2 code signing isn't enabled the agent extension won't install/upgrade as expected. Learn more about SHA-2 upgrade and requirements .
Windows Server 2008 with SP2 or later (64-bit/32-bit)	Supported for migration only. Learn more . From version 9.30 of the Mobility service agent, you need servicing stack update (SSU) and SHA-2 update installed on Windows 2008 SP2 machines. ISHA-1 isn't supported from September 2019, and if SHA-2 code signing isn't enabled the agent extension won't install/upgrade as expected. Learn more about SHA-2 upgrade and requirements .
Windows 10, Windows 8.1, Windows 8	Supported.
Windows 7 with SP1 64-bit	Supported from Update rollup 36 (version 9.22 of the Mobility service) onwards. From 9.30 of the Mobility service agent, you need servicing stack update (SSU) and SHA-2 update installed on Windows 7 SP1 machines. SHA-1 isn't supported from September 2019, and if SHA-2 code signing isn't enabled the agent extension won't install/upgrade as expected. Learn more about SHA-2 upgrade and requirements .

COMPONENT	DETAILS
Linux	<p>Only 64-bit system is supported. 32-bit system isn't supported.</p> <p>Every Linux server should have Linux Integration Services (LIS) components installed. It is required to boot the server in Azure after test failover/failover. If LIS components are missing, ensure to install the components before enabling replication for the machines to boot in Azure.</p> <p>Site Recovery orchestrates failover to run Linux servers in Azure. However Linux vendors might limit support to only distribution versions that haven't reached end-of-life.</p> <p>On Linux distributions, only the stock kernels that are part of the distribution minor version release/update are supported.</p> <p>Upgrading protected machines across major Linux distribution versions isn't supported. To upgrade, disable replication, upgrade the operating system, and then enable replication again.</p> <p>Learn more about support for Linux and open-source technology in Azure.</p>
Linux Red Hat Enterprise	<p>5.2 to 5.11 6.1 to 6.10 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 8.0, 8.1</p> <p>Servers running Red Hat Enterprise Linux 5.2-5.11 & 6.1-6.10 do not have Linux Integration Services (LIS) components pre-installed. Ensure to install the components before enabling replication for the machines to boot in Azure.</p>
Linux: CentOS	<p>5.2 to 5.11 6.1 to 6.10 7.0 to 7.6 8.0 to 8.1</p> <p>Servers running CentOS 5.2-5.11 & 6.1-6.10 do not have Linux Integration Services (LIS) components pre-installed. Ensure to install the components before enabling replication for the machines to boot in Azure.</p>
Ubuntu	<p>Ubuntu 14.04 LTS server (review supported kernel versions)</p> <p>Ubuntu 16.04 LTS server (review supported kernel versions)</p> <p>Ubuntu 18.04 LTS server (review supported kernel versions)</p>
Debian	Debian 7/Debian 8 (review supported kernel versions)
SUSE Linux	<p>SUSE Linux Enterprise Server 12 SP1, SP2, SP3, SP4 (review supported kernel versions)</p> <p>SUSE Linux Enterprise Server 15, 15 SP1 (review supported kernel versions)</p> <p>SUSE Linux Enterprise Server 11 SP3, SUSE Linux Enterprise Server 11 SP4</p> <p>Upgrading replicated machines from SUSE Linux Enterprise Server 11 SP3 to SP4 isn't supported. To upgrade, disable replication and re-enable after the upgrade.</p>

COMPONENT	DETAILS
Oracle Linux	<p>6.4, 6.5, 6.6, 6.7, 6.8, 6.9, 6.10, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7</p> <p>Running the Red Hat compatible kernel or Unbreakable Enterprise Kernel Release 3, 4 & 5 (UEK3, UEK4, UEK5)</p>

NOTE

For each of the Windows versions, Azure Site Recovery only supports [Long-Term Servicing Channel \(LTSC\)](#) builds. [Semi-Annual Channel](#) releases are currently unsupported at this time.

Ubuntu kernel versions

SUPPORTED RELEASE	MOBILITY SERVICE VERSION	KERNEL VERSION
14.04 LTS	9.32	3.13.0-24-generic to 3.13.0-170-generic, 3.16.0-25-generic to 3.16.0-77-generic, 3.19.0-18-generic to 3.19.0-80-generic, 4.2.0-18-generic to 4.2.0-42-generic, 4.4.0-21-generic to 4.4.0-148-generic, 4.15.0-1023-azure to 4.15.0-1045-azure
14.04 LTS	9.31	3.13.0-24-generic to 3.13.0-170-generic, 3.16.0-25-generic to 3.16.0-77-generic, 3.19.0-18-generic to 3.19.0-80-generic, 4.2.0-18-generic to 4.2.0-42-generic, 4.4.0-21-generic to 4.4.0-148-generic, 4.15.0-1023-azure to 4.15.0-1045-azure
14.04 LTS	9.30	3.13.0-24-generic to 3.13.0-170-generic, 3.16.0-25-generic to 3.16.0-77-generic, 3.19.0-18-generic to 3.19.0-80-generic, 4.2.0-18-generic to 4.2.0-42-generic, 4.4.0-21-generic to 4.4.0-148-generic, 4.15.0-1023-azure to 4.15.0-1045-azure
14.04 LTS	9.29	3.13.0-24-generic to 3.13.0-170-generic, 3.16.0-25-generic to 3.16.0-77-generic, 3.19.0-18-generic to 3.19.0-80-generic, 4.2.0-18-generic to 4.2.0-42-generic, 4.4.0-21-generic to 4.4.0-148-generic, 4.15.0-1023-azure to 4.15.0-1045-azure

SUPPORTED RELEASE	MOBILITY SERVICE VERSION	KERNEL VERSION
16.04 LTS	9.32	4.4.0-21-generic to 4.4.0-171-generic, 4.8.0-34-generic to 4.8.0-58-generic, 4.10.0-14-generic to 4.10.0-42-generic, 4.11.0-13-generic to 4.11.0-14-generic, 4.13.0-16-generic to 4.13.0-45-generic, 4.15.0-13-generic to 4.15.0-74-generic 4.11.0-1009-azure to 4.11.0-1016- azure, 4.13.0-1005-azure to 4.13.0-1018- azure 4.15.0-1012-azure to 4.15.0-1066- azure
16.04 LTS	9.31	4.4.0-21-generic to 4.4.0-170-generic, 4.8.0-34-generic to 4.8.0-58-generic, 4.10.0-14-generic to 4.10.0-42-generic, 4.11.0-13-generic to 4.11.0-14-generic, 4.13.0-16-generic to 4.13.0-45-generic, 4.15.0-13-generic to 4.15.0-72-generic 4.11.0-1009-azure to 4.11.0-1016- azure, 4.13.0-1005-azure to 4.13.0-1018- azure 4.15.0-1012-azure to 4.15.0-1063- azure
16.04 LTS	9.30	4.4.0-21-generic to 4.4.0-166-generic, 4.8.0-34-generic to 4.8.0-58-generic, 4.10.0-14-generic to 4.10.0-42-generic, 4.11.0-13-generic to 4.11.0-14-generic, 4.13.0-16-generic to 4.13.0-45-generic, 4.15.0-13-generic to 4.15.0-66-generic 4.11.0-1009-azure to 4.11.0-1016- azure, 4.13.0-1005-azure to 4.13.0-1018- azure 4.15.0-1012-azure to 4.15.0-1061- azure
16.04 LTS	9.29	4.4.0-21-generic to 4.4.0-164-generic, 4.8.0-34-generic to 4.8.0-58-generic, 4.10.0-14-generic to 4.10.0-42-generic, 4.11.0-13-generic to 4.11.0-14-generic, 4.13.0-16-generic to 4.13.0-45-generic, 4.15.0-13-generic to 4.15.0-64-generic 4.11.0-1009-azure to 4.11.0-1016- azure, 4.13.0-1005-azure to 4.13.0-1018- azure 4.15.0-1012-azure to 4.15.0-1059- azure

SUPPORTED RELEASE	MOBILITY SERVICE VERSION	KERNEL VERSION
18.04 LTS	9.32	4.15.0-20-generic to 4.15.0-74-generic 4.18.0-13-generic to 4.18.0-25-generic 5.0.0-15-generic to 5.0.0-37-generic 5.3.0-19-generic to 5.3.0-24-generic 4.15.0-1009-azure to 4.15.0-1037-azure 4.18.0-1006-azure to 4.18.0-1025-azure 5.0.0-1012-azure to 5.0.0-1028-azure 5.3.0-1007-azure to 5.3.0-1009-azure
18.04 LTS	9.31	4.15.0-20-generic to 4.15.0-72-generic 4.18.0-13-generic to 4.18.0-25-generic 5.0.0-15-generic to 5.0.0-37-generic 5.3.0-19-generic to 5.3.0-24-generic 4.15.0-1009-azure to 4.15.0-1037-azure 4.18.0-1006-azure to 4.18.0-1025-azure 5.0.0-1012-azure to 5.0.0-1025-azure 5.3.0-1007-azure
18.04 LTS	9.30	4.15.0-20-generic to 4.15.0-66-generic 4.18.0-13-generic to 4.18.0-25-generic 5.0.0-15-generic to 5.0.0-32-generic 4.15.0-1009-azure to 4.15.0-1037-azure 4.18.0-1006-azure to 4.18.0-1025-azure 5.0.0-1012-azure to 5.0.0-1023-azure
18.04 LTS	9.29	4.15.0-20-generic to 4.15.0-62-generic 4.18.0-13-generic to 4.18.0-25-generic 5.0.0-15-generic to 5.0.0-27-generic 4.15.0-1009-azure to 4.15.0-1037-azure 4.18.0-1006-azure to 4.18.0-1025-azure 5.0.0-1012-azure to 5.0.0-1018-azure

Debian kernel versions

SUPPORTED RELEASE	MOBILITY SERVICE VERSION	KERNEL VERSION
Debian 7	9.29 , 9.30 , 9.31 , 9.32	3.2.0-4-amd64 to 3.2.0-6-amd64, 3.16.0-0.bpo.4-amd64
Debian 8	9.30 , 9.31 , 9.32	3.16.0-4-amd64 to 3.16.0-10-amd64, 4.9.0-0.bpo.4-amd64 to 4.9.0-0.bpo.11-amd64
Debian 8	9.29	3.16.0-4-amd64 to 3.16.0-10-amd64, 4.9.0-0.bpo.4-amd64 to 4.9.0-0.bpo.9-amd64

SUSE Linux Enterprise Server 12 supported kernel versions

RELEASE	MOBILITY SERVICE VERSION	KERNEL VERSION
SUSE Linux Enterprise Server 12 (SP1,SP2,SP3,SP4)	9.32	All stock SUSE 12 SP1,SP2,SP3,SP4 kernels are supported. 4.4.138-4.7-azure to 4.4.180-4.31-azure, 4.12.14-6.3-azure to 4.12.14-6.34-azure
SUSE Linux Enterprise Server 12 (SP1,SP2,SP3,SP4)	9.31	All stock SUSE 12 SP1,SP2,SP3,SP4 kernels are supported. 4.4.138-4.7-azure to 4.4.180-4.31-azure, 4.12.14-6.3-azure to 4.12.14-6.29-azure
SUSE Linux Enterprise Server 12 (SP1,SP2,SP3,SP4)	9.30	All stock SUSE 12 SP1,SP2,SP3,SP4 kernels are supported. 4.4.138-4.7-azure to 4.4.180-4.31-azure, 4.12.14-6.3-azure to 4.12.14-6.26-azure
SUSE Linux Enterprise Server 12 (SP1,SP2,SP3,SP4)	9.29	All stock SUSE 12 SP1,SP2,SP3,SP4 kernels are supported. 4.4.138-4.7-azure to 4.4.180-4.31-azure, 4.12.14-6.3-azure to 4.12.14-6.23-azure

SUSE Linux Enterprise Server 15 supported kernel versions

RELEASE	MOBILITY SERVICE VERSION	KERNEL VERSION
SUSE Linux Enterprise Server 15 and 15 SP1	9.32	All stock SUSE 15 and 15 kernels are supported. 4.12.14-5.5-azure to 4.12.14-8.22-azure

Linux file systems/guest storage

COMPONENT	SUPPORTED
File systems	ext3, ext4, XFS
Volume manager	- LVM is supported. - /boot on LVM is supported from Update Rollup 31 (version 9.20 of the Mobility service) onwards. It isn't supported in earlier Mobility service versions. - Multiple OS disks aren't supported.
Paravirtualized storage devices	Devices exported by paravirtualized drivers aren't supported.
Multi-queue block IO devices	Not supported.
Physical servers with the HP CCISST storage controller	Not supported.

COMPONENT	SUPPORTED
Device/Mount point naming convention	<p>Device name or mount point name should be unique. Ensure that no two devices/mount points have case-sensitive names. For example naming devices for the same VM as <i>device1</i> and <i>Device1</i> isn't supported.</p>
Directories	<p>If you're running a version of the Mobility service earlier than version 9.20 (released in Update Rollup 31), then these restrictions apply:</p> <ul style="list-style-type: none"> - These directories (if set up as separate partitions/file-systems) must be on the same OS disk on the source server: <code>/root</code>, <code>/boot</code>, <code>/usr</code>, <code>/usr/local</code>, <code>/var</code>, <code>/etc</code>. - The <code>/boot</code> directory should be on a disk partition and not be an LVM volume. <p>From version 9.20 onwards, these restrictions don't apply.</p>
Boot directory	<ul style="list-style-type: none"> - Boot disks mustn't be in GPT partition format. This is an Azure architecture limitation. GPT disks are supported as data disks. <p>Multiple boot disks on a VM aren't supported</p> <ul style="list-style-type: none"> - <code>/boot</code> on an LVM volume across more than one disk isn't supported. - A machine without a boot disk can't be replicated.
Free space requirements	<p>2 GB on the <code>/root</code> partition</p> <p>250 MB on the installation folder</p>
XFSv5	<p>XFSv5 features on XFS file systems, such as metadata checksum, are supported (Mobility service version 9.10 onwards).</p> <p>Use the <code>xfs_info</code> utility to check the XFS superblock for the partition. If <code>fstype</code> is set to 1, then XFSv5 features are in use.</p>
BTRFS	<p>BTRFS is supported from Update Rollup 34 (version 9.22 of the Mobility service) onwards. BTRFS isn't supported if:</p> <ul style="list-style-type: none"> - The BTRFS file system subvolume is changed after enabling protection. - The BTRFS file system is spread over multiple disks. - The BTRFS file system supports RAID.

VM/Disk management

ACTION	DETAILS
--------	---------

ACTION	DETAILS
Resize disk on replicated VM	<p>Supported on the source VM before failover, directly in the VM properties. No need to disable/re-enable replication.</p> <p>If you change the source VM after failover, the changes aren't captured.</p> <p>If you change the disk size on the Azure VM after failover, when you fail back, Site Recovery creates a new VM with the updates.</p>
Add disk on replicated VM	<p>Not supported.</p> <p>Disable replication for the VM, add the disk, and then re-enable replication.</p>

Network

COMPONENT	SUPPORTED
Host network NIC Teaming	<p>Supported for VMware VMs.</p> <p>Not supported for physical machine replication.</p>
Host network VLAN	Yes.
Host network IPv4	Yes.
Host network IPv6	No.
Guest/server network NIC Teaming	No.
Guest/server network IPv4	Yes.
Guest/server network IPv6	No.
Guest/server network static IP (Windows)	Yes.
Guest/server network static IP (Linux)	<p>Yes.</p> <p>VMs are configured to use DHCP on failback.</p>
Guest/server network multiple NICs	Yes.

Azure VM network (after failover)

COMPONENT	SUPPORTED
Azure ExpressRoute	Yes
ILB	Yes
ELB	Yes

COMPONENT	SUPPORTED
Azure Traffic Manager	Yes
Multi-NIC	Yes
Reserved IP address	Yes
IPv4	Yes
Retain source IP address	Yes
Azure virtual network service endpoints	Yes
Accelerated networking	No

Storage

COMPONENT	SUPPORTED
Dynamic disk	OS disk must be a basic disk. Data disks can be dynamic disks
Docker disk configuration	No
Host NFS	Yes for VMware No for physical servers
Host SAN (iSCSI/FC)	Yes
Host vSAN	Yes for VMware N/A for physical servers
Host multipath (MPIO)	Yes, tested with Microsoft DSM, EMC PowerPath 5.7 SP4, EMC PowerPath DSM for CLARiiON
Host Virtual Volumes (VVols)	Yes for VMware N/A for physical servers
Guest/server VMDK	Yes
Guest/server shared cluster disk	No
Guest/server encrypted disk	No
Guest/server NFS	No

COMPONENT	SUPPORTED
Guest/server iSCSI	For Migration - Yes For Disaster Recovery - No, iSCSI will fallback as an attached disk to the VM
Guest/server SMB 3.0	No
Guest/server RDM	Yes N/A for physical servers
Guest/server disk > 1 TB	Yes, disk must be larger than 1024 MB Up to 8,192 GB when replicating to managed disks (9.26 version onwards) Up to 4,095 GB when replicating to storage accounts
Guest/server disk with 4K logical and 4k physical sector size	No
Guest/server disk with 4K logical and 512-bytes physical sector size	No
Guest/server volume with striped disk >4 TB	Yes
Logical volume management (LVM)	
Guest/server - Storage Spaces	No
Guest/server hot add/remove disk	No
Guest/server - exclude disk	Yes
Guest/server multipath (MPIO)	No
Guest/server GPT partitions	Five partitions are supported from Update Rollup 37 (version 9.25 of the Mobility service) onwards. Previously four were supported.
ReFS	Resilient File System is supported with Mobility service version 9.23 or higher
Guest/server EFI/UEFI boot	- Supported for Windows Server 2012 or later, SLES 12 SP4 and RHEL 8.0 with mobility agent version 9.30 onwards - Secure UEFI boot type is not supported.

Replication channels

TYPE OF REPLICATION	SUPPORTED
Offloaded Data Transfers (ODX)	No
Offline Seeding	No

Type of replication	Supported
Azure Data Box	No

Azure storage

Component	Supported
Locally redundant storage	Yes
Geo-redundant storage	Yes
Read-access geo-redundant storage	Yes
Cool storage	No
Hot storage	No
Block blobs	No
Encryption-at-rest (SSE)	Yes
Encryption-at-rest (CMK)	Yes (via Powershell Az 3.3.0 module onwards)
Premium storage	Yes
Import/export service	No
Azure Storage firewalls for VNets	Yes. Configured on target storage/cache storage account (used to store replication data).
General-purpose v2 storage accounts (hot and cool tiers)	Yes (Transaction costs are substantially higher for V2 compared to V1)

Azure compute

Feature	Supported
Availability sets	Yes
Availability zones	No
HUB	Yes
Managed disks	Yes

Azure VM requirements

On-premises VMs replicated to Azure must meet the Azure VM requirements summarized in this table. When Site Recovery runs a prerequisites check for replication, the check will fail if some of the requirements aren't met.

Component	Requirements	Details
Guest operating system	Verify supported operating systems for replicated machines.	Check fails if unsupported.
Guest operating system architecture	64-bit.	Check fails if unsupported.
Operating system disk size	Up to 2,048 GB.	Check fails if unsupported.
Operating system disk count	1	Check fails if unsupported.
Data disk count	64 or less.	Check fails if unsupported.
Data disk size	Up to 8,192 GB when replicating to managed disk (9.26 version onwards) Up to 4,095 GB when replicating to storage account	Check fails if unsupported.
Network adapters	Multiple adapters are supported.	
Shared VHD	Not supported.	Check fails if unsupported.
FC disk	Not supported.	Check fails if unsupported.
BitLocker	Not supported.	BitLocker must be disabled before you enable replication for a machine.
VM name	From 1 to 63 characters. Restricted to letters, numbers, and hyphens. The machine name must start and end with a letter or number.	Update the value in the machine properties in Site Recovery.

Resource group limits

To understand the number of virtual machines that can be protected under a single resource group, refer to the article on [subscription limits and quotas](#)

Churn limits

The following table provides the Azure Site Recovery limits.

- These limits are based on our tests, but don't cover all possible app I/O combinations.
- Actual results can vary based on your application I/O mix.
- For best results, we strongly recommend that you run the [Deployment Planner tool](#), and perform extensive application testing using test failovers to get the true performance picture for your app.

Replication Target	Average Source Disk I/O Size	Average Source Disk Data Churn	Total Source Disk Data Churn per Day
Standard storage	8 KB	2 MB/s	168 GB per disk

REPLICATION TARGET	AVERAGE SOURCE DISK I/O SIZE	AVERAGE SOURCE DISK DATA CHURN	TOTAL SOURCE DISK DATA CHURN PER DAY
Premium P10 or P15 disk	8 KB	2 MB/s	168 GB per disk
Premium P10 or P15 disk	16 KB	4 MB/s	336 GB per disk
Premium P10 or P15 disk	32 KB or greater	8 MB/s	672 GB per disk
Premium P20 or P30 or P40 or P50 disk	8 KB	5 MB/s	421 GB per disk
Premium P20 or P30 or P40 or P50 disk	16 KB or greater	20 MB/s	1684 GB per disk

SOURCE DATA CHURN	MAXIMUM LIMIT
Peak data churn across all disks on a VM	54 MB/s
Maximum data churn per day supported by a Process Server	2 TB

- These are average numbers assuming a 30 percent I/O overlap.
- Site Recovery is capable of handling higher throughput based on overlap ratio, larger write sizes, and actual workload I/O behavior.
- These numbers assume a typical backlog of approximately five minutes. That is, after data is uploaded, it is processed and a recovery point is created within five minutes.

Vault tasks

ACTION	SUPPORTED
Move vault across resource groups	No
Move vault within and across subscriptions	No
Move storage, network, Azure VMs across resource groups	No
Move storage, network, Azure VMs within and across subscriptions.	No

Obtain latest components

NAME	DESCRIPTION	DETAILS
Configuration server	Installed on-premises. Coordinates communications between on-premises VMware servers or physical machines, and Azure.	- Learn about the configuration server. - Learn about upgrading to the latest version. - Learn about setting up the configuration server.

NAME	DESCRIPTION	DETAILS
Process server	<p>Installed by default on the configuration server.</p> <p>Receives replication data, optimizes it with caching, compression, and encryption, and sends it to Azure.</p> <p>As your deployment grows, you can add additional process servers to handle larger volumes of replication traffic.</p>	<ul style="list-style-type: none"> - Learn about the process server. - Learn about upgrading to the latest version. - Learn about setting up scale-out process servers.
Mobility Service	<p>Installed on VMware VM or physical servers you want to replicate.</p> <p>Coordinates replication between on-premises VMware servers/physical servers and Azure.</p>	<ul style="list-style-type: none"> - Learn about the Mobility service. - Learn about upgrading to the latest version.

Next steps

[Learn how](#) to prepare Azure for disaster recovery of VMware VMs.

About Site Recovery components (configuration, process, master target)

11/12/2019 • 2 minutes to read • [Edit Online](#)

This article describes the configuration, process, and master target servers used when replicating VMware VMs and physical servers to Azure with the [Site Recovery](#) service.

Configuration server

For disaster recovery of on-premises VMware VMs and physical servers, you need a Site Recovery configuration server deployed on-premises.

SETTING	DETAILS	LINKS
Components	<p>The configuration server machine runs all on-premises Site Recovery components, which include the configuration server, process server, and master target server.</p> <p>When you set up the configuration server, all the components are installed automatically.</p>	Read the configuration server FAQ.
Role	<p>The configuration server coordinates communications between on-premises and Azure, and manages data replication.</p>	Learn more about the architecture for VMware and physical server disaster recovery to Azure.
VMware requirements	<p>For disaster recovery of on-premises VMware VMs, you must install and run the configuration server as a on-premises, highly available VMware VM.</p>	Learn about the prerequisites.
VMware deployment	<p>We recommend that you deploy the configuration server using a downloaded OVA template. This method provides a simply way to set up a configuration server that complies with all requirements and prerequisites.</p> <p>If for some reason you're unable to deploy a VMware VM using an OVA template, you can set up the configuration server machines manually, as described below for physical machine disaster recovery.</p>	Deploy with an OVA template.
Physical server requirements	<p>For disaster recovery on on-premises physical servers, you deploy the configuration server manually.</p>	Learn about the prerequisites.

Setting	Details	Links
Physical server deployment	If it can't be installed as a VMware VM, you can install it on a physical server.	Deploy the configuration server manually.

Process server

Setting	Details	Links
Deployment	For disaster recovery and replication of on-premises VMware VMs and physical servers, you need a process server on-premises. By default, the process server is installed on the configuration server when you deploy it.	Learn more .
Role (on-premises)	<ul style="list-style-type: none"> - Receives replication data from machines enabled for replication. - Optimizes replication data with caching, compression, and encryption, and sends it to Azure Storage. - Performs a push installation of the Site Recovery Mobility Service on on-premises VMware VMs and physical servers that you want to replicate. - Performs automatic discovery of on-premises machines. 	Learn more .
Role (failback from Azure)	<p>After failover from your on-premises site, you set up a process server in Azure, as an Azure VM, to handle failback to your on-premises location.</p> <p>The process server in Azure is temporary. The Azure VM can be deleted after failback is done.</p>	Learn more .
Scaling	<p>For larger deployments, on-premises you can set up additional, scale-out process servers. Additional servers scale out capacity, by handling larger numbers of replicating machines, and larger volumes of replication traffic.</p> <p>You can move machines between two process servers, in order to load balance replication traffic.</p>	Learn more ,

Master target server

The master target server handles replication data during failback from Azure.

- It's installed by default on the configuration server.
- For large deployments, you can add an additional, separate master target server for failback.

Next steps

- Review the [architecture](#) for disaster recovery of VMware VMs and physical servers.

- Review the [requirements and prerequisites](#) for disaster recovery of VMware VMs and physical servers to Azure.

Configuration server requirements for VMware disaster recovery to Azure

11/6/2019 • 3 minutes to read • [Edit Online](#)

You deploy an on-premises configuration server when you use [Azure Site Recovery](#) for disaster recovery of VMware VMs and physical servers to Azure.

- The configuration server coordinates communications between on-premises VMware and Azure. It also manages data replication.
- [Learn more](#) about the configuration server components and processes.

Configuration server deployment

For disaster recovery of VMware VMs to Azure, you deploy the configuration server as a VMware VM.

- Site Recovery provides an OVA template that you download from the Azure portal, and import into vCenter Server to set up the configuration server VM.
- When you deploy the configuration server using the OVA template, the VM automatically complies with the requirements listed in this article.
- We strongly recommend that you set up the configuration server using the OVA template. However, if you're setting up disaster recovery for VMware VMs and can't use the OVA template, you can deploy the configuration server using [these instructions provided](#).
- If you're deploying the configuration server for disaster recovery of on-premises physical machines to Azure, follow the instructions in [this article](#).

Configuration and process server requirements

Hardware requirements

COMPONENT	REQUIREMENT
CPU cores	8
RAM	16 GB
Number of disks	3, including the OS disk, process server cache disk, and retention drive for failback
Free disk space (process server cache)	600 GB
Free disk space (retention disk)	600 GB

Software requirements

COMPONENT	REQUIREMENT

COMPONENT	REQUIREMENT
Operating system	Windows Server 2012 R2 Windows Server 2016
Operating system locale	English (en-us)
Windows Server roles	Don't enable these roles: - Active Directory Domain Services - Internet Information Services - Hyper-V
Group policies	Don't enable these group policies: - Prevent access to the command prompt. - Prevent access to registry editing tools. - Trust logic for file attachments. - Turn on Script Execution. Learn more
IIS	- No pre-existing default website - No pre-existing website/application listening on port 443 - Enable anonymous authentication - Enable FastCGI setting
FIPS (Federal Information Processing Standards)	Do not enable FIPS mode

Network requirements

COMPONENT	REQUIREMENT
IP address type	Static
Ports	443 (Control channel orchestration) 9443 (Data transport)
NIC type	VMXNET3 (if the configuration server is a VMware VM)
Internet access (the server needs access to the following URLs, directly or via proxy):	
*.backup.windowsazure.com	Used for replicated data transfer and coordination
*.store.core.windows.net	Used for replicated data transfer and coordination
*.blob.core.windows.net	Used to access storage account that stores replicated data
*.hypervrecoverymanager.windowsazure.com	Used for replication management operations and coordination
https://management.azure.com	Used for replication management operations and coordination
*.services.visualstudio.com	Used for telemetry purposes (optional)

COMPONENT	REQUIREMENT
time.nist.gov	Used to check time synchronization between system and global time
time.windows.com	Used to check time synchronization between system and global time
<ul style="list-style-type: none"> • https://login.microsoftonline.com • https://secure.aadcdn.microsoftonline-p.com • https://login.live.com • https://graph.windows.net • https://login.windows.net • https://www.live.com • https://www.microsoft.com 	OVF setup needs access to these URLs. They're used for access control and identity management by Azure Active Directory.
https://dev.mysql.com/get/Downloads/MySQLInstaller/mysql-installer-community-5.7.20.0.msi	To complete MySQL download. In a few regions, the download might be redirected to the CDN URL. Ensure that the CDN URL is also whitelisted, if necessary.

Required software

COMPONENT	REQUIREMENT
VMware vSphere PowerCLI	PowerCLI version 6.0 should be installed if the Configuration Server is running on a VMware VM.
MYSQL	MySQL should be installed. You can install manually, or Site Recovery can install it. (Refer to configure settings for more information)

Sizing and capacity requirements

The following table summarizes capacity requirements for the configuration server. If you're replicating multiple VMware VMs, review the [capacity planning considerations](#) and run the [Azure Site Recovery Deployment Planner tool](#).

CPU	MEMORY	CACHE DISK	DATA CHANGE RATE	REPLICATED MACHINES
8 vCPUs 2 sockets * 4 cores @ 2.5 GHz	16 GB	300 GB	500 GB or less	< 100 machines
12 vCPUs 2 socks * 6 cores @ 2.5 GHz	18 GB	600 GB	500 GB-1 TB	100 to 150 machines

CPU	MEMORY	CACHE DISK	DATA CHANGE RATE	REPLICATED MACHINES
16 vCPUs 2 socks * 8 cores @ 2.5 GHz	32 GB	1 TB	1-2 TB	150 -200 machines

Next steps

Set up disaster recovery of [VMware VMs](#) to Azure.

VMware to Azure disaster recovery architecture

1/22/2020 • 5 minutes to read • [Edit Online](#)

This article describes the architecture and processes used when you deploy disaster recovery replication, failover, and recovery of VMware virtual machines (VMs) between an on-premises VMware site and Azure using the [Azure Site Recovery](#) service.

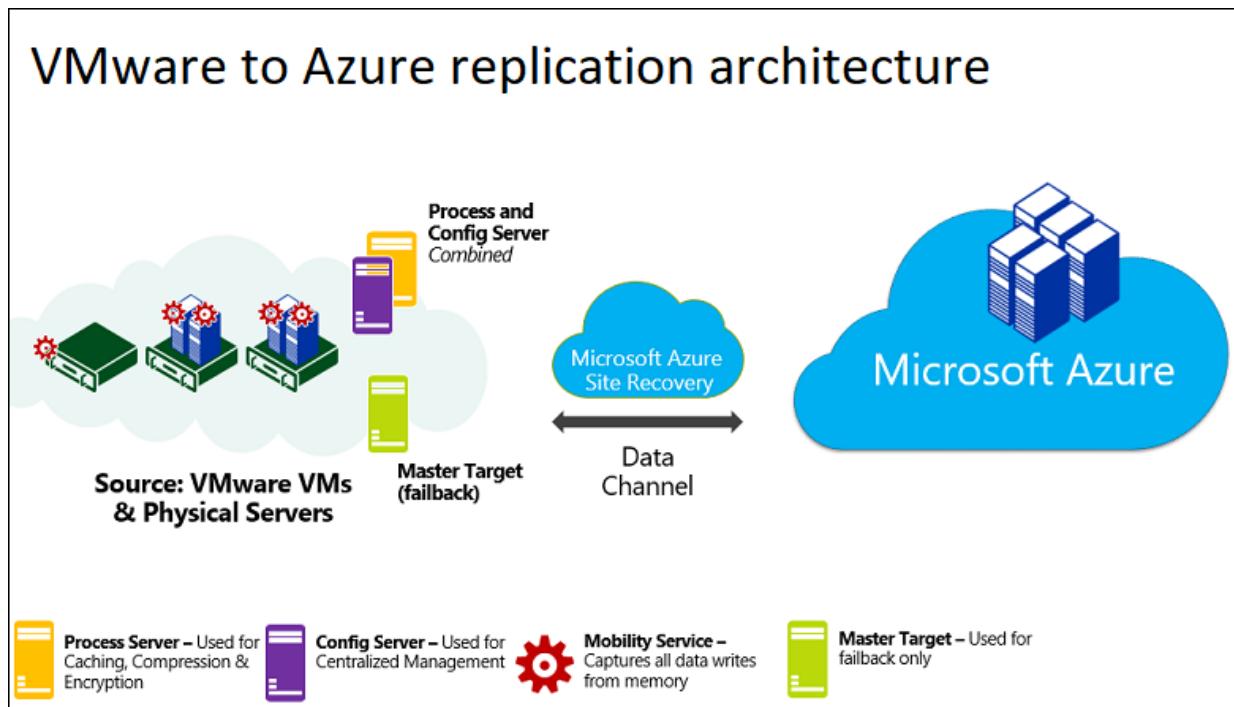
Architectural components

The following table and graphic provide a high-level view of the components used for VMware disaster recovery to Azure.

COMPONENT	REQUIREMENT	DETAILS
Azure	An Azure subscription, Azure Storage account for cache, Managed Disk and Azure network.	Replicated data from on-premises VMs is stored in Azure storage. Azure VMs are created with the replicated data when you run a failover from on-premises to Azure. The Azure VMs connect to the Azure virtual network when they're created.
Configuration server machine	<p>A single on-premises machine. We recommend that you run it as a VMware VM that can be deployed from a downloaded OVF template.</p> <p>The machine runs all on-premises Site Recovery components, which include the configuration server, process server, and master target server.</p>	<p>Configuration server: Coordinates communications between on-premises and Azure, and manages data replication.</p> <p>Process server: Installed by default on the configuration server. It receives replication data; optimizes it with caching, compression, and encryption; and sends it to Azure Storage. The process server also installs Azure Site Recovery Mobility Service on VMs you want to replicate, and performs automatic discovery of on-premises machines. As your deployment grows, you can add additional, separate process servers to handle larger volumes of replication traffic.</p> <p>Master target server: Installed by default on the configuration server. It handles replication data during failback from Azure. For large deployments, you can add an additional, separate master target server for failback.</p>
VMware servers	VMware VMs are hosted on on-premises vSphere ESXi servers. We recommend a vCenter server to manage the hosts.	During Site Recovery deployment, you add VMware servers to the Recovery Services vault.

COMPONENT	REQUIREMENT	DETAILS
Replicated machines	Mobility Service is installed on each VMware VM that you replicate.	We recommend that you allow automatic installation from the process server. Alternatively, you can install the service manually or use an automated deployment method, such as Configuration Manager.

VMware to Azure architecture



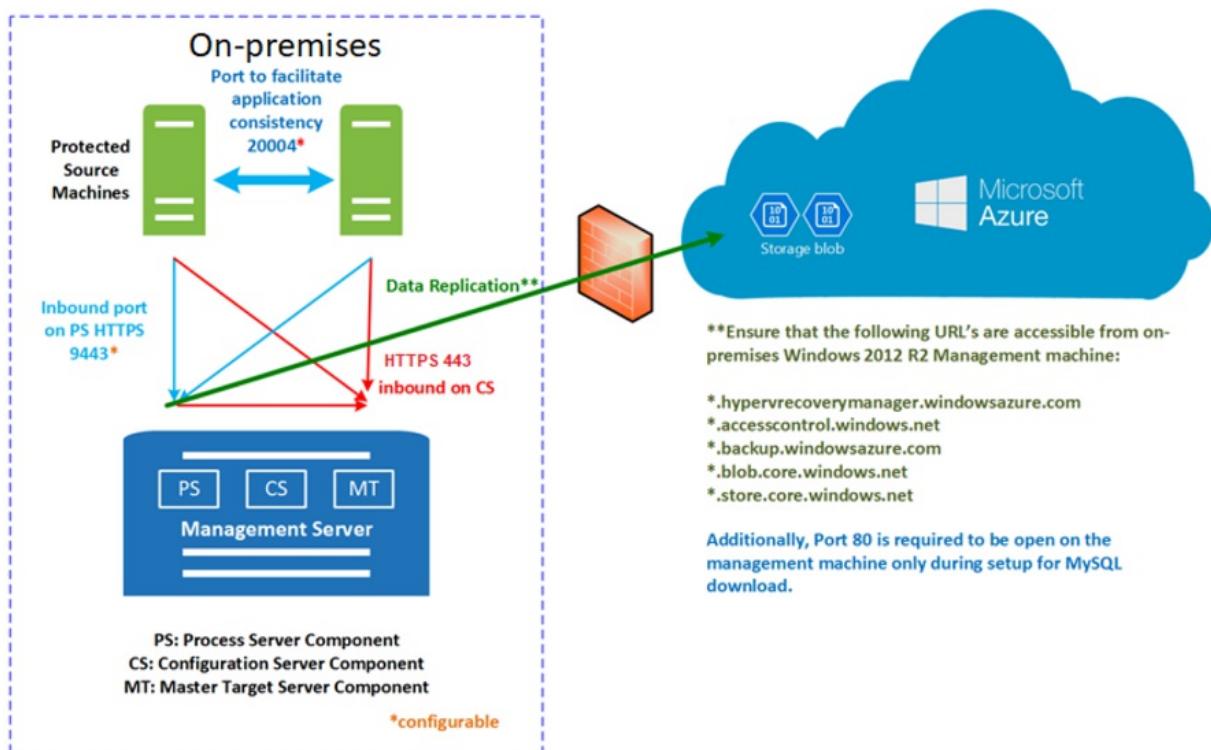
Replication process

- When you enable replication for a VM, initial replication to Azure storage begins, using the specified replication policy. Note the following:
 - For VMware VMs, replication is block-level, near-continuous, using the Mobility service agent running on the VM.
 - Any replication policy settings are applied:
 - RPO threshold**. This setting does not affect replication. It helps with monitoring. An event is raised, and optionally an email sent, if the current RPO exceeds the threshold limit that you specify.
 - Recovery point retention**. This setting specifies how far back in time you want to go when a disruption occurs. Maximum retention on premium storage is 24 hours. On standard storage it's 72 hours.
 - App-consistent snapshots**. App-consistent snapshot can be taken every 1 to 12 hours, depending on your app needs. Snapshots are standard Azure blob snapshots. The Mobility agent running on a VM requests a VSS snapshot in accordance with this setting, and bookmarks that point-in-time as an application consistent point in the replication stream.
- Traffic replicates to Azure storage public endpoints over the internet. Alternately, you can use Azure ExpressRoute with [Microsoft peering](#). Replicating traffic over a site-to-site virtual private network (VPN) from an on-premises site to Azure isn't supported.
- After initial replication finishes, replication of delta changes to Azure begins. Tracked changes for a machine are sent to the process server.

4. Communication happens as follows:

- VMs communicate with the on-premises configuration server on port HTTPS 443 inbound, for replication management.
 - The configuration server orchestrates replication with Azure over port HTTPS 443 outbound.
 - VMs send replication data to the process server (running on the configuration server machine) on port HTTPS 9443 inbound. This port can be modified.
 - The process server receives replication data, optimizes and encrypts it, and sends it to Azure storage over port 443 outbound.
5. The replication data logs first land in a cache storage account in Azure. These logs are processed and the data is stored in an Azure Managed Disk (called as asr seed disk). The recovery points are created on this disk.

VMware to Azure replication process



Failover and failback process

After replication is set up and you run a disaster recovery drill (test failover) to check that everything's working as expected, you can run failover and failback as you need to.

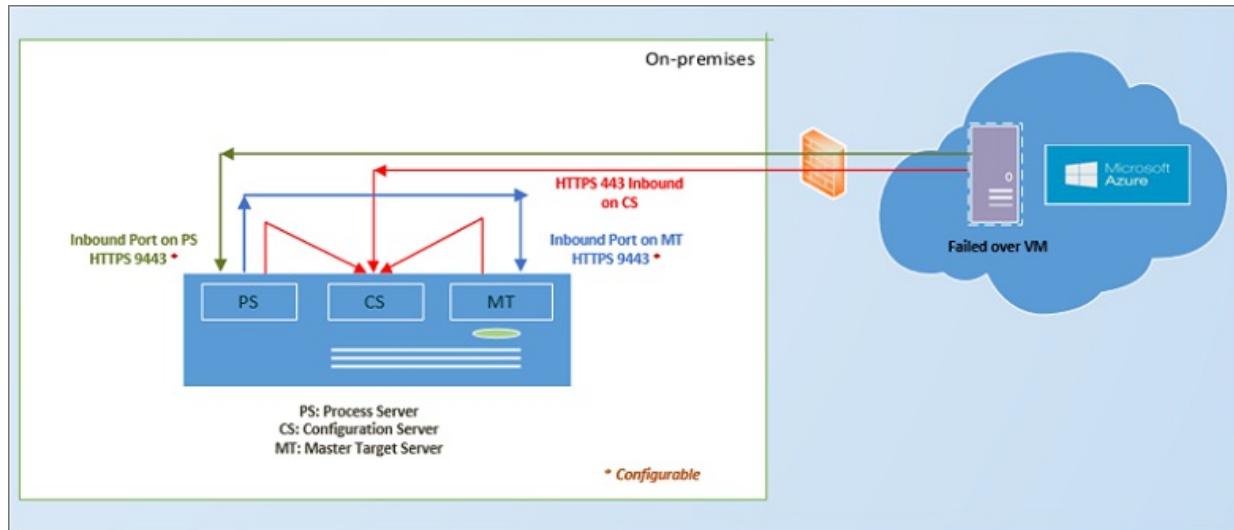
1. You run failover for a single machine, or create a recovery plan to fail over multiple VMs at the same time. The advantage of a recovery plan rather than single machine failover include:
 - You can model app-dependencies by including all the VMs across the app in a single recovery plan.
 - You can add scripts, Azure runbooks, and pause for manual actions.
2. After triggering the initial failover, you commit it to start accessing the workload from the Azure VM.
3. When your primary on-premises site is available again, you can prepare for fail back. In order to fail back, you need to set up a failback infrastructure, including:
 - **Temporary process server in Azure:** To fail back from Azure, you set up an Azure VM to act as a process server to handle replication from Azure. You can delete this VM after failback finishes.
 - **VPN connection:** To fail back, you need a VPN connection (or ExpressRoute) from the Azure network to the on-premises site.

- **Separate master target server:** By default, the master target server that was installed with the configuration server on the on-premises VMware VM handles failback. If you need to fail back large volumes of traffic, set up a separate on-premises master target server for this purpose.
- **Failback policy:** To replicate back to your on-premises site, you need a failback policy. This policy is automatically created when you create a replication policy from on-premises to Azure.

4. After the components are in place, failback occurs in three actions:

- Stage 1: Reprotect the Azure VMs so that they replicate from Azure back to the on-premises VMware VMs.
- Stage 2: Run a failover to the on-premises site.
- Stage 3: After workloads have failed back, you reenable replication for the on-premises VMs.

VMware failback from Azure



Next steps

Follow [this tutorial](#) to enable VMware to Azure replication.

Exclude disks from disaster recovery

12/26/2019 • 10 minutes to read • [Edit Online](#)

This article describes how to exclude disks from replication during disaster recovery from on-premises to Azure with [Azure Site Recovery](#). You might exclude disks from replication for a number of reasons:

- So that unimportant data churned on the excluded disk isn't replicated.
- To optimize consumed replication bandwidth, or target-side resources.
- To save storage and network resources by not replicating data that you don't need.
- Azure VMs have reached Site Recovery replication limits.

Supported scenarios

You can exclude disks from replication as summarized in the table.

AZURE TO AZURE	VMWARE TO AZURE	HYPER-V TO AZURE
Yes (using PowerShell)	Yes	Yes

Exclude limitations

LIMITATION	AZURE VMS	VMWARE VMS	HYPER-V VMS
Disk types	You can exclude basic disks from replication. You can't exclude operating system disks or dynamic disks. Temp disks are excluded by default.	You can exclude basic disks from replication. You can't exclude operating system disks or dynamic disks.	You can exclude basic disks from replication. You can't exclude operating system disks. We recommend that you don't exclude dynamic disks. Site Recovery can't identify which VHS is basic or dynamic in the guest VM. If all dependent dynamic volume disks aren't excluded, the protected dynamic disk becomes a failed disk on a failover VM, and the data on that disk isn't accessible.
Replicating disk	You can't exclude a disk that's replicating. Disable and reenable replication for the VM.	You can't exclude a disk that's replicating.	You can't exclude a disk that's replicating.

LIMITATION	AZURE VMS	VMWARE VMS	HYPER-V VMS
Mobility service (VMware)	Not relevant	<p>You can exclude disks only on VMs that have the Mobility service installed.</p> <p>This means that you have to manually install the Mobility service on the VMs for which you want to exclude disks. You can't use the push installation mechanism because it installs the Mobility service only after replication is enabled.</p>	Not relevant.
Add/Remove	You can add and remove disks on Azure VMs with managed disks.	You can't add or remove disks after replication is enabled. Disable and then reenable replication to add a disk.	You can't add or remove disks after replication is enabled. Disable and then reenable replication.
Failover	<p>If an app needs a disk that you excluded, after failover you need to create the disk manually so that the replicated app can run.</p> <p>Alternatively, you can create the disk during VM failover, by integrating Azure automation into a recovery plan.</p>	If you exclude a disk that an app needs, create it manually in Azure after failover.	If you exclude a disk that an app needs, create it manually in Azure after failover.
On-premises failback-disks created manually	Not relevant	<p>Windows VMs: Disks created manually in Azure aren't failed back. For example, if you fail over three disks and create two disks directly on an Azure VM, only the three disks that were failed over are then failed back.</p> <p>Linux VMs: Disks created manually in Azure are failed back. For example, if you fail over three disks and create two disks on an Azure VM, all five will be failed back. You can't exclude disks that were created manually from failback.</p>	Disks created manually in Azure aren't failed back. For example, if you fail over three disks and create two disks directly on an Azure VM, only the three disks that were failed over will be failed back.

LIMITATION	AZURE VMS	VMWARE VMS	HYPER-V VMS
On-premises fallback-Excluded disks	Not relevant	If you fail back to the original machine, the fallback VM disk configuration doesn't include the excluded disks. Disks that were excluded from VMware to Azure replication aren't available on the fallback VM.	When failback is to the original Hyper-V location, the fallback VM disk configuration remains the same as that of original source VM disk. Disks that were excluded from Hyper-V site to Azure replication are available on the fallback VM.

Typical scenarios

Examples of data churn that are great candidates for exclusion include writes to a paging file (pagefile.sys), and writes to the tempdb file of Microsoft SQL Server. Depending on the workload and the storage subsystem, the paging and tempdb files can register a significant amount of churn. Replicating this type of data to Azure is resource-intensive.

- To optimize replication for a VM with a single virtual disk that includes both the operating system and the paging file, you could:
 1. Split the single virtual disk into two virtual disks. One virtual disk has the operating system, and the other has the paging file.
 2. Exclude the paging file disk from replication.
- To optimize replication for a disk that includes both the Microsoft SQL Server tempdb file and the system database file, you could:
 1. Keep the system database and tempdb on two different disks.
 2. Exclude the tempdb disk from replication.

Example 1: Exclude the SQL Server tempdb disk

Let's look at how to handle disk exclusion, failover, and failover for a source SQL Server Windows VM - **SalesDB***, for which we want to exclude tempdb.

Exclude disks from replication

We have these disks on the source Windows VM SalesDB.

DISK NAME	GUEST OS DISK	DRIVE LETTER	DISK DATA TYPE
DB-Disk0-OS	Disk0	C:\	Operating system disk.
DB-Disk1	Disk1	D:\	SQL system database and User Database1.
DB-Disk2 (Excluded the disk from protection)	Disk2	E:\	Temp files.
DB-Disk3 (Excluded the disk from protection)	Disk3	F:\	SQL tempdb database. Folder path - F:\MSSQL\Data. Make a note of the folder path before failover.

DISK NAME	GUEST OS DISK	DRIVE LETTER	DISK DATA TYPE
DB-Disk4	Disk4	G:\	User Database2

1. We enable replication for the SalesDB VM.
2. We exclude Disk2 and Disk3 from replication because data churn on those disks is temporary.

Handle disks during failover

Since disks aren't replicated, when you fail over to Azure these disks aren't present on the Azure VM created after failover. The Azure VM has the disks summarized in this table.

GUEST OS DISK	DRIVE LETTER	DISK DATA TYPE
Disk0	C:\	Operating system disk.
Disk1	E:\	Temporary storage Azure adds this disk. Because Disk2 and Disk3 were excluded from replication, E: is the first drive letter from the available list. Azure assigns E: to the temporary storage volume. Other drive letters for replicated disks remain the same.
Disk2	D:\	SQL system database and User Database1
Disk3	G:\	User Database2

In our example, since Disk3, the SQL tempdb disk, was excluded from replication and isn't available on the Azure VM, the SQL service is in a stopped state, and it needs the F:\MSSQL\Data path. You can create this path in a couple of ways:

- Add a new disk after failover, and assign tempdb folder path.
- Use an existing temporary storage disk for the tempdb folder path.

Add a new disk after failover

1. Write down the paths of SQL tempdb.mdf and tempdb.ldf before failover.
2. From the Azure portal, add a new disk to the failover Azure VM. The disk should be the same size (or larger) as the source SQL tempdb disk (Disk3).
3. Sign in to the Azure VM.
4. From the disk management (diskmgmt.msc) console, initialize and format the newly added disk.
5. Assign the same drive letter that was used by the SQL tempdb disk (F:)
6. Create a tempdb folder on the F: volume (F:\MSSQL\Data).
7. Start the SQL service from the service console.

Use an existing temporary storage disk

1. Open a command prompt.
2. Run SQL Server in recovery mode from the command prompt.

```
Net start MSSQLSERVER /f / T3608
```

3. Run the following sqlcmd to change the tempdb path to the new path.

```

sqlcmd -A -S SalesDB **Use your SQL DBname**
USE master;
GO
ALTER DATABASE tempdb
MODIFY FILE (NAME = tempdev, FILENAME = 'E:\MSSQL\tempdata\tempdb.mdf');
GO
ALTER DATABASE tempdb
MODIFY FILE (NAME = templog, FILENAME = 'E:\MSSQL\tempdata\templog.ldf');
GO

```

4. Stop the Microsoft SQL Server service.

```
Net stop MSSQLSERVER
```

5. Start the Microsoft SQL Server service.

```
Net start MSSQLSERVER
```

VMware VMs: Disks during failback to original location

Now let's see how to handle disks on VMware VMs when you fail back to your original on-premises location.

- **Disks created in Azure:** Since our example uses a Windows VM, disks that you create manually in Azure aren't replicated back to your site when you fail back or reprotect a VM.
- **Temporary storage disk in Azure:** The temporary storage disk isn't replicated back to on-premises hosts.
- **Excluded disks:** Disks that were excluded from VMware to Azure replication aren't available on the on-premises VM after failback.

Before you fail back the VMware VMs to the original location, the Azure VM disk settings are as follows.

GUEST OS DISK	DRIVE LETTER	DISK DATA TYPE
Disk0	C:\	Operating system disk.
Disk1	E:\	Temporary storage.
Disk2	D:\	SQL system database and User Database1.
Disk3	G:\	User Database2.

After failback, the VMware VM in the original location has the disks summarized in the table.

GUEST OS DISK	DRIVE LETTER	DISK DATA TYPE
Disk0	C:\	Operating system disk.
Disk1	D:\	SQL system database and User Database1.
Disk2	G:\	User Database2.

Hyper-V VMs: Disks during failback to original location

Now let's see how to handle disks on Hyper-V VMs when you fail back to your original on-premises location.

- **Disks created in Azure:** Disks that you create manually in Azure aren't replicated back to your site when you fail back or reprotect a VM.
- **Temporary storage disk in Azure:** The temporary storage disk isn't replicated back to on-premises hosts.
- **Excluded disks:** After failback the VM disk configuration is the same as the original VM disk configuration. Disks that were excluded from replication from Hyper-V to Azure are available on the failback VM.

Before you fail back the Hyper-V VMs to the original location, the Azure VM disk settings are as follows.

GUEST OS DISK	DRIVE LETTER	DISK DATA TYPE
Disk0	C:\	Operating system disk.
Disk1	E:\	Temporary storage.
Disk2	D:\	SQL system database and User Database1.
Disk3	G:\	User Database2.

After planned failover (failback) from Azure to on-premises Hyper-V, the Hyper-V VM in the original location has the disks summarized in the table.

DISK NAME	GUEST OS DISK#	DRIVE LETTER	DISK DATA TYPE
DB-Disk0-OS	Disk0	C:\	Operating system disk.
DB-Disk1	Disk1	D:\	SQL system database and User Database1.
DB-Disk2 (Excluded disk)	Disk2	E:\	Temp files.
DB-Disk3 (Excluded disk)	Disk3	F:\	SQL tempdb database Folder path (F:\MSSQL\Data).
DB-Disk4	Disk4	G:\	User Database2

Example 2: Exclude the paging file disk

Let's look at how to handle disk exclusion, failover, and failover for a source Windows VM, for which we want to exclude the pagefile.sys file disk on both the D drive, and an alternate drive.

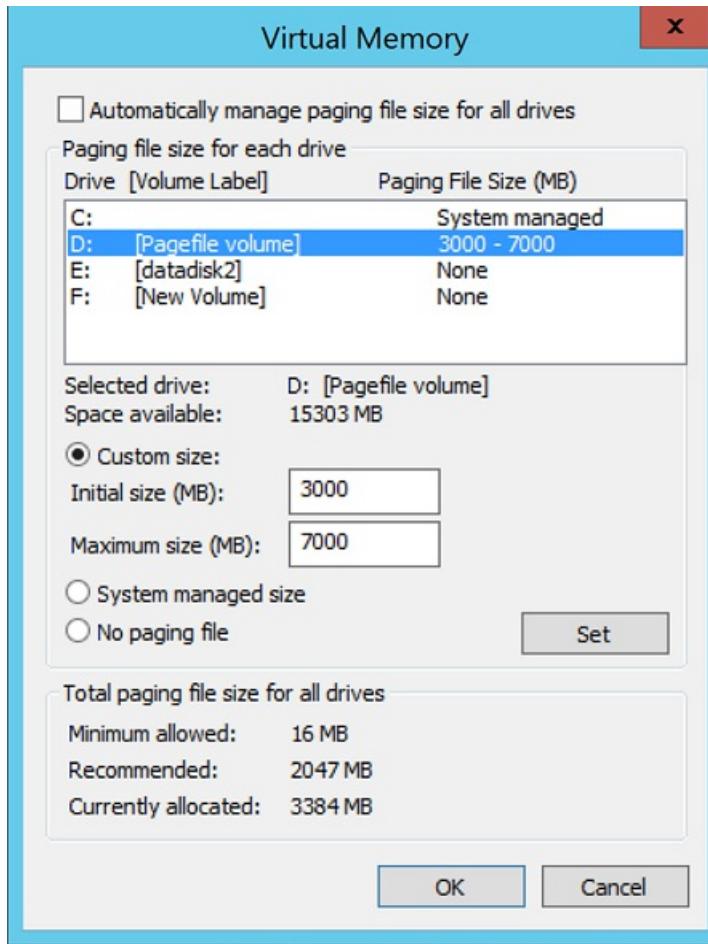
Paging file on the D drive

We have these disks on the source VM.

DISK NAME	GUEST OS DISK	DRIVE LETTER	DISK DATA TYPE
DB-Disk0-OS	Disk0	C:\	Operating system disk
DB-Disk1 (Exclude from replication)	Disk1	D:\	pagefile.sys
DB-Disk2	Disk2	E:\	User data 1

DISK NAME	GUEST OS DISK	DRIVE LETTER	DISK DATA TYPE
DB-Disk3	Disk3	F:\	User data 2

Our paging file settings on the source VM are as follows:



1. We enable replication for the VM.
2. We exclude DB-Disk1 from replication.

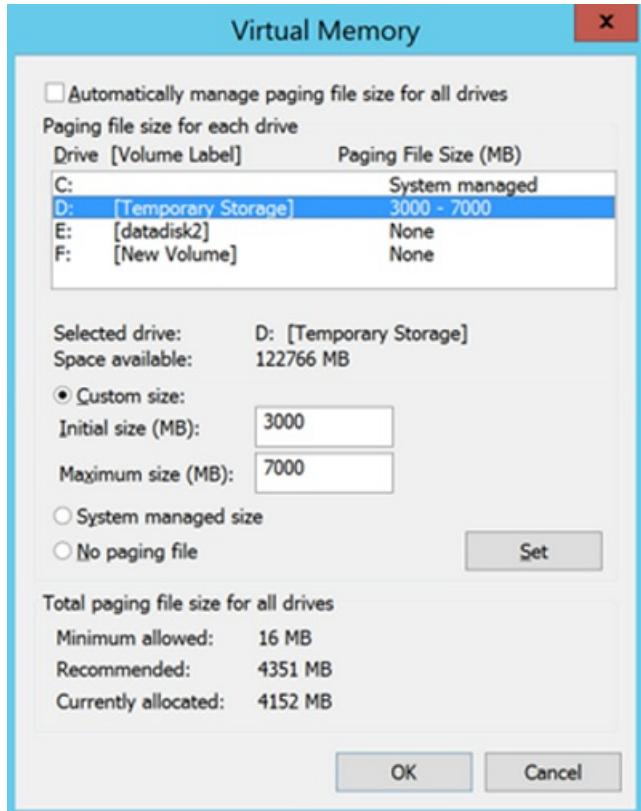
Disks after failover

After failover the Azure VM has the disks summarized in the table.

DISK NAME	GUEST OPERATING SYSTEM DISK#	DRIVE LETTER	DATA TYPE ON THE DISK
DB-Disk0-OS	Disk0	C:\	Operating system disk
DB-Disk1	Disk1	D:\	<p>Temporary storage/pagefile.sys</p> <p>Because DB-Disk1 (D:) was excluded, D: is the first drive letter from the available list.</p> <p>Azure assigns D: to the temporary storage volume.</p> <p>Because D: is available, the VM paging file setting remains the same).</p>

DISK NAME	GUEST OPERATING SYSTEM DISK#	DRIVE LETTER	DATA TYPE ON THE DISK
DB-Disk2	Disk2	E:\	User data 1
DB-Disk3	Disk3	F:\	User data 2

Our paging file settings on the Azure VM are as follows:



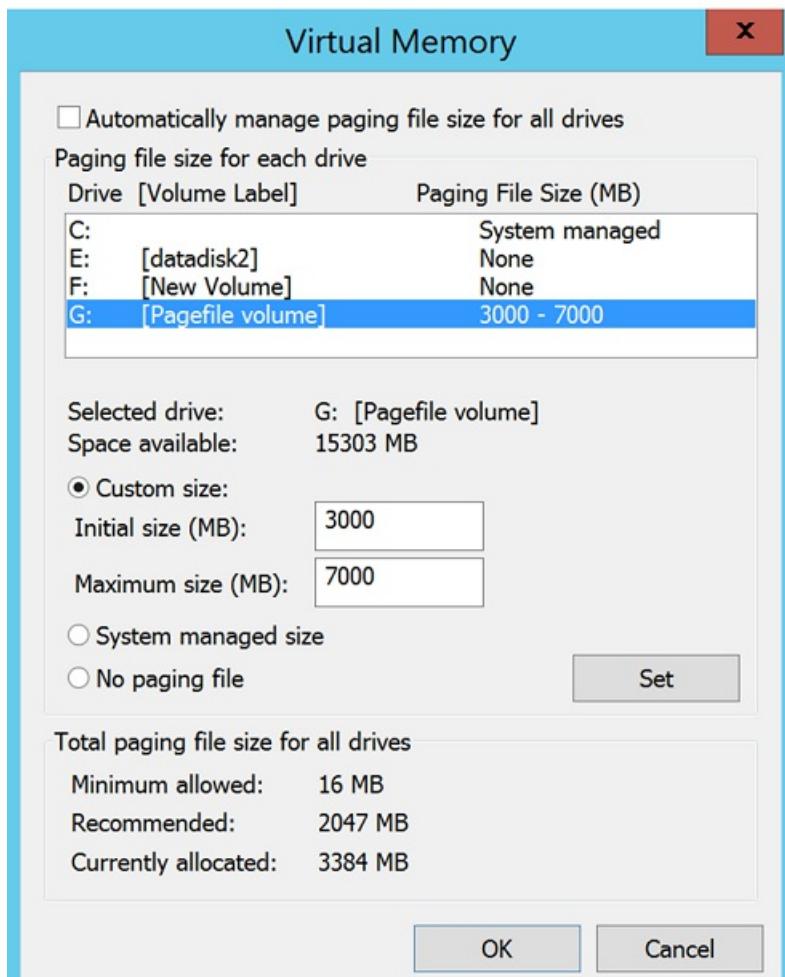
Paging file on another drive (not D:)

Let's look at example in which the paging file isn't on the D drive.

We have these disks on the source VM.

DISK NAME	GUEST OS DISK	DRIVE LETTER	DISK DATA TYPE
DB-Disk0-OS	Disk0	C:\	Operating system disk
DB-Disk1 (Exclude from replication)	Disk1	G:\	pagefile.sys
DB-Disk2	Disk2	E:\	User data 1
DB-Disk3	Disk3	F:\	User data 2

Our paging file settings on the on-premises VM are as follows:



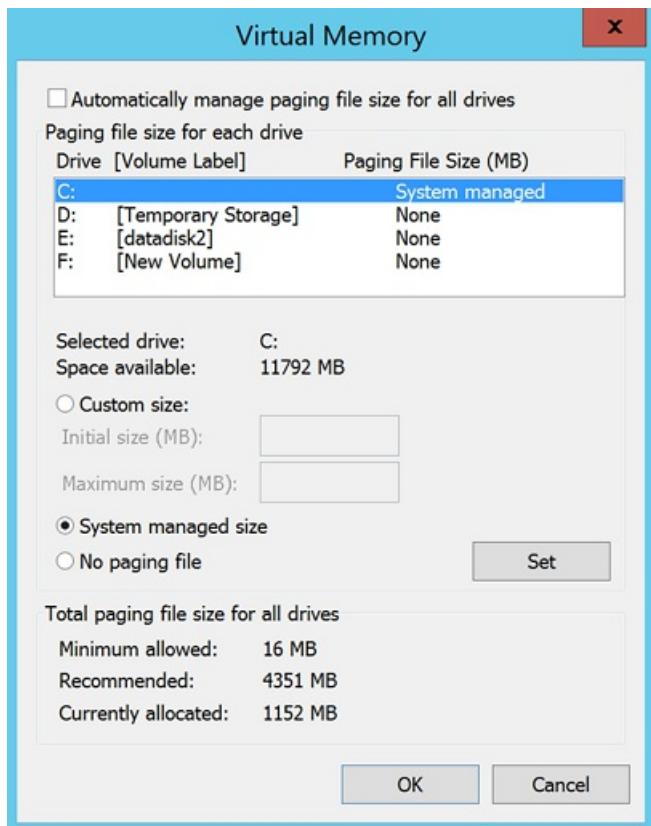
1. We enable replication for the VM.
2. We exclude DB-Disk1 from replication.

Disks after failover

After failover the Azure VM has the disks summarized in the table.

DISK NAME	GUEST OS DISK#	DRIVE LETTER	DISK DATA TYPE
DB-Disk0-OS	Disk0	C:\	Operating system disk
DB-Disk1	Disk1	D:\	<p>Temporary storage</p> <p>Because D: is the first drive letter from available the list, Azure assigns D: to the temporary storage volume.</p> <p>For all the replicated disks, the drive letter remains the same.</p> <p>Because the G: disk isn't available, the system will use the C: drive for the paging file.</p>
DB-Disk2	Disk2	E:\	User data 1
DB-Disk3	Disk3	F:\	User data 2

Our paging file settings on the Azure VM are as follows:



Next steps

- Learn more about guidelines for the temporary storage disk:
 - [Learn about](#) using SSDs in Azure VMs to store SQL Server TempDB and Buffer Pool Extensions
 - [Review](#) performance best practices for SQL Server in Azure VMs.
- After your deployment is set up and running, [learn more](#) about different types of failover.

Failback of VMware VMs after disaster recovery to Azure

8/7/2019 • 3 minutes to read • [Edit Online](#)

After you have failed over to Azure as part of your disaster recovery process, you can fail back to your on-premises site. There are two different types of failback that are possible with Azure Site Recovery:

- Fail back to the original location
- Fail back to an alternate location

If you failed over a VMware virtual machine, you can fail back to the same source on-premises virtual machine if it still exists. In this scenario, only the changes are replicated back. This scenario is known as **original location recovery**. If the on-premises virtual machine does not exist, the scenario is an **alternate location recovery**.

NOTE

You can only fail back to the original vCenter and Configuration server. You cannot deploy a new Configuration server and fail back using it. Also, you cannot add a new vCenter to the existing Configuration server and failback into the new vCenter.

Original Location Recovery (OLR)

If you choose to fail back to the original virtual machine, the following conditions need to be met:

- If the virtual machine is managed by a vCenter server, then the master target's ESX host should have access to the virtual machine's datastore.
- If the virtual machine is on an ESX host but isn't managed by vCenter, then the hard disk of the virtual machine must be in a datastore that the master target's host can access.
- If your virtual machine is on an ESX host and doesn't use vCenter, then you should complete discovery of the ESX host of the master target before you reprotect. This applies if you're failing back physical servers, too.
- You can fail back to a virtual storage area network (vSAN) or a disk that based on raw device mapping (RDM) if the disks already exist and are connected to the on-premises virtual machine.

IMPORTANT

It is important to enable `disk.enableUUID= TRUE` so that during failback, the Azure Site Recovery service is able to identify the original VMDK on the virtual machine to which the pending changes will be written. If this value is not set to be TRUE, then the service tries to identify the corresponding on-premises VMDK on a best effort basis. If the right VMDK is not found, it creates an extra disk and the data gets written on to that.

Alternate location recovery (ALR)

If the on-premises virtual machine does not exist before reprotecting the virtual machine, the scenario is called an alternate location recovery. The reprotect workflow creates the on-premises virtual machine again. This will also cause a full data download.

- When you fail back to an alternate location, the virtual machine is recovered to the same ESX host on which the master target server is deployed. The datastore that's used to create the disk will be the same datastore that was selected when reprotecting the virtual machine.

- You can fail back only to a virtual machine file system (VMFS) or vSAN datastore. If you have an RDM, reprotect and fallback will not work.
- Reprotect involves one large initial data transfer that's followed by the changes. This process exists because the virtual machine does not exist on premises. The complete data has to be replicated back. This reprotect will also take more time than an original location recovery.
- You cannot fail back to RDM-based disks. Only new virtual machine disks (VMDKs) can be created on a VMFS/vSAN datastore.

NOTE

A physical machine, when failed over to Azure, can be failed back only as a VMware virtual machine. This follows the same workflow as the alternate location recovery. Ensure that you discover at least one master target server and the necessary ESX/ESXi hosts to which you need to fail back.

Next steps

Follow the steps to perform the [failback operation](#).

Overview of multi-tenant support for VMware disaster recovery to Azure with CSP

11/14/2019 • 6 minutes to read • [Edit Online](#)

Azure Site Recovery supports multi-tenant environments for tenant subscriptions. It also supports multi-tenancy for tenant subscriptions that are created and managed through the Microsoft Cloud Solution Provider (CSP) program.

This article provides an overview of implementing and managing multi-tenant VMware to Azure replication.

Multi-tenant environments

There are three major multi-tenant models:

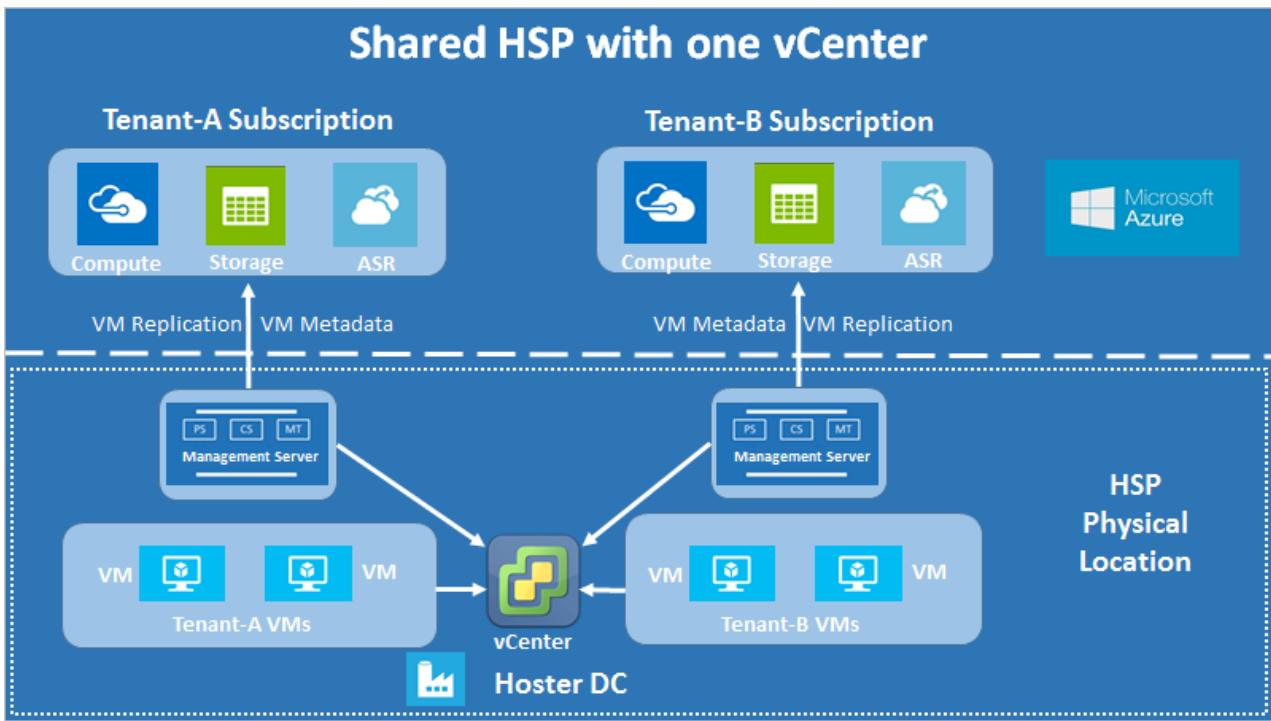
- **Shared Hosting Services Provider (HSP):** The partner owns the physical infrastructure, and uses shared resources (vCenter, datacenters, physical storage, and so on) to host multiple tenant VMs on the same infrastructure. The partner can provide disaster-recovery management as a managed service, or the tenant can own disaster recovery as a self-service solution.
- **Dedicated Hosting Services Provider:** The partner owns the physical infrastructure, but uses dedicated resources (multiple vCenters, physical datastores, and so on) to host each tenant's VMs on a separate infrastructure. The partner can provide disaster-recovery management as a managed service, or the tenant can own it as a self-service solution.
- **Managed Services Provider (MSP):** The customer owns the physical infrastructure that hosts the VMs, and the partner provides disaster-recovery enablement and management.

Shared-hosting services provider (HSP)

The other two scenarios are subsets of the shared-hosting scenario, and they use the same principles. The differences are described at the end of the shared-hosting guidance.

The basic requirement in a multi-tenant scenario is that tenants must be isolated. One tenant should not be able to observe what another tenant has hosted. In a partner-managed environment, this requirement is not as important as it is in a self-service environment, where it can be critical. This article assumes that tenant isolation is required.

The architecture is shown in the following diagram.



Shared-hosting with one vCenter server

In the diagram, each customer has a separate management server. This configuration limits tenant access to tenant-specific VMs, and enables tenant isolation. VMware VM replication uses the configuration server to discover VMs, and install agents. The same principles apply to multi-tenant environments, with the addition of restricting VM discovery using vCenter access control.

The data isolation requirement means that all sensitive infrastructure information (such as access credentials) remains undisclosed to tenants. For this reason, we recommend that all components of the management server remain under the exclusive control of the partner. The management server components are:

- Configuration server
- Process server
- Master target server

A separate scaled-out process server is also under the partner's control.

Configuration server accounts

Every configuration server in the multi-tenant scenario uses two accounts:

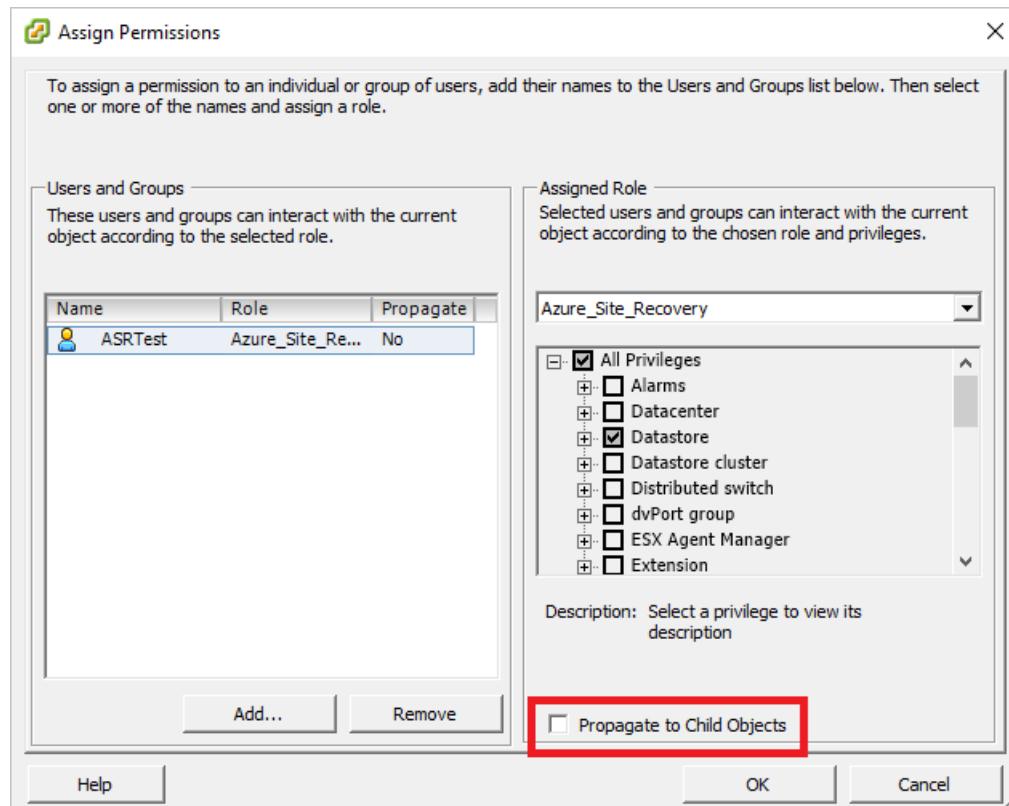
- **vCenter access account:** This account is used to discover tenant VMs. It has vCenter access permissions assigned to it. To help avoid access leaks, we recommend that partners enter these credentials themselves in the configuration tool.
- **Virtual machine access account:** This account is used to install the Mobility service agent on tenant VMs, with an automatic push. It is usually a domain account that a tenant might provide to a partner, or an account that the partner might manage directly. If a tenant doesn't want to share the details with the partner directly, they can enter the credentials through limited-time access to the configuration server. Or, with the partner's assistance, they can install the Mobility service agent manually.

vCenter account requirements

Configure the configuration server with an account that has a special role assigned to it.

- The role assignment must be applied to the vCenter access account for each vCenter object, and not

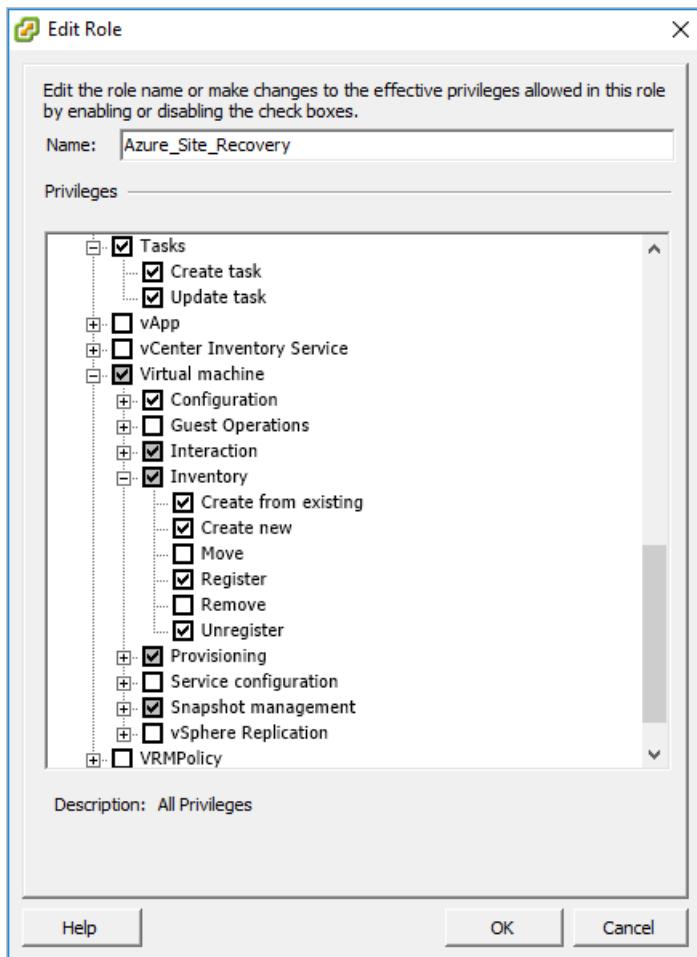
propagated to the child objects. This configuration ensures tenant isolation, because access propagation can result in accidental access to other objects.



- The alternative approach is to assign the user account and role at the datacenter object, and propagate them to the child objects. Then give the account a **No access** role for every object (such as VMs that belong to other tenants) that should be inaccessible to a particular tenant. This configuration is cumbersome. It exposes accidental access controls, because every new child object is also automatically granted access that's inherited from the parent. Therefore, we recommend that you use the first approach.

Create a vCenter account

- Create a new role by cloning the predefined *Read-only* role, and then give it a convenient name (such as *Azure_Site_Recovery*, as shown in this example).
- Assign the following permissions to this role:
 - Datastore:** Allocate space, Browse datastore, Low-level file operations, Remove file, Update virtual machine files
 - Network:** Network assign
 - Resource:** Assign VM to resource pool, Migrate powered off VM, Migrate powered on VM
 - Tasks:** Create task, Update task
 - VM - Configuration:** All
 - VM - Interaction** > Answer question, Device connection, Configure CD media, Configure floppy media, Power off, Power on, VMware tools install
 - VM - Inventory** > Create from existing, Create new, Register, Unregister
 - VM - Provisioning** > Allow virtual machine download, Allow virtual machine files upload
 - VM - Snapshot management** > Remove snapshots



3. Assign access levels to the vCenter account (used in the tenant configuration server) for various objects, as follows:

OBJECT	ROLE	REMARKS
vCenter	Read-Only	Needed only to allow vCenter access for managing different objects. You can remove this permission if the account is never going to be provided to a tenant or used for any management operations on the vCenter.
Datacenter	Azure_Site_Recovery	
Host and host cluster	Azure_Site_Recovery	Re-ensures that access is at the object level, so that only accessible hosts have tenant VMs before failover and after failback.
Datastore and datastore cluster	Azure_Site_Recovery	Same as preceding.
Network	Azure_Site_Recovery	
Management server	Azure_Site_Recovery	Includes access to all components (CS, PS, and MT) outside the CS machine.

OBJECT	ROLE	REMARKS
Tenant VMs	Azure_Site_Recovery	Ensures that any new tenant VMs of a particular tenant also get this access, or they will not be discoverable through the Azure portal.

The vCenter account access is now complete. This step fulfills the minimum permissions requirement to complete failback operations. You can also use these access permissions with your existing policies. Just modify your existing permissions set to include role permissions from step 2, detailed previously.

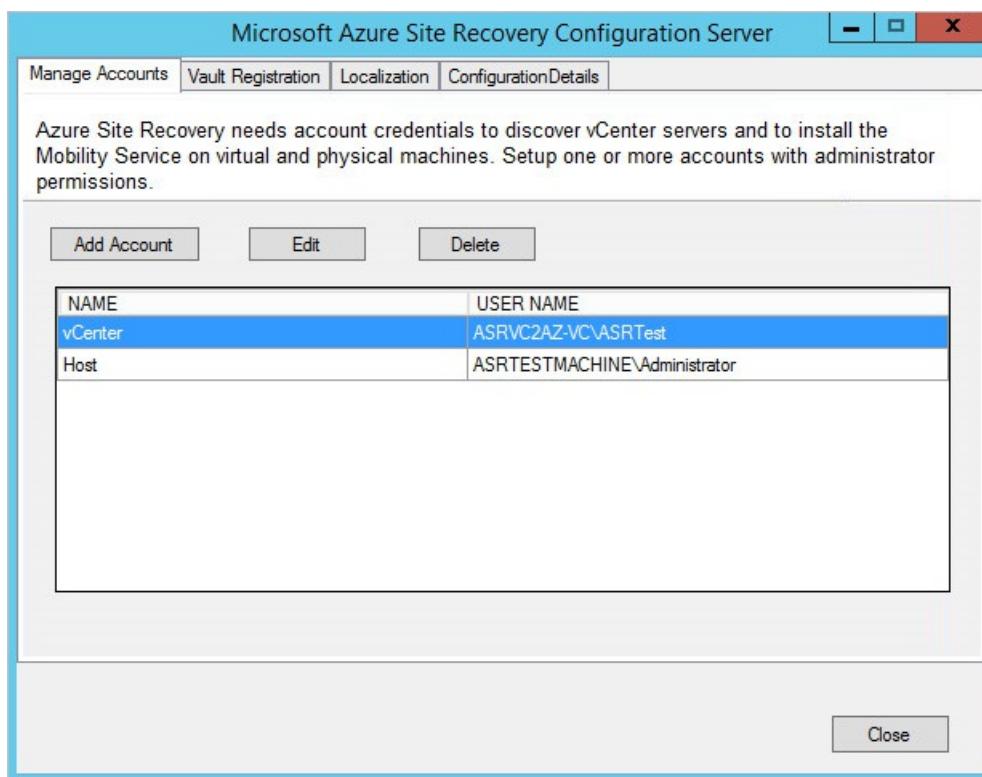
Failover only

To restrict disaster recovery operations up until failover only (that is, without failback capabilities), use the previous procedure, with these exceptions:

- Instead of assigning the *Azure_Site_Recovery* role to the vCenter access account, assign only a *Read-Only* role to that account. This permission set allows VM replication and failover, and it does not allow failback.
- Everything else in the preceding process remains as is. To ensure tenant isolation and restrict VM discovery, every permission is still assigned at the object level only, and not propagated to child objects.

Deploy resources to the tenant subscription

1. On the Azure portal, create a resource group, and then deploy a Recovery Services vault per the usual process.
2. Download the vault registration key.
3. Register the CS for the tenant by using the vault registration key.
4. Enter the credentials for the two access accounts, the account to access the vCenter server, and the account to access the VM.



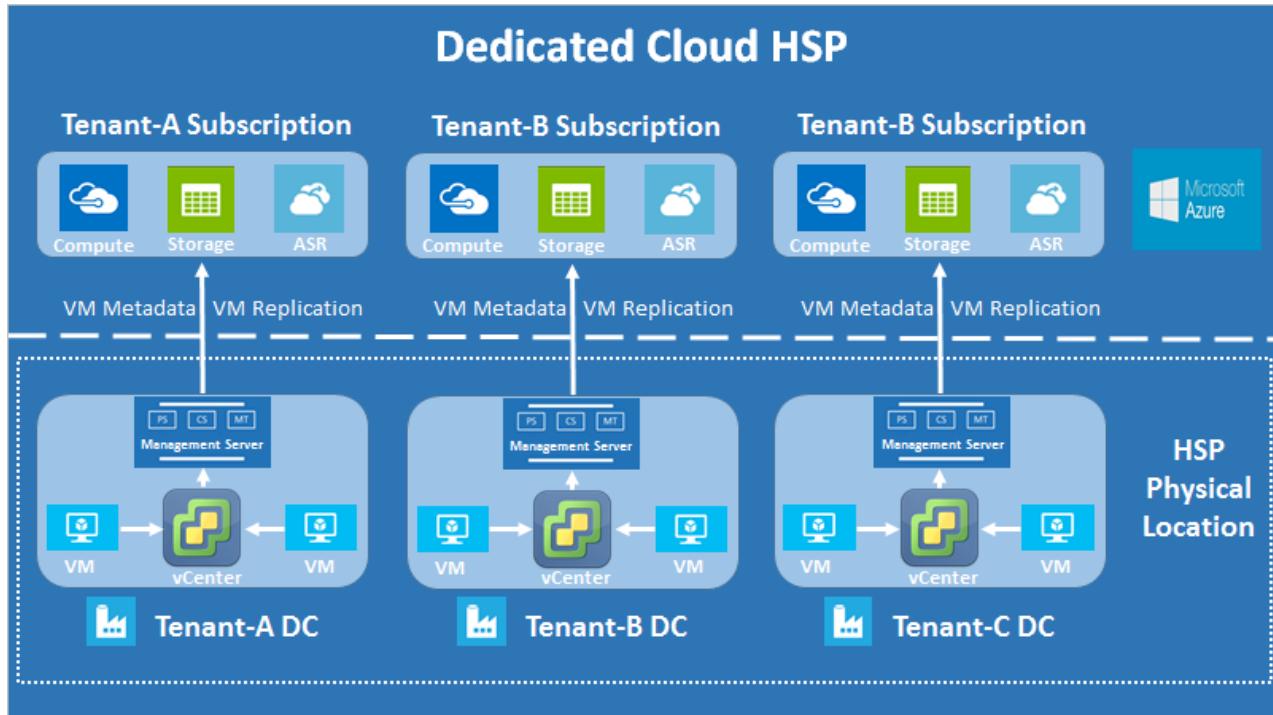
Register servers in the vault

1. In the Azure portal, in the vault that you created earlier, register the vCenter server to the configuration server, using the vCenter account you created.

2. Finish the "Prepare infrastructure" process for Site Recovery per the usual process.
3. The VMs are now ready to be replicated. Verify that only the tenant's VMs are displayed in **Replicate > Select virtual machines**.

Dedicated hosting solution

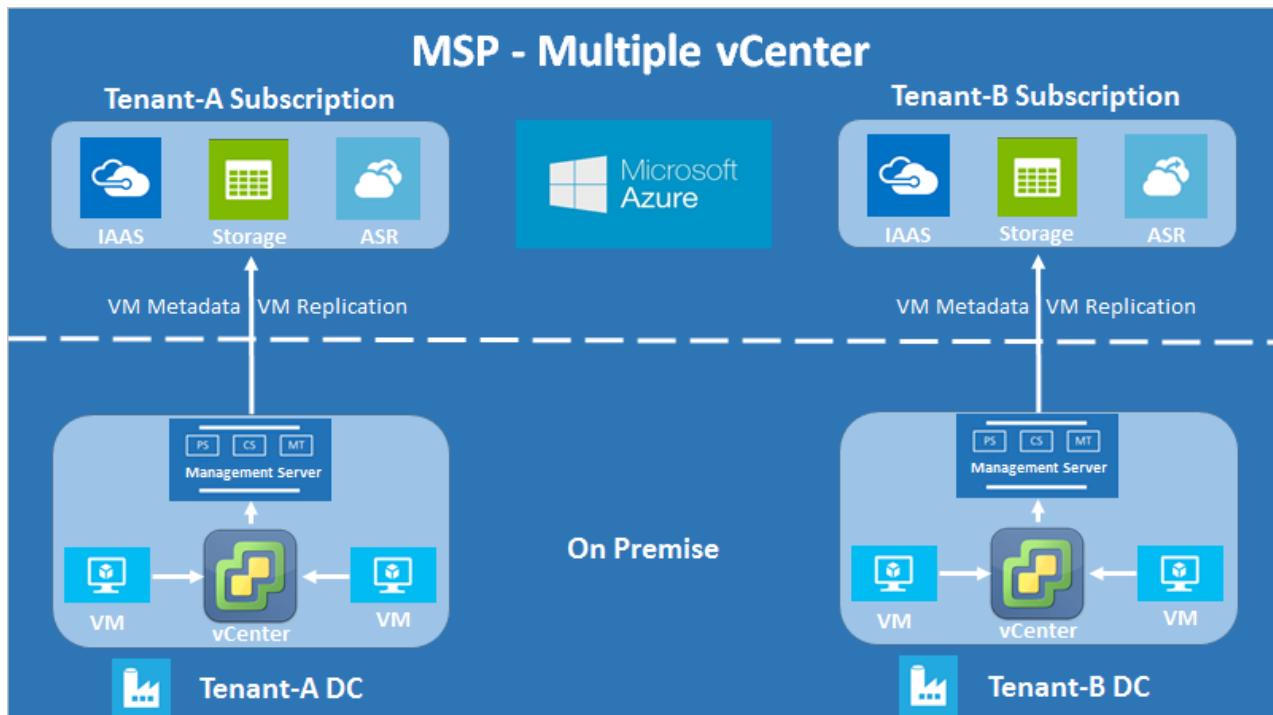
As shown in the following diagram, the architectural difference in a dedicated hosting solution is that each tenant's infrastructure is set up for that tenant only.



Dedicated hosting scenario with multiple vCenters

Managed service solution

As shown in the following diagram, the architectural difference in a managed service solution is that each tenant's infrastructure is also physically separate from other tenants' infrastructure. This scenario usually exists when the tenant owns the infrastructure and wants a solution provider to manage disaster recovery.



Managed service scenario with multiple vCenters

Next steps

- [Learn more](#) about role-based access control in Site Recovery.
- Learn how to [set up disaster recovery of VMware VMs to Azure](#).
- Learn more about [multi-tenancy with CSP for VMWare VMs](#).

Common questions - Hyper-V to Azure disaster recovery

12/26/2019 • 12 minutes to read • [Edit Online](#)

This article provides answers to common questions we see when replicating on-premises Hyper-V VMs to Azure.

General

How is Site Recovery priced?

Review [Azure Site Recovery pricing](#) details.

How do I pay for Azure VMs?

During replication, data is replicated to Azure storage, and you don't pay any VM changes. When you run a failover to Azure, Site Recovery automatically creates Azure IaaS virtual machines. After that you're billed for the compute resources that you consume in Azure.

Is there any difference in cost when replicating to General Purpose v2 storage account?

You will typically see an increase in the transactions cost incurred on GPv2 storage accounts since Azure Site Recovery is transactions heavy. [Read more](#) to estimate the change.

Azure

What do I need in Hyper-V to orchestrate replication with Site Recovery?

For the Hyper-V host server what you need depends on the deployment scenario. Check out the Hyper-V prerequisites in:

- [Replicating Hyper-V VMs \(without VMM\) to Azure](#)
- [Replicating Hyper-V VMs \(with VMM\) to Azure](#)
- [Replicating Hyper-V VMs to a secondary datacenter](#)
- If you're replicating to a secondary datacenter read about [Supported guest operating systems for Hyper-V VMs](#).
- If you're replicating to Azure, Site Recovery supports all the guest operating systems that are [supported by Azure](#).

Can I protect VMs when Hyper-V is running on a client operating system?

No, VMs must be located on a Hyper-V host server that's running on a supported Windows server machine. If you need to protect a client computer you could replicate it as a physical machine to [Azure](#) or a [secondary datacenter](#).

Do Hyper-V hosts need to be in VMM clouds?

If you want to replicate to a secondary datacenter, then Hyper-V VMs must be on Hyper-V hosts servers located in a VMM cloud. If you want to replicate to Azure, then you can replicate VMs with or without VMM clouds. [Read more](#) about Hyper-V replication to Azure.

Can I replicate Hyper-V generation 2 virtual machines to Azure?

Yes. Site Recovery converts from generation 2 to generation 1 during failover. At failback the machine is converted back to generation 2. [Read more](#).

Can I deploy Site Recovery with VMM if I only have one VMM server?

Yes. You can either replicate VMs in Hyper-V servers in the VMM cloud to Azure, or you can replicate between VMM clouds on the same server. For on-premises to on-premises replication, we recommend that you have a VMM server in both the primary and secondary sites.

What do I need in Azure?

You need an Azure subscription, a Recovery Services vault, a storage account, and a virtual network. The vault, storage account and network must be in the same region.

What Azure storage account do I need?

You need an LRS or GRS storage account. We recommend GRS so that data is resilient if a regional outage occurs, or if the primary region can't be recovered. Premium storage is supported.

Does my Azure account need permissions to create VMs?

If you're a subscription administrator, you have the replication permissions you need. If you're not, you need permissions to create an Azure VM in the resource group and virtual network you specify when you configure Site Recovery, and permissions to write to the selected storage account. [Learn more](#).

Is replication data sent to Site Recovery?

No, Site Recovery doesn't intercept replicated data, and doesn't have any information about what's running on your VMs. Replication data is exchanged between Hyper-V hosts and Azure storage. Site Recovery has no ability to intercept that data. Only the metadata needed to orchestrate replication and failover is sent to the Site Recovery service.

Site Recovery is ISO 27001:2013, 27018, HIPAA, DPA certified, and is in the process of SOC2 and FedRAMP JAB assessments.

Can we keep on-premises metadata within a geographic region?

Yes. When you create a vault in a region, we ensure that all metadata used by Site Recovery remains within that region's geographic boundary.

Does Site Recovery encrypt replication?

Yes, both encryption-in-transit and [encryption in Azure](#) are supported.

Deployment

What can I do with Hyper-V to Azure replication?

- **Disaster recovery:** You can set up full disaster recovery. In this scenario, you replicate on-premises Hyper-V VMs to Azure storage:
 - You can replicate VMs to Azure. If your on-premises infrastructure is unavailable, you fail over to Azure.
 - When you fail over, Azure VMs are created using the replicated data. You can access apps and workloads on the Azure VMs.
 - When your on-premises datacenter is available again, you can fail back from Azure to your on-premises site.
- **Migration:** You can use Site Recovery to migrate on-premises Hyper-V VMs to Azure storage. Then, you fail over from on-premises to Azure. After failover, your apps and workloads are available and running on Azure VMs.

What do I need on-premises?

You need one or more VMs running on one or more standalone or clustered Hyper-V hosts. You can also replicate VMs running on hosts managed by System Center Virtual Machine Manager (VMM).

- If you're not running VMM, during Site Recovery deployment, you gather Hyper-V hosts and clusters into Hyper-V sites. You install the Site Recovery agents (Azure Site Recovery Provider and Recovery Services agent) on each Hyper-V host.

- If Hyper-V hosts are located in a VMM cloud, you orchestrate replication in VMM. You install the Site Recovery Provider on the VMM server, and the Recovery Services agent on each Hyper-V host. You map between VMM logical/VM networks, and Azure VNets.
- [Learn more](#) about Hyper-V to Azure architecture.

Can I replicate VMs located on a Hyper-V cluster?

Yes, Site Recovery supports clustered Hyper-V hosts. Note that:

- All nodes of the cluster should be registered to the same vault.
- If you're not using VMM, all Hyper-V hosts in the cluster should be added to the same Hyper-V site.
- You install the Azure Site Recovery Provider and Recovery Services agent on each Hyper-V host in the cluster, and add each host to a Hyper-V site.
- No specific steps need to be done on the cluster.
- If you run the Deployment Planner tool for Hyper-V, the tool collects the profile data from the node which is running and where the VM is running. The tool can't collect any data from a node that's turned off, but it will track that node. After the node is up and running, the tool starts collecting the VM profile data from it (if the VM is part of the profile VM list and is running on the node).
- If a VM on a Hyper-V host in a Site Recovery vault migrates to a different Hyper-V host in the same cluster, or to a standalone host, replication for the VM isn't impacted. The Hyper-V host must meet [prerequisites](#), and be configured in a Site Recovery vault.

Can I protect VMs when Hyper-V is running on a client operating system?

No, VMs must be located on a Hyper-V host server that's running on a supported Windows server machine. If you need to protect a client computer you could [replicate it as a physical machine](#) to Azure.

Can I replicate Hyper-V generation 2 virtual machines to Azure?

Yes. Site Recovery converts from generation 2 to generation 1 during failover. At failback the machine is converted back to generation 2.

Can I automate Site Recovery scenarios with an SDK?

Yes. You can automate Site Recovery workflows using the Rest API, PowerShell, or the Azure SDK. Currently supported scenarios for replicating Hyper-V to Azure using PowerShell:

- [Replicate Hyper-V without VMM using PowerShell](#)
- [Replicating Hyper-V with VMM using Powershell](#)

Replication

Where do on-premises VMs replicate to?

Data replicates to Azure storage. When you run a failover, Site Recovery automatically creates Azure VMs from the storage account.

What apps can I replicate?

You can replicate any app or workload running a Hyper-V VM that complies with [replication requirements](#). Site Recovery provides support for application-aware replication, so that apps can be failed over and failed back to an intelligent state. Site Recovery integrates with Microsoft applications such as SharePoint, Exchange, Dynamics, SQL Server and Active Directory, and works closely with leading vendors, including Oracle, SAP, IBM and Red Hat. [Learn more](#) about workload protection.

What's the replication process?

1. When initial replication is triggered, a Hyper-V VM snapshot is taken.
2. Virtual hard disks on the VM are replicated one by one, until they're all copied to Azure. This might take a while, depending on the VM size, and network bandwidth. Learn how to increase network bandwidth.

3. If disk changes occur while initial replication is in progress, the Hyper-V Replica Replication Tracker tracks the changes as Hyper-V replication logs (.hrl). These log files are located in the same folder as the disks. Each disk has an associated .hrl file that's sent to secondary storage. The snapshot and log files consume disk resources while initial replication is in progress.
4. When the initial replication finishes, the VM snapshot is deleted.
5. Any disk changes in the log are synchronized and merged to the parent disk.
6. After the initial replication finishes, the Finalize protection on the virtual machine job runs. It configures network and other post-replication settings, so that the VM is protected.
7. At this stage you can check the VM settings to make sure that it's ready for failover. You can run a disaster recovery drill (test failover) for the VM, to check that it fails over as expected.
8. After the initial replication, delta replication begins, in accordance with the replication policy.
9. Changes are logged .hrl files. Each disk that's configured for replication has an associated .hrl file.
10. The log is sent to the customer's storage account. When a log is in transit to Azure, the changes in the primary disk are tracked in another log file, in the same folder.
11. During both initial and delta replication, you can monitor the VM in the Azure portal.

[Learn more](#) about the replication process.

Can I replicate to Azure with a site-to-site VPN?

Site Recovery replicates data from on-premises to Azure storage over a public endpoint, or using ExpressRoute Microsoft peering. Replication over a site-to-site VPN network isn't supported.

Can I replicate to Azure with ExpressRoute?

Yes, ExpressRoute can be used to replicate VMs to Azure. Site Recovery replicates data to an Azure Storage Account over a public endpoint, and you need to set up [Microsoft peering](#) for Site Recovery replication. After VMs fail over to an Azure virtual network, you can access them using [private peering](#).

Why can't I replicate over VPN?

When you replicate to Azure, replication traffic reaches the public endpoints of an Azure Storage account. Thus you can only replicate over the public internet with ExpressRoute (Microsoft peering), and VPN doesn't work.

What are the replicated VM requirements?

For replication, a Hyper-V VM must be running a supported operating system. In addition, the VM must meet the requirements for Azure VMs. [Learn more](#) in the support matrix.

How often can I replicate to Azure?

Hyper-V VMs can be replicated every 30 seconds (except for premium storage), 5 minutes or 15 minutes.

Can I extend replication?

Extended or chained replication isn't supported. Request this feature in [feedback forum](#).

Can I do an offline initial replication?

This isn't supported. Request this feature in the [feedback forum](#).

Can I exclude disks?

Yes, you can exclude disks from replication.

Can I replicate VMs with dynamic disks?

Dynamic disks can be replicated. The operating system disk must be a basic disk.

Security

What access does Site Recovery need to Hyper-V hosts

Site Recovery needs access to Hyper-V hosts to replicate the VMs you select. Site Recovery installs the following on Hyper-V hosts:

- If you're not running VMM, the Azure Site Recovery Provider and Recovery Services agent are installed on each host.
- If you're running VMM, the Recovery Services agent is installed on each host. The Provider runs on the VMM server.

What does Site Recovery install on Hyper-V VMs?

Site Recovery doesn't explicitly install anything on Hyper-V VMs enabled for replication.

Failover and fallback

How do I fail over to Azure?

You can run a planned or unplanned failover from on-premises Hyper-V VMs to Azure.

- If you run a planned failover, then source VMs are shut down to ensure no data loss.
- You can run an unplanned failover if your primary site isn't accessible.
- You can fail over a single machine, or create recovery plans, to orchestrate failover of multiple machines.
- Failover is in two parts:
 - After the first stage of failover completes, you should be able to see the created replica VMs in Azure.
You can assign a public IP address to the VM if required.
 - You then commit the failover, to start accessing the workload from the replica Azure VM.

How do I access Azure VMs after failover?

After failover, you can access Azure VMs over a secure Internet connection, over a site-to-site VPN, or over Azure ExpressRoute. You'll need to prepare a number of things in order to connect. [Learn more](#).

Is failed over data resilient?

Azure is designed for resilience. Site Recovery is engineered for failover to a secondary Azure datacenter, in accordance with the Azure SLA. When failover occurs, we make sure your metadata and vaults remain within the same geographic region that you chose for your vault.

Is failover automatic?

[Failover](#) isn't automatic. You initiate failovers with single click in the portal, or you can use [PowerShell](#) to trigger a failover.

How do I fail back?

After your on-premises infrastructure is up and running again, you can fail back. Failback occurs in three stages:

1. You kick off a planned failover from Azure to the on-premises site using a couple of different options:
 - Minimize downtime: If you use this option Site Recovery synchronizes data before failover. It checks for changed data blocks and downloads them to the on-premises site, while the Azure VM keeps running, minimizing downtime. When you manually specify that the failover should complete, the Azure VM is shut down, any final delta changes are copied, and the failover starts.
 - Full download: With this option data is synchronized during failover. This option downloads the entire disk. It's faster because no checksums are calculated, but there's more downtime. Use this option if you've been running the replica Azure VMs for some time, or if the on-premises VM was deleted.
2. You can select to fail back to the same VM or to an alternate VM. You can specify that Site Recovery should create the VM if it doesn't already exist.
3. After initial synchronization finishes, you select to complete the failover. After it completes, you can sign in to the on-premises VM to check everything's working as expected. In the Azure portal, you can see that the

Azure VMs have been stopped.

4. You commit the failover to finish up, and start accessing the workload from the on-premises VM again.
5. After workloads have failed back, you enable reverse replication, so that the on-premises VMs replicate to Azure again.

Can I fail back to a different location?

Yes, if you failed over to Azure, you can fail back to a different location if the original one isn't available. [Learn more](#).

Support matrix for disaster recovery of on-premises Hyper-V VMs to Azure

1/27/2020 • 6 minutes to read • [Edit Online](#)

This article summarizes the supported components and settings for disaster recovery of on-premises Hyper-V VMs to Azure by using [Azure Site Recovery](#).

Supported scenarios

SCENARIO	DETAILS
Hyper-V with Virtual Machine Manager	<p>You can perform disaster recovery to Azure for VMs running on Hyper-V hosts that are managed in the System Center Virtual Machine Manager fabric.</p> <p>You can deploy this scenario in the Azure portal or by using PowerShell.</p> <p>When Hyper-V hosts are managed by Virtual Machine Manager, you also can perform disaster recovery to a secondary on-premises site. To learn more about this scenario, read this tutorial.</p>
Hyper-V without Virtual Machine Manager	<p>You can perform disaster recovery to Azure for VMs running on Hyper-V hosts that aren't managed by Virtual Machine Manager.</p> <p>You can deploy this scenario in the Azure portal or by using PowerShell.</p>

On-premises servers

SERVER	REQUIREMENTS	DETAILS
Hyper-V (running without Virtual Machine Manager)	Windows Server 2019, Windows Server 2016 (including server core installation), Windows Server 2012 R2 with latest updates	If you have already configured Windows Server 2012 R2 with/or SCVMM 2012 R2 with Azure Site Recovery and plan to upgrade the OS, please follow the guidance documentation .
Hyper-V (running with Virtual Machine Manager)	Virtual Machine Manager 2019, Virtual Machine Manager 2016, Virtual Machine Manager 2012 R2	<p>If Virtual Machine Manager is used, Windows Server 2019 hosts should be managed in Virtual Machine Manager 2019. Similarly, Windows Server 2016 hosts should be managed in Virtual Machine Manager 2016.</p> <p>Note: Fallback to alternate location is not supported for Windows Server 2019 hosts.</p>

Replicated VMs

The following table summarizes VM support. Site Recovery supports any workloads running on a supported operating system.

COMPONENT	DETAILS
VM configuration	VMs that replicate to Azure must meet Azure requirements .
Guest operating system	Any guest OS supported for Azure .. Windows Server 2016 Nano Server isn't supported.

VM/Disk management

ACTION	DETAILS
Resize disk on replicated Hyper-V VM	Not supported. Disable replication, make the change, and then re-enable replication for the VM.
Add disk on replicated Hyper-V VM	Not supported. Disable replication, make the change, and then re-enable replication for the VM.

Hyper-V network configuration

COMPONENT	HYPER-V WITH VIRTUAL MACHINE MANAGER	HYPER-V WITHOUT VIRTUAL MACHINE MANAGER
Host network: NIC Teaming	Yes	Yes
Host network: VLAN	Yes	Yes
Host network: IPv4	Yes	Yes
Host network: IPv6	No	No
Guest VM network: NIC Teaming	No	No
Guest VM network: IPv4	Yes	Yes
Guest VM network: IPv6	No	Yes
Guest VM network: Static IP (Windows)	Yes	Yes
Guest VM network: Static IP (Linux)	No	No
Guest VM network: Multi-NIC	Yes	Yes

Azure VM network configuration (after failover)

COMPONENT	HYPER-V WITH VIRTUAL MACHINE MANAGER	HYPER-V WITHOUT VIRTUAL MACHINE MANAGER
Azure ExpressRoute	Yes	Yes

COMPONENT	HYPER-V WITH VIRTUAL MACHINE MANAGER	HYPER-V WITHOUT VIRTUAL MACHINE MANAGER
ILB	Yes	Yes
ELB	Yes	Yes
Azure Traffic Manager	Yes	Yes
Multi-NIC	Yes	Yes
Reserved IP	Yes	Yes
IPv4	Yes	Yes
Retain source IP address	Yes	Yes
Azure Virtual Network service endpoints (without Azure Storage firewalls)	Yes	Yes
Accelerated Networking	No	No

Hyper-V host storage

STORAGE	HYPER-V WITH VIRTUAL MACHINE MANAGER	HYPER-V WITHOUT VIRTUAL MACHINE MANAGER
NFS	NA	NA
SMB 3.0	Yes	Yes
SAN (iSCSI)	Yes	Yes
Multi-path (MPIO). Tested with: Microsoft DSM, EMC PowerPath 5.7 SP4, EMC PowerPath DSM for CLARiON	Yes	Yes

Hyper-V VM guest storage

STORAGE	HYPER-V WITH VIRTUAL MACHINE MANAGER	HYPER-V WITHOUT VIRTUAL MACHINE MANAGER
VMDK	NA	NA
VHD/VHDX	Yes	Yes
Generation 2 VM	Yes	Yes

STORAGE	HYPER-V WITH VIRTUAL MACHINE MANAGER	HYPER-V WITHOUT VIRTUAL MACHINE MANAGER
EFI/UEFI The migrated VM in Azure will be automatically converted to a BIOS boot VM. The VM should be running Windows Server 2012 and later only. The OS disk should have up to five partitions or fewer and the size of OS disk should be less than 300 GB.	Yes	Yes
Shared cluster disk	No	No
Encrypted disk	No	No
NFS	NA	NA
SMB 3.0	No	No
RDM	NA	NA
Disk > 1 TB	Yes, up to 4,095 GB	Yes, up to 4,095 GB
Disk: 4K logical and physical sector	Not supported: Gen 1/Gen 2	Not supported: Gen 1/Gen 2
Disk: 4K logical and 512-bytes physical sector	Yes	Yes
Logical volume management (LVM). LVM is supported on data disks only. Azure provides only a single OS disk.	Yes	Yes
Volume with striped disk > 1 TB	Yes	Yes
Storage Spaces	No	No
Hot add/remove disk	No	No
Exclude disk	Yes	Yes
Multi-path (MPIO)	Yes	Yes

Azure Storage

COMPONENT	HYPER-V WITH VIRTUAL MACHINE MANAGER	HYPER-V WITHOUT VIRTUAL MACHINE MANAGER
Locally redundant storage	Yes	Yes
Geo-redundant storage	Yes	Yes
Read-access geo-redundant storage	Yes	Yes

COMPONENT	HYPER-V WITH VIRTUAL MACHINE MANAGER	HYPER-V WITHOUT VIRTUAL MACHINE MANAGER
Cool storage	No	No
Hot storage	No	No
Block blobs	No	No
Encryption at rest (SSE)	Yes	Yes
Encryption at rest (CMK) (Only for failover to managed disks)	Yes (via PowerShell Az 3.3.0 module onwards)	Yes (via PowerShell Az 3.3.0 module onwards)
Premium storage	Yes	Yes
Import/Export service	No	No
Azure Storage accounts with firewall enabled	Yes. For target storage and cache.	Yes. For target storage and cache.
Modify storage account	No. The target Azure Storage account can't be modified after enabling replication. To modify, disable and then re-enable disaster recovery.	No

Azure compute features

FEATURE	HYPER-V WITH VIRTUAL MACHINE MANAGER	HYPER-V WITHOUT VIRTUAL MACHINE MANAGER
Availability sets	Yes	Yes
HUB	Yes	Yes
Managed disks	Yes, for failover. Fallback of managed disks isn't supported.	Yes, for failover. Fallback of managed disks isn't supported.

Azure VM requirements

On-premises VMs that you replicate to Azure must meet the Azure VM requirements summarized in this table.

COMPONENT	REQUIREMENTS	DETAILS
Guest operating system	Site Recovery supports all operating systems that are supported by Azure .	Prerequisites check fails if unsupported.
Guest operating system architecture	32-bit (Windows Server 2008)/64-bit	Prerequisites check fails if unsupported.
Operating system disk size	Up to 2,048 GB for generation 1 VMs. Up to 300 GB for generation 2 VMs.	Prerequisites check fails if unsupported.

COMPONENT	REQUIREMENTS	DETAILS
Operating system disk count	1	Prerequisites check fails if unsupported.
Data disk count	16 or less	Prerequisites check fails if unsupported.
Data disk VHD size	Up to 4,095 GB	Prerequisites check fails if unsupported.
Network adapters	Multiple adapters are supported	
Shared VHD	Not supported	Prerequisites check fails if unsupported.
FC disk	Not supported	Prerequisites check fails if unsupported.
Hard disk format	VHD VHDX	Site Recovery automatically converts VHDX to VHD when you fail over to Azure. When you fail back to on-premises, the virtual machines continue to use the VHDX format.
BitLocker	Not supported	BitLocker must be disabled before you enable replication for a VM.
VM name	Between 1 and 63 characters. Restricted to letters, numbers, and hyphens. The VM name must start and end with a letter or number.	Update the value in the VM properties in Site Recovery.
VM type	Generation 1 Generation 2--Windows	Generation 2 VMs with an OS disk type of basic (which includes one or two data volumes formatted as VHDX) and less than 300 GB of disk space are supported. Linux Generation 2 VMs aren't supported. Learn more .

Recovery Services vault actions

ACTION	HYPER-V WITH VMM	HYPER-V WITHOUT VMM
Move vault across resource groups Within and across subscriptions	No	No
Move storage, network, Azure VMs across resource groups Within and across subscriptions	No	No

NOTE

When replicating Hyper-VMs from on-premises to Azure, you can replicate to only one AD tenant from one specific environment - Hyper-V site or Hyper-V with VMM as applicable.

Provider and agent

To make sure your deployment is compatible with settings in this article, make sure you're running the latest provider and agent versions.

NAME	DESCRIPTION	DETAILS
Azure Site Recovery provider	<p>Coordinates communications between on-premises servers and Azure</p> <p>Hyper-V with Virtual Machine Manager: Installed on Virtual Machine Manager servers</p> <p>Hyper-V without Virtual Machine Manager: Installed on Hyper-V hosts</p>	<p>Latest version: 5.1.2700.1 (available from the Azure portal)</p> <p>Latest features and fixes</p>
Microsoft Azure Recovery Services agent	<p>Coordinates replication between Hyper-V VMs and Azure</p> <p>Installed on on-premises Hyper-V servers (with or without Virtual Machine Manager)</p>	Latest agent available from the portal

Next steps

Learn how to [prepare Azure](#) for disaster recovery of on-premises Hyper-V VMs.

Hyper-V to Azure disaster recovery architecture

11/14/2019 • 7 minutes to read • [Edit Online](#)

This article describes the architecture and processes used when you replicate, fail over, and recover Hyper-V virtual machines (VMs) between on-premises Hyper-V hosts and Azure, using the [Azure Site Recovery](#) service.

Hyper-V hosts can optionally be managed in System Center Virtual Machine Manager (VMM) private clouds.

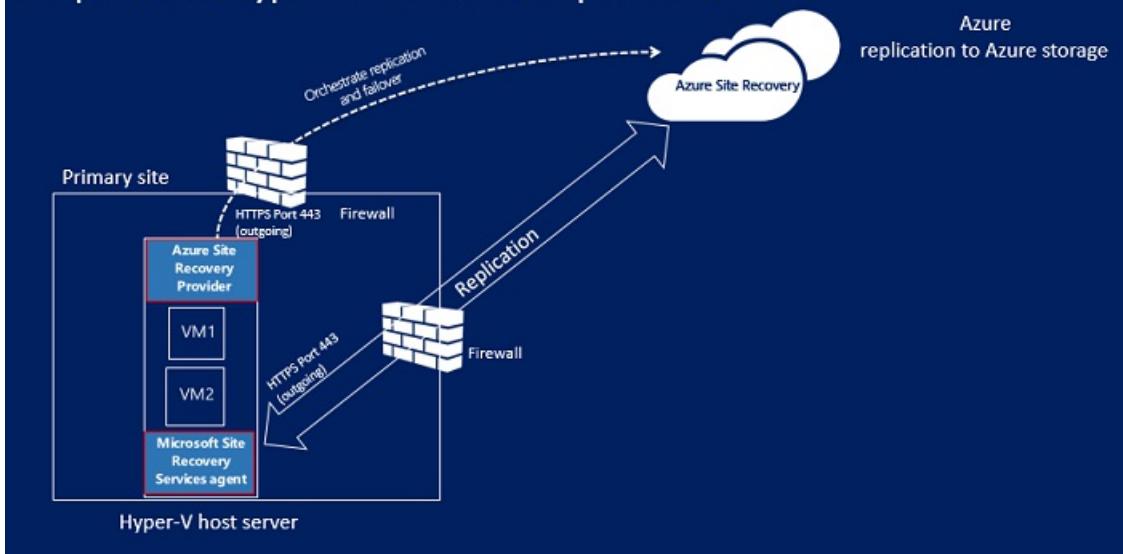
Architectural components - Hyper-V without VMM

The following table and graphic provide a high-level view of the components used for Hyper-V replication to Azure, when Hyper-V hosts aren't managed by VMM.

COMPONENT	REQUIREMENT	DETAILS
Azure	An Azure subscription, Azure storage account, and Azure network.	Replicated data from on-premises VM workloads is stored in the storage account. Azure VMs are created with the replicated workload data when failover from your on-premises site occurs. The Azure VMs connect to the Azure virtual network when they're created.
Hyper-V	During Site Recovery deployment, you gather Hyper-V hosts and clusters into Hyper-V sites. You install the Azure Site Recovery Provider and Recovery Services agent on each standalone Hyper-V host, or on each Hyper-V cluster node.	The Provider orchestrates replication with Site Recovery over the internet. The Recovery Services agent handles data replication. Communications from both the Provider and the agent are secure and encrypted. Replicated data in Azure storage is also encrypted.
Hyper-V VMs	One or more VMs running on Hyper-V.	Nothing needs to be explicitly installed on VMs.

Hyper-V to Azure architecture (without VMM)

On-premises Hyper-V site to Azure protection



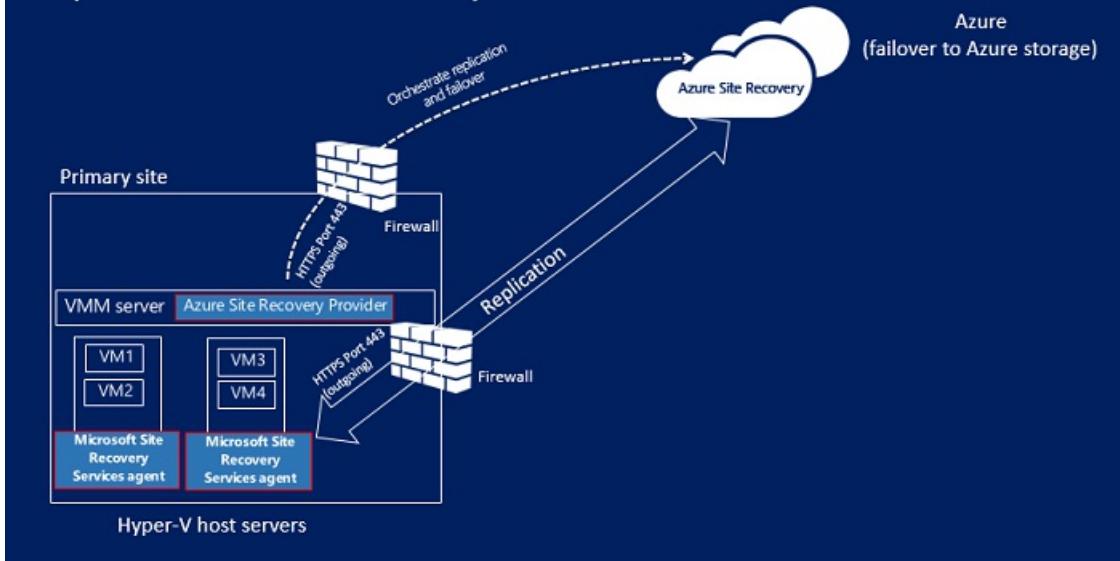
Architectural components - Hyper-V with VMM

The following table and graphic provide a high-level view of the components used for Hyper-V replication to Azure, when Hyper-V hosts are managed in VMM clouds.

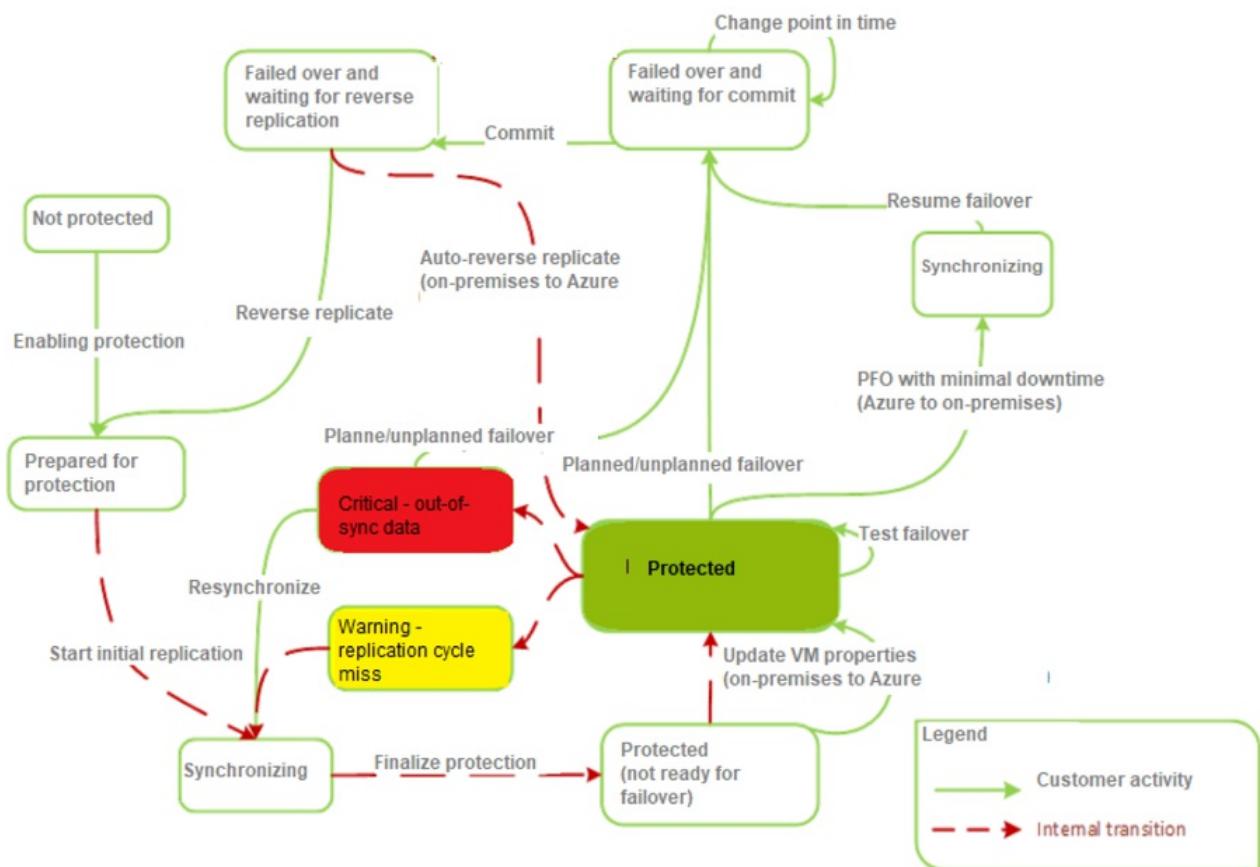
COMPONENT	REQUIREMENT	DETAILS
Azure	An Azure subscription, Azure storage account, and Azure network.	Replicated data from on-premises VM workloads is stored in the storage account. Azure VMs are created with the replicated data when failover from your on-premises site occurs. The Azure VMs connect to the Azure virtual network when they're created.
VMM server	The VMM server has one or more clouds containing Hyper-V hosts.	You install the Site Recovery Provider on the VMM server, to orchestrate replication with Site Recovery, and register the server in the Recovery Services vault.
Hyper-V host	One or more Hyper-V hosts/clusters managed by VMM.	You install the Recovery Services agent on each Hyper-V host or cluster node.
Hyper-V VMs	One or VMs running on a Hyper-V host server.	Nothing needs to explicitly installed on VMs.
Networking	Logical and VM networks set up on the VMM server. The VM network should be linked to a logical network that's associated with the cloud.	VM networks are mapped to Azure virtual networks. When Azure VMs are created after failover, they are added to the Azure network that's mapped to the VM network.

Hyper-V to Azure architecture (with VMM)

On-premises VMM to Azure protection



Replication process



Replication and recovery process

Enable protection

1. After you enable protection for a Hyper-V VM, in the Azure portal or on-premises, the **Enable protection** starts.
2. The job checks that the machine complies with prerequisites, before invoking the [CreateReplicationRelationship](#), to set up replication with the settings you've configured.
3. The job starts initial replication by invoking the [StartReplication](#) method, to initialize a full VM replication, and send the VM's virtual disks to Azure.
4. You can monitor the job in the **Jobs** tab.

The screenshot shows two windows related to a Site Recovery job.

Jobs window (Top):

- VaultName: robinnehraVault1
- Filter: Export jobs
- Message: More than 200 jobs found. Please refine your query.

Action	Status	Protected item	VM Size	Start Time	Duration
Enable protection	Successful	Protected item	VM2GB	8/30/2016 5:15:44 PM	00:00:42
Disable protection	Successful	Protected item	VMmissingFO	8/30/2016 5:15:07 PM	00:00:09
Refresh server details	Successful	Server	CP-B3L40405-04.ntdev.corp.m...	8/30/2016 5:11:35 PM	00:01:26
Planned failover	Failed	Protected item	VMmissingFO	8/30/2016 1:46:30 PM	00:07:54
Finalize protection on the virtu...	Successful	Protected item	VMmissingFO	8/30/2016 1:34:47 PM	00:02:00
Enable protection	Successful	Protected item	VMmissingFO	8/30/2016 12:36:50 PM	00:46:26

Enable protection window (Bottom):

- Site Recovery Job
- Export job

Properties section:

Vault	robinnehraVault1
Protected item	VMmissingFO
Job id	843e1b28-ba5f-40b2-9327-a32aacff47e-2016-08-30 07:06:50Z-lbz ActivityId: da7fa882-5958-4ff8-a3e1
Source server	ronehrB2Asite101
Target server	Microsoft Azure

Job section:

NAME	STATUS	START TIME	DURATION
Prerequisites check for enabling protection	Successful	8/30/2016 12:36:50 PM	00:00:07
Identifying the replication target	Successful	8/30/2016 12:36:58 PM	00:45:57
Enable replication	Successful	8/30/2016 1:22:56 PM	00:00:12
Starting initial replication	Successful	8/30/2016 1:23:08 PM	00:00:08
Updating the provider states	Successful	8/30/2016 1:23:16 PM	00:00:00

Initial data replication

- When initial replication is triggered, a [Hyper-V VM snapshot](#) snapshot is taken.
- Virtual hard disks on the VM are replicated one by one, until they're all copied to Azure. This might take a while, depending on the VM size, and network bandwidth. [Learn how](#) to increase network bandwidth.
- If disk changes occur while initial replication is in progress, the Hyper-V Replica Replication Tracker tracks the changes as Hyper-V replication logs (.hrl). These log files are located in the same folder as the disks. Each disk has an associated .hrl file that's sent to secondary storage. The snapshot and log files consume disk resources while initial replication is in progress.
- When the initial replication finishes, the VM snapshot is deleted.
- Delta disk changes in the log are synchronized and merged to the parent disk.

Finalize protection process

- After the initial replication finishes, the **Finalize protection on the virtual machine** job runs. It configures network and other post-replication settings, so that the VM is protected.
- At this stage you can check the VM settings to make sure that it's ready for failover. You can run a disaster recovery drill (test failover) for the VM, to check that it fails over as expected.

Delta replication

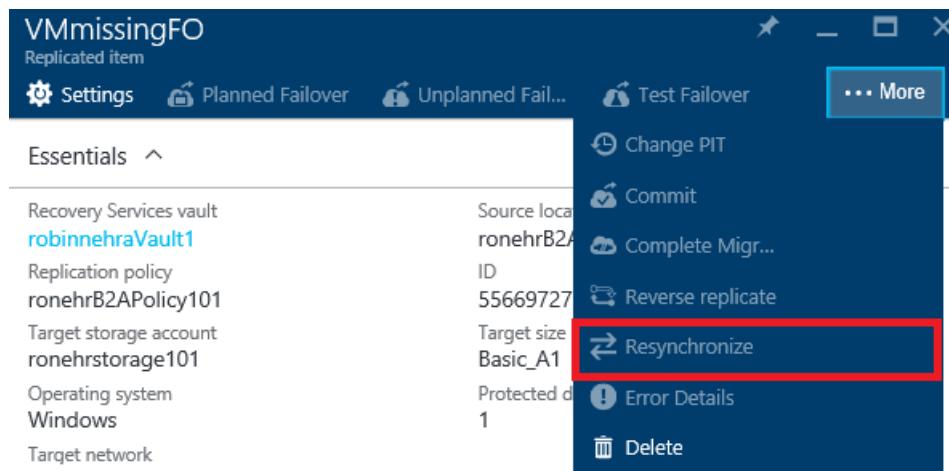
- After the initial replication, delta replication begins, in accordance with the replication policy.
- The Hyper-V Replica Replication Tracker tracks changes to a virtual hard disk as .hrl files. Each disk that's

configured for replication has an associated .hrl file.

3. The log is sent to the customer's storage account. When a log is in transit to Azure, the changes in the primary disk are tracked in another log file, in the same folder.
4. During initial and delta replication, you can monitor the VM in the Azure portal.

Resynchronization process

1. If delta replication fails, and a full replication would be costly in terms of bandwidth or time, then a VM is marked for resynchronization.
 - For example, if the .hrl files reach 50% of the disk size, then the VM will be marked for resynchronization.
 - By default resynchronization is scheduled to run automatically outside office hours.
2. Resynchronization sends delta data only.
 - It minimizes the amount of data sent by computing checksums of the source and target VMs.
 - It uses a fixed-block chunking algorithm where source and target files are divided into fixed chunks.
 - Checksums for each chunk are generated. These are compared to determine which blocks from the source need to be applied to the target.
3. After resynchronization finishes, normal delta replication should resume.
4. If you don't want to wait for default resynchronization outside hours, you can resynchronize a VM manually. For example, if an outage occurs. To do this, in the Azure portal, select the VM > **Resynchronize**.



Retry process

If a replication error occurs, there's a built-in retry. Retry is classified as described in the table.

CATEGORY	DETAILS
Non-recoverable errors	No retry is attempted. VM status will be Critical , and administrator intervention is required. Examples of these errors include a broken VHD chain, an invalid state for the replica VM, network authentication errors, authorization errors, and VM not found errors (for standalone Hyper-V servers).
Recoverable errors	Retries occur every replication interval, using an exponential back-off that increases the retry interval from the start of the first attempt by 1, 2, 4, 8, and 10 minutes. If an error persists, retry every 30 minutes. Examples of these include network errors, low disk errors, and low memory conditions.

Failover and failback process

1. You can run a planned or unplanned failover from on-premises Hyper-V VMs to Azure. If you run a planned failover, then source VMs are shut down to ensure no data loss. Run an unplanned failover if your primary site isn't accessible.
2. You can fail over a single machine, or create recovery plans, to orchestrate failover of multiple machines.
3. You run a failover. After the first stage of failover completes, you should be able to see the created replica VMs in Azure. You can assign a public IP address to the VM if required.
4. You then commit the failover, to start accessing the workload from the replica Azure VM.

After your on-premises infrastructure is up and running again, you can fail back. Failback occurs in three stages:

1. Kick off a planned failover from Azure to the on-premises site:
 - **Minimize downtime:** If you use this option Site Recovery synchronizes data before failover. It checks for changed data blocks and downloads them to the on-premises site, while the Azure VM keeps running, minimizing downtime. When you manually specify that the failover should complete, the Azure VM is shut down, any final delta changes are copied, and the failover starts.
 - **Full download:** With this option data is synchronized during failover. This option downloads the entire disk. It's faster because no checksums are calculated, but there's more downtime. Use this option if you've been running the replica Azure VMs for some time, or if the on-premises VM was deleted.
 - **Create VM:** You can select to fail back to the same VM or to an alternate VM. You can specify that Site Recovery should create the VM if it doesn't already exist.
2. After initial synchronization finishes, you select to complete the failover. After it completes, you can log onto the on-premises VM to check everything's working as expected. In the Azure portal, you can see that the Azure VMs have been stopped.
3. Then, you commit the failover to finish up, and start accessing the workload from the on-premises VM again.
4. After workloads have failed back, you enable reverse replication, so that the on-premises VMs replicate to Azure again.

Next steps

Follow [this tutorial](#) to get started with Hyper-V to Azure replication.

Exclude disks from disaster recovery

12/26/2019 • 10 minutes to read • [Edit Online](#)

This article describes how to exclude disks from replication during disaster recovery from on-premises to Azure with [Azure Site Recovery](#). You might exclude disks from replication for a number of reasons:

- So that unimportant data churned on the excluded disk isn't replicated.
- To optimize consumed replication bandwidth, or target-side resources.
- To save storage and network resources by not replicating data that you don't need.
- Azure VMs have reached Site Recovery replication limits.

Supported scenarios

You can exclude disks from replication as summarized in the table.

AZURE TO AZURE	VMWARE TO AZURE	HYPER-V TO AZURE
Yes (using PowerShell)	Yes	Yes

Exclude limitations

LIMITATION	AZURE VMS	VMWARE VMS	HYPER-V VMS
Disk types	You can exclude basic disks from replication. You can't exclude operating system disks or dynamic disks. Temp disks are excluded by default.	You can exclude basic disks from replication. You can't exclude operating system disks or dynamic disks.	You can exclude basic disks from replication. You can't exclude operating system disks. We recommend that you don't exclude dynamic disks. Site Recovery can't identify which VHS is basic or dynamic in the guest VM. If all dependent dynamic volume disks aren't excluded, the protected dynamic disk becomes a failed disk on a failover VM, and the data on that disk isn't accessible.
Replicating disk	You can't exclude a disk that's replicating. Disable and reenable replication for the VM.	You can't exclude a disk that's replicating.	You can't exclude a disk that's replicating.

LIMITATION	AZURE VMS	VMWARE VMS	HYPER-V VMS
Mobility service (VMware)	Not relevant	<p>You can exclude disks only on VMs that have the Mobility service installed.</p> <p>This means that you have to manually install the Mobility service on the VMs for which you want to exclude disks. You can't use the push installation mechanism because it installs the Mobility service only after replication is enabled.</p>	Not relevant.
Add/Remove	You can add and remove disks on Azure VMs with managed disks.	You can't add or remove disks after replication is enabled. Disable and then reenable replication to add a disk.	You can't add or remove disks after replication is enabled. Disable and then reenable replication.
Failover	<p>If an app needs a disk that you excluded, after failover you need to create the disk manually so that the replicated app can run.</p> <p>Alternatively, you can create the disk during VM failover, by integrating Azure automation into a recovery plan.</p>	If you exclude a disk that an app needs, create it manually in Azure after failover.	If you exclude a disk that an app needs, create it manually in Azure after failover.
On-premises failback-disks created manually	Not relevant	<p>Windows VMs: Disks created manually in Azure aren't failed back. For example, if you fail over three disks and create two disks directly on an Azure VM, only the three disks that were failed over are then failed back.</p> <p>Linux VMs: Disks created manually in Azure are failed back. For example, if you fail over three disks and create two disks on an Azure VM, all five will be failed back. You can't exclude disks that were created manually from failback.</p>	Disks created manually in Azure aren't failed back. For example, if you fail over three disks and create two disks directly on an Azure VM, only the three disks that were failed over will be failed back.

LIMITATION	AZURE VMS	VMWARE VMS	HYPER-V VMS
On-premises fallback- Excluded disks	Not relevant	If you fail back to the original machine, the fallback VM disk configuration doesn't include the excluded disks. Disks that were excluded from VMware to Azure replication aren't available on the fallback VM.	When failback is to the original Hyper-V location, the fallback VM disk configuration remains the same as that of original source VM disk. Disks that were excluded from Hyper-V site to Azure replication are available on the fallback VM.

Typical scenarios

Examples of data churn that are great candidates for exclusion include writes to a paging file (pagefile.sys), and writes to the tempdb file of Microsoft SQL Server. Depending on the workload and the storage subsystem, the paging and tempdb files can register a significant amount of churn. Replicating this type of data to Azure is resource-intensive.

- To optimize replication for a VM with a single virtual disk that includes both the operating system and the paging file, you could:
 1. Split the single virtual disk into two virtual disks. One virtual disk has the operating system, and the other has the paging file.
 2. Exclude the paging file disk from replication.
- To optimize replication for a disk that includes both the Microsoft SQL Server tempdb file and the system database file, you could:
 1. Keep the system database and tempdb on two different disks.
 2. Exclude the tempdb disk from replication.

Example 1: Exclude the SQL Server tempdb disk

Let's look at how to handle disk exclusion, failover, and failover for a source SQL Server Windows VM - **SalesDB***, for which we want to exclude tempdb.

Exclude disks from replication

We have these disks on the source Windows VM SalesDB.

DISK NAME	GUEST OS DISK	DRIVE LETTER	DISK DATA TYPE
DB-Disk0-OS	Disk0	C:\	Operating system disk.
DB-Disk1	Disk1	D:\	SQL system database and User Database1.
DB-Disk2 (Excluded the disk from protection)	Disk2	E:\	Temp files.
DB-Disk3 (Excluded the disk from protection)	Disk3	F:\	SQL tempdb database. Folder path - F:\MSSQL\Data. Make a note of the folder path before failover.

DISK NAME	GUEST OS DISK	DRIVE LETTER	DISK DATA TYPE
DB-Disk4	Disk4	G:\	User Database2

1. We enable replication for the SalesDB VM.
2. We exclude Disk2 and Disk3 from replication because data churn on those disks is temporary.

Handle disks during failover

Since disks aren't replicated, when you fail over to Azure these disks aren't present on the Azure VM created after failover. The Azure VM has the disks summarized in this table.

GUEST OS DISK	DRIVE LETTER	DISK DATA TYPE
Disk0	C:\	Operating system disk.
Disk1	E:\	Temporary storage Azure adds this disk. Because Disk2 and Disk3 were excluded from replication, E: is the first drive letter from the available list. Azure assigns E: to the temporary storage volume. Other drive letters for replicated disks remain the same.
Disk2	D:\	SQL system database and User Database1
Disk3	G:\	User Database2

In our example, since Disk3, the SQL tempdb disk, was excluded from replication and isn't available on the Azure VM, the SQL service is in a stopped state, and it needs the F:\MSSQL\Data path. You can create this path in a couple of ways:

- Add a new disk after failover, and assign tempdb folder path.
- Use an existing temporary storage disk for the tempdb folder path.

Add a new disk after failover

1. Write down the paths of SQL tempdb.mdf and tempdb.ldf before failover.
2. From the Azure portal, add a new disk to the failover Azure VM. The disk should be the same size (or larger) as the source SQL tempdb disk (Disk3).
3. Sign in to the Azure VM.
4. From the disk management (diskmgmt.msc) console, initialize and format the newly added disk.
5. Assign the same drive letter that was used by the SQL tempdb disk (F:)
6. Create a tempdb folder on the F: volume (F:\MSSQL\Data).
7. Start the SQL service from the service console.

Use an existing temporary storage disk

1. Open a command prompt.
2. Run SQL Server in recovery mode from the command prompt.

```
Net start MSSQLSERVER /f / T3608
```

3. Run the following sqlcmd to change the tempdb path to the new path.

```

sqlcmd -A -S SalesDB **Use your SQL DBname**
USE master;
GO
ALTER DATABASE tempdb
MODIFY FILE (NAME = tempdev, FILENAME = 'E:\MSSQL\tempdata\tempdb.mdf');
GO
ALTER DATABASE tempdb
MODIFY FILE (NAME = templog, FILENAME = 'E:\MSSQL\tempdata\templog.ldf');
GO

```

4. Stop the Microsoft SQL Server service.

```
Net stop MSSQLSERVER
```

5. Start the Microsoft SQL Server service.

```
Net start MSSQLSERVER
```

VMware VMs: Disks during failback to original location

Now let's see how to handle disks on VMware VMs when you fail back to your original on-premises location.

- **Disks created in Azure:** Since our example uses a Windows VM, disks that you create manually in Azure aren't replicated back to your site when you fail back or reprotect a VM.
- **Temporary storage disk in Azure:** The temporary storage disk isn't replicated back to on-premises hosts.
- **Excluded disks:** Disks that were excluded from VMware to Azure replication aren't available on the on-premises VM after failback.

Before you fail back the VMware VMs to the original location, the Azure VM disk settings are as follows.

GUEST OS DISK	DRIVE LETTER	DISK DATA TYPE
Disk0	C:\	Operating system disk.
Disk1	E:\	Temporary storage.
Disk2	D:\	SQL system database and User Database1.
Disk3	G:\	User Database2.

After failback, the VMware VM in the original location has the disks summarized in the table.

GUEST OS DISK	DRIVE LETTER	DISK DATA TYPE
Disk0	C:\	Operating system disk.
Disk1	D:\	SQL system database and User Database1.
Disk2	G:\	User Database2.

Hyper-V VMs: Disks during failback to original location

Now let's see how to handle disks on Hyper-V VMs when you fail back to your original on-premises location.

- **Disks created in Azure:** Disks that you create manually in Azure aren't replicated back to your site when you fail back or reprotect a VM.
- **Temporary storage disk in Azure:** The temporary storage disk isn't replicated back to on-premises hosts.
- **Excluded disks:** After failback the VM disk configuration is the same as the original VM disk configuration. Disks that were excluded from replication from Hyper-V to Azure are available on the failback VM.

Before you fail back the Hyper-V VMs to the original location, the Azure VM disk settings are as follows.

GUEST OS DISK	DRIVE LETTER	DISK DATA TYPE
Disk0	C:\	Operating system disk.
Disk1	E:\	Temporary storage.
Disk2	D:\	SQL system database and User Database1.
Disk3	G:\	User Database2.

After planned failover (failback) from Azure to on-premises Hyper-V, the Hyper-V VM in the original location has the disks summarized in the table.

DISK NAME	GUEST OS DISK#	DRIVE LETTER	DISK DATA TYPE
DB-Disk0-OS	Disk0	C:\	Operating system disk.
DB-Disk1	Disk1	D:\	SQL system database and User Database1.
DB-Disk2 (Excluded disk)	Disk2	E:\	Temp files.
DB-Disk3 (Excluded disk)	Disk3	F:\	SQL tempdb database Folder path (F:\MSSQL\Data).
DB-Disk4	Disk4	G:\	User Database2

Example 2: Exclude the paging file disk

Let's look at how to handle disk exclusion, failover, and failover for a source Windows VM, for which we want to exclude the pagefile.sys file disk on both the D drive, and an alternate drive.

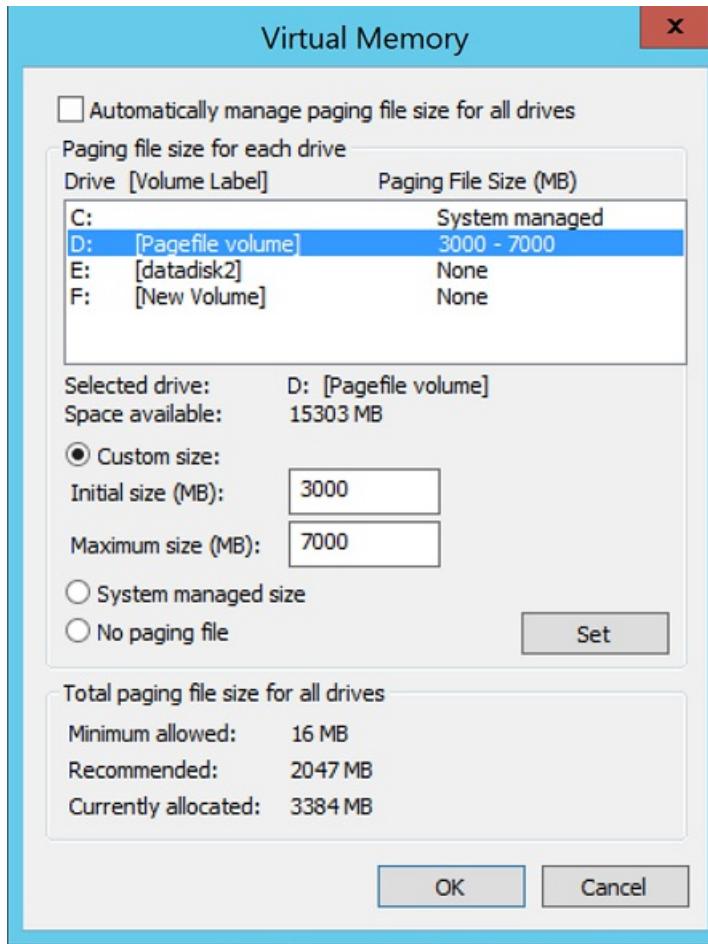
Paging file on the D drive

We have these disks on the source VM.

DISK NAME	GUEST OS DISK	DRIVE LETTER	DISK DATA TYPE
DB-Disk0-OS	Disk0	C:\	Operating system disk
DB-Disk1 (Exclude from replication)	Disk1	D:\	pagefile.sys
DB-Disk2	Disk2	E:\	User data 1

DISK NAME	GUEST OS DISK	DRIVE LETTER	DISK DATA TYPE
DB-Disk3	Disk3	F:\	User data 2

Our paging file settings on the source VM are as follows:



1. We enable replication for the VM.
2. We exclude DB-Disk1 from replication.

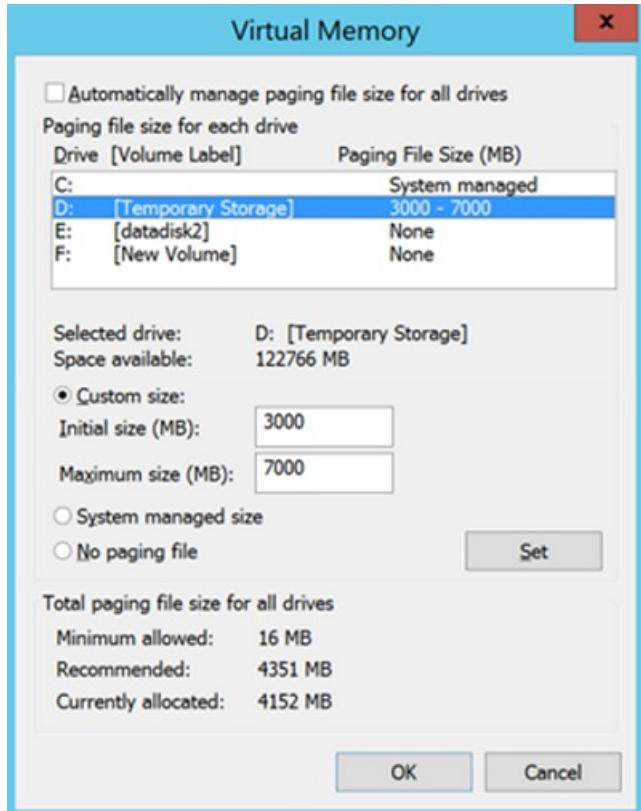
Disks after failover

After failover the Azure VM has the disks summarized in the table.

DISK NAME	GUEST OPERATING SYSTEM DISK#	DRIVE LETTER	DATA TYPE ON THE DISK
DB-Disk0-OS	Disk0	C:\	Operating system disk
DB-Disk1	Disk1	D:\	<p>Temporary storage/pagefile.sys</p> <p>Because DB-Disk1 (D:) was excluded, D: is the first drive letter from the available list.</p> <p>Azure assigns D: to the temporary storage volume.</p> <p>Because D: is available, the VM paging file setting remains the same).</p>

DISK NAME	GUEST OPERATING SYSTEM DISK#	DRIVE LETTER	DATA TYPE ON THE DISK
DB-Disk2	Disk2	E:\	User data 1
DB-Disk3	Disk3	F:\	User data 2

Our paging file settings on the Azure VM are as follows:



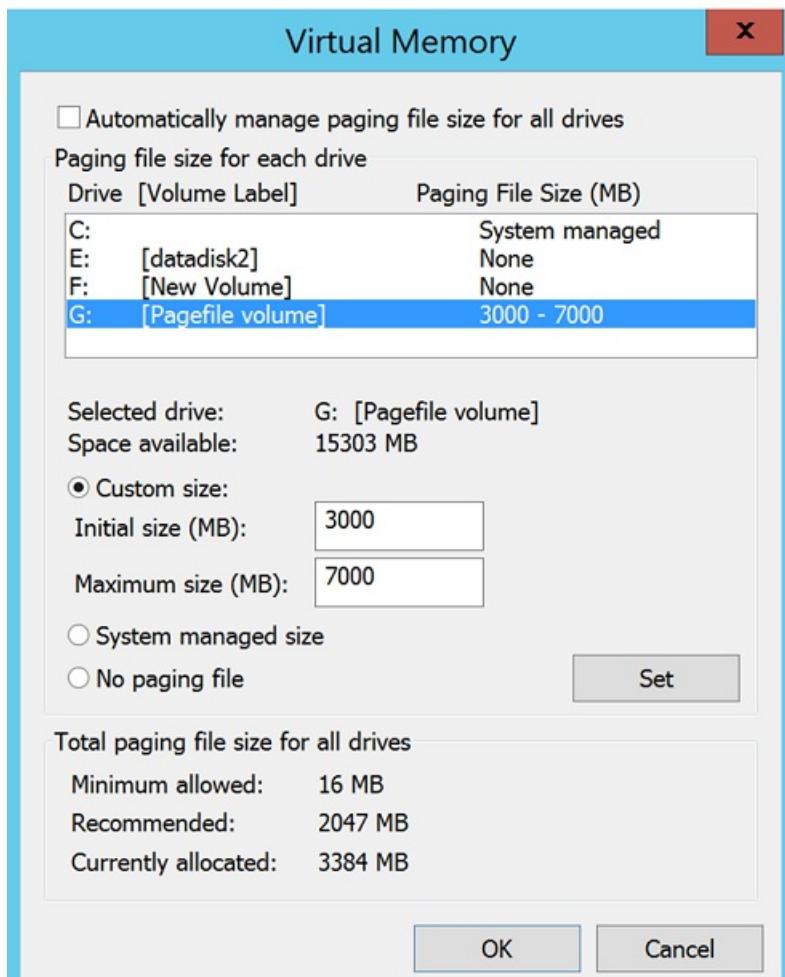
Paging file on another drive (not D:)

Let's look at example in which the paging file isn't on the D drive.

We have these disks on the source VM.

DISK NAME	GUEST OS DISK	DRIVE LETTER	DISK DATA TYPE
DB-Disk0-OS	Disk0	C:\	Operating system disk
DB-Disk1 (Exclude from replication)	Disk1	G:\	pagefile.sys
DB-Disk2	Disk2	E:\	User data 1
DB-Disk3	Disk3	F:\	User data 2

Our paging file settings on the on-premises VM are as follows:



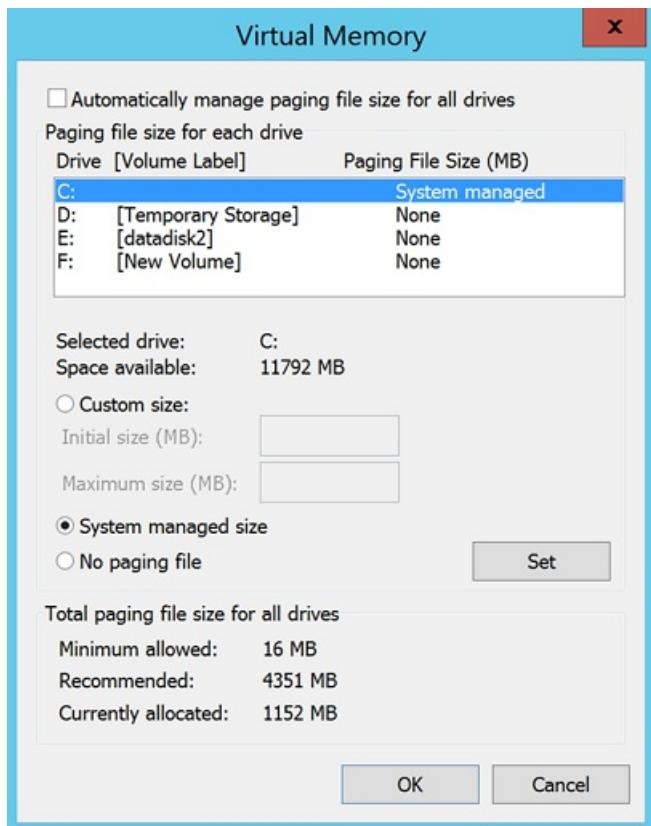
1. We enable replication for the VM.
2. We exclude DB-Disk1 from replication.

Disks after failover

After failover the Azure VM has the disks summarized in the table.

DISK NAME	GUEST OS DISK#	DRIVE LETTER	DISK DATA TYPE
DB-Disk0-OS	Disk0	C:\	Operating system disk
DB-Disk1	Disk1	D:\	Temporary storage Because D: is the first drive letter from available the list, Azure assigns D: to the temporary storage volume. For all the replicated disks, the drive letter remains the same.
			Because the G: disk isn't available, the system will use the C: drive for the paging file.
DB-Disk2	Disk2	E:\	User data 1
DB-Disk3	Disk3	F:\	User data 2

Our paging file settings on the Azure VM are as follows:



Next steps

- Learn more about guidelines for the temporary storage disk:
 - [Learn about](#) using SSDs in Azure VMs to store SQL Server TempDB and Buffer Pool Extensions
 - [Review](#) performance best practices for SQL Server in Azure VMs.
- After your deployment is set up and running, [learn more](#) about different types of failover.

Support matrix for disaster recovery of VMware VMs and physical servers to Azure

2/18/2020 • 15 minutes to read • [Edit Online](#)

This article summarizes supported components and settings for disaster recovery of VMware VMs and physical servers to Azure using [Azure Site Recovery](#).

- [Learn more](#) about VMware VM/physical server disaster recovery architecture.
- Follow our [tutorials](#) to try out disaster recovery.

Deployment scenarios

SCENARIO	DETAILS
Disaster recovery of VMware VMs	Replication of on-premises VMware VMs to Azure. You can deploy this scenario in the Azure portal or by using PowerShell .
Disaster recovery of physical servers	Replication of on-premises Windows/Linux physical servers to Azure. You can deploy this scenario in the Azure portal.

On-premises virtualization servers

SERVER	REQUIREMENTS	DETAILS
vCenter Server	Version 6.7, 6.5, 6.0, or 5.5	We recommend that you use a vCenter server in your disaster recovery deployment.
vSphere hosts	Version 6.7, 6.5, 6.0, or 5.5	We recommend that vSphere hosts and vCenter servers are located in the same network as the process server. By default the process server runs on the configuration server. Learn more .

Site Recovery configuration server

The configuration server is an on-premises machine that runs Site Recovery components, including the configuration server, process server, and master target server.

- For VMware VMs you set the configuration server by downloading an OVF template to create a VMware VM.
- For physical servers, you set up the configuration server machine manually.

COMPONENT	REQUIREMENTS
CPU cores	8
RAM	16 GB

COMPONENT	REQUIREMENTS
Number of disks	3 disks Disks include the OS disk, process server cache disk, and retention drive for fallback.
Disk free space	600 GB of space for the process server cache.
Disk free space	600 GB of space for the retention drive.
Operating system	Windows Server 2012 R2, or Windows Server 2016 with Desktop experience If you plan to use the in-built Master Target of this appliance for fallback, ensure that the OS version is same or higher than the replicated items.
Operating system locale	English (en-us)
PowerCLI	Not needed for configuration server version 9.14 or later.
Windows Server roles	Don't enable Active Directory Domain Services; Internet Information Services (IIS) or Hyper-V.
Group policies	- Prevent access to the command prompt. - Prevent access to registry editing tools. - Trust logic for file attachments. - Turn on Script Execution. - Learn more
IIS	Make sure you: - Don't have a preexisting default website - Enable anonymous authentication - Enable FastCGI setting - Don't have preexisting website/app listening on port 443
NIC type	VMXNET3 (when deployed as a VMware VM)
IP address type	Static
Ports	443 used for control channel orchestration 9443 for data transport

Replicated machines

Site Recovery supports replication of any workload running on a supported machine.

NOTE

The following table lists the support for machines with BIOS boot. Please refer to [Storage](#) section for support on UEFI based machines.

COMPONENT	DETAILS
Machine settings	Machines that replicate to Azure must meet Azure requirements .
Machine workload	Site Recovery supports replication of any workload running on a supported machine. Learn more .
Windows Server 2019	Supported from Update rollup 34 (version 9.22 of the Mobility service) onwards.
Windows Server 2016 64-bit	Supported for Server Core, Server with Desktop Experience.
Windows Server 2012 R2 / Windows Server 2012	Supported.
Windows Server 2008 R2 with SP1 onwards.	Supported. From version 9.30 of the Mobility service agent, you need servicing stack update (SSU) and SHA-2 update installed on machines running Windows 2008 R2 with SP1 or later. SHA-1 isn't supported from September 2019, and if SHA-2 code signing isn't enabled the agent extension won't install/upgrade as expected. Learn more about SHA-2 upgrade and requirements .
Windows Server 2008 with SP2 or later (64-bit/32-bit)	Supported for migration only. Learn more . From version 9.30 of the Mobility service agent, you need servicing stack update (SSU) and SHA-2 update installed on Windows 2008 SP2 machines. ISHA-1 isn't supported from September 2019, and if SHA-2 code signing isn't enabled the agent extension won't install/upgrade as expected. Learn more about SHA-2 upgrade and requirements .
Windows 10, Windows 8.1, Windows 8	Supported.
Windows 7 with SP1 64-bit	Supported from Update rollup 36 (version 9.22 of the Mobility service) onwards. From 9.30 of the Mobility service agent, you need servicing stack update (SSU) and SHA-2 update installed on Windows 7 SP1 machines. SHA-1 isn't supported from September 2019, and if SHA-2 code signing isn't enabled the agent extension won't install/upgrade as expected. Learn more about SHA-2 upgrade and requirements .

COMPONENT	DETAILS
Linux	<p>Only 64-bit system is supported. 32-bit system isn't supported.</p> <p>Every Linux server should have Linux Integration Services (LIS) components installed. It is required to boot the server in Azure after test failover/failover. If LIS components are missing, ensure to install the components before enabling replication for the machines to boot in Azure.</p> <p>Site Recovery orchestrates failover to run Linux servers in Azure. However Linux vendors might limit support to only distribution versions that haven't reached end-of-life.</p> <p>On Linux distributions, only the stock kernels that are part of the distribution minor version release/update are supported.</p> <p>Upgrading protected machines across major Linux distribution versions isn't supported. To upgrade, disable replication, upgrade the operating system, and then enable replication again.</p> <p>Learn more about support for Linux and open-source technology in Azure.</p>
Linux Red Hat Enterprise	<p>5.2 to 5.11 6.1 to 6.10 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 8.0, 8.1</p> <p>Servers running Red Hat Enterprise Linux 5.2-5.11 & 6.1-6.10 do not have Linux Integration Services (LIS) components pre-installed. Ensure to install the components before enabling replication for the machines to boot in Azure.</p>
Linux: CentOS	<p>5.2 to 5.11 6.1 to 6.10 7.0 to 7.6</p> <p>8.0 to 8.1</p> <p>Servers running CentOS 5.2-5.11 & 6.1-6.10 do not have Linux Integration Services (LIS) components pre-installed. Ensure to install the components before enabling replication for the machines to boot in Azure.</p>
Ubuntu	<p>Ubuntu 14.04 LTS server (review supported kernel versions)</p> <p>Ubuntu 16.04 LTS server (review supported kernel versions)</p> <p>Ubuntu 18.04 LTS server (review supported kernel versions)</p>
Debian	Debian 7/Debian 8 (review supported kernel versions)

COMPONENT	DETAILS
SUSE Linux	<p>SUSE Linux Enterprise Server 12 SP1, SP2, SP3, SP4 (review supported kernel versions)</p> <p>SUSE Linux Enterprise Server 15, 15 SP1 (review supported kernel versions)</p> <p>SUSE Linux Enterprise Server 11 SP3, SUSE Linux Enterprise Server 11 SP4</p> <p>Upgrading replicated machines from SUSE Linux Enterprise Server 11 SP3 to SP4 isn't supported. To upgrade, disable replication and re-enable after the upgrade.</p>
Oracle Linux	<p>6.4, 6.5, 6.6, 6.7, 6.8, 6.9, 6.10, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7</p> <p>Running the Red Hat compatible kernel or Unbreakable Enterprise Kernel Release 3, 4 & 5 (UEK3, UEK4, UEK5)</p>

NOTE

For each of the Windows versions, Azure Site Recovery only supports [Long-Term Servicing Channel \(LTSC\)](#) builds. [Semi-Annual Channel](#) releases are currently unsupported at this time.

Ubuntu kernel versions

SUPPORTED RELEASE	MOBILITY SERVICE VERSION	KERNEL VERSION
14.04 LTS	9.32	3.13.0-24-generic to 3.13.0-170-generic, 3.16.0-25-generic to 3.16.0-77-generic, 3.19.0-18-generic to 3.19.0-80-generic, 4.2.0-18-generic to 4.2.0-42-generic, 4.4.0-21-generic to 4.4.0-148-generic, 4.15.0-1023-azure to 4.15.0-1045-azure
14.04 LTS	9.31	3.13.0-24-generic to 3.13.0-170-generic, 3.16.0-25-generic to 3.16.0-77-generic, 3.19.0-18-generic to 3.19.0-80-generic, 4.2.0-18-generic to 4.2.0-42-generic, 4.4.0-21-generic to 4.4.0-148-generic, 4.15.0-1023-azure to 4.15.0-1045-azure
14.04 LTS	9.30	3.13.0-24-generic to 3.13.0-170-generic, 3.16.0-25-generic to 3.16.0-77-generic, 3.19.0-18-generic to 3.19.0-80-generic, 4.2.0-18-generic to 4.2.0-42-generic, 4.4.0-21-generic to 4.4.0-148-generic, 4.15.0-1023-azure to 4.15.0-1045-azure

SUPPORTED RELEASE	MOBILITY SERVICE VERSION	KERNEL VERSION
14.04 LTS	9.29	3.13.0-24-generic to 3.13.0-170-generic, 3.16.0-25-generic to 3.16.0-77-generic, 3.19.0-18-generic to 3.19.0-80-generic, 4.2.0-18-generic to 4.2.0-42-generic, 4.4.0-21-generic to 4.4.0-148-generic, 4.15.0-1023-azure to 4.15.0-1045-azure
16.04 LTS	9.32	4.4.0-21-generic to 4.4.0-171-generic, 4.8.0-34-generic to 4.8.0-58-generic, 4.10.0-14-generic to 4.10.0-42-generic, 4.11.0-13-generic to 4.11.0-14-generic, 4.13.0-16-generic to 4.13.0-45-generic, 4.15.0-13-generic to 4.15.0-74-generic 4.11.0-1009-azure to 4.11.0-1016-azure, 4.13.0-1005-azure to 4.13.0-1018-azure 4.15.0-1012-azure to 4.15.0-1066-azure
16.04 LTS	9.31	4.4.0-21-generic to 4.4.0-170-generic, 4.8.0-34-generic to 4.8.0-58-generic, 4.10.0-14-generic to 4.10.0-42-generic, 4.11.0-13-generic to 4.11.0-14-generic, 4.13.0-16-generic to 4.13.0-45-generic, 4.15.0-13-generic to 4.15.0-72-generic 4.11.0-1009-azure to 4.11.0-1016-azure, 4.13.0-1005-azure to 4.13.0-1018-azure 4.15.0-1012-azure to 4.15.0-1063-azure

SUPPORTED RELEASE	MOBILITY SERVICE VERSION	KERNEL VERSION
16.04 LTS	9.30	4.4.0-21-generic to 4.4.0-166-generic, 4.8.0-34-generic to 4.8.0-58-generic, 4.10.0-14-generic to 4.10.0-42-generic, 4.11.0-13-generic to 4.11.0-14-generic, 4.13.0-16-generic to 4.13.0-45-generic, 4.15.0-13-generic to 4.15.0-66-generic 4.11.0-1009-azure to 4.11.0-1016-azure, 4.13.0-1005-azure to 4.13.0-1018-azure 4.15.0-1012-azure to 4.15.0-1061-azure
16.04 LTS	9.29	4.4.0-21-generic to 4.4.0-164-generic, 4.8.0-34-generic to 4.8.0-58-generic, 4.10.0-14-generic to 4.10.0-42-generic, 4.11.0-13-generic to 4.11.0-14-generic, 4.13.0-16-generic to 4.13.0-45-generic, 4.15.0-13-generic to 4.15.0-64-generic 4.11.0-1009-azure to 4.11.0-1016-azure, 4.13.0-1005-azure to 4.13.0-1018-azure 4.15.0-1012-azure to 4.15.0-1059-azure
18.04 LTS	9.32	4.15.0-20-generic to 4.15.0-74-generic 4.18.0-13-generic to 4.18.0-25-generic 5.0.0-15-generic to 5.0.0-37-generic 5.3.0-19-generic to 5.3.0-24-generic 4.15.0-1009-azure to 4.15.0-1037-azure 4.18.0-1006-azure to 4.18.0-1025-azure 5.0.0-1012-azure to 5.0.0-1028-azure 5.3.0-1007-azure to 5.3.0-1009-azure

SUPPORTED RELEASE	MOBILITY SERVICE VERSION	KERNEL VERSION
18.04 LTS	9.31	4.15.0-20-generic to 4.15.0-72-generic 4.18.0-13-generic to 4.18.0-25-generic 5.0.0-15-generic to 5.0.0-37-generic 5.3.0-19-generic to 5.3.0-24-generic 4.15.0-1009-azure to 4.15.0-1037-azure 4.18.0-1006-azure to 4.18.0-1025-azure 5.0.0-1012-azure to 5.0.0-1025-azure 5.3.0-1007-azure
18.04 LTS	9.30	4.15.0-20-generic to 4.15.0-66-generic 4.18.0-13-generic to 4.18.0-25-generic 5.0.0-15-generic to 5.0.0-32-generic 4.15.0-1009-azure to 4.15.0-1037-azure 4.18.0-1006-azure to 4.18.0-1025-azure 5.0.0-1012-azure to 5.0.0-1023-azure
18.04 LTS	9.29	4.15.0-20-generic to 4.15.0-62-generic 4.18.0-13-generic to 4.18.0-25-generic 5.0.0-15-generic to 5.0.0-27-generic 4.15.0-1009-azure to 4.15.0-1037-azure 4.18.0-1006-azure to 4.18.0-1025-azure 5.0.0-1012-azure to 5.0.0-1018-azure

Debian kernel versions

SUPPORTED RELEASE	MOBILITY SERVICE VERSION	KERNEL VERSION
Debian 7	9.29 , 9.30 , 9.31 , 9.32	3.2.0-4-amd64 to 3.2.0-6-amd64, 3.16.0-0.bpo.4-amd64
Debian 8	9.30 , 9.31 , 9.32	3.16.0-4-amd64 to 3.16.0-10-amd64, 4.9.0-0.bpo.4-amd64 to 4.9.0-0.bpo.11-amd64
Debian 8	9.29	3.16.0-4-amd64 to 3.16.0-10-amd64, 4.9.0-0.bpo.4-amd64 to 4.9.0-0.bpo.9-amd64

SUSE Linux Enterprise Server 12 supported kernel versions

RELEASE	MOBILITY SERVICE VERSION	KERNEL VERSION
---------	--------------------------	----------------

RELEASE	MOBILITY SERVICE VERSION	KERNEL VERSION
SUSE Linux Enterprise Server 12 (SP1,SP2,SP3,SP4)	9.32	All stock SUSE 12 SP1,SP2,SP3,SP4 kernels are supported. 4.4.138-4.7-azure to 4.4.180-4.31-azure, 4.12.14-6.3-azure to 4.12.14-6.34-azure
SUSE Linux Enterprise Server 12 (SP1,SP2,SP3,SP4)	9.31	All stock SUSE 12 SP1,SP2,SP3,SP4 kernels are supported. 4.4.138-4.7-azure to 4.4.180-4.31-azure, 4.12.14-6.3-azure to 4.12.14-6.29-azure
SUSE Linux Enterprise Server 12 (SP1,SP2,SP3,SP4)	9.30	All stock SUSE 12 SP1,SP2,SP3,SP4 kernels are supported. 4.4.138-4.7-azure to 4.4.180-4.31-azure, 4.12.14-6.3-azure to 4.12.14-6.26-azure
SUSE Linux Enterprise Server 12 (SP1,SP2,SP3,SP4)	9.29	All stock SUSE 12 SP1,SP2,SP3,SP4 kernels are supported. 4.4.138-4.7-azure to 4.4.180-4.31-azure, 4.12.14-6.3-azure to 4.12.14-6.23-azure

SUSE Linux Enterprise Server 15 supported kernel versions

RELEASE	MOBILITY SERVICE VERSION	KERNEL VERSION
SUSE Linux Enterprise Server 15 and 15 SP1	9.32	All stock SUSE 15 and 15 kernels are supported. 4.12.14-5.5-azure to 4.12.14-8.22-azure

Linux file systems/guest storage

COMPONENT	SUPPORTED
File systems	ext3, ext4, XFS
Volume manager	- LVM is supported. - /boot on LVM is supported from Update Rollup 31 (version 9.20 of the Mobility service) onwards. It isn't supported in earlier Mobility service versions. - Multiple OS disks aren't supported.
Paravirtualized storage devices	Devices exported by paravirtualized drivers aren't supported.
Multi-queue block IO devices	Not supported.
Physical servers with the HP CCISST storage controller	Not supported.

COMPONENT	SUPPORTED
Device/Mount point naming convention	Device name or mount point name should be unique. Ensure that no two devices/mount points have case-sensitive names. For example naming devices for the same VM as <i>device1</i> and <i>Device1</i> isn't supported.
Directories	<p>If you're running a version of the Mobility service earlier than version 9.20 (released in Update Rollup 31), then these restrictions apply:</p> <ul style="list-style-type: none"> - These directories (if set up as separate partitions/file-systems) must be on the same OS disk on the source server: <code>/root</code>, <code>/boot</code>, <code>/usr</code>, <code>/usr/local</code>, <code>/var</code>, <code>/etc</code>. - The <code>/boot</code> directory should be on a disk partition and not be an LVM volume. <p>From version 9.20 onwards, these restrictions don't apply.</p>
Boot directory	<ul style="list-style-type: none"> - Boot disks mustn't be in GPT partition format. This is an Azure architecture limitation. GPT disks are supported as data disks. <p>Multiple boot disks on a VM aren't supported</p> <ul style="list-style-type: none"> - <code>/boot</code> on an LVM volume across more than one disk isn't supported. - A machine without a boot disk can't be replicated.
Free space requirements	<p>2 GB on the <code>/root</code> partition</p> <p>250 MB on the installation folder</p>
XFSv5	<p>XFSv5 features on XFS file systems, such as metadata checksum, are supported (Mobility service version 9.10 onwards).</p> <p>Use the <code>xfs_info</code> utility to check the XFS superblock for the partition. If <code>fstype</code> is set to 1, then XFSv5 features are in use.</p>
BTRFS	<p>BTRFS is supported from Update Rollup 34 (version 9.22 of the Mobility service) onwards. BTRFS isn't supported if:</p> <ul style="list-style-type: none"> - The BTRFS file system subvolume is changed after enabling protection. - The BTRFS file system is spread over multiple disks. - The BTRFS file system supports RAID.

VM/Disk management

ACTION	DETAILS
--------	---------

ACTION	DETAILS
Resize disk on replicated VM	<p>Supported on the source VM before failover, directly in the VM properties. No need to disable/re-enable replication.</p> <p>If you change the source VM after failover, the changes aren't captured.</p> <p>If you change the disk size on the Azure VM after failover, when you fail back, Site Recovery creates a new VM with the updates.</p>
Add disk on replicated VM	<p>Not supported.</p> <p>Disable replication for the VM, add the disk, and then re-enable replication.</p>

Network

COMPONENT	SUPPORTED
Host network NIC Teaming	<p>Supported for VMware VMs.</p> <p>Not supported for physical machine replication.</p>
Host network VLAN	Yes.
Host network IPv4	Yes.
Host network IPv6	No.
Guest/server network NIC Teaming	No.
Guest/server network IPv4	Yes.
Guest/server network IPv6	No.
Guest/server network static IP (Windows)	Yes.
Guest/server network static IP (Linux)	<p>Yes.</p> <p>VMs are configured to use DHCP on failback.</p>
Guest/server network multiple NICs	Yes.

Azure VM network (after failover)

COMPONENT	SUPPORTED
Azure ExpressRoute	Yes
ILB	Yes
ELB	Yes

COMPONENT	SUPPORTED
Azure Traffic Manager	Yes
Multi-NIC	Yes
Reserved IP address	Yes
IPv4	Yes
Retain source IP address	Yes
Azure virtual network service endpoints	Yes
Accelerated networking	No

Storage

COMPONENT	SUPPORTED
Dynamic disk	OS disk must be a basic disk. Data disks can be dynamic disks
Docker disk configuration	No
Host NFS	Yes for VMware No for physical servers
Host SAN (iSCSI/FC)	Yes
Host vSAN	Yes for VMware N/A for physical servers
Host multipath (MPIO)	Yes, tested with Microsoft DSM, EMC PowerPath 5.7 SP4, EMC PowerPath DSM for CLARiiON
Host Virtual Volumes (VVols)	Yes for VMware N/A for physical servers
Guest/server VMDK	Yes
Guest/server shared cluster disk	No
Guest/server encrypted disk	No
Guest/server NFS	No

COMPONENT	SUPPORTED
Guest/server iSCSI	For Migration - Yes For Disaster Recovery - No, iSCSI will fallback as an attached disk to the VM
Guest/server SMB 3.0	No
Guest/server RDM	Yes N/A for physical servers
Guest/server disk > 1 TB	Yes, disk must be larger than 1024 MB Up to 8,192 GB when replicating to managed disks (9.26 version onwards) Up to 4,095 GB when replicating to storage accounts
Guest/server disk with 4K logical and 4k physical sector size	No
Guest/server disk with 4K logical and 512-bytes physical sector size	No
Guest/server volume with striped disk >4 TB	Yes
Logical volume management (LVM)	
Guest/server - Storage Spaces	No
Guest/server hot add/remove disk	No
Guest/server - exclude disk	Yes
Guest/server multipath (MPIO)	No
Guest/server GPT partitions	Five partitions are supported from Update Rollup 37 (version 9.25 of the Mobility service) onwards. Previously four were supported.
ReFS	Resilient File System is supported with Mobility service version 9.23 or higher
Guest/server EFI/UEFI boot	- Supported for Windows Server 2012 or later, SLES 12 SP4 and RHEL 8.0 with mobility agent version 9.30 onwards - Secure UEFI boot type is not supported.

Replication channels

TYPE OF REPLICATION	SUPPORTED
Offloaded Data Transfers (ODX)	No
Offline Seeding	No

TYPE OF REPLICATION	SUPPORTED
Azure Data Box	No

Azure storage

COMPONENT	SUPPORTED
Locally redundant storage	Yes
Geo-redundant storage	Yes
Read-access geo-redundant storage	Yes
Cool storage	No
Hot storage	No
Block blobs	No
Encryption-at-rest (SSE)	Yes
Encryption-at-rest (CMK)	Yes (via Powershell Az 3.3.0 module onwards)
Premium storage	Yes
Import/export service	No
Azure Storage firewalls for VNets	Yes. Configured on target storage/cache storage account (used to store replication data).
General-purpose v2 storage accounts (hot and cool tiers)	Yes (Transaction costs are substantially higher for V2 compared to V1)

Azure compute

FEATURE	SUPPORTED
Availability sets	Yes
Availability zones	No
HUB	Yes
Managed disks	Yes

Azure VM requirements

On-premises VMs replicated to Azure must meet the Azure VM requirements summarized in this table. When Site Recovery runs a prerequisites check for replication, the check will fail if some of the requirements aren't met.

COMPONENT	REQUIREMENTS	DETAILS
Guest operating system	Verify supported operating systems for replicated machines.	Check fails if unsupported.
Guest operating system architecture	64-bit.	Check fails if unsupported.
Operating system disk size	Up to 2,048 GB.	Check fails if unsupported.
Operating system disk count	1	Check fails if unsupported.
Data disk count	64 or less.	Check fails if unsupported.
Data disk size	Up to 8,192 GB when replicating to managed disk (9.26 version onwards) Up to 4,095 GB when replicating to storage account	Check fails if unsupported.
Network adapters	Multiple adapters are supported.	
Shared VHD	Not supported.	Check fails if unsupported.
FC disk	Not supported.	Check fails if unsupported.
BitLocker	Not supported.	BitLocker must be disabled before you enable replication for a machine.
VM name	From 1 to 63 characters. Restricted to letters, numbers, and hyphens. The machine name must start and end with a letter or number.	Update the value in the machine properties in Site Recovery.

Resource group limits

To understand the number of virtual machines that can be protected under a single resource group, refer to the article on [subscription limits and quotas](#)

Churn limits

The following table provides the Azure Site Recovery limits.

- These limits are based on our tests, but don't cover all possible app I/O combinations.
- Actual results can vary based on your application I/O mix.
- For best results, we strongly recommend that you run the [Deployment Planner tool](#), and perform extensive application testing using test failovers to get the true performance picture for your app.

REPLICATION TARGET	AVERAGE SOURCE DISK I/O SIZE	AVERAGE SOURCE DISK DATA CHURN	TOTAL SOURCE DISK DATA CHURN PER DAY
Standard storage	8 KB	2 MB/s	168 GB per disk

REPLICATION TARGET	AVERAGE SOURCE DISK I/O SIZE	AVERAGE SOURCE DISK DATA CHURN	TOTAL SOURCE DISK DATA CHURN PER DAY
Premium P10 or P15 disk	8 KB	2 MB/s	168 GB per disk
Premium P10 or P15 disk	16 KB	4 MB/s	336 GB per disk
Premium P10 or P15 disk	32 KB or greater	8 MB/s	672 GB per disk
Premium P20 or P30 or P40 or P50 disk	8 KB	5 MB/s	421 GB per disk
Premium P20 or P30 or P40 or P50 disk	16 KB or greater	20 MB/s	1684 GB per disk

SOURCE DATA CHURN	MAXIMUM LIMIT
Peak data churn across all disks on a VM	54 MB/s
Maximum data churn per day supported by a Process Server	2 TB

- These are average numbers assuming a 30 percent I/O overlap.
- Site Recovery is capable of handling higher throughput based on overlap ratio, larger write sizes, and actual workload I/O behavior.
- These numbers assume a typical backlog of approximately five minutes. That is, after data is uploaded, it is processed and a recovery point is created within five minutes.

Vault tasks

ACTION	SUPPORTED
Move vault across resource groups	No
Move vault within and across subscriptions	No
Move storage, network, Azure VMs across resource groups	No
Move storage, network, Azure VMs within and across subscriptions.	No

Obtain latest components

NAME	DESCRIPTION	DETAILS
Configuration server	Installed on-premises. Coordinates communications between on-premises VMware servers or physical machines, and Azure.	- Learn about the configuration server. - Learn about upgrading to the latest version. - Learn about setting up the configuration server.

NAME	DESCRIPTION	DETAILS
Process server	Installed by default on the configuration server. Receives replication data, optimizes it with caching, compression, and encryption, and sends it to Azure. As your deployment grows, you can add additional process servers to handle larger volumes of replication traffic.	<ul style="list-style-type: none"> - Learn about the process server. - Learn about upgrading to the latest version. - Learn about setting up scale-out process servers.
Mobility Service	Installed on VMware VM or physical servers you want to replicate. Coordinates replication between on-premises VMware servers/physical servers and Azure.	<ul style="list-style-type: none"> - Learn about the Mobility service. - Learn about upgrading to the latest version.

Next steps

[Learn how](#) to prepare Azure for disaster recovery of VMware VMs.

Physical server to Azure disaster recovery architecture

2/12/2020 • 4 minutes to read • [Edit Online](#)

This article describes the architecture and processes used when you replicate, fail over, and recover physical Windows and Linux servers between an on-premises site and Azure, using the [Azure Site Recovery](#) service.

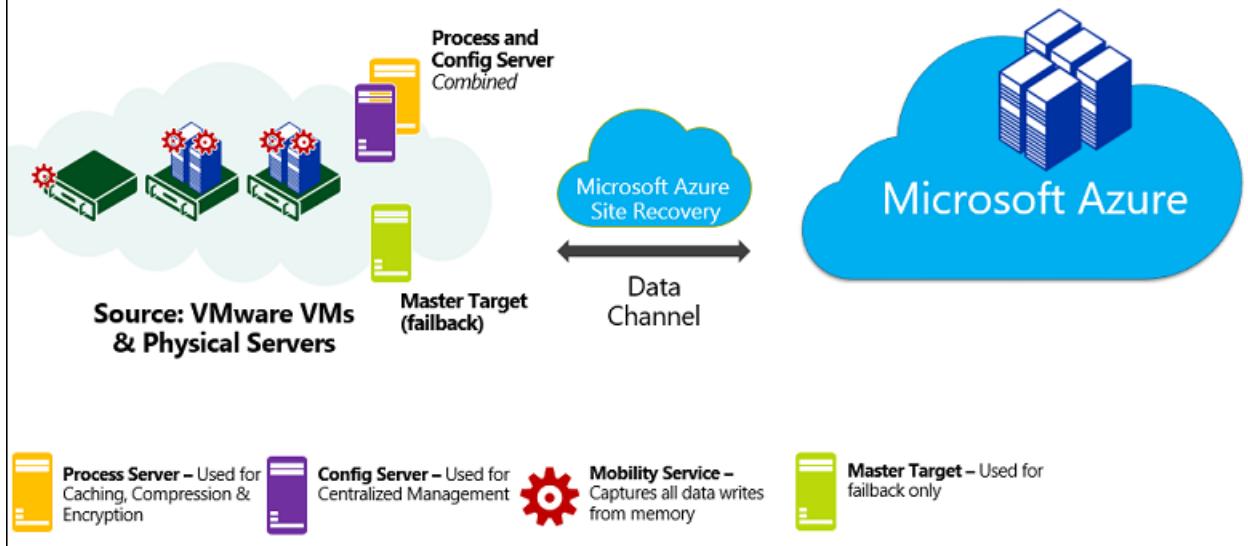
Architectural components

The following table and graphic provides a high-level view of the components used for physical server replication to Azure.

COMPONENT	REQUIREMENT	DETAILS
Azure	An Azure subscription and an Azure network.	Replicated data from on-premises physical machines is stored in Azure managed disks. Azure VMs are created with the replicated data when you run a failover from on-premises to Azure. The Azure VMs connect to the Azure virtual network when they're created.
Process server	Installed by default together with the configuration server.	<p>Acts as a replication gateway. Receives replication data, optimizes it with caching, compression, and encryption, and sends it to Azure storage.</p> <p>The process server also installs the Mobility service on servers you want to replicate.</p> <p>As your deployment grows, you can add additional, separate process servers to handle larger volumes of replication traffic.</p>
Master target server	Installed by default together with the configuration server.	<p>Handles replication data during failback from Azure.</p> <p>For large deployments, you can add an additional, separate master target server for failback.</p>
Replicated servers	The Mobility service is installed on each server you replicate.	We recommend you allow automatic installation from the process server. Or, you can install the service manually, or use an automated deployment method such as Configuration Manager.

Physical to Azure architecture

Physical to Azure replication architecture



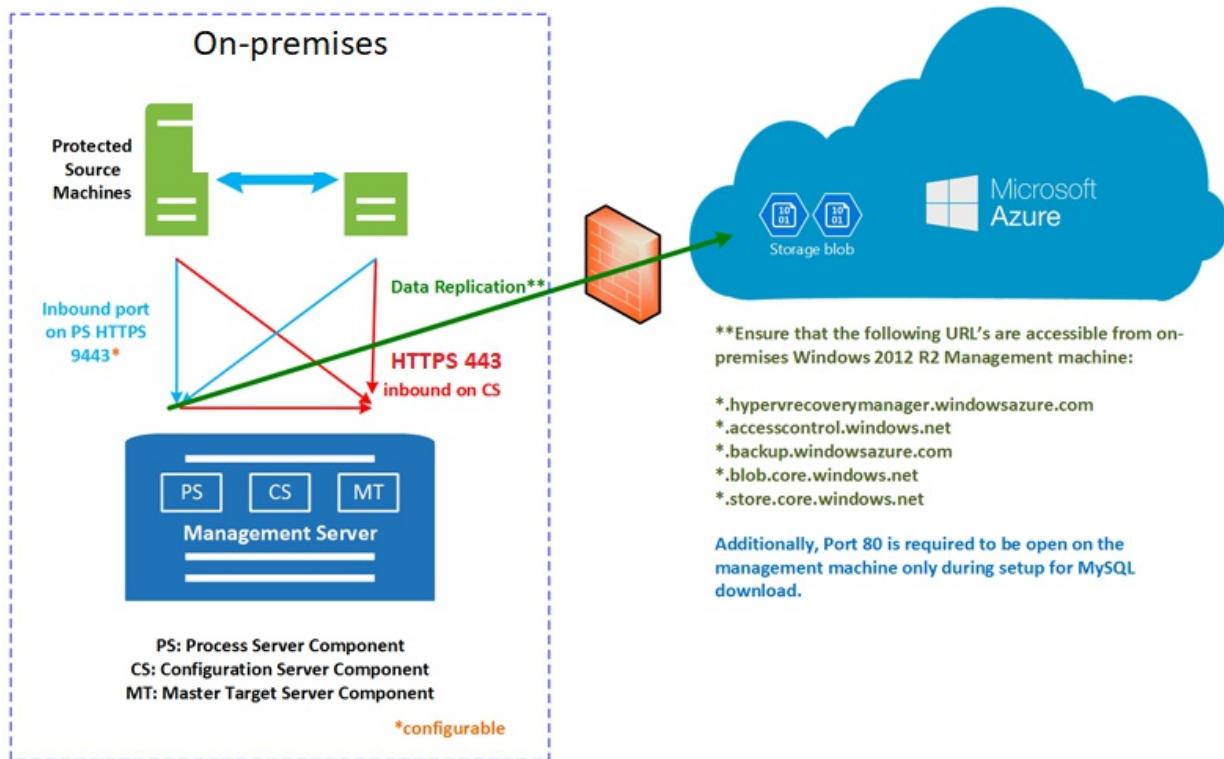
Replication process

1. You set up the deployment, including on-premises and Azure components. In the Recovery Services vault, you specify the replication source and target, set up the configuration server, create a replication policy, and enable replication.
2. Machines replicate using the replication policy, and an initial copy of the server data is replicated to Azure storage.
3. After initial replication finishes, replication of delta changes to Azure begins. Tracked changes for a machine are held in a file with the *.hrl* extension.
 - Machines communicate with the configuration server on HTTPS port 443 inbound, for replication management.
 - Machines send replication data to the process server on HTTPS port 9443 inbound (can be modified).
 - The configuration server orchestrates replication management with Azure over HTTPS port 443 outbound.
 - The process server receives data from source machines, optimizes and encrypts it, and sends it to Azure storage over HTTPS port 443 outbound.
 - If you enable multi-VM consistency, machines in the replication group communicate with each other over port 20004. Multi-VM is used if you group multiple machines into replication groups that share crash-consistent and app-consistent recovery points when they fail over. These groups are useful if machines are running the same workload and need to be consistent.
4. Traffic is replicated to Azure storage public endpoints, over the internet. Alternately, you can use Azure ExpressRoute [public peering](#).

NOTE

Replication isn't supported over a site-to-site VPN from an on-premises site or Azure ExpressRoute [private peering](#).

Physical to Azure replication process

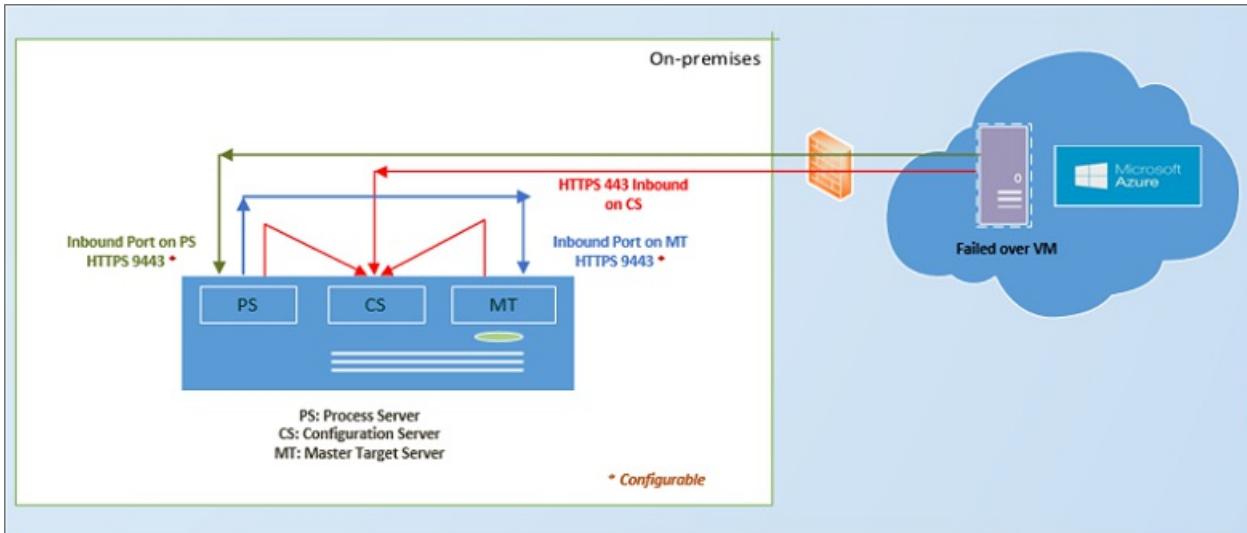


Failover and fallback process

After replication is set up, you can run a disaster recovery drill (test failover) to check that everything works as expected. Then, you can fail over and fail back as needed. Consider the following items:

- Planned failover isn't supported.
- Fail back to an on-premises VMware VM is necessary. You need an on-premises VMware infrastructure, even when you replicate on-premises physical servers to Azure.
- You fail over a single machine, or create recovery plans, to fail over multiple machines together.
- When you run a failover, Azure VMs are created from replicated data in Azure storage.
- After the initial failover is triggered, you commit it to start accessing the workload from the Azure VM.
- When your primary on-premises site is available again, you can fail back.
- Set up a fallback infrastructure that includes:
 - **Temporary process server in Azure:** To fail back from Azure, you set up an Azure VM to act as a process server, to handle replication from Azure. You can delete this VM after fail back finishes.
 - **VPN connection:** To fail back, you need a VPN connection (or Azure ExpressRoute) from the Azure network to the on-premises site.
 - **Separate master target server:** By default, the fail back is handled by the master target server that was installed with the configuration server on the on-premises VMware VM. If you need to fail back large volumes of traffic, you should set up a separate on-premises master target server.
 - **Failback policy:** To replicate back to your on-premises site, you need a failback policy. The policy was automatically created when you created your replication policy from on-premises to Azure.
 - **VMware infrastructure:** To fail back, you need a VMware infrastructure. You can't fail back to a physical server.
- After the components are in place, fail back occurs in three stages:
 - **Stage 1:** Reprotect the Azure VMs so that they replicate from Azure back to the on-premises VMware VMs.
 - **Stage 2:** Run a failover to the on-premises site.
 - **Stage 3:** After workloads have failed back, you reenable replication.

VMware failback from Azure



Next steps

To set up disaster recovery for physical servers to Azure, see the [how-to guide](#).

Exclude disks from disaster recovery

12/26/2019 • 10 minutes to read • [Edit Online](#)

This article describes how to exclude disks from replication during disaster recovery from on-premises to Azure with [Azure Site Recovery](#). You might exclude disks from replication for a number of reasons:

- So that unimportant data churned on the excluded disk isn't replicated.
- To optimize consumed replication bandwidth, or target-side resources.
- To save storage and network resources by not replicating data that you don't need.
- Azure VMs have reached Site Recovery replication limits.

Supported scenarios

You can exclude disks from replication as summarized in the table.

AZURE TO AZURE	VMWARE TO AZURE	HYPER-V TO AZURE
Yes (using PowerShell)	Yes	Yes

Exclude limitations

LIMITATION	AZURE VMS	VMWARE VMS	HYPER-V VMS
Disk types	You can exclude basic disks from replication. You can't exclude operating system disks or dynamic disks. Temp disks are excluded by default.	You can exclude basic disks from replication. You can't exclude operating system disks or dynamic disks.	You can exclude basic disks from replication. You can't exclude operating system disks. We recommend that you don't exclude dynamic disks. Site Recovery can't identify which VHS is basic or dynamic in the guest VM. If all dependent dynamic volume disks aren't excluded, the protected dynamic disk becomes a failed disk on a failover VM, and the data on that disk isn't accessible.
Replicating disk	You can't exclude a disk that's replicating. Disable and reenable replication for the VM.	You can't exclude a disk that's replicating.	You can't exclude a disk that's replicating.

LIMITATION	AZURE VMS	VMWARE VMS	HYPER-V VMS
Mobility service (VMware)	Not relevant	<p>You can exclude disks only on VMs that have the Mobility service installed.</p> <p>This means that you have to manually install the Mobility service on the VMs for which you want to exclude disks. You can't use the push installation mechanism because it installs the Mobility service only after replication is enabled.</p>	Not relevant.
Add/Remove	You can add and remove disks on Azure VMs with managed disks.	You can't add or remove disks after replication is enabled. Disable and then reenable replication to add a disk.	You can't add or remove disks after replication is enabled. Disable and then reenable replication.
Failover	<p>If an app needs a disk that you excluded, after failover you need to create the disk manually so that the replicated app can run.</p> <p>Alternatively, you can create the disk during VM failover, by integrating Azure automation into a recovery plan.</p>	If you exclude a disk that an app needs, create it manually in Azure after failover.	If you exclude a disk that an app needs, create it manually in Azure after failover.
On-premises failback-disks created manually	Not relevant	<p>Windows VMs: Disks created manually in Azure aren't failed back. For example, if you fail over three disks and create two disks directly on an Azure VM, only the three disks that were failed over are then failed back.</p> <p>Linux VMs: Disks created manually in Azure are failed back. For example, if you fail over three disks and create two disks on an Azure VM, all five will be failed back. You can't exclude disks that were created manually from failback.</p>	Disks created manually in Azure aren't failed back. For example, if you fail over three disks and create two disks directly on an Azure VM, only the three disks that were failed over will be failed back.

LIMITATION	AZURE VMS	VMWARE VMS	HYPER-V VMS
On-premises fallback-Excluded disks	Not relevant	If you fail back to the original machine, the fallback VM disk configuration doesn't include the excluded disks. Disks that were excluded from VMware to Azure replication aren't available on the fallback VM.	When failback is to the original Hyper-V location, the fallback VM disk configuration remains the same as that of original source VM disk. Disks that were excluded from Hyper-V site to Azure replication are available on the fallback VM.

Typical scenarios

Examples of data churn that are great candidates for exclusion include writes to a paging file (pagefile.sys), and writes to the tempdb file of Microsoft SQL Server. Depending on the workload and the storage subsystem, the paging and tempdb files can register a significant amount of churn. Replicating this type of data to Azure is resource-intensive.

- To optimize replication for a VM with a single virtual disk that includes both the operating system and the paging file, you could:
 1. Split the single virtual disk into two virtual disks. One virtual disk has the operating system, and the other has the paging file.
 2. Exclude the paging file disk from replication.
- To optimize replication for a disk that includes both the Microsoft SQL Server tempdb file and the system database file, you could:
 1. Keep the system database and tempdb on two different disks.
 2. Exclude the tempdb disk from replication.

Example 1: Exclude the SQL Server tempdb disk

Let's look at how to handle disk exclusion, failover, and failover for a source SQL Server Windows VM - **SalesDB***, for which we want to exclude tempdb.

Exclude disks from replication

We have these disks on the source Windows VM SalesDB.

DISK NAME	GUEST OS DISK	DRIVE LETTER	DISK DATA TYPE
DB-Disk0-OS	Disk0	C:\	Operating system disk.
DB-Disk1	Disk1	D:\	SQL system database and User Database1.
DB-Disk2 (Excluded the disk from protection)	Disk2	E:\	Temp files.
DB-Disk3 (Excluded the disk from protection)	Disk3	F:\	SQL tempdb database. Folder path - F:\MSSQL\Data. Make a note of the folder path before failover.

DISK NAME	GUEST OS DISK	DRIVE LETTER	DISK DATA TYPE
DB-Disk4	Disk4	G:\	User Database2

1. We enable replication for the SalesDB VM.
2. We exclude Disk2 and Disk3 from replication because data churn on those disks is temporary.

Handle disks during failover

Since disks aren't replicated, when you fail over to Azure these disks aren't present on the Azure VM created after failover. The Azure VM has the disks summarized in this table.

GUEST OS DISK	DRIVE LETTER	DISK DATA TYPE
Disk0	C:\	Operating system disk.
Disk1	E:\	Temporary storage Azure adds this disk. Because Disk2 and Disk3 were excluded from replication, E: is the first drive letter from the available list. Azure assigns E: to the temporary storage volume. Other drive letters for replicated disks remain the same.
Disk2	D:\	SQL system database and User Database1
Disk3	G:\	User Database2

In our example, since Disk3, the SQL tempdb disk, was excluded from replication and isn't available on the Azure VM, the SQL service is in a stopped state, and it needs the F:\MSSQL\Data path. You can create this path in a couple of ways:

- Add a new disk after failover, and assign tempdb folder path.
- Use an existing temporary storage disk for the tempdb folder path.

Add a new disk after failover

1. Write down the paths of SQL tempdb.mdf and tempdb.ldf before failover.
2. From the Azure portal, add a new disk to the failover Azure VM. The disk should be the same size (or larger) as the source SQL tempdb disk (Disk3).
3. Sign in to the Azure VM.
4. From the disk management (diskmgmt.msc) console, initialize and format the newly added disk.
5. Assign the same drive letter that was used by the SQL tempdb disk (F:)
6. Create a tempdb folder on the F: volume (F:\MSSQL\Data).
7. Start the SQL service from the service console.

Use an existing temporary storage disk

1. Open a command prompt.
2. Run SQL Server in recovery mode from the command prompt.

```
Net start MSSQLSERVER /f / T3608
```

3. Run the following sqlcmd to change the tempdb path to the new path.

```

sqlcmd -A -S SalesDB **Use your SQL DBname**
USE master;
GO
ALTER DATABASE tempdb
MODIFY FILE (NAME = tempdev, FILENAME = 'E:\MSSQL\tempdata\tempdb.mdf');
GO
ALTER DATABASE tempdb
MODIFY FILE (NAME = templog, FILENAME = 'E:\MSSQL\tempdata\templog.ldf');
GO

```

4. Stop the Microsoft SQL Server service.

```
Net stop MSSQLSERVER
```

5. Start the Microsoft SQL Server service.

```
Net start MSSQLSERVER
```

VMware VMs: Disks during failback to original location

Now let's see how to handle disks on VMware VMs when you fail back to your original on-premises location.

- Disks created in Azure:** Since our example uses a Windows VM, disks that you create manually in Azure aren't replicated back to your site when you fail back or reprotect a VM.
- Temporary storage disk in Azure:** The temporary storage disk isn't replicated back to on-premises hosts.
- Excluded disks:** Disks that were excluded from VMware to Azure replication aren't available on the on-premises VM after failback.

Before you fail back the VMware VMs to the original location, the Azure VM disk settings are as follows.

GUEST OS DISK	DRIVE LETTER	DISK DATA TYPE
Disk0	C:\	Operating system disk.
Disk1	E:\	Temporary storage.
Disk2	D:\	SQL system database and User Database1.
Disk3	G:\	User Database2.

After failback, the VMware VM in the original location has the disks summarized in the table.

GUEST OS DISK	DRIVE LETTER	DISK DATA TYPE
Disk0	C:\	Operating system disk.
Disk1	D:\	SQL system database and User Database1.
Disk2	G:\	User Database2.

Hyper-V VMs: Disks during failback to original location

Now let's see how to handle disks on Hyper-V VMs when you fail back to your original on-premises location.

- **Disks created in Azure:** Disks that you create manually in Azure aren't replicated back to your site when you fail back or reprotect a VM.
- **Temporary storage disk in Azure:** The temporary storage disk isn't replicated back to on-premises hosts.
- **Excluded disks:** After failback the VM disk configuration is the same as the original VM disk configuration. Disks that were excluded from replication from Hyper-V to Azure are available on the failback VM.

Before you fail back the Hyper-V VMs to the original location, the Azure VM disk settings are as follows.

GUEST OS DISK	DRIVE LETTER	DISK DATA TYPE
Disk0	C:\	Operating system disk.
Disk1	E:\	Temporary storage.
Disk2	D:\	SQL system database and User Database1.
Disk3	G:\	User Database2.

After planned failover (failback) from Azure to on-premises Hyper-V, the Hyper-V VM in the original location has the disks summarized in the table.

DISK NAME	GUEST OS DISK#	DRIVE LETTER	DISK DATA TYPE
DB-Disk0-OS	Disk0	C:\	Operating system disk.
DB-Disk1	Disk1	D:\	SQL system database and User Database1.
DB-Disk2 (Excluded disk)	Disk2	E:\	Temp files.
DB-Disk3 (Excluded disk)	Disk3	F:\	SQL tempdb database Folder path (F:\MSSQL\Data).
DB-Disk4	Disk4	G:\	User Database2

Example 2: Exclude the paging file disk

Let's look at how to handle disk exclusion, failover, and failover for a source Windows VM, for which we want to exclude the pagefile.sys file disk on both the D drive, and an alternate drive.

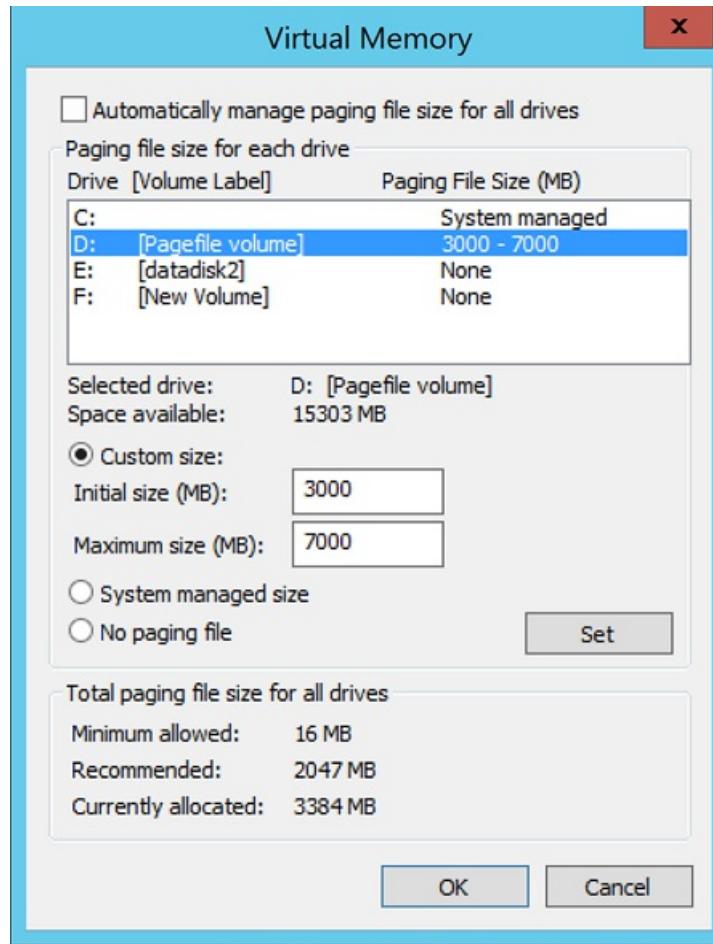
Paging file on the D drive

We have these disks on the source VM.

DISK NAME	GUEST OS DISK	DRIVE LETTER	DISK DATA TYPE
DB-Disk0-OS	Disk0	C:\	Operating system disk
DB-Disk1 (Exclude from replication)	Disk1	D:\	pagefile.sys
DB-Disk2	Disk2	E:\	User data 1

DISK NAME	GUEST OS DISK	DRIVE LETTER	DISK DATA TYPE
DB-Disk3	Disk3	F:\	User data 2

Our paging file settings on the source VM are as follows:



1. We enable replication for the VM.
2. We exclude DB-Disk1 from replication.

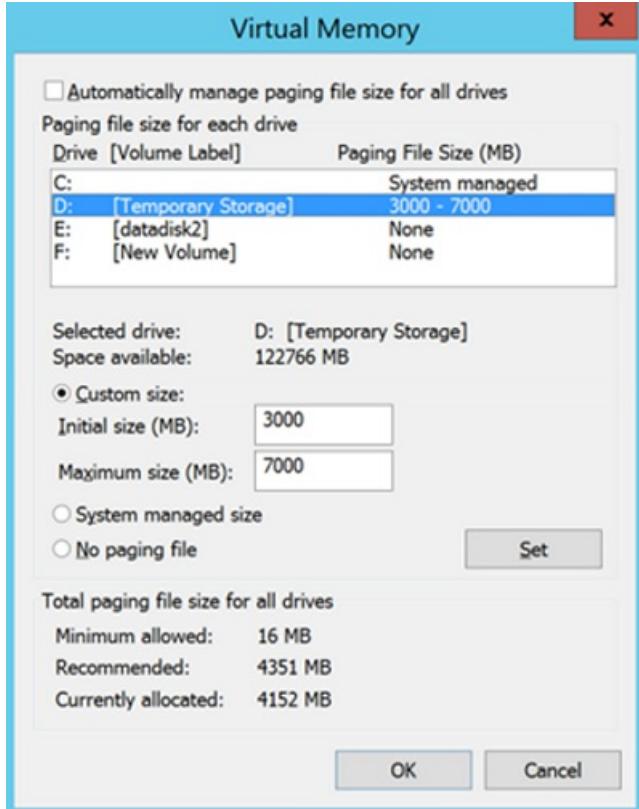
Disks after failover

After failover the Azure VM has the disks summarized in the table.

DISK NAME	GUEST OPERATING SYSTEM DISK#	DRIVE LETTER	DATA TYPE ON THE DISK
DB-Disk0-OS	Disk0	C:\	Operating system disk
DB-Disk1	Disk1	D:\	<p>Temporary storage/pagefile.sys</p> <p>Because DB-Disk1 (D:) was excluded, D: is the first drive letter from the available list.</p> <p>Azure assigns D: to the temporary storage volume.</p> <p>Because D: is available, the VM paging file setting remains the same).</p>

DISK NAME	GUEST OPERATING SYSTEM DISK#	DRIVE LETTER	DATA TYPE ON THE DISK
DB-Disk2	Disk2	E:\	User data 1
DB-Disk3	Disk3	F:\	User data 2

Our paging file settings on the Azure VM are as follows:



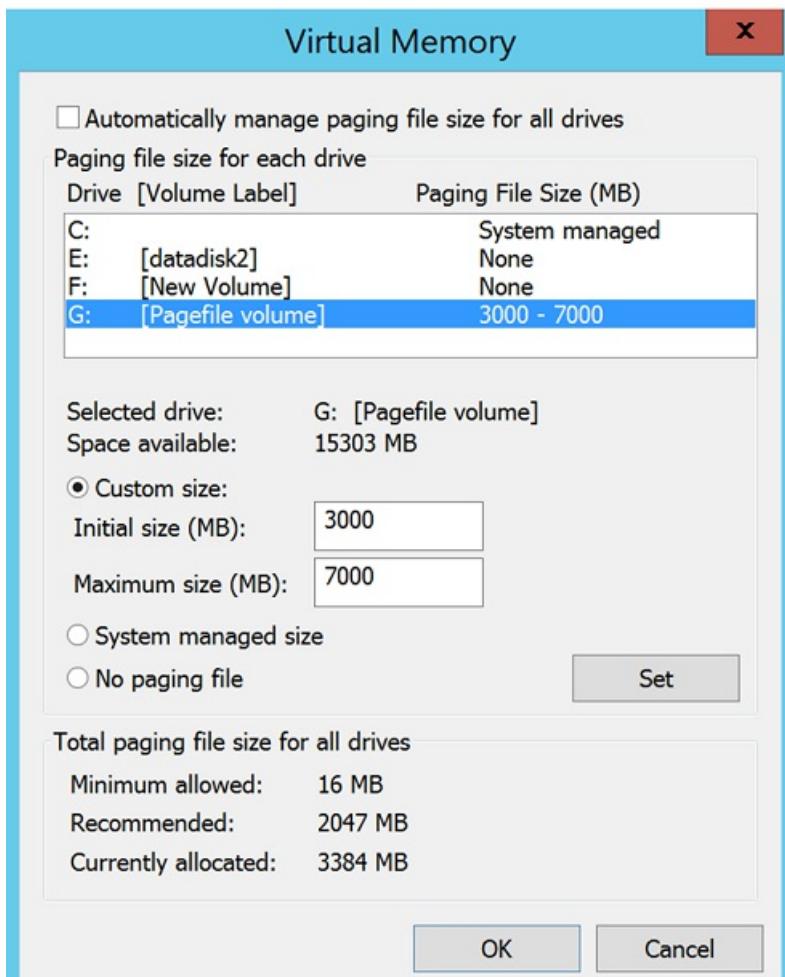
Paging file on another drive (not D:)

Let's look at example in which the paging file isn't on the D drive.

We have these disks on the source VM.

DISK NAME	GUEST OS DISK	DRIVE LETTER	DISK DATA TYPE
DB-Disk0-OS	Disk0	C:\	Operating system disk
DB-Disk1 (Exclude from replication)	Disk1	G:\	pagefile.sys
DB-Disk2	Disk2	E:\	User data 1
DB-Disk3	Disk3	F:\	User data 2

Our paging file settings on the on-premises VM are as follows:



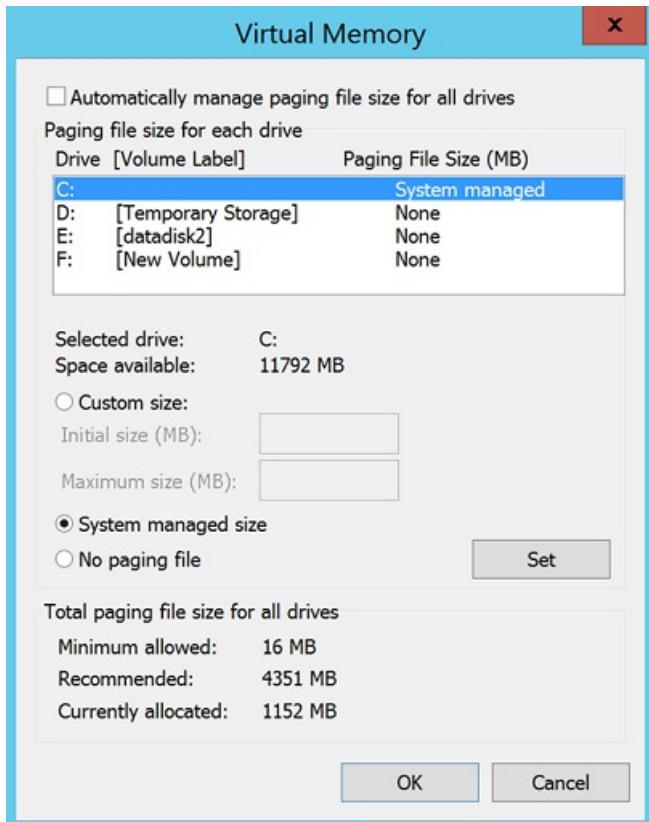
1. We enable replication for the VM.
2. We exclude DB-Disk1 from replication.

Disks after failover

After failover the Azure VM has the disks summarized in the table.

DISK NAME	GUEST OS DISK#	DRIVE LETTER	DISK DATA TYPE
DB-Disk0-OS	Disk0	C:\	Operating system disk
DB-Disk1	Disk1	D:\	<p>Temporary storage</p> <p>Because D: is the first drive letter from available the list, Azure assigns D: to the temporary storage volume.</p> <p>For all the replicated disks, the drive letter remains the same.</p> <p>Because the G: disk isn't available, the system will use the C: drive for the paging file.</p>
DB-Disk2	Disk2	E:\	User data 1
DB-Disk3	Disk3	F:\	User data 2

Our paging file settings on the Azure VM are as follows:



Next steps

- Learn more about guidelines for the temporary storage disk:
 - [Learn about](#) using SSDs in Azure VMs to store SQL Server TempDB and Buffer Pool Extensions
 - [Review](#) performance best practices for SQL Server in Azure VMs.
- After your deployment is set up and running, [learn more](#) about different types of failover.

Azure Traffic Manager with Azure Site Recovery

4/8/2019 • 8 minutes to read • [Edit Online](#)

Azure Traffic Manager enables you to control the distribution of traffic across your application endpoints. An endpoint is any Internet-facing service hosted inside or outside of Azure.

Traffic Manager uses the Domain Name System (DNS) to direct client requests to the most appropriate endpoint, based on a traffic-routing method and the health of the endpoints. Traffic Manager provides a range of [traffic-routing methods](#) and [endpoint monitoring options](#) to suit different application needs and automatic failover models. Clients connect to the selected endpoint directly. Traffic Manager is not a proxy or a gateway, and it does not see the traffic passing between the client and the service.

This article describes how you can combine Azure Traffic Monitor's intelligent routing with Azure Site Recovery's powerful disaster recovery and migration capabilities.

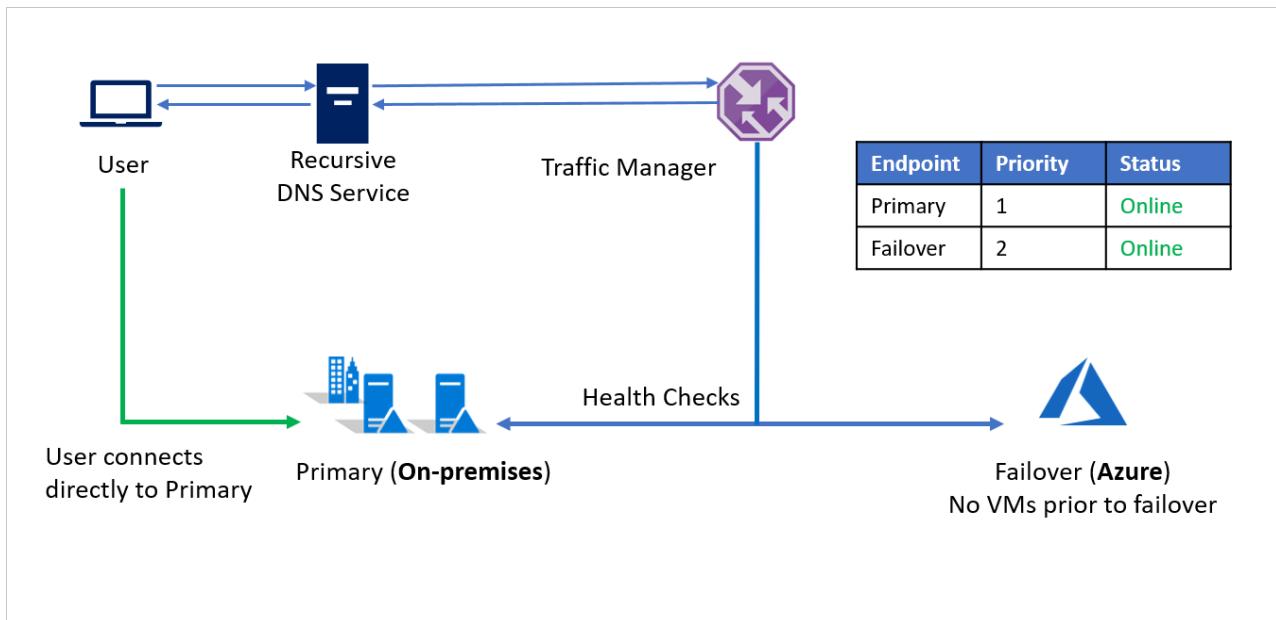
On-premises to Azure failover

For the first scenario, consider **Company A** that has all its application infrastructure running in its on-premises environment. For business continuity and compliance reasons, **Company A** decides to use Azure Site Recovery to protect its applications.

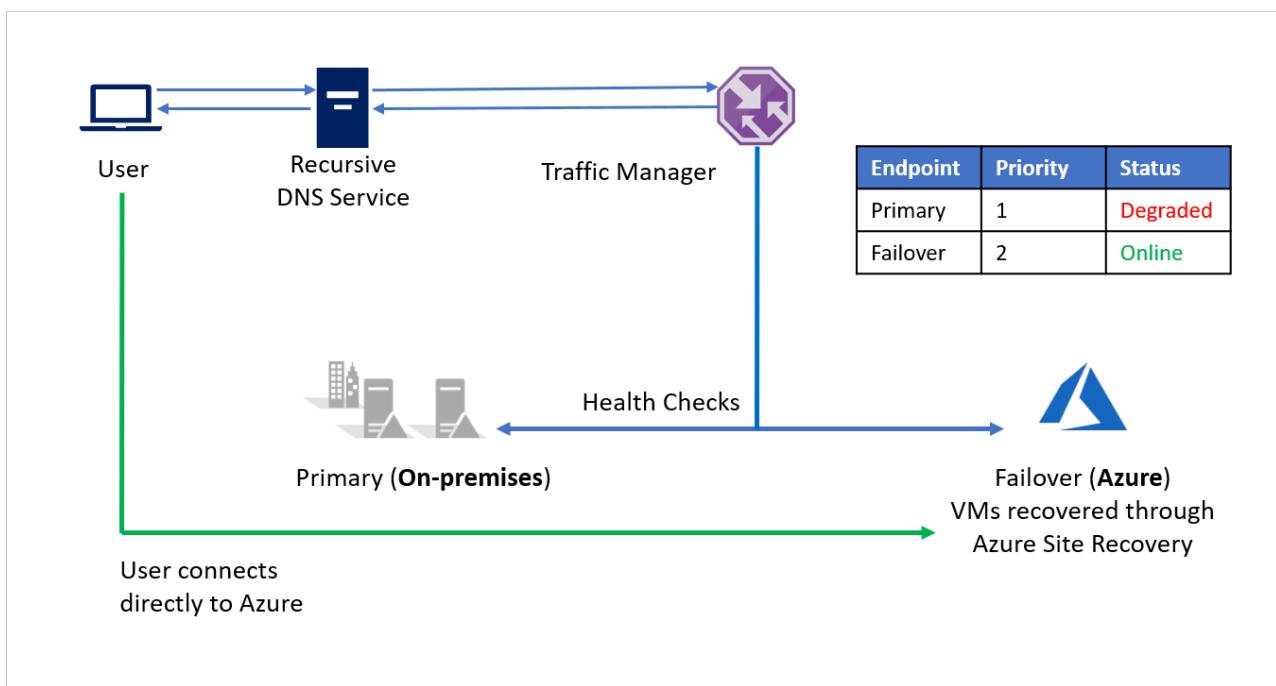
Company A is running applications with public endpoints and wants the ability to seamlessly redirect traffic to Azure in a disaster event. The [Priority](#) traffic-routing method in Azure Traffic Manager allows Company A to easily implement this failover pattern.

The setup is as follows:

- **Company A** creates a [Traffic Manager profile](#).
- Utilizing the [Priority](#) routing method, **Company A** creates two endpoints – **Primary** for on-premises and **Failover** for Azure. **Primary** is assigned Priority 1 and **Failover** is assigned Priority 2.
- Since the **Primary** endpoint is hosted outside Azure, the endpoint is created as an [External](#) endpoint.
- With Azure Site Recovery, the Azure site does not have any virtual machines or applications running prior to failover. So, the **Failover** endpoint is also created as an [External](#) endpoint.
- By default, user traffic is directed to the on-premises application because that endpoint has the highest priority associated with it. No traffic is directed to Azure if the **Primary** endpoint is healthy.



In a disaster event, Company A can trigger a [failover](#) to Azure and recover its applications on Azure. When Azure Traffic Manager detects that the **Primary** endpoint is no longer healthy, it automatically uses the **Failover** endpoint in the DNS response and users connect to the application recovered on Azure.



Depending on business requirements, **Company A** can choose a higher or lower [probing frequency](#) to switch between on-premises to Azure in a disaster event, and ensure minimal downtime for users.

When the disaster is contained, **Company A** can fallback from Azure to its on-premises environment ([VMware](#) or [Hyper-V](#)) using Azure Site Recovery. Now, when Traffic Manager detects that the **Primary** endpoint is healthy again, it automatically utilizes the **Primary** endpoint in its DNS responses.

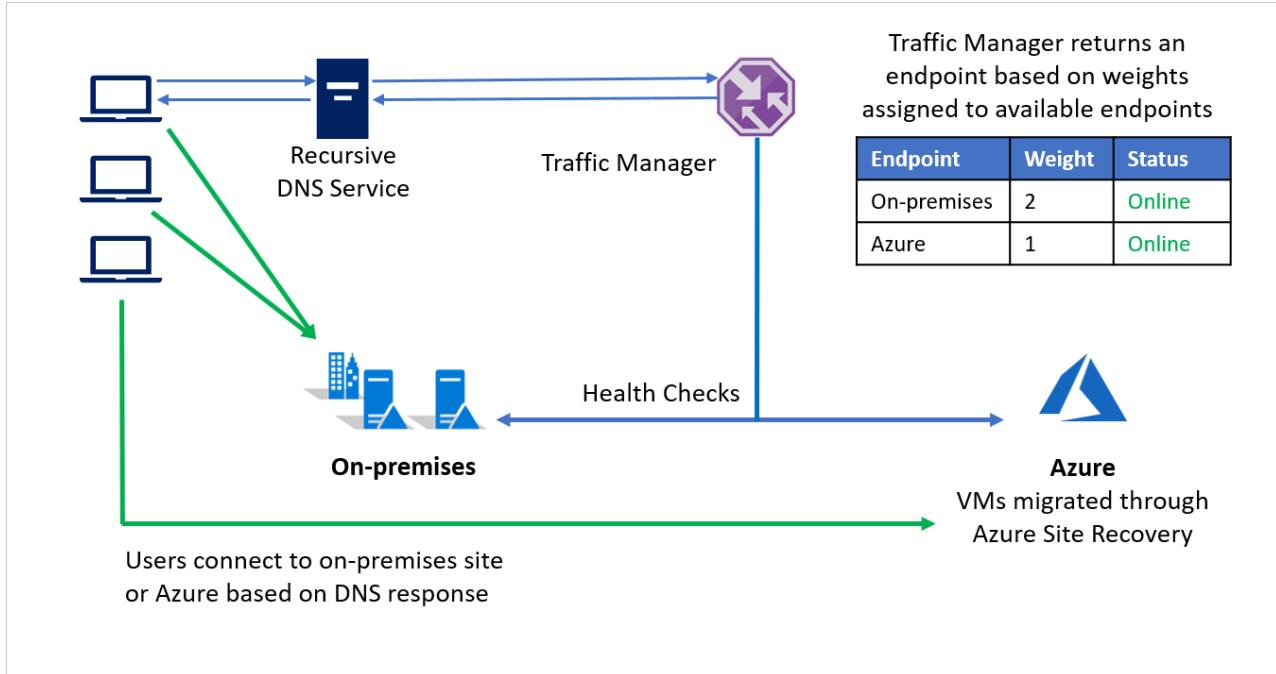
On-premises to Azure migration

In addition to disaster recovery, Azure Site Recovery also enables [migrations to Azure](#). Using Azure Site Recovery's powerful test failover capabilities, customers can assess application performance on Azure without affecting their on-premises environment. And when customers are ready to migrate, they can choose to migrate entire workloads together or choose to migrate and scale gradually.

Azure Traffic Manager's [Weighted](#) routing method can be used to direct some part of incoming traffic to Azure

while directing the majority to the on-premises environment. This approach can help assess scale performance as you can continue increasing the weight assigned to Azure as you migrate more and more of your workloads to Azure.

For example, **Company B** chooses to migrate in phases, moving some of its application environment while retaining the rest on-premises. During the initial stages when most of the environment is on-premises, a larger weight is assigned to the on-premises environment. Traffic manager returns an endpoint based on weights assigned to available endpoints.



During migration, both endpoints are active and most of the traffic is directed to the on-premises environment. As the migration proceeds, a larger weight can be assigned to the endpoint on Azure and finally the on-premises endpoint can be deactivated post migration.

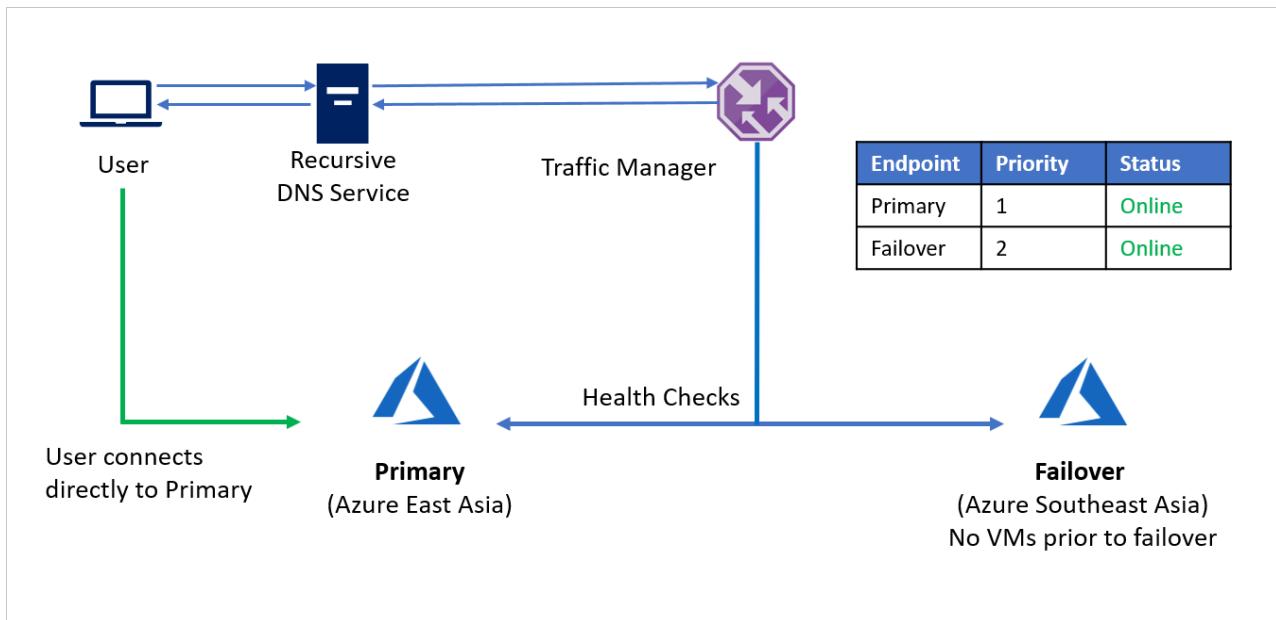
Azure to Azure failover

For this example, consider **Company C** that has all its application infrastructure running Azure. For business continuity and compliance reasons, **Company C** decides to use Azure Site Recovery to protect its applications.

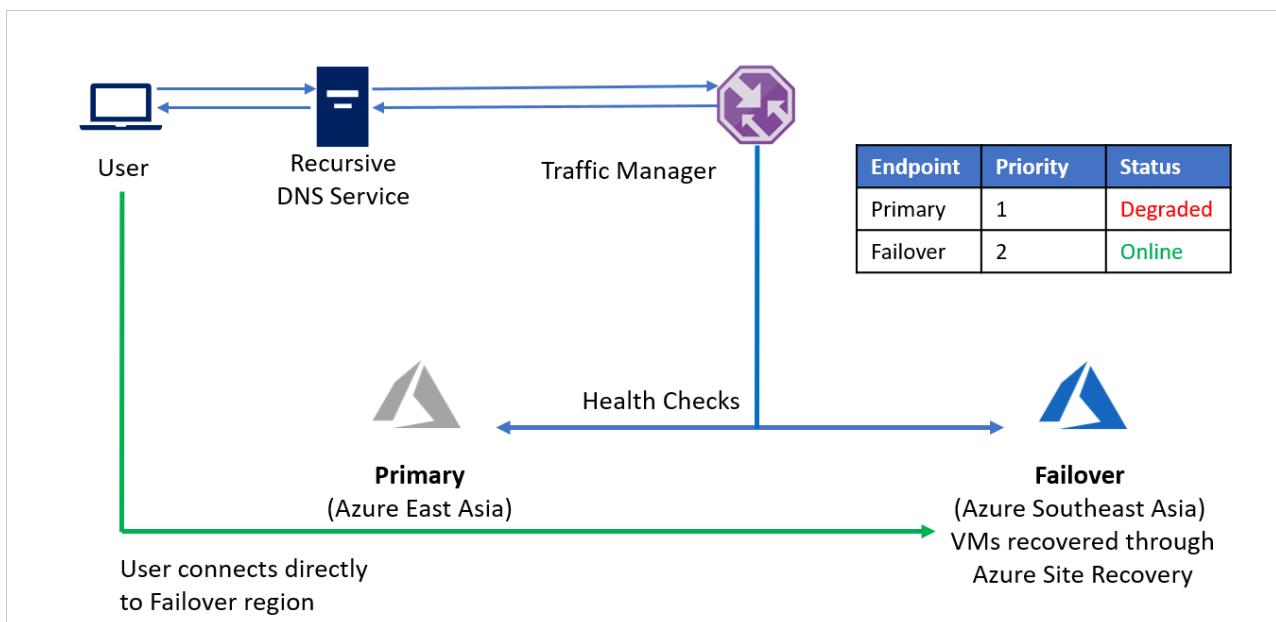
Company C is running applications with public endpoints and wants the ability to seamlessly redirect traffic to a different Azure region in a disaster event. The [Priority](#) traffic-routing method allows **Company C** to easily implement this failover pattern.

The setup is as follows:

- **Company C** creates a [Traffic Manager profile](#).
- Utilizing the [Priority](#) routing method, **Company C** creates two endpoints – **Primary** for the source region (Azure East Asia) and **Failover** for the recovery region (Azure Southeast Asia). **Primary** is assigned Priority 1 and **Failover** is assigned Priority 2.
- Since the **Primary** endpoint is hosted in Azure, the endpoint can be as an [Azure](#) endpoint.
- With Azure Site Recovery, the recovery Azure site does not have any virtual machines or applications running prior to failover. So, the **Failover** endpoint can be created as an [External](#) endpoint.
- By default, user traffic is directed to the source region (East Asia) application as that endpoint has the highest priority associated with it. No traffic is directed to the recovery region if the **Primary** endpoint is healthy.



In a disaster event, **Company C** can trigger a [failover](#) and recover its applications on the recovery Azure region. When Azure Traffic Manager detects that the Primary endpoint is no longer healthy, it automatically uses the **Failover** endpoint in the DNS response and users connect to the application recovered on the recovery Azure region (Southeast Asia).



Depending on business requirements, **Company C** can choose a higher or lower [probing frequency](#) to switch between source and recovery regions, and ensure minimal downtime for users.

When the disaster is contained, **Company C** can fallback from the recovery Azure region to the source Azure region using Azure Site Recovery. Now, when Traffic Manager detects that the **Primary** endpoint is healthy again, it automatically utilizes the **Primary** endpoint in its DNS responses.

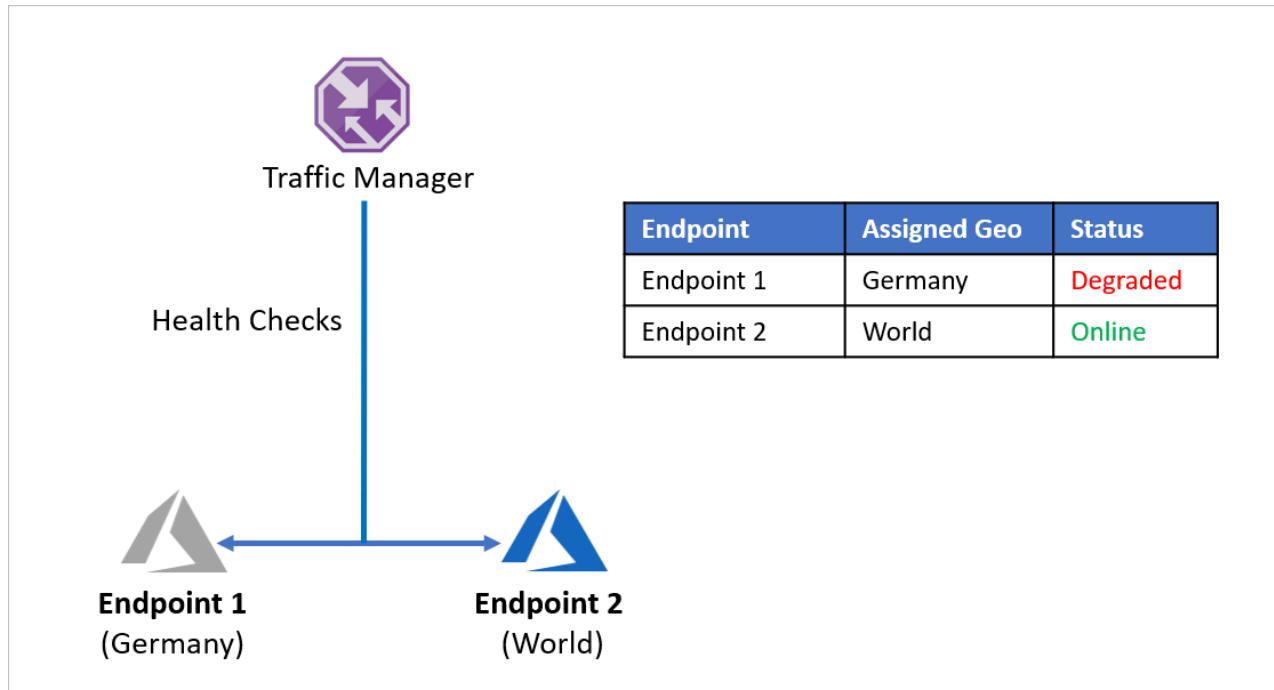
Protecting multi-region enterprise applications

Global enterprises often improve customer experience by tailoring their applications to serve regional needs. Localization and latency reduction can lead to application infrastructure split across regions. Enterprises are also bound by regional data laws in certain areas and choose to isolate a part of their application infrastructure within regional boundaries.

Let's consider an example where **Company D** has split its application endpoints to separately serve Germany and the rest of the world. **Company D** utilizes Azure Traffic Manager's [Geographic](#) routing method to set this up. Any

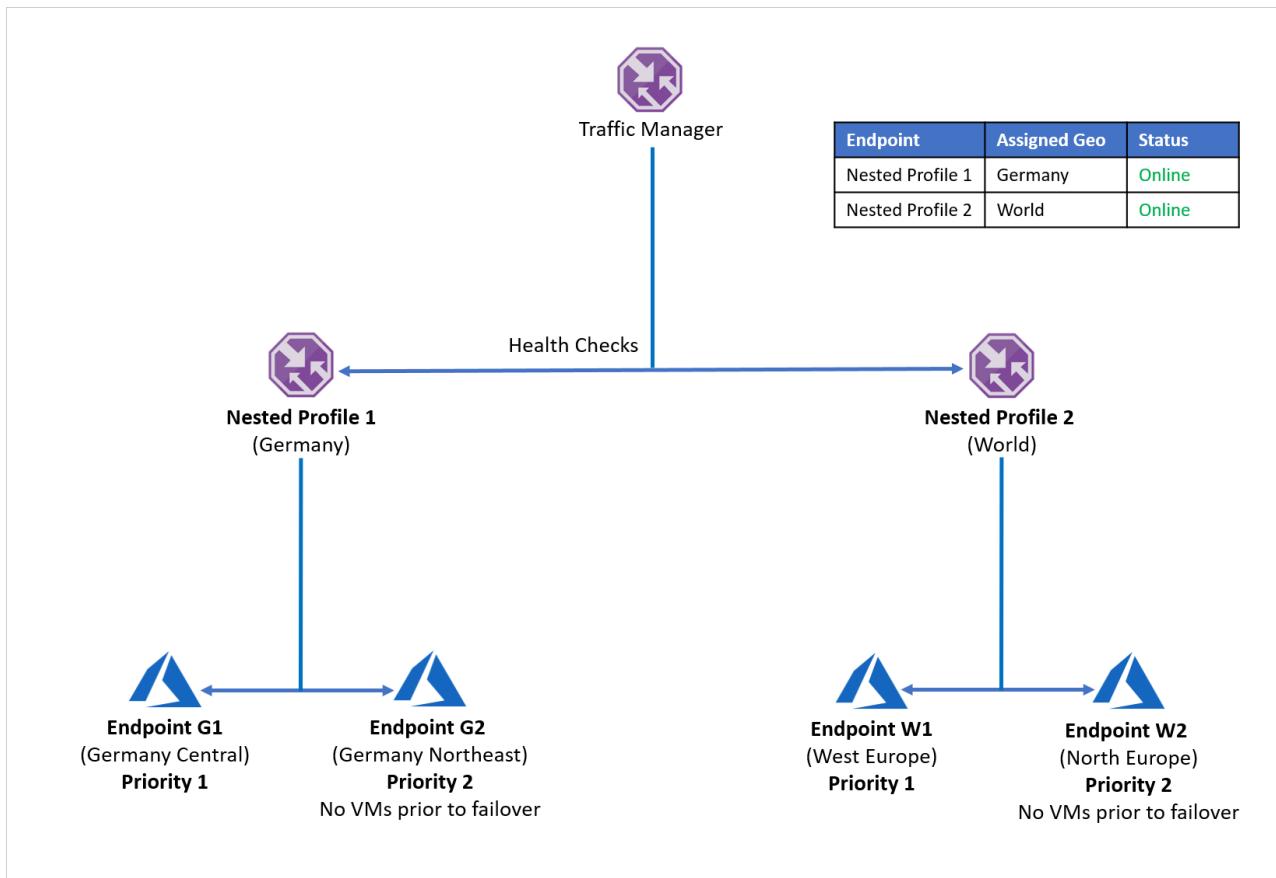
traffic originating from Germany is directed to **Endpoint 1** and any traffic originating outside Germany is directed to **Endpoint 2**.

The problem with this setup is that if **Endpoint 1** stops working for any reason, there is no redirection of traffic to **Endpoint 2**. Traffic originating from Germany continues to be directed to **Endpoint 1** regardless of the health of the endpoint, leaving German users without access to **Company D**'s application. Similarly, if **Endpoint 2** goes offline, there is no redirection of traffic to **Endpoint 1**.



To avoid running into this problem and ensure application resiliency, **Company D** uses [nested Traffic Manager profiles](#) with Azure Site Recovery. In a nested profile setup, traffic is not directed to individual endpoints, but instead to other Traffic Manager profiles. Here's how this setup works:

- Instead of utilizing Geographic routing with individual endpoints, **Company D** uses Geographic routing with Traffic Manager profiles.
- Each child Traffic Manager profile utilizes **Priority** routing with a primary and a recovery endpoint, hence nesting **Priority** routing within **Geographic** routing.
- To enable application resiliency, each workload distribution utilizes Azure Site Recovery to failover to a recovery region based in case of a disaster event.
- When the parent Traffic Manager receives a DNS query, it is directed to the relevant child Traffic Manager that responds to the query with an available endpoint.



For example, if the endpoint in Germany Central fails, the application can quickly be recovered to Germany Northeast. The new endpoint handles traffic originating from Germany with minimal downtime for users. Similarly an endpoint outage in West Europe can be handled by recovering the application workload to North Europe, with Azure Traffic Manager handling DNS redirects to the available endpoint.

The above setup can be expanded to include as many region and endpoint combinations required. Traffic Manager allows up to 10 levels of nested profiles and does not permit loops within the nested configuration.

Recovery Time Objective (RTO) considerations

In most organizations, adding or modifying DNS records is handled either by a separate team or by someone outside the organization. This makes the task of altering DNS records very challenging. The time taken to update DNS records by other teams or organizations managing DNS infrastructure varies from organization to organization, and impacts the RTO of the application.

By utilizing Traffic Manager, you can frontload the work required for DNS updates. No manual or scripted action is required at the time of actual failover. This approach helps in quick switching (and hence lowering RTO) as well as avoiding costly time-consuming DNS change errors in a disaster event. With Traffic Manager, even the fallback step is automated, which would otherwise have to be managed separately.

Setting the correct [probing interval](#) through basic or fast interval health checks can considerably bring down the RTO during failover and reduce downtime for users.

You can additionally optimize the DNS Time to Live (TTL) value for the Traffic Manager profile. TTL is the value for which a DNS entry would be cached by a client. For a record, DNS would not be queried twice within the span of TTL. Each DNS record has a TTL associated with it. Reducing this value results in more DNS queries to Traffic Manager but can reduce RTO by discovering outages faster.

The TTL experienced by the client also does not increase if the number of DNS resolvers between the client and the authoritative DNS server increases. DNS resolvers 'count down' the TTL and only pass on a TTL value that reflects the elapsed time since the record was cached. This ensures that the DNS record gets refreshed at the client after the TTL, irrespective of the number of DNS Resolvers in the chain.

Next steps

- Learn more about Traffic Manager routing methods.
- Learn more about [nested Traffic Manager profiles](#).
- Learn more about [endpoint monitoring](#).
- Learn more about [recovery plans](#) to automate application failover.

Azure ExpressRoute with Azure Site Recovery

12/17/2019 • 3 minutes to read • [Edit Online](#)

Microsoft Azure ExpressRoute lets you extend your on-premises networks into the Microsoft cloud over a private connection facilitated by a connectivity provider. With ExpressRoute, you can establish connections to Microsoft cloud services, such as Microsoft Azure, Office 365, and Dynamics 365.

This article describes how you can use Azure ExpressRoute with Azure Site Recovery for disaster recovery and migration.

ExpressRoute circuits

An ExpressRoute circuit represents a logical connection between your on-premises infrastructure and Microsoft cloud services through a connectivity provider. You can order multiple ExpressRoute circuits. Each circuit can be in the same or different regions, and can be connected to your premises through different connectivity providers.

Learn more about ExpressRoute circuits [here](#).

An ExpressRoute circuit has multiple routing domains associated with it. Learn more about and compare ExpressRoute routing domains [here](#).

On-premises to Azure replication with ExpressRoute

Azure Site Recovery enables disaster recovery and migration to Azure for on-premises [Hyper-V virtual machines](#), [VMware virtual machines](#), and [physical servers](#). For all on-premises to Azure scenarios, replication data is sent to and stored in an Azure Storage account. During replication, you don't pay any virtual machine charges. When you run a failover to Azure, Site Recovery automatically creates Azure IaaS virtual machines.

Site Recovery replicates data to an Azure Storage account or replica Managed Disk on the target Azure region over a public endpoint. To use ExpressRoute for Site Recovery replication traffic, you can utilize [Microsoft peering](#) or an existing [public peering](#) (deprecated for new creations). Microsoft peering is the recommended routing domain for replication. Note that replication is not supported over private peering.

Ensure that the [Networking Requirements](#) for Configuration Server are also met. Connectivity to specific URLs is required by Configuration Server for orchestration of Site Recovery replication. ExpressRoute cannot be used for this connectivity.

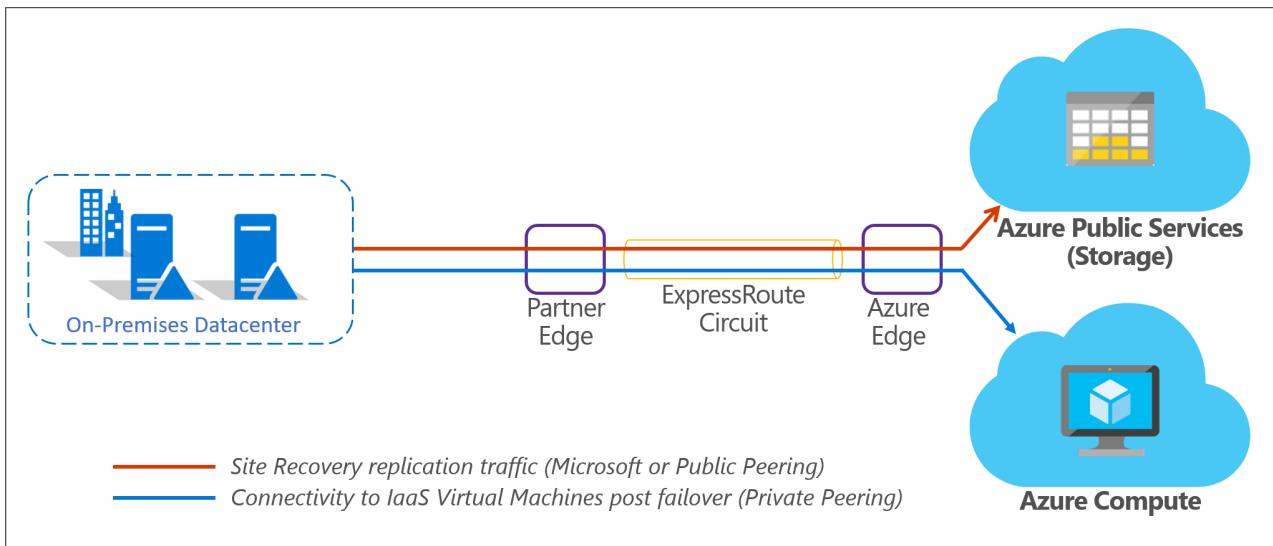
In case you use proxy at on-premises and wish to use ExpressRoute for replication traffic, you need to configure the Proxy bypass list on the Configuration Server and Process Servers. Follow the steps below:

- Download PsExec tool from [here](#) to access System user context.
- Open Internet Explorer in system user context by running the following command line psexec -s -i "%programfiles%\Internet Explorer\iexplore.exe"
- Add proxy settings in IE
- In the bypass list, add the Azure storage URL *.blob.core.windows.net

This will ensure that only replication traffic flows through ExpressRoute while the communication can go through proxy.

After virtual machines or servers fail over to an Azure virtual network, you can access them using [private peering](#).

The combined scenario is represented in the following diagram:



Azure to Azure replication with ExpressRoute

Azure Site Recovery enables disaster recovery of [Azure virtual machines](#). Depending on whether your Azure virtual machines use [Azure Managed Disks](#), replication data is sent to an Azure Storage account or replica Managed Disk on the target Azure region. Although the replication endpoints are public, replication traffic for Azure VM replication, by default, does not traverse the Internet, regardless of which Azure region the source virtual network exists in. You can override Azure's default system route for the 0.0.0.0/0 address prefix with a [custom route](#) and divert VM traffic to an on-premises network virtual appliance (NVA), but this configuration is not recommended for Site Recovery replication. If you're using custom routes, you should [create a virtual network service endpoint](#) in your virtual network for "Storage" so that the replication traffic does not leave the Azure boundary.

For Azure VM disaster recovery, by default, ExpressRoute is not required for replication. After virtual machines fail over to the target Azure region, you can access them using [private peering](#). Note that data transfer prices apply irrespective of the mode of data replication across Azure regions.

If you are already using ExpressRoute to connect from your on-premises datacenter to the Azure VMs on the source region, you can plan for re-establishing ExpressRoute connectivity at the failover target region. You can use the same ExpressRoute circuit to connect to the target region through a new virtual network connection or utilize a separate ExpressRoute circuit and connection for disaster recovery. The different possible scenarios are described [here](#).

You can replicate Azure virtual machines to any Azure region within the same geographic cluster as detailed [here](#). If the chosen target Azure region is not within the same geopolitical region as the source, you might need to enable ExpressRoute Premium. For more details, check [ExpressRoute locations](#) and [ExpressRoute pricing](#).

Next steps

- Learn more about [ExpressRoute circuits](#).
- Learn more about [ExpressRoute routing domains](#).
- Learn more about [ExpressRoute locations](#).
- Learn more about disaster recovery of [Azure virtual machines with ExpressRoute](#).

Network Security Groups with Azure Site Recovery

4/8/2019 • 5 minutes to read • [Edit Online](#)

Network Security Groups are used to limit network traffic to resources in a virtual network. A [Network Security Group \(NSG\)](#) contains a list of security rules that allow or deny inbound or outbound network traffic based on source or destination IP address, port, and protocol.

Under the Resource Manager deployment model, NSGs can be associated to subnets or individual network interfaces. When an NSG is associated to a subnet, the rules apply to all resources connected to the subnet. Traffic can further be restricted by also associating an NSG to individual network interfaces within a subnet that already has an associated NSG.

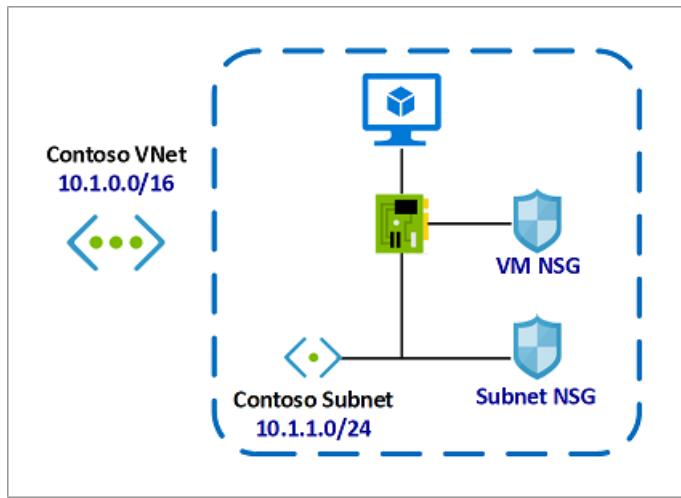
This article describes how you can use Network Security Groups with Azure Site Recovery.

Using Network Security Groups

An individual subnet can have zero, or one, associated NSG. An individual network interface can also have zero, or one, associated NSG. So, you can effectively have dual traffic restriction for a virtual machine by associating an NSG first to a subnet, and then another NSG to the VM's network interface. The application of NSG rules in this case depends on the direction of traffic and priority of applied security rules.

Consider a simple example with one virtual machine as follows:

- The virtual machine is placed inside the **Contoso Subnet**.
- **Contoso Subnet** is associated with **Subnet NSG**.
- The VM network interface is additionally associated with **VM NSG**.



In this example, for inbound traffic, the Subnet NSG is evaluated first. Any traffic allowed through Subnet NSG is then evaluated by VM NSG. The reverse is applicable for outbound traffic, with VM NSG being evaluated first. Any traffic allowed through VM NSG is then evaluated by Subnet NSG.

This allows for granular security rule application. For example, you might want to allow inbound internet access to a few application VMs (such as frontend VMs) under a subnet but restrict inbound internet access to other VMs (such as database and other backend VMs). In this case you can have a more lenient rule on the Subnet NSG, allowing internet traffic, and restrict access to specific VMs by denying access on VM NSG. The same can be applied for outbound traffic.

When setting up such NSG configurations, ensure that the correct priorities are applied to the [security rules](#). Rules

are processed in priority order, with lower numbers processed before higher numbers, because lower numbers have higher priority. Once traffic matches a rule, processing stops. As a result, any rules that exist with lower priorities (higher numbers) that have the same attributes as rules with higher priorities are not processed.

You may not always be aware when network security groups are applied to both a network interface and a subnet. You can verify the aggregate rules applied to a network interface by viewing the [effective security rules](#) for a network interface. You can also use the [IP flow verify](#) capability in [Azure Network Watcher](#) to determine whether communication is allowed to or from a network interface. The tool tells you whether communication is allowed, and which network security rule allows or denies traffic.

On-premises to Azure replication with NSG

Azure Site Recovery enables disaster recovery and migration to Azure for on-premises [Hyper-V virtual machines](#), [VMware virtual machines](#), and [physical servers](#). For all on-premises to Azure scenarios, replication data is sent to and stored in an Azure Storage account. During replication, you don't pay any virtual machine charges. When you run a failover to Azure, Site Recovery automatically creates Azure IaaS virtual machines.

Once VMs have been created after failover to Azure, NSGs can be used to limit network traffic to the virtual network and VMs. Site Recovery does not create NSGs as part of the failover operation. We recommend creating the required Azure NSGs before initiating failover. You can then associate NSGs to failed over VMs automatically during failover, using automation scripts with Site Recovery's powerful [recovery plans](#).

For example, if the post-failover VM configuration is similar to the [example scenario](#) detailed above:

- You can create **Contoso VNet** and **Contoso Subnet** as part of DR planning on the target Azure region.
- You can also create and configure both **Subnet NSG** as well as **VM NSG** as part of the same DR planning.
- **Subnet NSG** can then be immediately associated with **Contoso Subnet**, as both the NSG and the subnet are already available.
- **VM NSG** can be associated with VMs during failover using recovery plans.

Once the NSGs are created and configured, we recommend running a [test failover](#) to verify scripted NSG associations and post-failover VM connectivity.

Azure to Azure replication with NSG

Azure Site Recovery enables disaster recovery of [Azure virtual machines](#). When enabling replication for Azure VMs, Site Recovery can create the replica virtual networks (including subnets and gateway subnets) on the target region and create the required mappings between the source and target virtual networks. You can also pre-create the target side networks and subnets, and use the same while enabling replication. Site Recovery does not create any VMs on the target Azure region prior to [failover](#).

For Azure VM replication, ensure that the NSG rules on the source Azure region allow [outbound connectivity](#) for replication traffic. You can also test and verify these required rules through this [example NSG configuration](#).

Site Recovery does not create or replicate NSGs as part of the failover operation. We recommend creating the required NSGs on the target Azure region before initiating failover. You can then associate NSGs to failed over VMs automatically during failover, using automation scripts with Site Recovery's powerful [recovery plans](#).

Considering the [example scenario](#) described earlier:

- Site Recovery can create replicas of **Contoso VNet** and **Contoso Subnet** on the target Azure region when replication is enabled for the VM.
- You can create the desired replicas of **Subnet NSG** and **VM NSG** (named, for example, **Target Subnet NSG** and **Target VM NSG**, respectively) on the target Azure region, allowing for any additional rules required on the target region.
- **Target Subnet NSG** can then be immediately associated with the target region subnet, as both the NSG and

the subnet are already available.

- **Target VM NSG** can be associated with VMs during failover using recovery plans.

Once the NSGs are created and configured, we recommend running a [test failover](#) to verify scripted NSG associations and post-failover VM connectivity.

Next steps

- Learn more about [Network Security Groups](#).
- Learn more about [NSG security rules](#).
- Learn more about [effective security rules](#) for an NSG.
- Learn more about [recovery plans](#) to automate application failover.

Set up public IP addresses after failover

11/14/2019 • 2 minutes to read • [Edit Online](#)

Public IP addresses allow Internet resources to communicate inbound to Azure resources. Public IP addresses also enable Azure resources to communicate outbound to Internet and public-facing Azure services with an IP address assigned to the resource.

- Inbound communication from the Internet to the resource, such as Azure Virtual Machines (VM), Azure Application Gateways, Azure Load Balancers, Azure VPN Gateways, and others. You can still communicate with some resources, such as VMs, from the Internet, if a VM doesn't have a public IP address assigned to it, as long as the VM is part of a load balancer back-end pool, and the load balancer is assigned a public IP address.
- Outbound connectivity to the Internet using a predictable IP address. For example, a virtual machine can communicate outbound to the Internet without a public IP address assigned to it, but its address is network address translated by Azure to an unpredictable public address, by default. Assigning a public IP address to a resource enables you to know which IP address is used for the outbound connection. Though predictable, the address can change, depending on the assignment method chosen. For more information, see [Create a public IP address](#). To learn more about outbound connections from Azure resources, see [Understand outbound connections](#).

In Azure Resource Manager, a Public IP address is a resource that has its own properties. Some of the resources you can associate a public IP address resource with are:

- Virtual machine network interfaces
- Internet-facing load balancers
- VPN gateways
- Application gateways

This article describes how you can use Public IP addresses with Site Recovery.

Public IP address assignment using Recovery Plan

Public IP address of the production application **cannot be retained on failover**. Workloads brought up as part of failover process must be assigned an Azure Public IP resource available in the target region. This step can be done either manually or is automated with recovery plans. A recovery plan gathers machines into recovery groups. It helps you to define a systematic recovery process. You can use a recovery plan to impose order, and automate the actions needed at each step, using Azure Automation runbooks for failover to Azure, or scripts.

The setup is as follows:

- Create a [recovery plan](#) and group your workloads as necessary into the plan.
- Customize the plan by adding a step to attach a public IP address using [Azure Automation runbooks](#) scripts to the failed over VM.

Public endpoint switching with DNS level Routing

Azure Traffic Manager enables DNS level routing between endpoints and can assist with [driving down your RTOs](#) for a DR scenario.

Read more about failover scenarios with Traffic Manager:

1. [On-premises to Azure failover](#) with Traffic Manager

2. Azure to Azure failover with Traffic Manager

The setup is as follows:

- Create a [Traffic Manager profile](#).
- Utilizing the **Priority** routing method, create two endpoints – **Primary** for source and **Failover** for Azure. **Primary** is assigned Priority 1 and **Failover** is assigned Priority 2.
- The **Primary** endpoint can be [Azure](#) or [External](#) depending on whether your source environment is inside or outside Azure.
- The **Failover** endpoint is created as an [Azure](#) endpoint. Use a **static public IP address** as this will be external facing endpoint for Traffic Manager in the disaster event.

Next steps

- Learn more about [Traffic Manager with Azure Site Recovery](#)
- Learn more about [Traffic Manager routing methods](#).
- Learn more about [recovery plans](#) to automate application failover.

About on-premises disaster recovery failover/failback

2/21/2020 • 12 minutes to read • [Edit Online](#)

This article provides an overview of failover and fallback during disaster recovery of on-premises machines to Azure with [Azure Site Recovery](#).

Recovery stages

Failover and fallback in Site Recovery has four stages:

- **Stage 1: Fail over from on-premises:** After setting up replication to Azure for on-premises machines, when your on-premises site goes down, you fail those machines over to Azure. After failover, Azure VMs are created from replicated data.
- **Stage 2: Reprotect Azure VMs:** In Azure, you reprotect the Azure VMs so that they start replicating back to the on-premises site. The on-premises VM (if available) is turned off during reprottection, to help ensure data consistency.
- **Stage 3: Fail over from Azure:** When your on-premises site is running as normal again, you run another failover, this time to fail back Azure VMs to your on-premises site. You can fail back to the original location from which you failed over, or to an alternate location.
- **Stage 4: Reprotect on-premises machines:** After failing back, again enable replication of the on-premises machines to Azure.

Failover

You perform a failover as part of your business continuity and disaster recovery (BCDR) strategy.

- As a first step in your BCDR strategy, you replicate your on-premises machines to Azure on an ongoing basis. Users access workloads and apps running on the on-premises source machines.
- If the need arises, for example if there's an outage on-premises, you fail the replicating machines over to Azure. Azure VMs are created using the replicated data.
- For business continuity, users can continue accessing apps on the Azure VMs.

Failover is a two-phase activity:

- **Failover:** The failover that creates and brings up an Azure VM using the selected recovery point.
- **Commit:** After failover you verify the VM in Azure:
 - You can then commit the failover to the selected recovery point, or select a different point for the commit.
 - After committing the failover, the recovery point can't be changed.

Connect to Azure after failover

To connect to the Azure VMs created after failover using RDP/SSH, there are a number of requirements.

FAILOVER	LOCATION	ACTIONS
----------	----------	---------

FAILOVER	LOCATION	ACTIONS
Azure VM (Windows)	On the on-premises machine before failover	<p>Access over the internet: Enable RDP. Make sure that TCP and UDP rules are added for Public, and that RDP is allowed for all profiles in Windows Firewall > Allowed Apps.</p> <p>Access over site-to-site VPN: Enable RDP on the machine. Check that RDP is allowed in the Windows Firewall -> Allowed apps and features, for Domain and Private networks.</p> <p>Make sure the operating system SAN policy is set to OnlineAll. Learn more.</p> <p>Make sure there are no Windows updates pending on the VM when you trigger a failover. Windows Update might start when you fail over, and you won't be able to log onto the VM until updates are done.</p>
Azure VM running Windows	On the Azure VM after failover	<p>Add a public IP address for the VM.</p> <p>The network security group rules on the failed over VM (and the Azure subnet to which it is connected) must allow incoming connections to the RDP port.</p> <p>Check Boot diagnostics to verify a screenshot of the VM. If you can't connect, check that the VM is running, and review troubleshooting tips.</p>
Azure VM running Linux	On the on-premises machine before failover	<p>Ensure that the Secure Shell service on the VM is set to start automatically on system boot.</p> <p>Check that firewall rules allow an SSH connection to it.</p>
Azure VM running Linux	On the Azure VM after failover	<p>The network security group rules on the failed over VM (and the Azure subnet to which it is connected) need to allow incoming connections to the SSH port.</p> <p>Add a public IP address for the VM.</p> <p>Check Boot diagnostics for a screenshot of the VM.</p>

Types of failover

Site Recovery provides different failover options.

FAILOVER	DETAILS	RECOVERY	WORKFLOW
Test failover	Used to run a drill that validates your BCDR strategy, without any data loss or downtime.	Creates a copy of the VM in Azure, with no impact on ongoing replication, or on your production environment.	<ol style="list-style-type: none"> Run a test failover on a single VM, or on multiple VMs in a recovery plan. Select a recovery point to use for the test failover. Select an Azure network in which the Azure VM will be located when it's created after failover. The network is only used for the test failover. Verify that the drill worked as expected. Site Recovery automatically cleans up VMs created in Azure during the drill.
Planned failover-Hyper-V	<p>Usually used for planned downtime.</p> <p>Source VMs are shut down. The latest data is synchronized before initiating the failover.</p>	Zero data loss for the planned workflow.	<ol style="list-style-type: none"> Plan a downtime maintenance window and notify users. Take user-facing apps offline. Initiate a planned failover with the latest recovery point. The failover doesn't run if the machine isn't shut down, or if errors are encountered. After the failover, check that the replica Azure VM is active in Azure. Commit the failover to finish up. The commit action deletes all recovery points.

FAILOVER	DETAILS	RECOVERY	WORKFLOW
Failover-Hyper-V	<p>Usually run if there's an unplanned outage, or the primary site isn't available.</p> <p>Optionally shut down the VM, and synchronize final changes before initiating the failover.</p>	<p>Minimal data loss for apps.</p>	<ol style="list-style-type: none"> 1. Initiate your BCDR plan. 2. Initiate a failover. Specify whether Site Recovery should shut down the VM and synchronize/replicate the latest changes before triggering the failover. 3. You can fail over to a number of recovery point options, summarized in the table below. <p>If you don't enable the option to shut down the VM, or if Site Recovery can't shut it down, the latest recovery point is used. The failover runs even if the machine can't be shut down.</p> <ol style="list-style-type: none"> 4. After failover, you check that the replica Azure VM is active in Azure. If required, you can select a different recovery point from the retention window of 24 hours. 5. Commit the failover to finish up. The commit action deletes all available recovery points.

FAILOVER	DETAILS	RECOVERY	WORKFLOW
Failover-VMware	<p>Usually run if there's an unplanned outage, or the primary site isn't available.</p> <p>Optionally specify that Site Recovery should try to trigger a shutdown of the VM, and to synchronize and replicate final changes before initiating the failover.</p>	Minimal data loss for apps.	<ol style="list-style-type: none"> Initiate your BCDR plan. Initiate a failover from Site Recovery. Specify whether Site Recovery should try to trigger VM shutdown and synchronize before running the failover. The failover runs even if the machines can't be shut down. After the failover, check that the replica Azure VM is active in Azure. If required, you can select a different recovery point from the retention window of 72 hours. Commit the failover to finish up. The commit action deletes all recovery points. For Windows VMs, Site Recovery disables the VMware tools during failover.

Failover processing

In some scenarios, failover requires additional processing that takes around 8 to 10 minutes to complete. You might notice longer test failover times for:

- VMware VMs running a Mobility service version older than 9.8.
- Physical servers.
- VMware Linux VMs.
- Hyper-V VMs protected as physical servers.
- VMware VMs that don't have the DHCP service enabled.
- VMware VMs that don't have the following boot drivers: storvsc, vmbus, storflt, intelide, atapi.

Recovery point options

During failover, you can select a number of recovery point options.

OPTION	DETAILS
Latest (lowest RPO)	This option provides the lowest recovery point objective (RPO). It first processes all the data that has been sent to Site Recovery service, to create a recovery point for each VM, before failing over to it. This recovery point has all the data replicated to Site Recovery when the failover was triggered.

OPTION	DETAILS
Latest processed	This option fails over VMs to the latest recovery point processed by Site Recovery. To see the latest recovery point for a specific VM, check Latest Recovery Points in the VM settings. This option provides a low RTO (Recovery Time Objective), because no time is spent processing unprocessed data.
Latest app-consistent	This option fails over VMs to the latest application-consistent recovery point processed by Site Recovery, if app-consistent recovery points are enabled. Check the latest recovery point in the VM settings.
Latest multi-VM processed	This option is available for recovery plans with one or more VMs that have multi-VM consistency enabled. VMs with the setting enabled fail over to the latest common multi-VM consistent recovery point. Any other VMs in the plan fail over to the latest processed recovery point.
Latest multi-VM app-consistent	This option is available for recovery plans with one or more VMs that have multi-VM consistency enabled. VMs that are part of a replication group fail over to the latest common multi-VM application-consistent recovery point. Other VMs fail over to their latest application-consistent recovery point.
Custom	Use this option to fail over a specific VM to a particular recovery point in time. This option isn't available for recovery plans.

NOTE

Recovery points can't be migrated to another Recovery Services vault.

Reprotection/fallback

After failover to Azure, the replicated Azure VMs are in an unprotected state.

- As a first step to failing back to your on-premises site, you need to start the Azure VMs replicating to on-premises. The reprotection process depends on the type of machines you failed over.
- After machines are replicating from Azure to on-premises, you can run a failover from Azure to your on-premises site.
- After machines are running on-premises again, you can enable replication so that they replicate to Azure for disaster recovery.

Fallback works as follows:

- To fail back, a VM needs at least one recovery point in order to fail back. In a recovery plan, all VMs in the plan need at least one recovery point.
- We recommend that you use the **Latest** recovery point to fail back (this is a crash-consistent point).
 - There is an app-consistent recovery point option. In this case, a single VM recovers to its latest available app-consistent recovery point. For a recovery plan with a replication group, each replication group recovers to its common available recovery point.
 - App-consistent recovery points can be behind in time, and there might be loss in data.
- During failover from Azure to the on-premises site, Site Recovery shuts down the Azure VMs. When you

commit the failover, Site Recovery removes the failed back Azure VMs in Azure.

VMware/physical reprottection/failback

To reprotect and fail back VMware machines and physical servers from Azure to on-premises, you need a failback infrastructure, and there are a number of requirements.

- **Temporary process server in Azure:** To fail back from Azure, you set up an Azure VM to act as a process server to handle replication from Azure. You can delete this VM after failback finishes.
- **VPN connection:** To fail back, you need a VPN connection (or ExpressRoute) from the Azure network to the on-premises site.
- **Separate master target server:** By default, the master target server that was installed with the configuration server on the on-premises VMware VM handles failback. If you need to fail back large volumes of traffic, set up a separate on-premises master target server for this purpose.
- **Failback policy:** To replicate back to your on-premises site, you need a failback policy. This policy is automatically created when you create a replication policy from on-premises to Azure.
 - This policy is automatically associated with the configuration server.
 - You can't edit this policy.
 - Policy values: RPO threshold - 15 minutes; Recovery point retention - 24 Hours; App-consistent snapshot frequency - 60 minutes.

Learn more about VMware/physical reprottection and failback:

- [Review](#) additional requirements for reprottection and failback.
- [Deploy](#) a process server in Azure.
- [Deploy](#) a separate master target server.

When you reprotect Azure VMs to on-premises, you can specify that you want to fail back to the original location, or to an alternate location.

- **Original location recovery:** This fails back from Azure to the same source on-premises machine if it exists. In this scenario, only changes are replicated back to on-premises.
- **Alternate location recovery:** If the on-premises machine doesn't exist, you can fail back from Azure to an alternate location. When you reprotect the Azure VM to on-premises, the on-premises machine is created. Full data replication occurs from Azure to on-premises. -- [Review](#) the requirements and limitations for location failback.

Hyper-V reprottection/failback

To reprotect and fail back Hyper-V VMs from Azure to on-premises:

- You can only fail back Hyper-V VMs replicating using a storage account. Failback of Hyper-V VMs that replicate using managed disks isn't supported.
- On-premises Hyper-V hosts (or System Center VMM if used) should be connected to Azure.
- You run a planned failback from Azure to on-premises.
- No specific components need to be set up for Hyper-V VM failback.
- During planned failover, you can select options to synchronize data before failback:
 - **Synchronize data before failover:** This option minimizes downtime for virtual machines as it synchronizes machines without shutting them down.
 - Phase 1: Takes a snapshot of the Azure VM and copies it to the on-premises Hyper-V host. The machine continues running in Azure.
 - Phase 2: Shuts down the Azure VM so that no new changes occur there. The final set of delta changes is transferred to the on-premises server and the on-premises VM is started up.

- **Synchronize data during failover only:** This option is faster because we expect that most of the disk has changed, and thus don't perform checksum calculations. It performs a download of the disk. We recommend that you use this option if the VM has been running in Azure for a while (a month or more), or if the on-premises VM has been deleted.

[Learn more](#) about Hyper-V reprottection and failback.

When you reprotect Azure VMs to on-premises, you can specify that you want to fail back to the original location, or to an alternate location.

- **Original location recovery:** This fails back from Azure to the same source on-premises machine if it exists. In this scenario, you select one of the synchronization options described in the previous procedure.
- **Alternate location recovery:** If the on-premises machine doesn't exist, you can fail back from Azure to an alternate location. When you reprotect the Azure VM to on-premises, the on-premises machine is created. With this option, we recommend that you select the option to synchronize data before failover
- [Review](#) the requirements and limitations for location failback.

After failing back to the on-premises site, you enable **Reverse Replicate** to start replicating the VM to Azure, completing the cycle.

Next steps

- Fail over [specific VMware VMs](#)
- Fail over [specific Hyper-V VMs](#).
- [Create](#) a recovery plan.
- Fail over [VMs in a recovery plan](#).
- [Prepare for](#) VMware reprottection and failback.
- Fail back [Hyper-V VMs](#).

About recovery plans

1/23/2020 • 4 minutes to read • [Edit Online](#)

This article provides an overview of recovery plans in [Azure Site Recovery](#).

A recovery plan gathers machines into recovery groups for the purpose of failover. A recovery plan helps you to define a systematic recovery process, by creating small independent units that you can fail over. A unit typically represents an app in your environment.

- A recovery plan defines how machines fail over, and the sequence in which they start after failover.
- Recovery plans are used for failover to Azure, but can't be used for fallback from Azure.
- Up to 100 protected instances can be added to one recovery plan.
- You can customize a plan by adding order, instructions, and tasks to it.
- After a plan is defined, you can run a failover on it.
- Machines can be referenced in multiple recovery plans, in which subsequent plans skip the deployment/startup of a machine if it was previously deployed using another recovery plan.

Why use a recovery plan?

Use recovery plans to:

- Model an app around its dependencies.
- Automate recovery tasks to reduce recovery time objective (RTO).
- Verify that you're prepared for migration or disaster recovery by ensuring that your apps are part of a recovery plan.
- Run test failovers on recovery plans, to ensure disaster recovery or migration is working as expected.

Model apps

You can plan and create a recovery group to capture app-specific properties. As an example, let's consider a typical three-tier application with a SQL server backend, middleware, and a web frontend. Typically, you customize the recovery plan so that machines in each tier start in the correct order after failover.

- The SQL backend should start first, the middleware next, and finally the web frontend.
- This start order ensures that the app is working by the time the last machine starts.
- This order ensures that when the middleware starts and tries to connect to the SQL Server tier, the SQL Server tier is already running.
- This order also helps ensure that the front-end server starts last, so that end users don't connect to the app URL before all the components are up and running, and the app is ready to accept requests.

To create this order, you add groups to the recovery group, and add machines into the groups.

- Where order is specified, sequencing is used. Actions run in parallel as appropriate, to improve application recovery RTO.
- Machines in a single group fail over in parallel.
- Machines in different groups fail over in group order, so that Group 2 machines start their failover only after all the machines in Group 1 have failed over and started.



+ Group

Save

X Discard

↑↓ Change group



This recovery plan contains 3 machine(s).

STAGE NAME	DETAILS	
All groups shutdown	3 machines in 3 groups.	...
▼ All groups failover		...
▼ Machines	3 Machines	...
SQLServer	Machine	...
SalesAppController	Machine	...
Sales-Frontend	Machine	...
▼ Group 1: Start	1 Machine	...
SQLServer	Machine	...
▼ Group 2: Start	1 Machine	...
SalesAppController	Machine	...
▼ Group 3: Start	1 Machine	...
Sales-Frontend	Machine	...

With this customization in place, here's what happens when you run a failover on the recovery plan:

1. A shutdown step attempts to turn off the on-premises machines. The exception is if you run a test failover, in which case the primary site continues to run.
2. The shutdown triggers a parallel failover of all the machines in the recovery plan.
3. The failover prepares virtual machine disks using replicated data.
4. The startup groups run in order, and start the machines in each group. First, Group 1 runs, then Group 2, and finally, Group 3. If there's more than one machine in any group, then all the machines start in parallel.

Automate tasks in recovery plans

Recovering large applications can be a complex task. Manual steps make the process prone to error, and the person running the failover might not be aware of all app intricacies. You can use a recovery plan to impose order, and automate the actions needed at each step, using Azure Automation runbooks for failover to Azure, or scripts. For tasks that can't be automated, you can insert pauses for manual actions into recovery plans. There are a couple of types of tasks you can configure:

- **Tasks on the Azure VM after failover:** When you're failing over to Azure, you typically need to perform actions so that you can connect to the VM after failover. For example:
 - Create a public IP address on the Azure VM.
 - Assign a network security group to the network adapter of the Azure VM.
 - Add a load balancer to an availability set.
- **Tasks inside VM after failover:** These tasks typically reconfigure the app running on the machine, so that it continues to work correctly in the new environment. For example:
 - Modify the database connection string inside the machine.
 - Change the web server configuration or rules.

Run a test failover on recovery plans

You can use a recovery plan to trigger a test failover. Use the following best practices:

- Always complete a test failover on an app, before running a full failover. Test failovers help you to check whether the app comes up on the recovery site.
- If you find you've missed something, trigger a clean-up, and then rerun the test failover.
- Run a test failover multiple times, until you're sure that the app recovers smoothly.
- Because each app is unique, you need to build recovery plans that are customized for each application, and run a test failover on each.
- Apps and their dependencies change frequently. To ensure recovery plans are up to date, run a test failover for each app every quarter.

The screenshot shows the Azure Site Recovery Job blade for a 'Test failover' job. The job is named 'Site Recovery Job'. It has two tabs: 'Properties' and 'Job'. The 'Properties' tab displays the following details:

Vault	ContosoApps
Recovery plan	Wordpress
Job id	[Redacted]
Source	ContosoCSPS-1
Target	Microsoft Azure

The 'Job' tab lists the steps of the failover process:

NAME	STATUS	START TIME	DURATION
Prerequisites check for the recovery plan	Successful	3/12/2017, 6:58:23 PM	00:00:17
Create the test environment	Successful	3/12/2017, 6:58:41 PM	00:00:02
▶ Recovery plan failover	Successful	3/12/2017, 6:58:44 PM	00:01:40
▼ Group 1: Start (1)	Successful	3/12/2017, 7:00:24 PM	00:01:41
ContosoWordpressMysql	Successful	3/12/2017, 7:00:24 PM	00:01:41
▼ Group 2: Start (1)	Successful	3/12/2017, 7:02:06 PM	00:01:44
ContosoWordpress	Successful	3/12/2017, 7:02:06 PM	00:01:44
▼ Group 2: Post-steps (2)	Successful	3/12/2017, 7:03:51 PM	00:08:42
Script on recovery side: Change IP address	Successful	3/12/2017, 7:03:51 PM	00:05:23
Script on recovery side: Add Public IP	Successful	3/12/2017, 7:09:15 PM	00:03:18
Finalizing the recovery plan	Successful	3/12/2017, 7:12:33 PM	00:00:00

Watch a recovery plan video

Watch a quick example video showing an on-click failover for a recovery plan for a two-tier WordPress app.

Next steps

- [Create](#) a recovery plan.
- [Run](#) failovers.

About migration

11/5/2019 • 2 minutes to read • [Edit Online](#)

Read this article for a quick overview of how the [Azure Site Recovery](#) service helps you to migrate machines.

Here's what you can migrate using Site Recovery:

- **Migrate from on-premises to Azure:** Migrate on-premises Hyper-V VMs, VMware VMs, and physical servers to Azure. After the migration, workloads running on the on-premises machines will be running on Azure VMs.
- **Migrate within Azure:** Migrate Azure VMs between Azure regions.
- **Migrate AWS:** Migrate AWS Windows instances to Azure IaaS VMs.

NOTE

You can now migrate from on-premises to Azure using the Azure Migrate service. [Learn more.](#)

What do we mean by migration?

In addition to using Site Recovery for disaster recovery of on-premises and Azure VMs, you can use the Site Recovery service to migrate them. What's the difference?

- For disaster recovery, you replicate machines on a regular basis to Azure. When an outage occurs, you fail the machines over from the primary site to the secondary Azure site, and access them from there. When the primary site is available again, you fail back from Azure.
- For migration, you replicate on-premises machines to Azure, or Azure VMs to a secondary region. Then you fail the VM over from the primary site to the secondary, and complete the migration process. There's no failback involved.

Migration scenarios

SCENARIO	DETAILS
Migrate from on-premises to Azure	You can migrate on-premises VMware VMs, Hyper-V VMs, and physical servers to Azure. To do this, you complete almost the same steps as you would for full disaster recovery. You simply don't fail machines back from Azure to the on-premises site.
Migrate between Azure regions	You can migrate Azure VMs from one Azure region to another. After the migration is complete, you can configure disaster recovery for the Azure VMs now in the secondary region to which you migrated.
Migrate AWS to Azure	You can migrate AWS instances to Azure VMs. Site Recovery treats AWS instances as physical servers for migration purposes.

Next steps

- [Migrate on-premises machines to Azure](#)

- Migrate VMs from one Azure region to another
- Migrate AWS to Azure

Manage Site Recovery access with role-based access control (RBAC)

11/14/2019 • 2 minutes to read • [Edit Online](#)

Azure role-based access Control (RBAC) enables fine-grained access management for Azure. Using RBAC, you can segregate responsibilities within your team and grant only specific access permissions to users as needed to perform specific jobs.

Azure Site Recovery provides 3 built-in roles to control Site Recovery management operations. Learn more on [Azure RBAC built-in roles](#)

- [Site Recovery Contributor](#) - This role has all permissions required to manage Azure Site Recovery operations in a Recovery Services vault. A user with this role, however, can't create or delete a Recovery Services vault or assign access rights to other users. This role is best suited for disaster recovery administrators who can enable and manage disaster recovery for applications or entire organizations, as the case may be.
- [Site Recovery Operator](#) - This role has permissions to execute and manage Failover and Failback operations. A user with this role can't enable or disable replication, create or delete vaults, register new infrastructure or assign access rights to other users. This role is best suited for a disaster recovery operator who can failover virtual machines or applications when instructed by application owners and IT administrators in an actual or simulated disaster situation such as a DR drill. Post resolution of the disaster, the DR operator can re-protect and failback the virtual machines.
- [Site Recovery Reader](#) - This role has permissions to view all Site Recovery management operations. This role is best suited for an IT monitoring executive who can monitor the current state of protection and raise support tickets if required.

If you're looking to define your own roles for even more control, see how to [build Custom roles](#) in Azure.

Permissions required to enable replication for new virtual machines

When a new Virtual Machine is replicated to Azure using Azure Site Recovery, the associated user's access levels are validated to ensure that the user has the required permissions to use the Azure resources provided to Site Recovery.

To enable replication for a new virtual machine, a user must have:

- Permission to create a virtual machine in the selected resource group
- Permission to create a virtual machine in the selected virtual network
- Permission to write to the selected Storage account

A user needs the following permissions to complete replication of a new virtual machine.

IMPORTANT

Ensure that relevant permissions are added per the deployment model (Resource Manager/ Classic) used for resource deployment.

NOTE

If you are enabling replication for an Azure VM and want to allow Site Recovery to manage updates, then while enabling replication you may also want to create a new Automation account in which case you would need permission to create an automation account in the same subscription as the vault as well.

RESOURCE TYPE	DEPLOYMENT MODEL	PERMISSION
Compute	Resource Manager	Microsoft.Compute/availabilitySets/read
		Microsoft.Compute/virtualMachines/read
		Microsoft.Compute/virtualMachines/write
		Microsoft.Compute/virtualMachines/delete
	Classic	Microsoft.ClassicCompute/domainNames/read
		Microsoft.ClassicCompute/domainNames/write
		Microsoft.ClassicCompute/domainNames/delete
		Microsoft.ClassicCompute/virtualMachines/read
		Microsoft.ClassicCompute/virtualMachines/write
		Microsoft.ClassicCompute/virtualMachines/delete
Network	Resource Manager	Microsoft.Network/networkInterfaces/read
		Microsoft.Network/networkInterfaces/write
		Microsoft.Network/networkInterfaces/delete
		Microsoft.Network/networkInterfaces/join/action
		Microsoft.Network/virtualNetworks/read
		Microsoft.Network/virtualNetworks/subnets/read

RESOURCE TYPE	DEPLOYMENT MODEL	PERMISSION
		Microsoft.Network/virtualNetworks/subnets/join/action
	Classic	Microsoft.ClassicNetwork/virtualNetworks/read
		Microsoft.ClassicNetwork/virtualNetworks/join/action
Storage	Resource Manager	Microsoft.Storage/storageAccounts/read
		Microsoft.Storage/storageAccounts/listkeys/action
	Classic	Microsoft.ClassicStorage/storageAccounts/read
		Microsoft.ClassicStorage/storageAccounts/listKeys/action
Resource Group	Resource Manager	Microsoft.Resources/deployments/*
		Microsoft.Resources/subscriptions/resourceGroups/read

Consider using the 'Virtual Machine Contributor' and 'Classic Virtual Machine Contributor' [built-in roles](#) for Resource Manager and Classic deployment models respectively.

Next steps

- [Role-Based Access Control](#): Get started with RBAC in the Azure portal.
- Learn how to manage access with:
 - [PowerShell](#)
 - [Azure CLI](#)
 - [REST API](#)
- [Role-Based Access Control troubleshooting](#): Get suggestions for fixing common issues.

Support matrix for disaster recovery of VMware VMs and physical servers to a secondary site

11/14/2019 • 3 minutes to read • [Edit Online](#)

This article summarizes what's supported when you use the [Azure Site Recovery](#) service for disaster recovery of VMware VMs or Windows/Linux physical servers to a secondary VMware site.

- If you want to replicate VMware VMs or physical servers to Azure, review [this support matrix](#).
- If you want to replicate Hyper-V VMs to a secondary site, review [this support matrix](#).

NOTE

Replication of on-premises VMware VMs and physical servers is provided by InMage Scout. InMage Scout is included in Azure Site Recovery service subscription.

End-of-support announcement

The Site Recovery scenario for replication between on-premises VMware or physical datacenters is reaching end-of-support.

- From August 2018, the scenario can't be configured in the Recovery Services vault, and the InMage Scout software can't be downloaded from the vault. Existing deployments will be supported.
- - From December 31 2020, the scenario won't be supported. Existing partners can onboard new customers to the scenario until support ends.
- During 2018 and 2019, two updates will be released:
 - Update 7: Fixes network configuration and compliance issues, and provides TLS 1.2 support.
 - Update 8: Adds support for Linux operating systems RHEL/CentOS 7.3/7.4/7.5, and for SUSE 12
 - After Update 8, no further updates will be released. There will be limited hotfix support for the operating systems added in Update 8, and bug fixes based on best effort.

Host servers

OPERATING SYSTEM	DETAILS
vCenter server	vCenter 5.5, 6.0 and 6.5 If you run 6.0 or 6.5, note that only 5.5 features are supported.

Replicated VM support

The following table summarizes operating system support for machines replicated with Site Recovery. Any workload can be running on the supported operating system.

OPERATING SYSTEM	DETAILS
------------------	---------

OPERATING SYSTEM	DETAILS
Windows Server	64-bit Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2 with at least SP1.
Linux	<p>Red Hat Enterprise Linux 6.7, 6.8, 6.9, 7.1, 7.2</p> <p>Centos 6.5, 6.6, 6.7, 6.8, 6.9, 7.0, 7.1, 7.2</p> <p>Oracle Enterprise Linux 6.4, 6.5, 6.8 running the Red Hat compatible kernel, or Unbreakable Enterprise Kernel Release 3 (UEK3)</p> <p>SUSE Linux Enterprise Server 11 SP3, 11 SP4</p>

Linux machine storage

Only Linux machines with the following storage can be replicated:

- File system (EXT3, EXT4, ReiserFS, XFS).
- Multipath software-device Mapper.
- Volume manager (LVM2).
- Physical servers with HP CCISS controller storage are not supported.
- The ReiserFS file system is supported only on SUSE Linux Enterprise Server 11 SP3.

Network configuration - Host/Guest VM

CONFIGURATION	SUPPORTED
Host - NIC teaming	Yes
Host - VLAN	Yes
Host - IPv4	Yes
Host - IPv6	No
Guest VM - NIC teaming	No
Guest VM - IPv4	Yes
Guest VM - IPv6	No
Guest VM - Windows/Linux - Static IP address	Yes
Guest VM - Multi-NIC	Yes

Storage

Host storage

STORAGE (HOST)	SUPPORTED
NFS	Yes
SMB 3.0	N/A
SAN (iSCSI)	Yes
Multi-path (MPIO)	Yes

Guest or physical server storage

CONFIGURATION	SUPPORTED
VMDK	Yes
VHD/VHDX	N/A
Gen 2 VM	N/A
Shared cluster disk	Yes
Encrypted disk	No
UEFI	Yes
NFS	No
SMB 3.0	No
RDM	Yes
Disk > 1 TB	Yes
Volume with striped disk > 1 TB	Yes
LVM	
Storage Spaces	No
Hot add/remove disk	Yes
Exclude disk	Yes
Multi-path (MPIO)	N/A

Vaults

ACTION	SUPPORTED
Move vaults across resource groups (within or across subscriptions)	No

ACTION	SUPPORTED
Move storage, network, Azure VMs across resource groups (within or across subscriptions)	No

Mobility service and updates

The Mobility service coordinates replication between on-premises VMware servers or physical servers, and the secondary site. When you set up replication, you should make sure you have the latest version of the Mobility service, and of other components.

UPDATE	DETAILS
Scout updates	<p>Scout updates are cumulative.</p> <p>Learn about and download the latest Scout updates</p>
Component updates	<p>Scout updates include updates for all components, including the RX server, configuration server, process and master target servers, vContinuum servers, and source servers you want to protect.</p> <p>Learn more.</p>

Next steps

Download the [InMage Scout user guide](#)

- [Replicate Hyper-V VMs in VMM clouds to a secondary site](#)
- [Replicate VMware VMs and physical servers to a secondary site](#)

Architecture for VMware/physical server replication to a secondary on-premises site

11/12/2019 • 2 minutes to read • [Edit Online](#)

This article describes the architecture and processes used when set up disaster recovery replication, failover, and recovery of on-premises VMware virtual machines (VMs) or physical Windows/Linux servers to a secondary VMware site using [Azure Site Recovery](#).

Architectural components

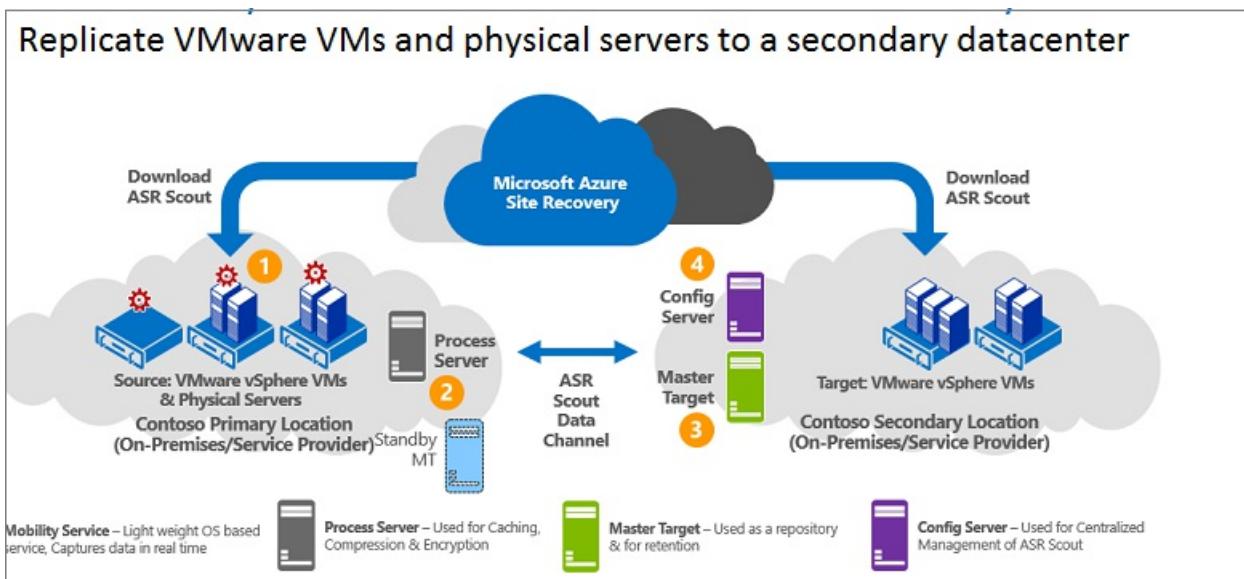
AREA	COMPONENT	DETAILS
Azure	You deploy this scenario using InMage Scout.	To obtain InMage Scout you need an Azure subscription. After you create a Recovery Services vault, you download InMage Scout and install the latest updates to set up the deployment.
Process server	Located in primary site	You deploy the process server to handle caching, compression, and data optimization. It also handles push installation of the Unified Agent to machines you want to protect.
Configuration server	Located in secondary site	The configuration server manages, configure, and monitor your deployment, either using the management website or the vContinuum console.
vContinuum server	Optional. Installed in the same location as the configuration server.	It provides a console for managing and monitoring your protected environment.
Master target server	Located in the secondary site	The master target server holds replicated data. It receives data from the process server, creates a replica machine in the secondary site, and holds the data retention points. The number of master target servers you need depends on the number of machines you're protecting. If you want to fail back to the primary site, you need a master target server there too. The Unified Agent is installed on this server.

AREA	COMPONENT	DETAILS
VMware ESX/ESXi and vCenter server	VMs are hosted on ESX/ESXi hosts. Hosts are managed with a vCenter server	You need a VMware infrastructure to replicate VMware VMs.
VMs/physical servers	Unified Agent installed on VMware VMs and physical servers you want to replicate.	The agent acts as a communication provider between all of the components.

Replication process

1. You set up the component servers in each site (configuration, process, master target), and install the Unified Agent on machines that you want to replicate.
2. After initial replication, the agent on each machine sends delta replication changes to the process server.
3. The process server optimizes the data, and transfers it to the master target server on the secondary site. The configuration server manages the replication process.

Figure 6: VMware to VMware replication



Next steps

[Set up](#) disaster recovery of VMware VMs and physical servers to a secondary site.

Support matrix for disaster recovery of Hyper-V VMs to a secondary site

11/15/2019 • 2 minutes to read • [Edit Online](#)

This article summarizes what's supported when you use the [Azure Site Recovery](#) service to replicate Hyper-V VMs managed in System Center Virtual Machine Manager (VMM) clouds to a secondary site. If you want to replicate Hyper-V VMs to Azure, review [this support matrix](#).

NOTE

You can only replicate to a secondary site when your Hyper-V hosts are managed in VMM clouds.

Host servers

OPERATING SYSTEM	DETAILS
Windows Server 2012 R2	Servers must be running the latest updates.
Windows Server 2016	VMM 2016 clouds with a mixture of Windows Server 2016 and 2012 R2 hosts aren't currently supported. Deployments that upgraded from System Center 2012 R2 VMM 2012 R2 to System Center 2016 aren't currently supported.

Replicated VM support

The following table summarizes operating system support for machines replicated with Site Recovery. Any workload can be running on the supported operating system.

WINDOWS VERSION	HYPER-V (WITH VMM)
Windows Server 2016	Any guest operating system supported by Hyper-V on Windows Server 2016
Windows Server 2012 R2	Any guest operating system supported by Hyper-V on Windows Server 2012 R2

Linux machine storage

Only Linux machines with the following storage can be replicated:

- File system (EXT3, ETX4, ReiserFS, XFS).
- Multipath software-device Mapper.
- Volume manager (LVM2).
- Physical servers with HP CCISS controller storage are not supported.
- The ReiserFS file system is supported only on SUSE Linux Enterprise Server 11 SP3.

Network configuration - Host/Guest VM

CONFIGURATION	SUPPORTED
Host - NIC teaming	Yes
Host - VLAN	Yes
Host - IPv4	Yes
Host - IPv6	No
Guest VM - NIC teaming	No
Guest VM - IPv4	Yes
Guest VM - IPv6	No
Guest VM - Windows/Linux - Static IP address	Yes
Guest VM - Multi-NIC	Yes

Storage

Host storage

STORAGE (HOST)	SUPPORTED
NFS	N/A
SMB 3.0	Yes
SAN (iSCSI)	Yes
Multi-path (MPIO)	Yes

Guest or physical server storage

CONFIGURATION	SUPPORTED
VMDK	N/A
VHD/VHDX	Yes (up to 16 disks)
Gen 2 VM	Yes
Shared cluster disk	No
Encrypted disk	No
UEFI	N/A

CONFIGURATION	SUPPORTED
NFS	No
SMB 3.0	No
RDM	N/A
Disk > 1 TB	Yes
Volume with striped disk > 1 TB	Yes
LVM	
Storage Spaces	Yes
Hot add/remove disk	No
Exclude disk	Yes
Multi-path (MPIO)	Yes

Vaults

ACTION	SUPPORTED
Move vaults across resource groups (within or across subscriptions)	No
Move storage, network, Azure VMs across resource groups (within or across subscriptions)	No

Azure Site Recovery Provider

The Provider coordinates communications between VMM servers.

LATEST	UPDATES
5.1.19 (available from portal)	Latest features and fixes

Next steps

[Replicate Hyper-V VMs in VMM clouds to a secondary site](#)

Architecture - Hyper-V replication to a secondary site

11/15/2019 • 2 minutes to read • [Edit Online](#)

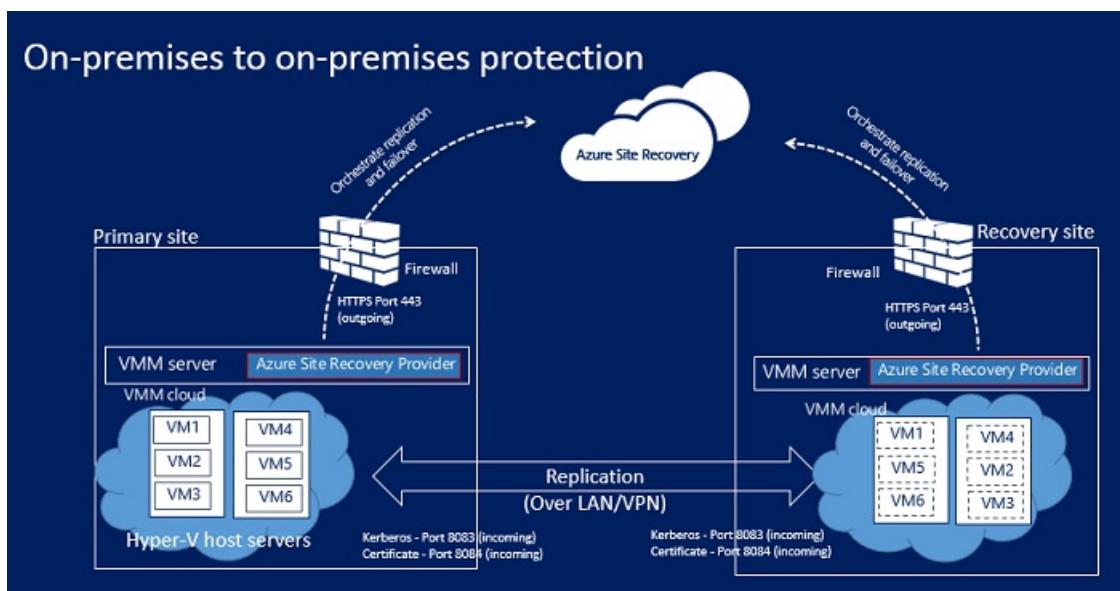
This article describes the components and processes involved when replicating on-premises Hyper-V virtual machines (VMs) in System Center Virtual Machine Manager (VMM) clouds, to a secondary VMM site using the [Azure Site Recovery](#) service in the Azure portal.

Architectural components

The following table and graphic provide a high-level view of the components used for Hyper-V replication to a secondary site.

COMPONENT	REQUIREMENT	DETAILS
Azure	Azure subscription	You create a Recovery Services vault in the Azure subscription, to orchestrate and manage replication between VMM locations.
VMM server	You need a VMM primary and secondary location.	We recommend a VMM server in the primary site, and one in the secondary site.
Hyper-V server	One or more Hyper-V host servers in the primary and secondary VMM clouds.	Data is replicated between the primary and secondary Hyper-V host servers over the LAN or VPN, using Kerberos or certificate authentication.
Hyper-V VMs	On Hyper-V host server.	The source host server should have at least one VM that you want to replicate.

On-premises to on-premises architecture



Replication process

1. When initial replication is triggered, a [Hyper-V VM snapshot](#) snapshot is taken.
2. Virtual hard disks on the VM are replicated one by one, to the secondary location.
3. If disk changes occur while initial replication is in progress, the Hyper-V Replica Replication Tracker tracks the changes as Hyper-V replication logs (.hrl). These log files are located in the same folder as the disks. Each disk has an associated .hrl file that's sent to the secondary location. The snapshot and log files consume disk resources while initial replication is in progress.
4. When the initial replication finishes, the VM snapshot is deleted, and delta replication begins.
5. Delta disk changes in the log are synchronized and merged to the parent disk.

Failover and failback process

- You can fail over a single machine, or create recovery plans, to orchestrate failover of multiple machines.
- You can run a planned or unplanned failover between on-premises sites. If you run a planned failover, then source VMs are shut down to ensure no data loss.
 - If you perform an unplanned failover to a secondary site, after the failover machines in the secondary location aren't protected.
 - If you ran a planned failover, after the failover, machines in the secondary location are protected.
- After the initial failover runs, you commit it, to start accessing the workload from the replica VM.
- When the primary location is available again, you can fail back.
 - You initiate reverse replication, to start replicating from the secondary site to the primary. Reverse replication brings the virtual machines into a protected state, but the secondary datacenter is still the active location.
 - To make the primary site into the active location again, you initiate a planned failover from secondary to primary, followed by another reverse replication.

Next steps

Follow [this tutorial](#) to enable Hyper-V replication between VMM clouds.

About networking in Azure VM disaster recovery

1/24/2020 • 4 minutes to read • [Edit Online](#)

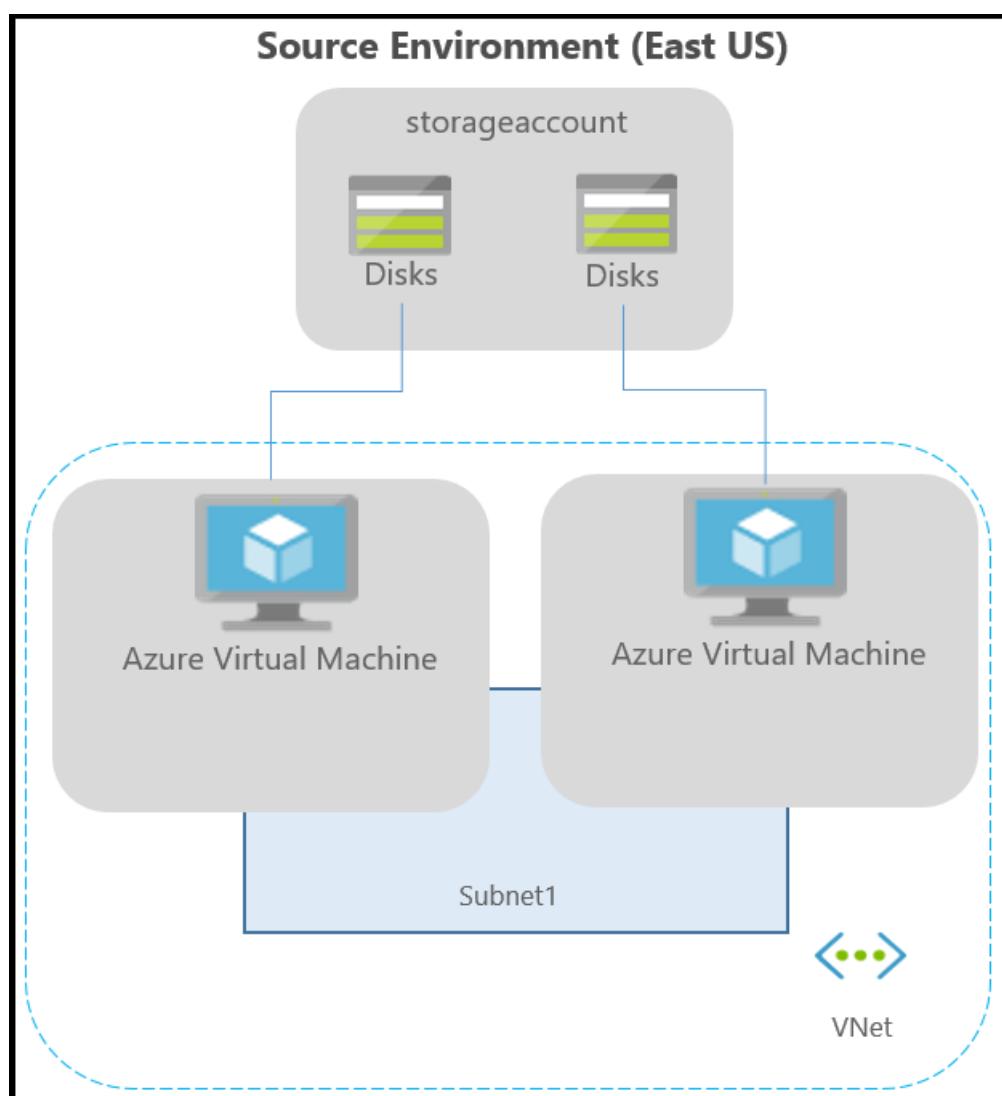
This article provides networking guidance when you're replicating and recovering Azure VMs from one region to another, using [Azure Site Recovery](#).

Before you start

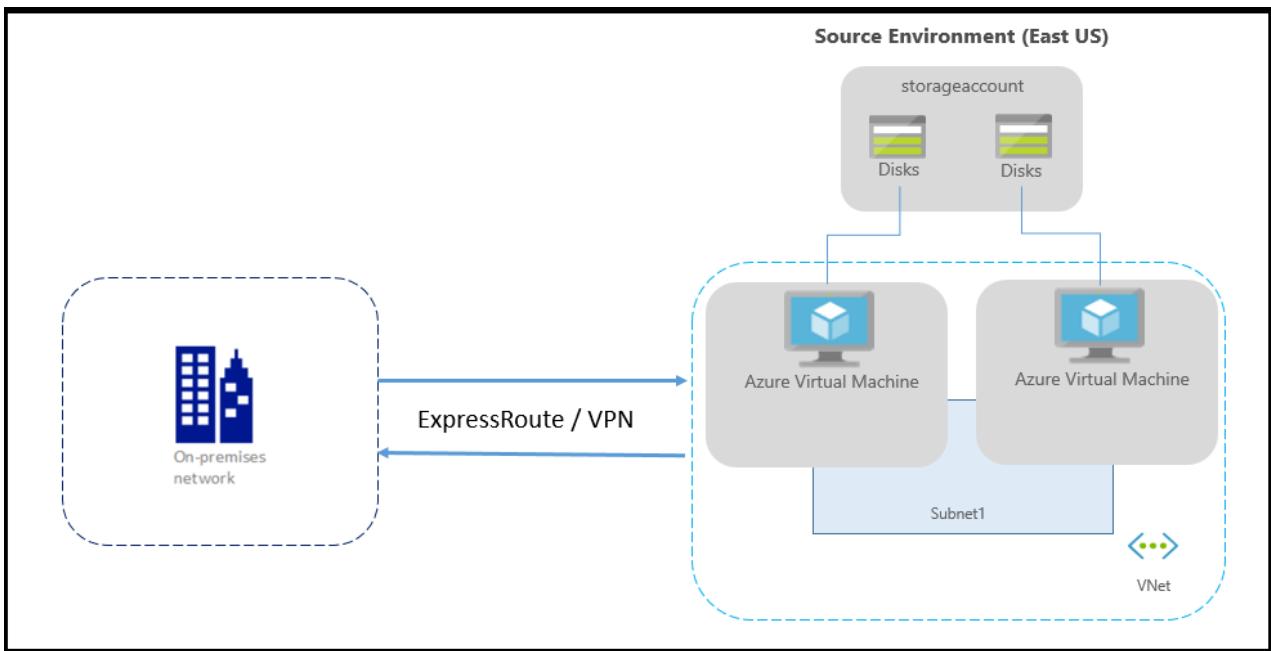
Learn how Site Recovery provides disaster recovery for [this scenario](#).

Typical network infrastructure

The following diagram depicts a typical Azure environment, for applications running on Azure VMs:



If you're using Azure ExpressRoute or a VPN connection from your on-premises network to Azure, the environment is as follows:



Typically, networks are protected using firewalls and network security groups (NSGs). Firewalls use URL or IP-based whitelisting to control network connectivity. NSGs provide rules that use IP address ranges to control network connectivity.

IMPORTANT

Using an authenticated proxy to control network connectivity isn't supported by Site Recovery, and replication can't be enabled.

Outbound connectivity for URLs

If you are using a URL-based firewall proxy to control outbound connectivity, allow these Site Recovery URLs:

URL	DETAILS
*.blob.core.windows.net	Required so that data can be written to the cache storage account in the source region from the VM. If you know all the cache storage accounts for your VMs, you can allow access to the specific storage account URLs (Ex: cache1.blob.core.windows.net and cache2.blob.core.windows.net) instead of *.blob.core.windows.net
login.microsoftonline.com	Required for authorization and authentication to the Site Recovery service URLs.
*.hypervrecoverymanager.windowsazure.com	Required so that the Site Recovery service communication can occur from the VM.
*.servicebus.windows.net	Required so that the Site Recovery monitoring and diagnostics data can be written from the VM.

Outbound connectivity for IP address ranges

If you are using an NSG to control outbound connectivity, these service tags need to be allowed.

- All IP address ranges that correspond to the storage accounts in source region

- Create a [Storage service tag](#) based NSG rule for the source region.
- Allow these addresses so that data can be written to the cache storage account, from the VM.
- Create a [Azure Active Directory \(AAD\) service tag](#) based NSG rule for allowing access to all IP addresses corresponding to AAD
- Create an EventsHub service tag based NSG rule for the target region, allowing access to Site Recovery monitoring.
- Create an AzureSiteRecovery service tag based NSG rule for allowing access to Site Recovery service in any region.
- We recommend that you create the required NSG rules on a test NSG, and verify that there are no problems before you create the rules on a production NSG.

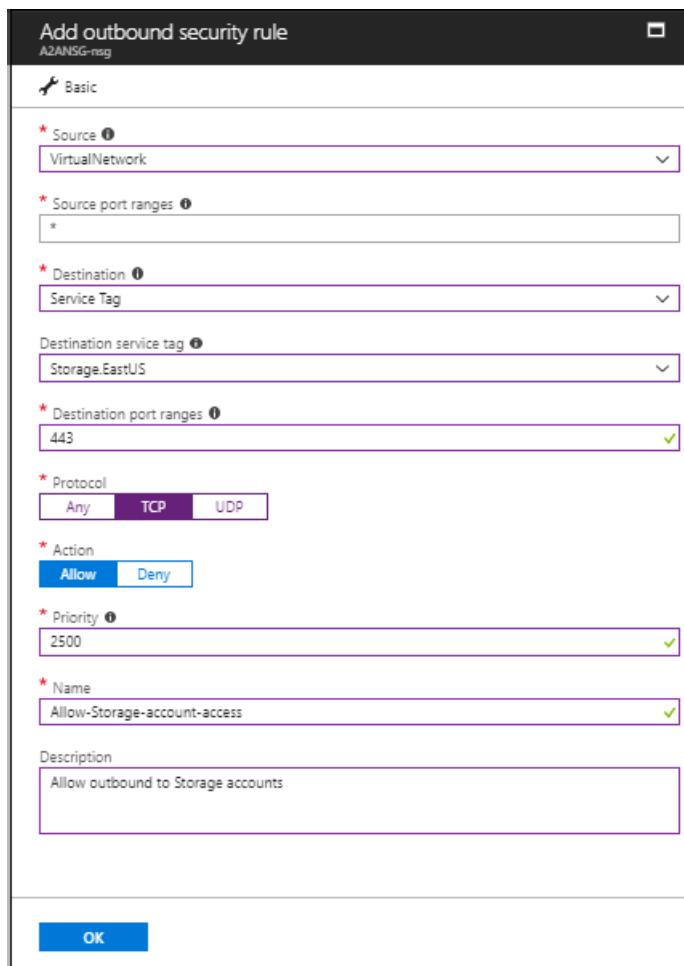
Example NSG configuration

This example shows how to configure NSG rules for a VM to replicate.

- If you're using NSG rules to control outbound connectivity, use "Allow HTTPS outbound" rules to port:443 for all the required IP address ranges.
- The example presumes that the VM source location is "East US" and the target location is "Central US".

NSG rules - East US

1. Create an outbound HTTPS (443) security rule for "Storage.EastUS" on the NSG as shown in the screenshot below.



2. Create an outbound HTTPS (443) security rule for "AzureActiveDirectory" on the NSG as shown in the screenshot below.

The screenshot shows the 'Add outbound security rule' dialog box. The configuration is as follows:

- Source:** VirtualNetwork
- Source port ranges:** *
- Destination:** Service Tag
- Destination service tag:** AzureActiveDirectory
- Destination port ranges:** 443
- Protocol:** TCP (selected)
- Action:** Allow (selected)
- Priority:** 2600
- Name:** Allow-Azure-Active-Directory
- Description:** Allow outbound to Azure Active Directory

Add

- Similar to above security rules, create outbound HTTPS (443) security rule for "EventHub.CentralUS" on the NSG that correspond to the target location. This allows access to Site Recovery monitoring.
- Create an outbound HTTPS (443) security rule for "AzureSiteRecovery" on the NSG. This allows access to Site Recovery Service in any region.

NSG rules - Central US

These rules are required so that replication can be enabled from the target region to the source region post-failover:

- Create an outbound HTTPS (443) security rule for "Storage.CentralUS" on the NSG.
- Create an outbound HTTPS (443) security rule for "AzureActiveDirectory" on the NSG.
- Similar to above security rules, create outbound HTTPS (443) security rule for "EventHub.EastUS" on the NSG that correspond to the source location. This allows access to Site Recovery monitoring.
- Create an outbound HTTPS (443) security rule for "AzureSiteRecovery" on the NSG. This allows access to Site Recovery Service in any region.

Network virtual appliance configuration

If you are using network virtual appliances (NVAs) to control outbound network traffic from VMs, the appliance might get throttled if all the replication traffic passes through the NVA. We recommend creating a network service endpoint in your virtual network for "Storage" so that the replication traffic does not go to the NVA.

Create network service endpoint for Storage

You can create a network service endpoint in your virtual network for "Storage" so that the replication traffic does not leave Azure boundary.

- Select your Azure virtual network and click on 'Service endpoints'

- Click 'Add' and 'Add service endpoints' tab opens
- Select 'Microsoft.Storage' under 'Service' and the required subnets under 'Subnets' field and click 'Add'

NOTE

Do not restrict virtual network access to your storage accounts used for ASR. You should allow access from 'All networks'

Forced tunneling

You can override Azure's default system route for the 0.0.0.0/0 address prefix with a [custom route](#) and divert VM traffic to an on-premises network virtual appliance (NVA), but this configuration is not recommended for Site Recovery replication. If you're using custom routes, you should [create a virtual network service endpoint](#) in your virtual network for "Storage" so that the replication traffic does not leave the Azure boundary.

Next steps

- Start protecting your workloads by [replicating Azure virtual machines](#).
- Learn more about [IP address retention](#) for Azure virtual machine failover.
- Learn more about disaster recovery of [Azure virtual machines with ExpressRoute](#).

Customize networking configurations of the target Azure VM

1/21/2020 • 3 minutes to read • [Edit Online](#)

This article provides guidance on customizing networking configurations on the target Azure virtual machine (VM) when you're replicating and recovering Azure VMs from one region to another, using [Azure Site Recovery](#).

Before you start

Learn how Site Recovery provides disaster recovery for [this scenario](#).

Supported networking resources

You can provide the following key resource configurations for the failover VM while replicating Azure VMs:

- [Internal load balancer](#)
- [Public IP](#)
- [Network security group](#) both for the subnet and for the NIC

Prerequisites

- Ensure that you plan your recovery side configurations in advance.
- Create the networking resources in advance. Provide it as an input so that Azure Site Recovery service can honor these settings and ensure that the failover VM adheres to these settings.

Customize failover and test failover networking configurations

1. Go to [Replicated Items](#).
2. Select the desired Azure VM.
3. Select **Compute and Network** and select **Edit**. Notice that the NIC configuration settings include the corresponding resources at the source.

The screenshot shows the Azure portal interface with the title '- Compute and Network' at the top. On the left, there's a sidebar with 'Replicated items' at the top, followed by 'Search (Ctrl+J)' and a 'Edit' button. Below these are sections for 'Overview', 'General', 'Properties', and 'Compute and Network' (which is highlighted in blue). At the bottom of the sidebar are 'Disks' and other collapsed sections. The main content area has a header 'Network properties' with columns for 'Properties', 'Source network', 'Test failover network', and 'Target network'. Under 'Properties', 'Virtual network' is set to 'maygrvnet956'. Under 'Source network', 'maygrvnet956' is listed. Under 'Test failover network', 'maygrvnet956-asr' is listed. Under 'Target network', 'maygrvnet956-asr' is listed. Below this, under 'Network interfaces', there's a list for 'maygvm140'. It shows a table with columns for 'Properties', 'Source settings', 'Test failover settings', and 'Target settings'. The table rows are: Name (maygvm140), Subnet (default), Private IP address (172.21.6.4 (Dynamic)), Accelerated Networking (Disabled), Public IP (maygvm1-ip), Load balancer (maygvm1-lb), and Network security group (maygvm1-nsg). The 'Source settings' column lists the source values for each property. The 'Test failover settings' and 'Target settings' columns show the current settings for the failover and target environments respectively.

4. Select a test failover virtual network. You can choose to leave it blank and select one at the time of test failover.
5. Failover network is Select **Edit** near the NIC you want to configure. In the next blade that opens, select the

corresponding pre-created resources in the test failover and failover location.

Properties	Source settings	Test failover settings	Failover settings
Name	maygvm140		
▼ Subnet	default	default (172.21.6.0/24)	default (172.21.6.0/24)
Network security group	rg-cleanupservice-nsg10	None	None
Private IP address	172.21.6.4 (Dynamic)	Dynamic	Dynamic
Accelerated Networking	Disabled	Disabled	Disabled
Public IP	maygvm1-ip	testingPIPFTFO	None
▼ Load balancer	maygvm1-lb	None	None
Backend pool	1 Backend pool(s)	Choose the Backend pool	Choose the Backend pool
Network security group	maygvm1-nsg	None	None

6. Select **OK**.

Site Recovery will now honor these settings and ensure that the VM on failover is connected to the selected resource via the corresponding NIC.

When you trigger the test failover via Recovery Plan, it will always ask the Azure virtual network. This virtual network will be used for test failover for the machines that did not have test failover settings pre-configured.

Troubleshooting

Unable to view or select a resource

If you can't select or view a networking resource, go through the following checks and conditions:

- The target field for a networking resource is enabled only if the source VM had a corresponding input. This is based on the principle that for a disaster recovery scenario, you would want either the exact or a scaled-down version of your source.
- For each networking resource, some filters are applied in the drop-down list to ensure that the failover VM can attach itself to the resource selected and the failover reliability is maintained. These filters are based on the same networking conditions that would have been verified when you configured the source VM.

Internal load balancer validations:

- The Subscription and Region of the load balancer and the target VM should be the same.
- The virtual network associated with the internal load balancer and that of the target VM should be the same.
- The target VM's public IP SKU and the internal load balancer's SKU should be the same.
- If the target VM is configured to be placed in an availability zone, then check if the load balancer is zone redundant or part of any availability zone. (Basic SKU load balancers don't support zones and won't be shown in the drop-down list in this case.)
- Ensure that the internal load balancer has a pre-created back-end pool and front-end configuration.

Public IP address:

- The Subscription and Region of the public IP and the target VM should be the same.
- The target VM's public IP SKU and the internal load balancer's SKU should be the same.

Network security group:

- The Subscription and Region of the network security group and the target VM should be the same.

WARNING

If the target VM is associated with an availability set, then you need to associate the public IP and internal load balancer of the same SKU with that of the other VM's public IP and internal load balancer in the availability set. If you don't, failover might not succeed.

Set up network mapping and IP addressing for VNets

11/12/2019 • 4 minutes to read • [Edit Online](#)

This article describes how to map two instances of Azure virtual networks (VNets) located in different Azure regions, and how to set up IP addressing between networks. Network mapping provides a default behavior for target network selection based on source network at the time of enabling replication.

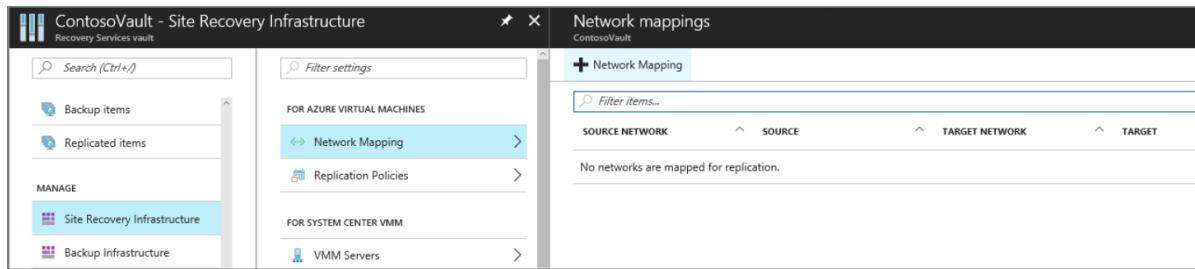
Prerequisites

Before you map networks, you should have [Azure VNets](#) in the source and target Azure regions.

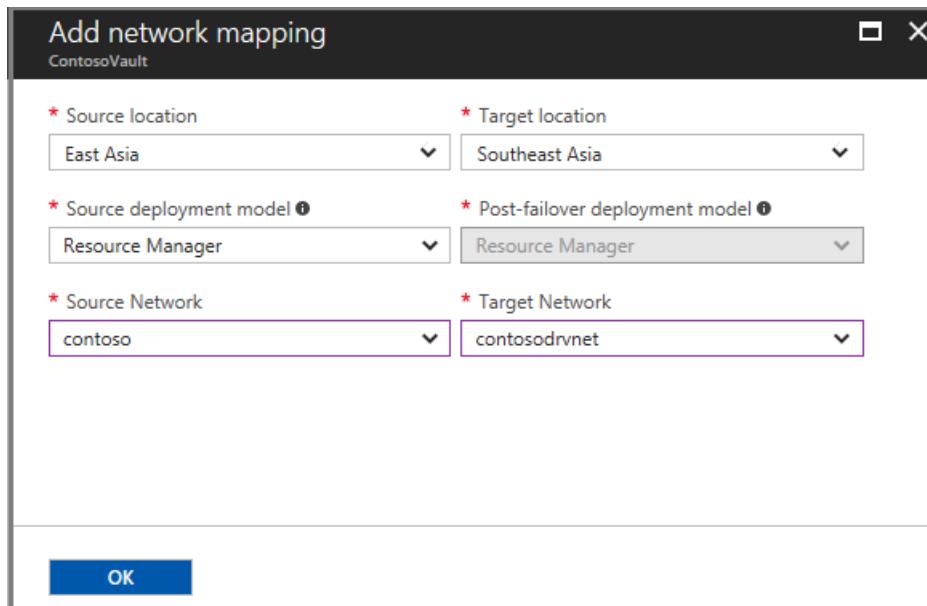
Set up network mapping manually (Optional)

Map networks as follows:

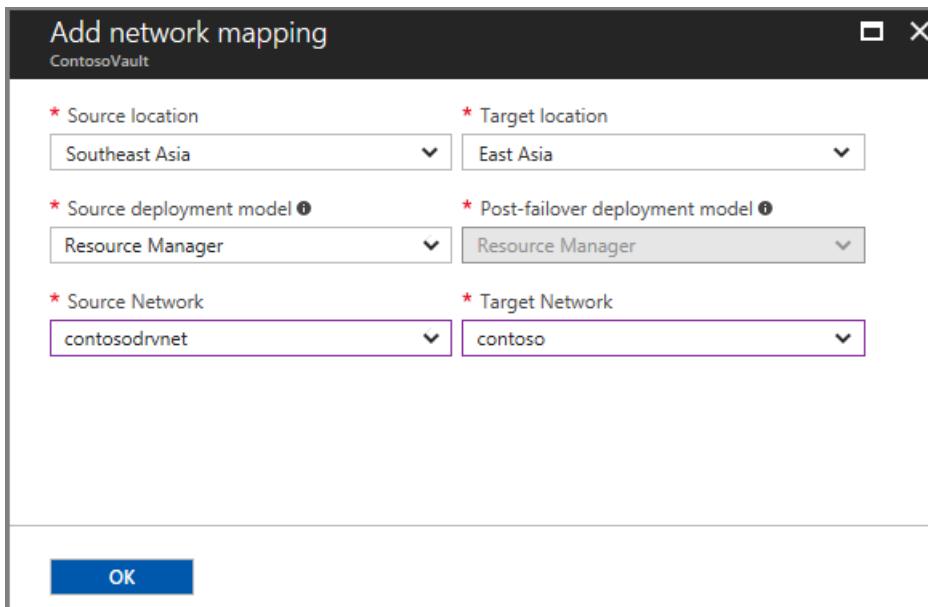
1. In **Site Recovery Infrastructure**, click **+Network Mapping**.



2. In **Add network mapping**, select the source and target locations. In our example, the source VM is running in the East Asia region, and replicates to the Southeast Asia region.



3. Now create a network mapping in the opposite direction. In our example, the source will now be Southeast Asia, and the target will be East Asia.



Map networks when you enable replication

If you haven't prepared network mapping before you configure disaster recovery for Azure VMs, you can specify a target network when you [set up and enable replication](#). When you do this the following happens:

- Based on the target you select, Site Recovery automatically creates network mappings from the source to target region, and from the target to source region.
- By default, Site Recovery creates a network in the target region that's identical to the source network. Site Recovery adds **-asr** as a suffix to the name of the source network. You can customize the target network.
- If network mapping has already occurred for a source network, the mapped target network will always be the default at the time of enabling replications for more VMs. You can choose to change the target virtual network by choosing other available options from the dropdown.
- To change the default target virtual network for new replications, you need to modify the existing network mapping.
- If you wish to modify a network mapping from region A to region B, ensure that you first delete the network mapping from region B to region A. After reverse mapping deletion, modify the network mapping from region A to region B and then create the relevant reverse mapping.

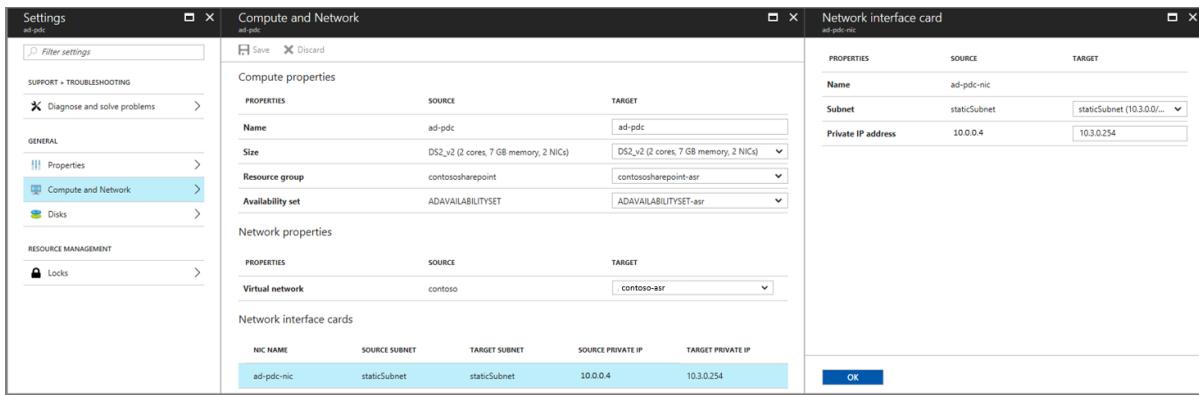
NOTE

- Modifying the network mapping only changes the defaults for new VM replications. It does not impact the target virtual network selections for existing replications.
- If you wish to modify the target network for an existing replication, go to Compute and Network Settings of the replicated item.

Specify a subnet

The subnet of the target VM is selected based on the name of the subnet of the source VM.

- If a subnet with the same name as the source VM subnet is available in the target network, that subnet is set for the target VM.
- If a subnet with the same name doesn't exist in the target network, the first subnet in the alphabetical order is set as the target subnet.
- You can modify the target subnet in the **Compute and Network** settings for the VM.



Set up IP addressing for target VMs

The IP address for each NIC on a target virtual machine is configured as follows:

- DHCP:** If the NIC of the source VM uses DHCP, the NIC of the target VM is also set to use DHCP.
- Static IP address:** If the NIC of the source VM uses static IP addressing, the target VM NIC will also use a static IP address.

IP address assignment during failover

SOURCE AND TARGET SUBNETS	DETAILS
Same address space	<p>IP address of the source VM NIC is set as the target VM NIC IP address.</p> <p>If the address isn't available, the next available IP address is set as the target.</p>
Different address space	The next available IP address in the target subnet is set as the target VM NIC address.

IP address assignment during test failover

TARGET NETWORK	DETAILS
Target network is the failover VNet	<ul style="list-style-type: none"> - Target IP address will be static with the same IP address. - If the same IP address is already assigned, then the IP address is the next one available at the end of the subnet range. For example: If the source IP address is 10.0.0.19 and failover network uses range 10.0.0.0/24, then the next IP address assigned to the target VM is 10.0.0.254.
Target network isn't the failover VNet	<ul style="list-style-type: none"> - Target IP address will be static with the same IP address. - If the same IP address is already assigned, then the IP address is the next one available at the end of the subnet range. <p>For example: If the source static IP address is 10.0.0.19 and failover is on a network that isn't the failover network, with the range 10.0.0.0/24, then the target static IP address will be 10.0.0.19 if available, and otherwise it will be 10.0.0.254.</p>

- The failover VNet is the target network that you select when you set up disaster recovery.

- We recommend that you always use a non-production network for test failover.
- You can modify the target IP address in the **Compute and Network** settings of the VM.

Next steps

- Review [networking guidance](#) for Azure VM disaster recovery.
- [Learn more](#) about retaining IP addresses after failover.

Retain IP addresses during failover

11/14/2019 • 7 minutes to read • [Edit Online](#)

Azure Site Recovery enables disaster recovery for Azure VMs by replicating VMs to another Azure region, failing over if an outage occurs, and failing back to the primary region when things are back to normal.

During failover, you might want to keep the IP addressing in the target region identical to the source region:

- By default, when you enable disaster recovery for Azure VMs, Site Recovery creates target resources based on source resource settings. For Azure VMs configured with static IP addresses, Site Recovery tries to provision the same IP address for the target VM, if it's not in use. For a full explanation of how Site Recovery handles addressing, [review this article](#).
- For simple applications, the default configuration is sufficient. For more complex apps, you might need to provision additional resource to make sure that connectivity works as expected after failover.

This article provides some examples for retaining IP addresses in more complex example scenarios. The examples include:

- Failover for a company with all resources running in Azure
- Failover for a company with a hybrid deployment, and resources running both on-premises and in Azure

Resources in Azure: full failover

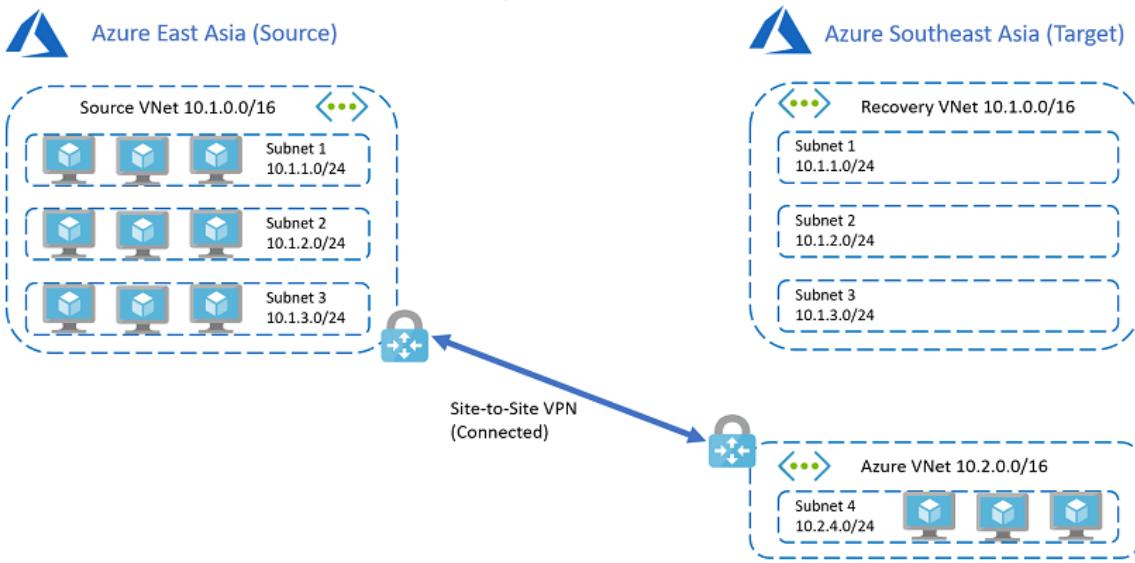
Company A has all its apps running in Azure.

Before failover

Here's the architecture before failover.

- Company A has identical networks and subnets in source and target Azure regions.
- To reduce recovery time objective (RTO), company uses replica nodes for SQL Server Always On, domain controllers, etc. These replica nodes are in a different VNet in the target region, so that they can establish VPN site-to-site connectivity between the source and target regions. This isn't possible if the same IP address space is used in the source and target.
- Before failover, the network architecture is as follows:
 - Primary region is Azure East Asia
 - East Asia has a VNet (**Source VNet**) with address space 10.1.0.0/16.
 - East Asia has workloads split across three subnets in the VNet:
 - **Subnet 1**: 10.1.1.0/24
 - **Subnet 2**: 10.1.2.0/24
 - **Subnet 3**: 10.1.3.0/24
 - Secondary (target) region is Azure Southeast Asia
 - Southeast Asia has a recovery VNet (**Recovery VNet**) identical to **Source VNet**.
 - Southeast Asia has an additional VNet (**Azure VNet**) with address space 10.2.0.0/16.
 - **Azure VNet** contains a subnet (**Subnet 4**) with address space 10.2.4.0/24.
 - Replica nodes for SQL Server Always On, domain controller etc. are located in **Subnet 4**.
 - **Source VNet** and **Azure VNet** are connected with a VPN site-to-site connection.
 - **Recovery VNet** is not connected with any other virtual network.
 - **Company A** assigns/verifies target IP addresses for replicated items. The target IP is the same as source IP for each VM.

Azure to Azure connectivity – Before failover

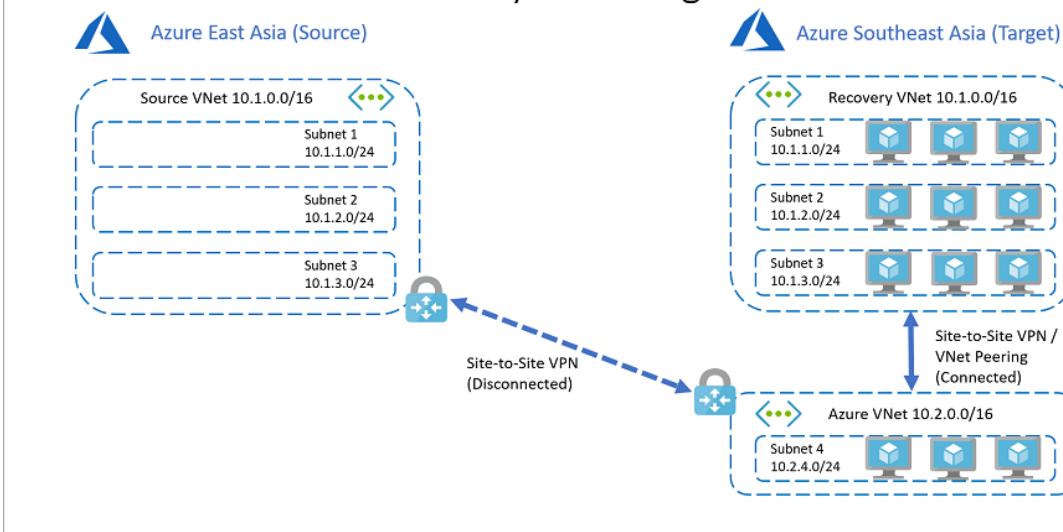


After failover

If a source regional outage occurs, Company A can fail over all its resources to the target region.

- With target IP addresses already in place before the failover, Company A can orchestrate failover and automatically establish connections after failover between **Recovery VNet** and **Azure VNet**. This is illustrated in the following diagram..
- Depending on app requirements, connections between the two VNets (**Recovery VNet** and **Azure VNet**) in the target region can be established before, during (as an intermediate step) or after the failover.
 - The company can use [recovery plans](#) to specify when connections will be established.
 - They can connect between the VNets using VNet peering or site-to-site VPN.
 - VNet peering doesn't use a VPN gateway and has different constraints.
 - VNet peering [pricing](#) is calculated differently than VNet-to-VNet VPN Gateway [pricing](#). For failovers, we generally advise to use the same connectivity method as source networks, including the connection type, to minimize unpredictable network incidents.

Azure to Azure connectivity – Full region failover



Resources in Azure: isolated app failover

You might need to fail over at the app level. For example, to fail over a specific app or app tier located in a dedicated subnet.

- In this scenario, although you can retain IP addressing, it's not generally advisable since it increases the chance of connectivity inconsistencies. You'll also lose subnet connectivity to other subnets within the same Azure VNet.
- A better way to do subnet-level app failover is to use different target IP addresses for failover (if you need connectivity to other subnets on source VNet), or to isolate each app in its own dedicated VNet in the source region. With the latter approach you can establish connectivity between networks in the source region, and emulate the same behavior when you fail over to the target region.

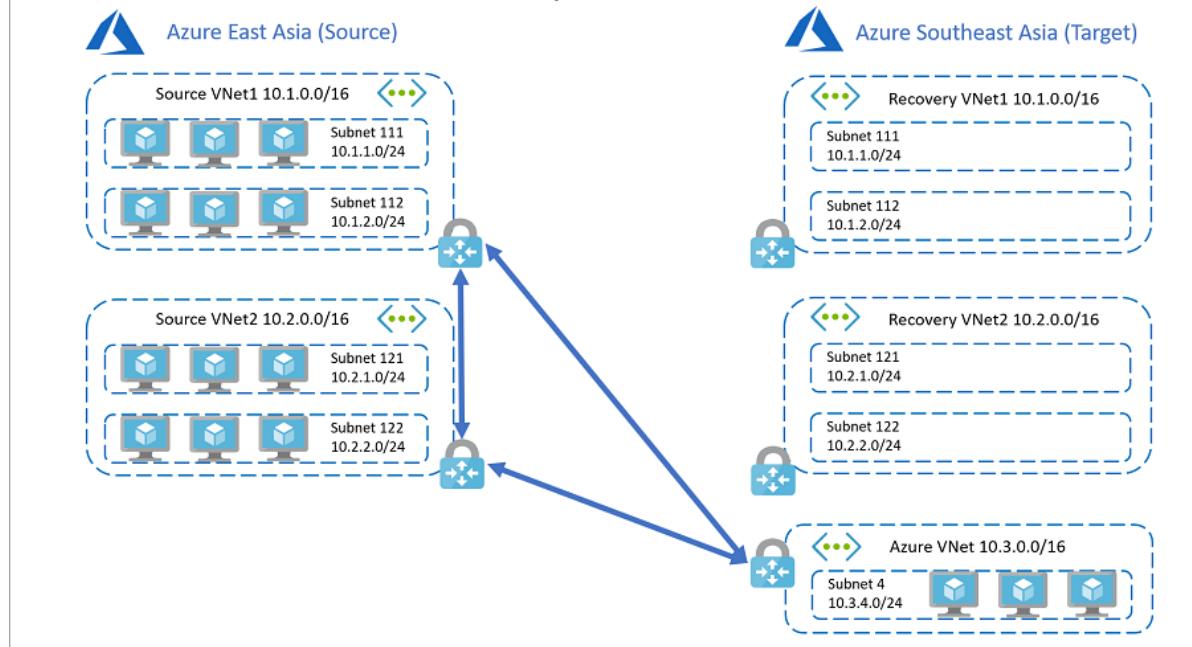
In this example, Company A places apps in the source region in dedicated VNets, and establishes connectivity between those VNets. With this design, they can perform isolated app failover, and retain the source private IP addresses in the target network.

Before failover

Before failover, the architecture is as follows:

- Application VMs are hosted in the primary Azure East Asia region:
 - **App1** VMs are located in VNet **Source VNet 1**: 10.1.0.0/16.
 - **App2** VMs are located in VNet **Source VNet 2**: 10.2.0.0/16.
 - **Source VNet 1** has two subnets.
 - **Source VNet 2** has two subnets.
- Secondary (target) region is Azure Southeast Asia - Southeast Asia has a recovery VNets (**Recovery VNet 1** and **Recovery VNet 2**) that are identical to **Source VNet 1** and **Source VNet 2**. - **Recovery VNet 1** and **Recovery VNet 2** each have two subnets that match the subnets in **Source VNet 1** and **Source VNet 2** - Southeast Asia has an additional VNet (**Azure VNet**) with address space 10.3.0.0/16. - **Azure VNet** contains a subnet (**Subnet 4**) with address space 10.3.4.0/24. - Replica nodes for SQL Server Always On, domain controller etc. are located in **Subnet 4**.
- There are a number of site-to-site VPN connections:
 - **Source VNet 1** and **Azure VNet**
 - **Source VNet 2** and **Azure VNet**
 - **Source VNet 1** and **Source VNet 2** are connected with VPN site-to-site
- **Recovery VNet 1** and **Recovery VNet 2** aren't connected to any other VNets.
- **Company A** configures VPN gateways on **Recovery VNet 1** and **Recovery VNet 2**, to reduce RTO.
- **Recovery VNet1** and **Recovery VNet2** are not connected with any other virtual network.
- To reduce recovery time objective (RTO), VPN gateways are configured on **Recovery VNet1** and **Recovery VNet2** prior to failover.

Azure to Azure connectivity – Before failover

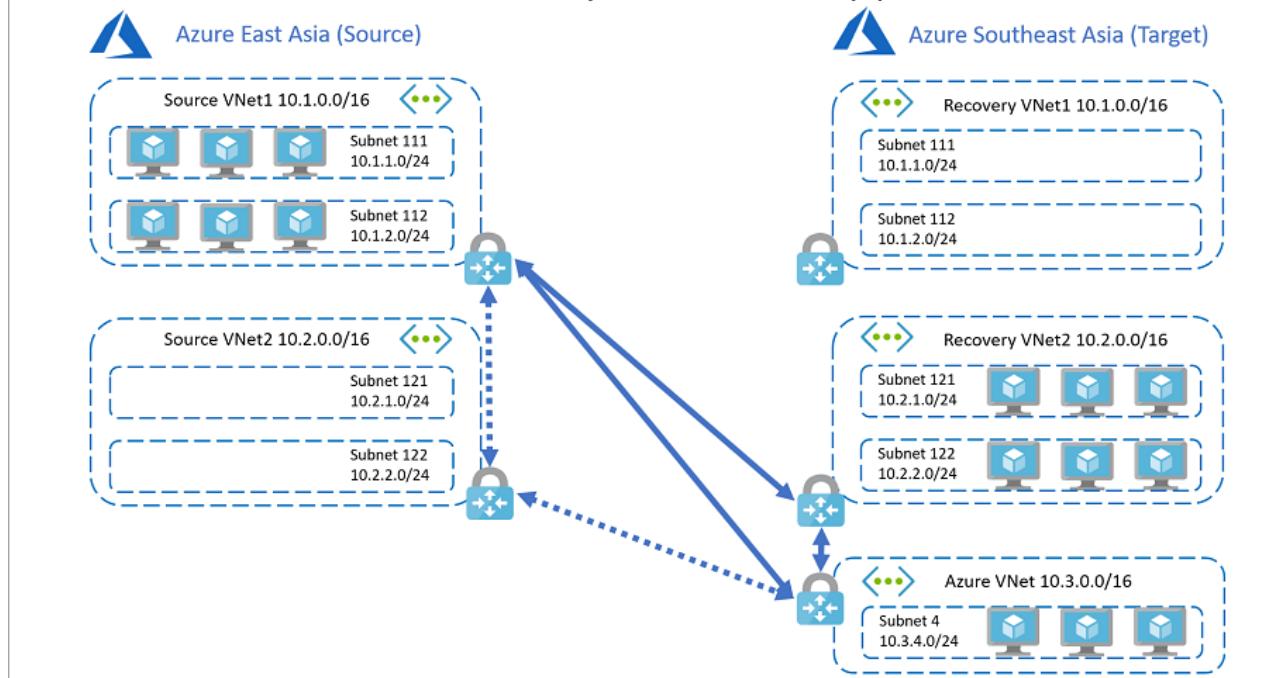


After failover

In the event of an outage or issue that affects a single app (in **Source VNet 2 in our example), Company A can recover the affected app as follows:

- Disconnect VPN connections between **Source VNet1** and **Source VNet2**, and between **Source VNet2** and **Azure VNet**.
- Establish VPN connections between **Source VNet1** and **Recovery VNet2**, and between **Recovery VNet2** and **Azure VNet**.
- Fail over VMs in **Source VNet2** to **Recovery VNet2**.

Azure to Azure connectivity – Isolated application failover



- This example can be expanded to include more applications and network connections. The recommendation is to follow a like-like connection model, as far as possible, when failing over from source to target.
- VPN Gateways use public IP addresses and gateway hops to establish connections. If you don't want to use public IP addresses, or you want to avoid extra hops, you can use [Azure VNet peering](#) to peer virtual networks

across [supported Azure regions](#).

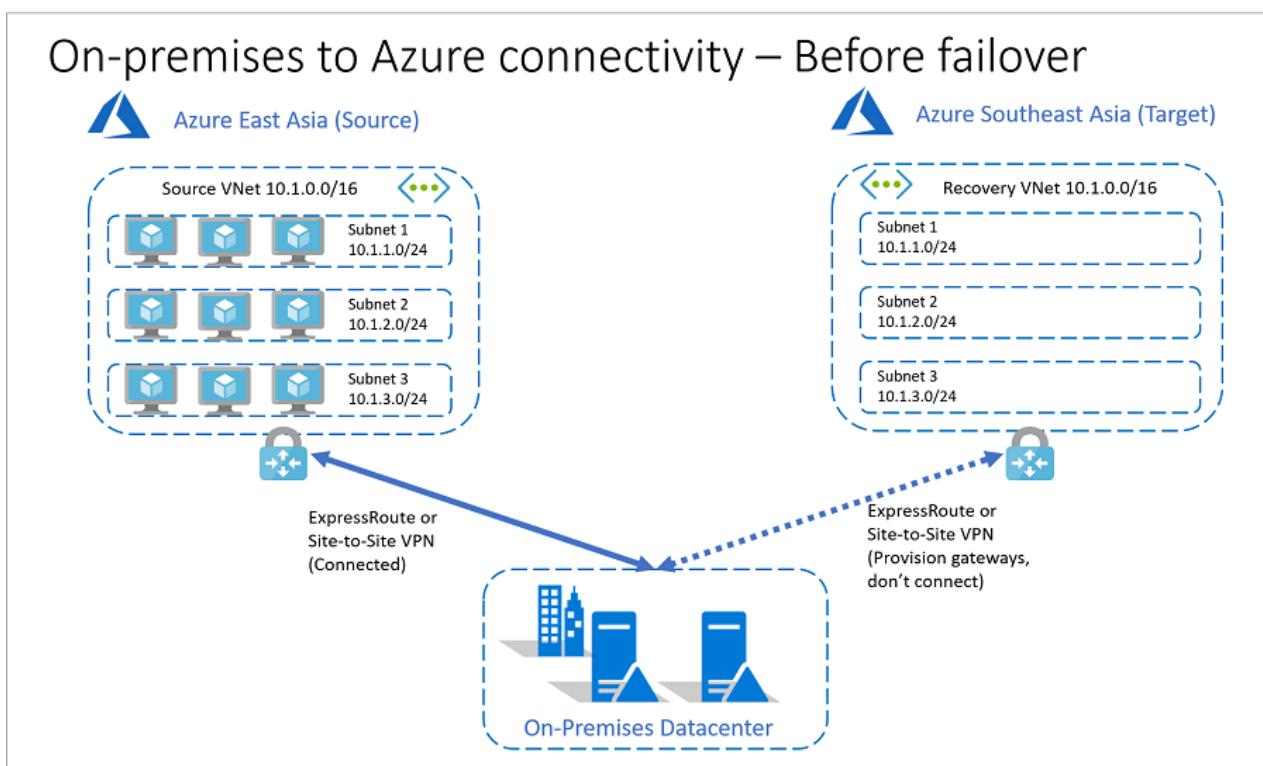
Hybrid resources: full failover

In this scenario, **Company B** runs a hybrid business, with part of the application infrastructure running on Azure, and the remainder running on-premises.

Before failover

Here's what the network architecture looks like before failover.

- Application VMs are hosted in Azure East Asia.
- East Asia has a VNet (**Source VNet**) with address space 10.1.0.0/16.
 - East Asia has workloads split across three subnets in **Source VNet**:
 - **Subnet 1**: 10.1.1.0/24
 - **Subnet 2**: 10.1.2.0/24
 - **Subnet 3**: 10.1.3.0/24, utilizing an Azure virtual network with address space 10.1.0.0/16. This virtual network is named **Source VNet**
 - The secondary (target) region is Azure Southeast Asia:
 - Southeast Asia has a recovery VNet (**Recovery VNet**) identical to **Source VNet**.
- VMs in East Asia are connected to an on-premises datacenter with Azure ExpressRoute or site-to-site VPN.
- To reduce RTO, Company B provisions gateways on Recovery VNet in Azure Southeast Asia prior to failover.
- Company B assigns/verifies target IP addresses for replicated VMs. The target IP address is the same as source IP address for each VM.

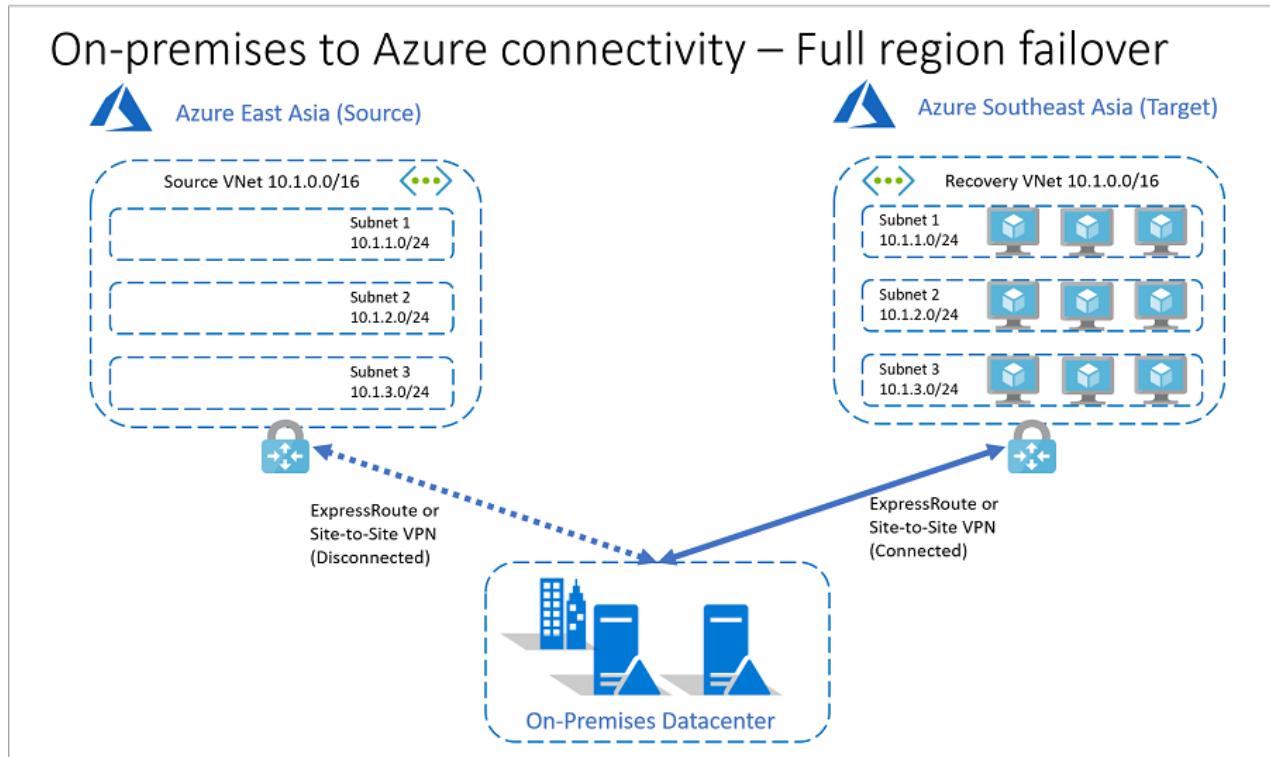


After failover

If a source regional outage occurs, Company B can fail over all its resources to the target region.

- With target IP addresses already in place before the failover, Company B can orchestrate failover and automatically establish connections after failover between **Recovery VNet** and **Azure VNet**.
- Depending on app requirements, connections between the two VNets (**Recovery VNet** and **Azure VNet**) in the target region can be established before, during (as an intermediate step) or after the failover. The company can use [recovery plans](#) to specify when connections will be established.

- The original connection between Azure East Asia and the on-premises datacenter should be disconnected before establishing the connection between Azure Southeast Asia and on-premises datacenter.
- The on-premises routing is reconfigured to point to the target region and gateways post failover.



Hybrid resources: isolated app failover

Company B can't fail over isolated apps at the subnet level. This is because the address space on source and recovery VNets is the same, and the original source to on-premises connection is active.

- For app resiliency Company B will need to place each app in its own dedicated Azure VNet.
- With each app in a separate VNet, Company B can fail over isolated apps, and route source connections to the target region.

Next steps

Learn about [recovery plans](#).

Integrate ExpressRoute with disaster recovery for Azure VMs

11/12/2019 • 9 minutes to read • [Edit Online](#)

This article describes how to integrate Azure ExpressRoute with [Azure Site Recovery](#), when you set up disaster recovery for Azure VMs to a secondary Azure region.

Site Recovery enables disaster recovery of Azure VMs by replicating Azure VM data to Azure.

- If Azure VMs use [Azure managed disks](#), VM data is replicated to an replicated managed disk in the secondary region.
- If Azure VMs don't use managed disks, VM data is replicated to an Azure storage account.
- Replication endpoints are public, but replication traffic for Azure VMs doesn't cross the internet.

ExpressRoute enables you to extend on-premises networks into the Microsoft Azure cloud over a private connection, facilitated by a connectivity provider. If you have ExpressRoute configured, it integrates with Site Recovery as follows:

- **During replication between Azure regions:** Replication traffic for Azure VM disaster recovery is within Azure only, and ExpressRoute isn't needed or used for replication. However, if you're connecting from an on-premises site to the Azure VMs in the primary Azure site, there are a number of issues to be aware of when you're setting up disaster recovery for those Azure VMs.
- **Failover between Azure regions:** When outages occur, you fail over Azure VMs from the primary to secondary Azure region. After failing over to a secondary region, there are a number of steps to take in order to access the Azure VMs in the secondary region using ExpressRoute.

Before you begin

Before you begin, make sure you understand the following concepts:

- ExpressRoute circuits
- ExpressRoute routing domains
- ExpressRoute locations.
- Azure VM [replication architecture](#)
- How to [set up replication](#) for Azure VMs.
- How to [fail over](#) Azure VMs.

General recommendations

For best practice, and to ensure efficient Recovery Time Objectives (RTOs) for disaster recovery, we recommend you do the following when you set up Site Recovery to integrate with ExpressRoute:

- Provision networking components before failover to a secondary region:
 - When you enable replication for Azure VMs, Site Recovery can automatically deploy networking resources such as networks, subnets, and gateways in the target Azure region, based on source network settings.
 - Site Recovery can't automatically set up networking resources such as VNet gateways.
 - We recommend you provision these additional networking resources before failover. A small downtime is associated with this deployment, and it can impact the overall recovery time, if you didn't account for

it during deployment planning.

- Run regular disaster recovery drills:
 - A drill validates your replication strategy without data loss or downtime, and doesn't affect your production environment. It helps avoid last-minute configuration issues that can adversely impact RTO.
 - When you run a test failover for the drill, we recommend that you use a separate Azure VM network, instead of the default network that's set up when you enable replication.
- Use different IP address spaces if you have a single ExpressRoute circuit.
 - We recommend that you use a different IP address space for the target virtual network. This avoids issues when establishing connections during regional outages.
 - If you can't use a separate address space, be sure to run the disaster recovery drill test failover on a separate test network with different IP addresses. You can't connect two VNets with overlapping IP address space to the same ExpressRoute circuit.

Replicate Azure VMs when using ExpressRoute

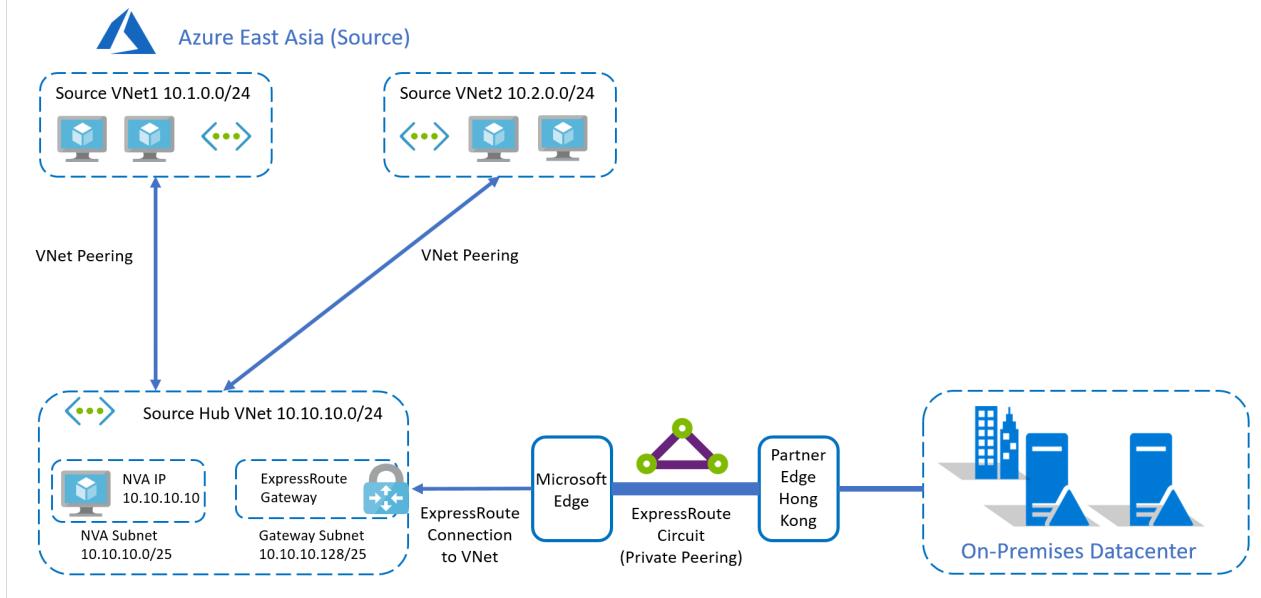
If you want to set up replication for Azure VMs in a primary site, and you're connecting to these VMs from your on-premises site over ExpressRoute, here's what you need to do:

1. [Enable replication](#) for each Azure VM.
2. Optionally let Site Recovery set up networking:
 - When you configure and enable replication, Site Recovery sets up networks, subnets, and gateway subnets in the target Azure region, to match those in the source region. Site Recovery also maps between the source and target virtual networks.
 - If you don't want Site Recovery to do this automatically, create the target-side network resources before you enable replication.
3. Create other networking elements:
 - Site Recovery doesn't create route tables, VNet gateways, VNet gateway connections, VNet peering, or other networking resources and connections in the secondary region.
 - You need to create these additional networking elements in the secondary region, any time before running a failover from the primary region.
 - You can use [recovery plans](#) and automation scripts to set up and connect these networking resources.
4. If you have a network virtual appliance (NVA) deployed to control the flow of network traffic, note that:
 - Azure's default system route for Azure VM replication is 0.0.0.0/0.
 - Typically, NVA deployments also define a default route (0.0.0.0/0) that forces outbound Internet traffic to flow through the NVA. The default route is used when no other specific route configuration can be found.
 - If this is the case, the NVA might be overloaded if all replication traffic passes through the NVA.
 - The same limitation also applies when using default routes for routing all Azure VM traffic to on-premises deployments.
 - In this scenario, we recommend that you [create a network service endpoint](#) in your virtual network for the Microsoft.Storage service, so that the replication traffic doesn't leave Azure boundary.

Replication example

Typically enterprise deployments have workloads split across multiple Azure VNets, with a central connectivity hub for external connectivity to the internet and to on-premises sites. A hub and spoke topology is typically used together with ExpressRoute.

On-premises to Azure connectivity – Before failover



- **Region.** Apps are deployed in the Azure East Asia region.
- **Spoke vNets.** Apps are deployed in two spoke vNets:
 - **Source vNet1:** 10.1.0.0/24.
 - **Source vNet2:** 10.2.0.0/24.
 - Each spoke virtual network is connected to **Hub vNet**.
- **Hub vNet.** There's a hub vNet **Source Hub vNet:** 10.10.10.0/24.
 - This hub vNet acts as the gatekeeper.
 - All communications across subnets go through this hub.
 - **Hub vNet subnets.** The hub vNet has two subnets:
 - **NVA subnet:** 10.10.10.0/25. This subnet contains an NVA (10.10.10.10).
 - **Gateway subnet:** 10.10.10.128/25. This subnet contains an ExpressRoute gateway connected to an ExpressRoute connection that routes to the on-premises site via a private peering routing domain.
- The on-premises datacenter has an ExpressRoute circuit connection through a partner edge in Hong Kong.
- All routing is controlled through Azure route tables (UDR).
- All outbound traffic between vNets, or to the on-premises datacenter is routed through the NVA.

Hub and spoke peering settings

Spoke to hub

DIRECTION	SETTING	STATE
Spoke to hub	Allow virtual network address	Enabled
Spoke to hub	Allow forwarded traffic	Enabled
Spoke to hub	Allow gateway transit	Disabled
Spoke to hub	Use remove gateways	Enabled

Configuration

Allow virtual network access [?](#)

Disabled **Enabled**

Allow forwarded traffic [?](#)

Allow gateway transit [?](#)

Use remote gateways [?](#)

Hub to spoke

DIRECTION	SETTING	STATE
Hub to spoke	Allow virtual network address	Enabled
Hub to spoke	Allow forwarded traffic	Enabled
Hub to spoke	Allow gateway transit	Enabled
Hub to spoke	Use remove gateways	Disabled

Configuration

Allow virtual network access [?](#)

Disabled **Enabled**

Allow forwarded traffic [?](#)

Allow gateway transit [?](#)

Use remote gateways [?](#)

Example steps

In our example, the following should happen when enabling replication for Azure VMs in the source network:

1. You [enable replication](#) for a VM.
2. Site Recovery will create replica vNets, subnets, and gateway subnets in the target region.
3. Site Recovery creates mappings between the source networks and the replica target networks it creates.
4. You manually create virtual network gateways, virtual network gateway connections, virtual network peering, or any other networking resources or connections.

Fail over Azure VMs when using ExpressRoute

After you fail Azure VMs over to the target Azure region using Site Recovery, you can access them using ExpressRoute [private peering](#).

- You need to connect ExpressRoute to the target vNet with a new connection. The existing ExpressRoute connection isn't automatically transferred.
- The way in which you set up your ExpressRoute connection to the target vNet depends on your ExpressRoute topology.

Access with two circuits

Two circuits with two peering locations

This configuration helps protect ExpressRoute circuits against regional disaster. If your primary peering location goes down, connections can continue from the other location.

- The circuit connected to the production environment is usually the primary. The secondary circuit typically has lower bandwidth, which can be increased if a disaster occurs.
- After failover, you can establish connections from the secondary ExpressRoute circuit to the target vNet. Alternatively, you can have connections set up and ready in case of disaster, to reduce overall recovery time.
- With simultaneous connections to both primary and target vNets, make sure that your on-premises routing only uses the secondary circuit and connection after failover.
- The source and target vNets can receive new IP addresses, or keep the same ones, after failover. In both cases, the secondary connections can be established prior to failover.

Two circuits with single peering location

This configuration helps protect against failure of the primary ExpressRoute circuit, but not if the single ExpressRoute peering location goes down, impacting both circuits.

- You can have simultaneous connections from the on-premises datacenter to source vNEt with the primary circuit, and to the target vNet with the secondary circuit.
- With simultaneous connections to primary and target, make sure that on-premises routing only uses the secondary circuit and connection after failover.
- You can't connect both circuits to the same vNet when circuits are created at the same peering location.

Access with a single circuit

In this configuration there's only one Expressroute circuit. Although the circuit has a redundant connection in case one goes down, a single route circuit will not provide resilience if your peering region goes down. Note that:

- You can replicate Azure VMs to any Azure region in the [same geographic location](#). If the target Azure region isn't in the same location as the source, you need to enable ExpressRoute Premium if you're using a single ExpressRoute circuit. Learn about [ExpressRoute locations](#) and [ExpressRoute pricing](#).
- You can't connect source and target vNets simultaneously to the circuit if the same IP address space is used on the target region. In this scenario:
 - Disconnect the source side connection, and then establish the target side connection. This connection change can be scripted as part of a Site Recovery recovery plan. Note that:
 - In a regional failure, if the primary region is inaccessible, the disconnect operation could fail. This could impact connection creation to the target region.
 - If you created the connection in the target region, and primary region recovers later, you might experience packet drops if two simultaneous connections attempt to connect to the same address space.
 - To prevent this, terminate the primary connection immediately.
 - After VM failback to the primary region, the primary connection can again be established, after you disconnect the secondary connection.
- If a different address spaces is used on the target vNet, you can simultaneously connect to the source and target vNets from the same ExpressRoute circuit.

Failover example

In our example, we're using the following topology:

- Two different ExpressRoute circuits in two different peering locations.
- Retain private IP addresses for the Azure VMs after failover.
- The target recovery region is Azure SouthEast Asia.
- A secondary ExpressRoute circuit connection is established through a partner edge in Singapore.

For a simple topology that uses a single ExpressRoute circuit, with same IP address after failover, [review this article](#).

Example steps

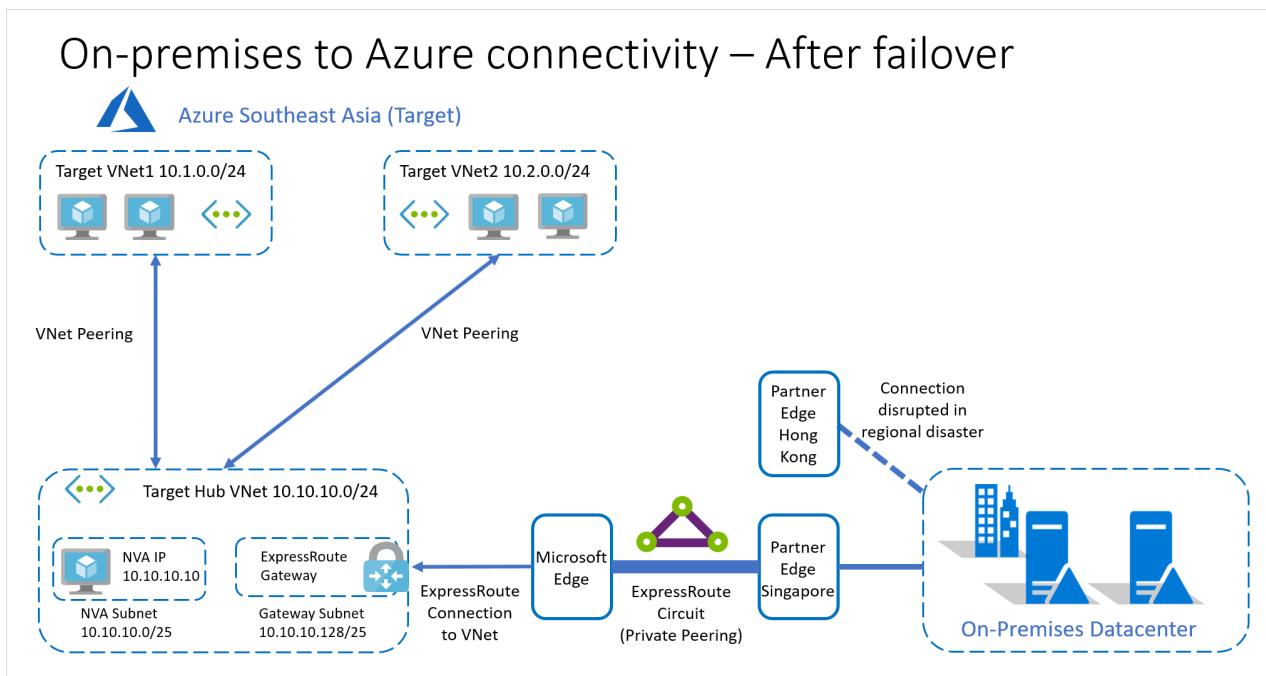
To automate recovery in this example, here's what you need to do:

1. Follow the steps to set up replication.
2. **Fail over the Azure VMs**, with these additional steps during or after the failover.
 - a. Create the Azure ExpressRoute Gateway in the target region hub VNet. This is needed to connect the target hub vNet to the ExpressRoute circuit.
 - b. Create the connection from the target hub vNet to the target ExpressRoute circuit.
 - c. Set up the VNet peerings between the target region's hub and spoke virtual networks. The peering properties on the target region will be the same as those on the source region.
 - d. Set up the UDRs in the hub VNet, and the two spoke VNets.
 - The properties of the target side UDRs are the same as those on the source side when using the same IP addresses.
 - With different target IP addresses, the UDRs should be modified accordingly.

The above steps can be scripted as part of a [recovery plan](#). Depending on the application connectivity and recovery time requirements, the above steps can also be completed prior to starting the failover.

After recovery

After recovering the VMs and completing connectivity, the recovery environment is as follows.



Next steps

Learn more about using [recovery plans](#) to automate app failover.

Replicate Azure VMs to another Azure region

1/14/2020 • 6 minutes to read • [Edit Online](#)

This article describes how to enable replication of Azure VMs, from one Azure region to another.

Before you start

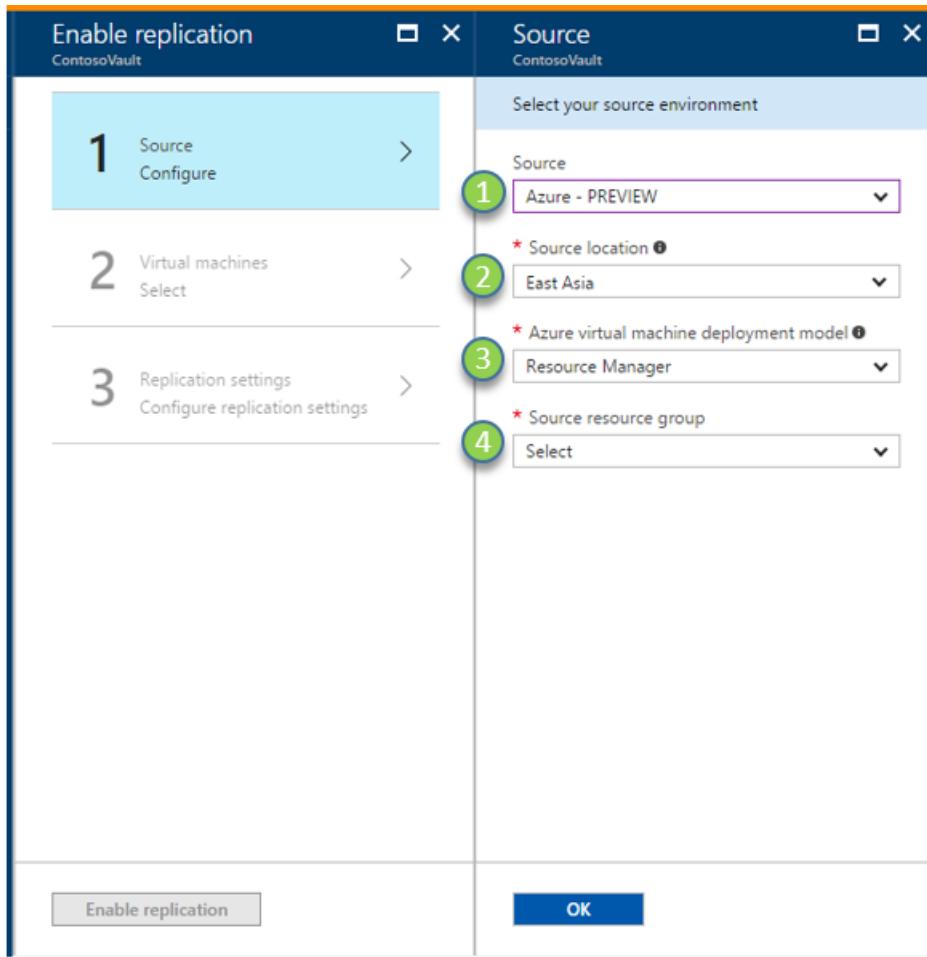
This article assumes that you've prepared for Site Recovery deployment, as described in the [Azure to Azure disaster recovery tutorial](#).

Prerequisites should be in place, and you should have created a Recovery Services vault.

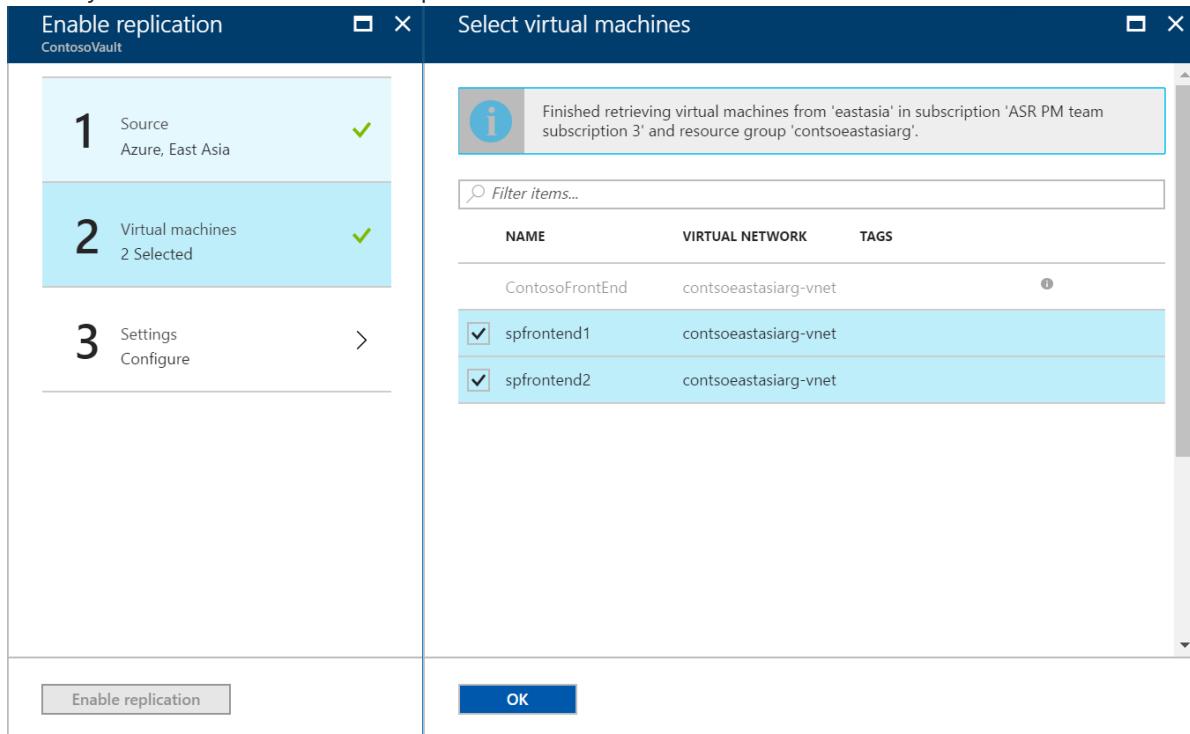
Enable replication

Enable replication. This procedure assumes that the primary Azure region is East Asia, and the secondary region is South East Asia.

1. In the vault, click **+Replicate**.
2. Note the following fields:
 - **Source:** The point of origin of the VMs, which in this case is **Azure**.
 - **Source location:** The Azure region from where you want to protect your VMs. For this illustration, the source location is 'East Asia'
 - **Deployment model:** Azure deployment model of the source machines.
 - **Source subscription:** The subscription to which your source VMs belong. This can be any subscription within the same Azure Active Directory tenant where your recovery services vault exists.
 - **Resource Group:** The resource group to which your source virtual machines belong. All the VMs under the selected resource group are listed for protection in the next step.



3. In **Virtual Machines > Select virtual machines**, click and select each VM that you want to replicate. You can only select machines for which replication can be enabled. Then click **OK**.



4. In **Settings**, you can optionally configure target site settings:

- **Target Location:** The location where your source virtual machine data will be replicated. Depending upon your selected machines location, Site Recovery will provide you the list of suitable target regions. We recommend that you keep the target location the same as the Recovery Services vault location.

- **Target subscription:** The target subscription used for disaster recovery. By default, the target subscription will be same as the source subscription.
- **Target resource group:** The resource group to which all your replicated virtual machines belong.
 - By default Site Recovery creates a new resource group in the target region with an "asr" suffix in the name.
 - If the resource group created by Site Recovery already exists, it is reused.
 - You can customize the resource group settings.
 - The location of the target resource group can be any Azure region, except the region in which the source VMs are hosted.
- **Target virtual network:** By default, Site Recovery creates a new virtual network in the target region with an "asr" suffix in the name. This is mapped to your source network, and used for any future protection. [Learn more](#) about network mapping.
- **Target storage accounts (source VM doesn't use managed disks):** By default, Site Recovery creates a new target storage account mimicking your source VM storage configuration. In case storage account already exists, it is reused.
- **Replica-managed disks (source VM uses managed disks):** Site Recovery creates new replica-managed disks in the target region to mirror the source VM's managed disks with the same storage type (Standard or premium) as the source VM's managed disk.
- **Cache Storage accounts:** Site Recovery needs extra storage account called cache storage in the source region. All the changes happening on the source VMs are tracked and sent to cache storage account before replicating those to the target location. This storage account should be Standard.
- **Target availability sets:** By default, Site Recovery creates a new availability set in the target region with the "asr" suffix in the name, for VMs that are part of an availability set in the source region. If the availability set created by Site Recovery already exists, it is reused.
- **Target availability zones:** By default, Site Recovery assigns the same zone number as the source region in target region if the target region supports availability zones.

If the target region does not support availability zones, the target VMs are configured as single instances by default. If required, you can configure such VMs to be part of availability sets in target region by clicking 'Customize'.

NOTE

You cannot change the availability type - single instance, availability set or availability zone, after you enable replication. You need to disable and enable replication to change the availability type.

- **Replication Policy:** It defines the settings for recovery point retention history and app consistent snapshot frequency. By default, Azure Site Recovery creates a new replication policy with default settings of '24 hours' for recovery point retention and '4 hours' for app consistent snapshot frequency.

The screenshot shows two overlapping windows. The left window, titled 'Enable replication' under 'ContosoVault', lists three steps: 1. Source (Azure, East Asia) with a green checkmark; 2. Virtual machines (2 Selected) with a green checkmark; and 3. Settings (Configure) with a blue background and a right-pointing arrow. The right window, titled 'Configure settings', details the target configuration. It includes fields for 'Target location' (Southeast Asia), 'Target resource group' (contsoeastasiarg-asr), 'Target virtual network' (contsoeastasiarg-vnet-asr), 'Cache storage accounts' (contsoeastasiarcacheasr, contosostorageecacheasr), 'Target storage accounts' (contsoeastasiardisksasr, contosostorageeastasasr), 'Target availability sets' (AVSETEASTASIA-asr), and a 'Replication Policy' section with a retention policy of 24 hours. Buttons at the bottom include 'Enable replication' and 'Create target resources'.

Enable replication for added disks

If you add disks to an Azure VM for which replication is enabled, the following occurs:

- Replication health for the VM shows a warning, and a note informs telling you that one or more disks are available for protection.
- If you enable protection for the added disks, the warning will disappear after the initial replication of the disk.
- If you choose not to enable replication for the disk, you can select to dismiss the warning.

The screenshot shows the Azure portal's 'Replicated items' blade for a VM named 'Contososdd'. The 'Overview' tab is selected. A prominent yellow warning message states: 'New disk attached to the VM. Your VM is partially protected. We recommend to protect disk. Click here to dismiss the warning.' Below this, the 'Essentials' section displays 'Health and status' (Replication Health: Warning, Status: Protected, RPO: 1 min [As on 4/29/2019, 3:02:09 PM]), 'Failover readiness' (Last successful Test Failover: Never performed successfully, Configuration issues: No issues), and a 'Latest recovery points' panel. The 'Errors(1)' section shows an error ID (153039) with a message: 'One or more disk(s) are available for add disks protection.' The 'Events - Last 72 hours(0)' section shows no events.

To enable replication for an added disk, do the following:

1. In the vault > **Replicated Items**, click the VM to which you added the disk.
2. Click **Disk**, and then select the data disk for which you want to enable replication (these disks have a **Not protected** status).

3. In **Disk Details**, click **Enable replication**.

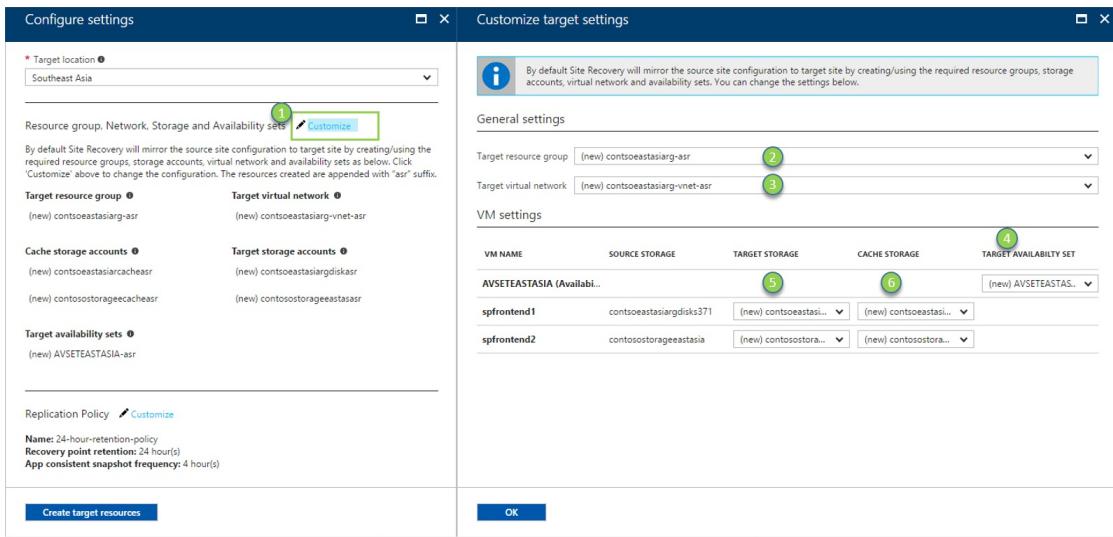
The screenshot shows the 'Disk Details' page for a disk named 'newdisk'. At the top, there's a breadcrumb navigation: Home > All resources > ContosoVault - Replicated items > Contosossd - Disks > Disk Details. Below the breadcrumb, the title 'Disk Details' is followed by 'newdisk'. To the right are a refresh icon and a close ('X') button. A red box highlights the 'Enable replication' button, which has a plus sign icon and the text 'Enable replication'. The page is divided into two main sections: 'Source disk details' and 'Target disk details'. Under 'Source disk details', there are four entries: 'Name' (newdisk), 'Id' (/subscriptions/155c4768-b71c-4e4b-a990-...), 'Location' (empty), and 'Status' (Not protected). Under 'Target disk details', it says 'Target disk details will be available after performing failover operation.'

After the enable replication job runs, and the initial replication finishes, the replication health warning for the disk issue is removed.

Customize target resources

You can modify the default target settings used by Site Recovery.

1. Click **Customize:** next to 'Target subscription' to modify the default target subscription. Select the subscription from the list of all the subscriptions available in the same Azure Active Directory (AAD) tenant.
2. Click **Customize:** to modify default settings:
 - In **Target resource group**, select the resource group from the list of all the resource groups in the target location of the subscription.
 - In **Target virtual network**, select the network from a list of all the virtual network in the target location.
 - In **Availability set**, you can add availability set settings to the VM, if they're part of an availability set in the source region.
 - In **Target Storage accounts**, select the account you want to use.



3. Click **Customize:** to modify replication settings.
4. In **Multi-VM consistency**, select the VMs that you want to replicate together.
 - All the machines in a replication group will have shared crash consistent and app-consistent recovery points when failed over.
 - Enabling multi-VM consistency can impact workload performance (as it is CPU intensive). It should only be enabled if machines are running the same workload, and you need consistency across multiple machines.
 - For example, if an application has 2 SQL Server virtual machines and two web servers, then you should add only the SQL Server VMs to a replication group.
 - You can choose to have a maximum of 16 VMs in a replication group.
 - If you enable multi-VM consistency, machines in the replication group communicate with each other over port 20004.
 - Ensure there's no firewall appliance blocking the internal communication between the VMs over port 20004.
 - If you want Linux VMs to be part of a replication group, ensure the outbound traffic on port 20004 is manually opened according to guidance for the specific Linux version.

Configure replication settings

□ X

Replication policy

24-hour-retention-policy ▾

Recovery point retention 24 Hours

App consistent snapshot frequency 1 Hour

Multi-VM consistency

Do you want to enable Multi-VM consistency by creating a new Replication group? ⓘ

Yes

No



When you select 'Yes' all machines will replicate together and have shared crash consistent and app-consistent recovery points when failed over. Enabling multi-VM consistency can impact workload performance and should only be used if machines are running the same workload and you need consistency across multiple machines.

* Replication group

Create new Use existing

* Replication group name

Enter replication group name

Select Machines to include in this replication group

ContosoPoIAudit

Contosoweb

ContosoWeb2

5. Click **Create target resource > Enable Replication**.

6. After the VMs are enabled for replication, you can check the status of VM health under **Replicated items**

NOTE

During initial replication the status might take some time to refresh, without progress. Click the **Refresh** button, to get the latest status.

Next steps

[Learn more](#) about running a test failover.

Replicate Azure Disk Encryption-enabled virtual machines to another Azure region

1/8/2020 • 8 minutes to read • [Edit Online](#)

This article describes how to replicate Azure VMs with Azure Disk Encryption (ADE) enabled, from one Azure region to another.

NOTE

Site Recovery currently supports ADE, with and without Azure Active Directory (AAD) for VMs running Windows and Linux operating systems. For machines running ADE 1.1 (without AAD), the VMs must be using managed disks. VMs with unmanaged disks aren't supported. If you switch from ADE 0.1 (with AAD) to 1.1 , you need to disable replication and enable replication for a VM after enabling 1.1.

Required user permissions

Site Recovery requires the user to have permissions to create the key vault in the target region and copy keys from source region key vault to the target region key vault.

To enable replication of Disk Encryption-enabled VMs from the Azure portal, the user needs the following permissions on both the **source region and target region** key vaults.

- Key vault permissions
 - List, Create and Get
- Key vault secret permissions
 - Secret Management Operations
 - Get, List and Set
- Key vault key permissions (required only if the VMs use key encryption key to encrypt disk encryption keys)
 - Key Management Operations
 - Get, List and Create
 - Cryptographic Operations
 - Decrypt and Encrypt

To manage permissions, go to the key vault resource in the portal. Add the required permissions for the user. The following example shows how to enable permissions to the key vault *ContosoWeb2KeyVault*, which is in the source region.

1. Go to **Home > Keyvaults > ContosoWeb2KeyVault > Access policies**.

ContosoWeb2KeyVault - Access policies

Key vault

Search (Ctrl+ /)

Save Discard Refresh

Click to show advanced access policies

Add new ...

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Keys

Secrets

Certificates

Access policies

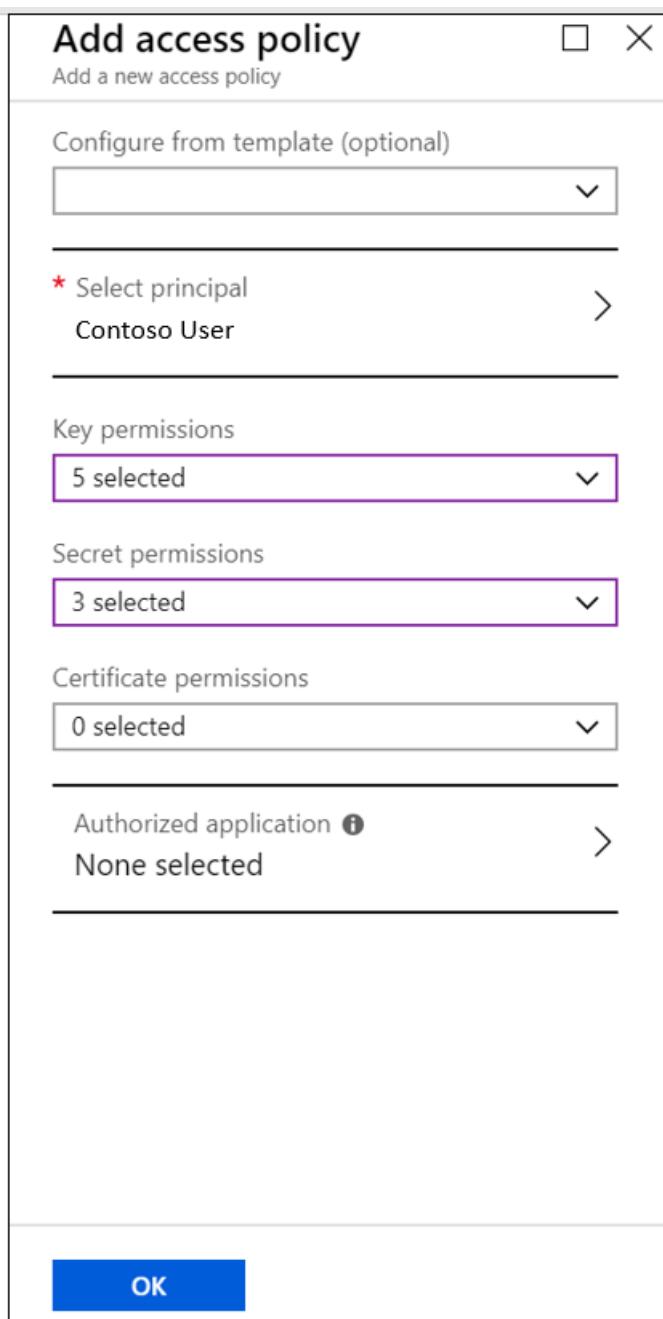
Firewalls and virtual networks

Properties

Locks

Automation script

2. You can see that there are no user permissions. Select **Add new**. Enter the user and permissions information.



If the user who's enabling disaster recovery (DR) doesn't have permissions to copy the keys, a security administrator who has appropriate permissions can use the following script to copy the encryption secrets and keys to the target region.

To troubleshoot permissions, refer to [key vault permission issues](#) later in this article.

NOTE

To enable replication of Disk Encryption-enabled VMs from the portal, you need at least "List" permissions on the key vaults, secrets, and keys.

Copy Disk Encryption keys to the DR region by using the PowerShell script

1. [Open the "CopyKeys" raw script code.](#)
2. Copy the script to a file, and name it **Copy-keys.ps1**.
3. Open the Windows PowerShell application, and go to the folder where you saved the file.

4. Execute Copy-keys.ps1.
5. Provide Azure credentials to sign in.
6. Select the **Azure subscription** of your VMs.
7. Wait for the resource groups to load, and then select the **Resource group** of your VMs.
8. Select the VMs from the list that's displayed. Only VMs that are enabled for disk encryption are on the list.
9. Select the **Target location**.

- **Disk encryption key vaults**
- **Key encryption key vaults**

By default, Site Recovery creates a new key vault in the target region. The vault's name has an "asr" suffix that's based on the source VM disk encryption keys. If a key vault already exists that was created by Site Recovery, it's reused. Select a different key vault from the list if necessary.

Enable replication

For this example, the primary Azure region is East Asia, and the secondary region is South East Asia.

1. In the vault, select **+Replicate**.
2. Note the following fields.
 - **Source**: The point of origin of the VMs, which in this case is **Azure**.
 - **Source location**: The Azure region where you want to protect your virtual machines. For this example, the source location is "East Asia."
 - **Deployment model**: The Azure deployment model of the source machines.
 - **Source subscription**: The subscription to which your source virtual machines belong. It can be any subscription that's in the same Azure Active Directory tenant as your recovery services vault.
 - **Resource Group**: The resource group to which your source virtual machines belong. All the VMs in the selected resource group are listed for protection in the next step.
3. In **Virtual Machines > Select virtual machines**, select each VM that you want to replicate. You can only select machines for which replication can be enabled. Then, select **OK**.
4. In **Settings**, you can configure the following target-site settings.
 - **Target location**: The location where your source virtual machine data will be replicated. Site Recovery provides a list of suitable target regions based on the selected machine's location. We recommend that you use the same location as the Recovery Services vault's location.
 - **Target subscription**: The target subscription that's used for disaster recovery. By default, the target subscription is the same as the source subscription.
 - **Target resource group**: The resource group to which all your replicated virtual machines belong. By default, Site Recovery creates a new resource group in the target region. The name gets the "asr" suffix. If a resource group already exists that was created by Azure Site Recovery, it's reused. You can also choose to customize it, as shown in the following section. The location of the target resource group can be any Azure region except the region where the source virtual machines are hosted.
 - **Target virtual network**: By default, Site Recovery creates a new virtual network in the target region. The name gets the "asr" suffix. It's mapped to your source network and used for any future protection. [Learn more](#) about network mapping.
 - **Target storage accounts (if your source VM doesn't use managed disks)**: By default, Site Recovery creates a new target storage account by mimicking your source VM storage configuration. If a storage account already exists, it's reused.

- **Replica managed disks (if your source VM uses managed disks):** Site Recovery creates new replica managed disks in the target region to mirror the source VM's managed disks of the same storage type (standard or premium) as the source VM's managed disks.
- **Cache storage accounts:** Site Recovery needs an extra storage account called *cache storage* in the source region. All the changes on the source VMs are tracked and sent to the cache storage account. They're then replicated to the target location.
- **Availability set:** By default, Site Recovery creates a new availability set in the target region. The name has the "asr" suffix. If an availability set that was created by Site Recovery already exists, it's reused.
- **Disk encryption key vaults:** By default, Site Recovery creates a new key vault in the target region. It has an "asr" suffix that's based on the source VM disk encryption keys. If a key vault that was created by Azure Site Recovery already exists, it's reused.
- **Key encryption key vaults:** By default, Site Recovery creates a new key vault in the target region. The name has an "asr" suffix that's based on the source VM key encryption keys. If a key vault created by Azure Site Recovery already exists, it's reused.
- **Replication policy:** Defines the settings for recovery point retention history and app-consistent snapshot frequency. By default, Site Recovery creates a new replication policy with default settings of *24 hours* for recovery point retention and *60 minutes* for app-consistent snapshot frequency.

Customize target resources

Follow these steps to modify the Site Recovery default target settings.

1. Select **Customize** next to "Target subscription" to modify the default target subscription. Select the subscription from the list of subscriptions that are available in the Azure AD tenant.
2. Select **Customize** next to "Resource group, Network, Storage, and Availability sets" to modify the following default settings:
 - For **Target resource group**, select the resource group from the list of resource groups in the target location of the subscription.
 - For **Target virtual network**, select the network from a list of virtual networks in the target location.
 - For **Availability set**, you can add availability set settings to the VM, if they're part of an availability set in the source region.
 - For **Target Storage accounts**, select the account to use.
3. Select **Customize** next to "Encryption settings" to modify the following default settings:
 - For **Target disk encryption key vault**, select the target disk encryption key vault from the list of key vaults in the target location of the subscription.
 - For **Target key encryption key vault**, select the target key encryption key vault from the list of key vaults in the target location of the subscription.
4. Select **Create target resource > Enable Replication**.
5. After the VMs are enabled for replication, you can check the VMs' health status under **Replicated items**.

NOTE

During initial replication, the status might take some time to refresh, without apparent progress. Click **Refresh** to get the latest status.

Update target VM encryption settings

In the following scenarios, you'll be required to update the target VM encryption settings:

- You enabled Site Recovery replication on the VM. Later, you enabled disk encryption on the source VM.
- You enabled Site Recovery replication on the VM. Later, you changed the disk encryption key or key encryption key on the source VM.

You can use a [script](#) to copy the encryption keys to the target region and then update the target encryption settings in **Recovery services vault > replicated item > Properties > Compute and Network**.

PROPERTIES		SOURCE	TARGET
Subscription	DR_Prod_TenantSubB	ASR PM team subscription	
Name	umdsOsBekKek	umdsOsBekKek	
Resource group	adevmsg	ADEVmsRg_asr	
Size	D2s v3 (2 cores, 8 GB memory, 2 NICs)	D2s v3 (2 cores, 8 GB memory, 2 NICs)	
Disk encryption key vaults	belkKeyVault	belkKeyVault-asr-1	
Key encryption key vaults		belkKeyVault-asr-1	
NETWORK PROPERTIES		SOURCE NETWORK	TARGET NETWORK
Virtual network	adevmsgvnet167	adevmsgvnet167-asr	

Troubleshoot key vault permission issues during Azure-to-Azure VM replication

Azure Site Recovery requires at least read permission on the Source region Key vault and write permission on the target region key vault to read the secret and copy it to the target region key vault.

Cause 1: You don't have "GET" permission on the **source region Key vault** to read the keys.

How to fix: Regardless of whether you are a subscription admin or not, it is important that you have get permission on the key vault.

1. Go to source region Key vault which in this example is "ContososourceKeyvault" > **Access policies**
2. Under **Select Principal** add your user name for example: "dradmin@contoso.com"
3. Under **Key permissions** select GET
4. Under **Secret Permission** select GET
5. Save the access policy

Cause 2: You don't have required permission on the **Target region Key vault** to write the keys.

For example: You try to replicate a VM that has key vault *ContososourceKeyvault* on a source region. You have all the permissions on the source region key vault. But during protection, you select the already-created key vault *ContosotargetKeyvault*, which doesn't have permissions. An error occurs.

Permission required on [target Key vault](#)

How to fix: Go to **Home > Keyvaults > ContosotargetKeyvault > Access policies** and add the appropriate permissions.

Next steps

[Learn more](#) about running a test failover.

Replicate machines with Customer-Managed Keys (CMK) enabled disks

1/10/2020 • 5 minutes to read • [Edit Online](#)

This article describes how to replicate Azure VMs with Customer-Managed Keys (CMK) enabled managed disks, from one Azure region to another.

Prerequisite

You must create the Disk Encryption set(s) in the target region for the target subscription before enabling replication for your virtual machines that have CMK-enabled managed disks.

Enable replication

For this example, the primary Azure region is East Asia, and the secondary region is South East Asia.

1. In the vault, select **+Replicate**.
2. Note the following fields.
 - **Source:** The point of origin of the VMs, which in this case is **Azure**.
 - **Source location:** The Azure region where you want to protect your virtual machines. For this example, the source location is "East Asia."
 - **Deployment model:** The Azure deployment model of the source machines.
 - **Source subscription:** The subscription to which your source virtual machines belong. It can be any subscription that's in the same Azure Active Directory tenant as your recovery services vault.
 - **Resource Group:** The resource group to which your source virtual machines belong. All the VMs in the selected resource group are listed for protection in the next step.
3. In **Virtual Machines > Select virtual machines**, select each VM that you want to replicate. You can only select machines for which replication can be enabled. Then, select **OK**.
4. In **Settings**, you can configure the following target-site settings.
 - **Target location:** The location where your source virtual machine data will be replicated. Site Recovery provides a list of suitable target regions based on the selected machine's location. We recommend that you use the same location as the Recovery Services vault's location.
 - **Target subscription:** The target subscription that's used for disaster recovery. By default, the target subscription is the same as the source subscription.
 - **Target resource group:** The resource group to which all your replicated virtual machines belong. By default, Site Recovery creates a new resource group in the target region. The name gets the `asr` suffix. If a resource group already exists that was created by Azure Site Recovery, it's reused. You can also choose to customize it, as shown in the following section. The location of the target resource group can be any Azure region except the region where the source virtual machines are hosted.
 - **Target virtual network:** By default, Site Recovery creates a new virtual network in the target region. The name gets the `asr` suffix. It's mapped to your source network and used for any future protection. [Learn more](#) about network mapping.
 - **Target storage accounts (if your source VM doesn't use managed disks):** By default, Site Recovery creates a new target storage account by mimicking your source VM storage configuration. If a storage account already exists, it's reused.

- **Replica managed disks (if your source VM uses managed disks):** Site Recovery creates new replica managed disks in the target region to mirror the source VM's managed disks of the same storage type (standard or premium) as the source VM's managed disks.
- **Cache storage accounts:** Site Recovery needs an extra storage account called *cache storage* in the source region. All the changes on the source VMs are tracked and sent to the cache storage account. They're then replicated to the target location.
- **Availability set:** By default, Site Recovery creates a new availability set in the target region. The name has the `asr` suffix. If an availability set that was created by Site Recovery already exists, it's reused.
- **Disk encryption sets (DES):** Site Recovery needs the disk encryption set(s) to be used for replica and target managed disks. You must pre-create DES in the target subscription and the target region before enabling the replication. By default, a DES is not selected. You must click on 'Customize' to choose a DES per source disk.
- **Replication policy:** Defines the settings for recovery point retention history and app-consistent snapshot frequency. By default, Site Recovery creates a new replication policy with default settings of *24 hours* for recovery point retention and *60 minutes* for app-consistent snapshot frequency.

Configure settings

Target location * ⓘ
Central US EUAP

Target subscription ⚙ Customize
ASR Canary Test Subscription 2

 If you are choosing General Purpose v2 storage accounts, ensure that operations and data transfer prices are understood clearly before you proceed. [Learn more](#)

Resource group, Network, Storage and Availability ⚙ Customize
By default Site Recovery will mirror the source site configuration to target site by creating/using the required resource groups, storage accounts, virtual network and availability sets as below. Click 'Customize' above to change the configuration. The resources created are appended with "asr" suffix.

Target resource group ⓘ Nandeesh-CMK-TestRG-asr-1	Target virtual network ⓘ nandeesh-cmk-vm1_vnet-asr
Cache storage accounts ⓘ nSet8xnancmkccyascrcache	Replica managed disks ⓘ (new) 4 premium disk(s), 0 standard disk(s)

Target availability sets ⓘ
Not Applicable

Storage encryption settings ⚙ Customize

Disk Encryption Sets
Not selected

Replication Policy ⚙ Customize

Name: 24-hour-retention-policy
Recovery point retention: 24 hour(s)
App consistent snapshot frequency: 4 hour(s)
Replication group: None

Extension settings [+ Show details]
Site Recovery manages site recovery extension updates for all your replicated items. 1 new automation account will be created.

 You do not have permissions to create an Azure Run As account (service principal) and to grant the Contributor role to the service principal. Note that enable replication will continue, site recovery extension auto-update will be set to 'manage manually'. You can resolve the error and retry or change the settings later. [Learn more](#)

Create target resources

Customize target resources

Follow these steps to modify the Site Recovery default target settings.

1. Select **Customize** next to "Target subscription" to modify the default target subscription. Select the subscription from the list of subscriptions that are available in the Azure AD tenant.
2. Select **Customize** next to "Resource group, Network, Storage, and Availability sets" to modify the following default settings:
 - For **Target resource group**, select the resource group from the list of resource groups in the target location of the subscription.
 - For **Target virtual network**, select the network from a list of virtual networks in the target location.
 - For **Availability set**, you can add availability set settings to the VM, if they're part of an availability set in the source region.
 - For **Target Storage accounts**, select the account to use.
3. Select **Customize** next to "Storage encryption settings" to select the target DES for every customer-managed key (CMK) enabled source managed disk. At the time of selection, you will also be able to see which target key vault the DES is associated with.
4. Select **Create target resource > Enable Replication**.
5. After the VMs are enabled for replication, you can check the VMs' health status under **Replicated items**.

VM Name	Source managed disk	Source DES	Source key vault	Target DES	Target key vault
Nandeesh-CMKV2	4 managed disks	NandeeshDiskEncryptionSet2	/subscriptions/509099b2-9d2c-...	cmkdiskSetNK	cmkTestKVNK

NOTE

During initial replication, the status might take some time to refresh, without apparent progress. Click **Refresh** to get the latest status.

FAQs

- I have enabled CMK on an existing replicated item, how can I ensure that CMK is applied on the target region as well?

You can find out the name of the replica managed disk (created by Azure Site Recovery in the target region) and attach DES to this replica disk. However, you will not be able to see the DES details in the Disks blade once you attach it. Alternatively, you can choose to disable the replication of the VM and enable it again. It will ensure you see DES and key vault details in the Disks blade for the replicated item.

- I have added a new CMK enabled disk to the replicated item. How can I replicate this disk with Azure Site Recovery?

Addition of a new CMK enabled disk to an existing replicated item is not supported. Disable the replication

and enable the replication again for the virtual machine.

Replicate Azure VMs running Storage Spaces Direct to another region

1/14/2020 • 3 minutes to read • [Edit Online](#)

This article describes how to enable disaster recovery of Azure VMs running storage spaces direct.

NOTE

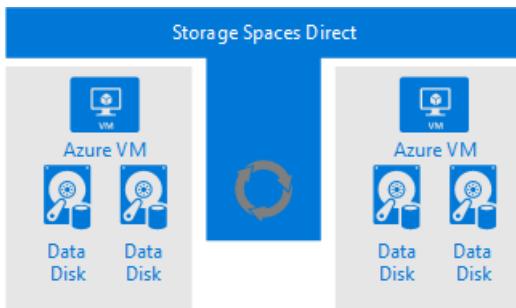
Only crash consistent recovery points are supported for storage spaces direct clusters.

Storage spaces direct (S2D) is software-defined storage, which provides a way to create [guest clusters](#) on Azure. A guest cluster in Microsoft Azure is a failover cluster comprised of IaaS VMs. It allows hosted VM workloads to fail over across guest clusters, achieving higher availability SLA for applications, than a single Azure VM can provide. It is useful in scenarios where a VM hosts a critical application like SQL or scale-out file server.

Disaster recovery with storage spaces direct

In a typical scenario, you may have virtual machines guest cluster on Azure for higher resiliency of your application like Scale out file server. While this can provide your application higher availability, you would like to protect these applications using Site Recovery for any region level failure. Site Recovery replicates the data from one region to another Azure region and brings up the cluster in disaster recovery region in an event of failover.

Below diagram shows a two-node Azure VM failover cluster using storage spaces direct.



- Two Azure virtual machines in a Windows Failover Cluster and each virtual machine have two or more data disks.
- S2D synchronizes the data on the data disk and presents the synchronized storage as a storage pool.
- The storage pool presents as a cluster shared volume (CSV) to the failover cluster.
- The Failover cluster uses the CSV for the data drives.

Disaster Recovery Considerations

1. When you are setting up [cloud witness](#) for the cluster, keep witness in the Disaster Recovery region.
2. If you are going to fail over the virtual machines to the subnet on the DR region which is different from the source region then cluster IP address needs to be change after failover. To change IP of the cluster you need to use the Site Recovery [recovery plan script](#).

[Sample script](#) to execute command inside VM using custom script extension

Enabling Site Recovery for S2D cluster:

1. Inside the recovery services vault, click "+replicate"

2. Select all the nodes in the cluster and make them part of a [Multi-VM consistency group](#)
3. Select replication policy with application consistency off* (only crash consistency support is available)
4. Enable the replication

Configure replication settings

Replication policy

Name	S2Dreplication ... <input checked="" type="checkbox"/>
Recovery point retention	24 Hours
App consistent snapshot frequency	Off <input type="button" value="Edit"/> Hours

Multi-VM consistency

Do you want to enable Multi-VM consistency by creating a new Replication group? [?](#)

Yes No

i When you select 'Yes' all machines will replicate together and have shared crash consistent and app-consistent recovery points when failed over. Enabling multi-VM consistency can impact workload performance and should only be used if machines are running the same workload and you need consistency across multiple machines.

* Replication group
 Create new Use existing

* Replication group name

Select Machines to include in this replication group

<input checked="" type="checkbox"/> ContosowebS2D1
<input checked="" type="checkbox"/> ContosoWebS2D2

OK

5. Go to replicated items and you can see both the virtual machine status.
6. Both the virtual machines are getting protected and are also shown as part of multi-VM consistency group.

NAME	R...	STATUS	ACTIVE LOCATI...	RPO
▼ S2DReplicationgroup (2 ...	-	-	-	-
ContosoWebS2d1	✓ Protected	Protected	East Asia	5 minutes
ContososWebS2d2	✓ Protected	Protected	East Asia	2 minutes

Creating a recovery plan

A recovery plan supports the sequencing of various tiers in a multi-tier application during a failover. Sequencing helps maintain application consistency. When you create a recovery plan for a multi-tier web application, complete the steps described in [Create a recovery plan by using Site Recovery](#).

Adding virtual machines to failover groups

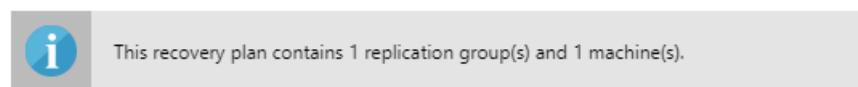
1. Create a recovery plan by adding the virtual machines.
2. Click on 'Customize' to group the VMs. By default, all VMs are part of 'Group 1'.

Add scripts to the recovery plan

For your applications to function correctly, you might need to do some operations on the Azure virtual machines after the failover or during a test failover. You can automate some post-failover operations. For example, here we are attaching load balancer and changing cluster IP.

Failover of the virtual machines

Both the nodes of the VMs need to be fail over using the Site Recovery [recovery plan](#)



STAGE NAME	DETAILS	
All groups shut down	1 machine in 2 groups.	...
▶ All groups failover		...
▼ Group 1: Start	1 Machine	...
adVM	Machine	...
▼ Group 1: Post-steps	1 Step	...
Script: addloadbalancer	Script	...
▼ Group 2: Start	2 Machines	...
ContosowebS2D1	Machine	...
ContosowebS2D2	Machine	...
▼ Group 2: Post-steps	1 Step	...
Script: changing clusterip	Script	...

Run a test failover

1. In the Azure portal, select your Recovery Services vault.
2. Select the recovery plan that you created.
3. Select **Test Failover**.
4. To start the test failover process, select the recovery point and the Azure virtual network.
5. When the secondary environment is up, perform validations.
6. When validations are complete, to clean the failover environment, select **Cleanup test failover**.

For more information, see [Test failover to Azure in Site Recovery](#).

Run a failover

1. In the Azure portal, select your Recovery Services vault.
2. Select the recovery plan that you created for SAP applications.
3. Select **Failover**.
4. To start the failover process, select the recovery point.

For more information, see [Failover in Site Recovery](#).

Next steps

[Learn more](#) about running failback.

Enable replication for a disk added to an Azure VM

1/14/2020 • 2 minutes to read • [Edit Online](#)

This article describes how to enable replication for data disks that are added to an Azure VM that's already enabled for disaster recovery to another Azure region, using [Azure Site Recovery](#).

Enabling replication for a disk you add to a VM is supported for Azure VMs with managed disks.

When you add a new disk to an Azure VM that's replicating to another Azure region, the following occurs:

- Replication health for the VM shows a warning, and a note in the portal informs you that one or more disks are available for protection.
- If you enable protection for the added disks, the warning will disappear after initial replication of the disk.
- If you choose not to enable replication for the disk, you can select to dismiss the warning.

The screenshot shows the Azure portal interface for managing replicated items. The main area displays the 'Contosossd' VM details. A key feature highlighted is the ability to enable replication for newly added disks directly from the portal. The interface includes various management actions like Failover, Test Failover, and Commit, along with monitoring tools for health, errors, and events.

Before you start

This article assumes that you've already set up disaster recovery for the VM to which you're adding the disk. If you haven't, follow the [Azure to Azure disaster recovery tutorial](#).

Enable replication for an added disk

To enable replication for an added disk, do the following:

1. In the vault > **Replicated Items**, click the VM to which you added the disk.
2. Click **Disks**, and then select the data disk for which you want to enable replication (these disks have a **Not protected** status).
3. In **Disk Details**, click **Enable replication**.

Disk Details

newdisk



+ Enable replication

Source disk details

Name	newdisk
Id	/subscriptions/155c4768-b71c-4e4b-a990-...
Location	
Status	Not protected

Target disk details

Target disk details will be available after performing failover operation.

After the enable replication job runs and the initial replication finishes, the replication health warning for the disk issue is removed.

Next steps

[Learn more](#) about running a test failover.

Exclude disks from PowerShell replication of Azure VMs

1/14/2020 • 3 minutes to read • [Edit Online](#)

This article describes how to exclude disks when you replicate Azure VMs. You might exclude disks to optimize the consumed replication bandwidth or the target-side resources that those disks use. Currently, this capability is available only through Azure PowerShell.

NOTE

This article has been updated to use the new Azure PowerShell Az module. You can still use the AzureRM module, which will continue to receive bug fixes until at least December 2020. To learn more about the new Az module and AzureRM compatibility, see [Introducing the new Azure PowerShell Az module](#). For Az module installation instructions, see [Install Azure PowerShell](#).

Prerequisites

Before you start:

- Make sure that you understand the [disaster-recovery architecture and components](#).
- Review the [support requirements](#) for all components.
- Make sure that you have AzureRm PowerShell "Az" module. To install or update PowerShell, see [Install the Azure PowerShell module](#).
- Make sure that you have created a recovery services vault and protected virtual machines at least once. If you haven't done these things, follow the process at [Set up disaster recovery for Azure virtual machines using Azure PowerShell](#).
- If you're looking for information on adding disks to an Azure VM enabled for replication, [review this article](#).

Why exclude disks from replication

You might need to exclude disks from replication because:

- Your virtual machine has reached [Azure Site Recovery limits to replicate data change rates](#).
- The data that's churned on the excluded disk isn't important or doesn't need to be replicated.
- You want to save storage and network resources by not replicating the data.

How to exclude disks from replication

In our example, we replicate a virtual machine that has one OS and three data disks that's in the East US region to the West US 2 region. The name of the virtual machine is *AzureDemoVM*. We exclude disk 1 and keep disks 2 and 3.

Get details of the virtual machines to replicate

```
# Get details of the virtual machine
$VM = Get-AzVM -ResourceGroupName "A2AdemoRG" -Name "AzureDemoVM"

Write-Output $VM
```

```
ResourceGroupName : A2AdemoRG
Id              : /subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx/resourceGroups/A2AdemoRG/providers/Microsoft.Compute/virtualMachines/AzureDemoVM
VmId           : 1b864902-c7ea-499a-ad0f-65da2930b81b
Name            : AzureDemoVM
Type            : Microsoft.Compute/virtualMachines
Location        : eastus
Tags            : {}
DiagnosticsProfile : {BootDiagnostics}
HardwareProfile   : {VmSize}
NetworkProfile    : {NetworkInterfaces}
OSProfile         : {ComputerName, AdminUsername, WindowsConfiguration, Secrets}
ProvisioningState : Succeeded
StorageProfile    : {ImageReference, OsDisk, DataDisks}
```

Get details about the virtual machine's disks. This information will be used later when you start replication of the VM.

```
$OSDiskVhdURI = $VM.StorageProfile.OsDisk.Vhd
$DataDisk1VhdURI = $VM.StorageProfile.DataDisks[0].Vhd
```

Replicate an Azure virtual machine

For the following example, we assume that you already have a cache storage account, replication policy, and mappings. If you don't have these things, follow the process at [Set up disaster recovery for Azure virtual machines using Azure PowerShell](#).

Replicate an Azure virtual machine with *managed disks*.

```

#Get the resource group that the virtual machine must be created in when failed over.
$RecoveryRG = Get-AzResourceGroup -Name "a2ademorecoveryrg" -Location "West US 2"

#Specify replication properties for each disk of the VM that is to be replicated (create disk replication configuration).

#OsDisk
$OSdiskId = $vm.StorageProfile.OsDisk.ManagedDisk.Id
$RecoveryOSDiskAccountType = $vm.StorageProfile.OsDisk.ManagedDisk.StorageAccountType
$RecoveryReplicaDiskAccountType = $vm.StorageProfile.OsDisk.ManagedDisk.StorageAccountType

$OSDiskReplicationConfig = New-AzRecoveryServicesAsrAzureToAzureDiskReplicationConfig -ManagedDisk -
LogStorageAccountId $EastUSCacheStorageAccount.Id ` 
    -DiskId $OSdiskId -RecoveryResourceGroupId $RecoveryRG.ResourceId -RecoveryReplicaDiskAccountType
$RecoveryReplicaDiskAccountType ` 
    -RecoveryTargetDiskAccountType $RecoveryOSDiskAccountType

# Data Disk 1 i.e StorageProfile.DataDisks[0] is excluded, so we will provide it during the time of replication.

# Data disk 2
$datadiskId2 = $vm.StorageProfile.DataDisks[1].ManagedDisk.id
$RecoveryReplicaDiskAccountType = $vm.StorageProfile.DataDisks[1].StorageAccountType
$RecoveryTargetDiskAccountType = $vm.StorageProfile.DataDisks[1].StorageAccountType

$DataDisk2ReplicationConfig = New-AzRecoveryServicesAsrAzureToAzureDiskReplicationConfig -ManagedDisk -
LogStorageAccountId $CacheStorageAccount.Id ` 
    -DiskId $datadiskId2 -RecoveryResourceGroupId $RecoveryRG.ResourceId -RecoveryReplicaDiskAccountType
$RecoveryReplicaDiskAccountType ` 
    -RecoveryTargetDiskAccountType $RecoveryTargetDiskAccountType

# Data Disk 3

$datadiskId3 = $vm.StorageProfile.DataDisks[2].ManagedDisk.id
$RecoveryReplicaDiskAccountType = $vm.StorageProfile.DataDisks[2].StorageAccountType
$RecoveryTargetDiskAccountType = $vm.StorageProfile.DataDisks[2].StorageAccountType

$DataDisk3ReplicationConfig = New-AzRecoveryServicesAsrAzureToAzureDiskReplicationConfig -ManagedDisk -
LogStorageAccountId $CacheStorageAccount.Id ` 
    -DiskId $datadiskId3 -RecoveryResourceGroupId $RecoveryRG.ResourceId -RecoveryReplicaDiskAccountType
$RecoveryReplicaDiskAccountType ` 
    -RecoveryTargetDiskAccountType $RecoveryTargetDiskAccountType

#Create a list of disk replication configuration objects for the disks of the virtual machine that are to be replicated.
$diskconfigs = @()
$diskconfigs += $OSDiskReplicationConfig, $DataDisk2ReplicationConfig, $DataDisk3ReplicationConfig

#Start replication by creating a replication protected item. Using a GUID for the name of the replication protected item to ensure uniqueness of name.
$tempASRJob = New-ASRReplicationProtectedItem -AzureToAzure -AzureVmId $VM.Id -Name (New-Guid).Guid - 
ProtectionContainerMapping $EusToWusPCMAPPING -AzureToAzureDiskReplicationConfiguration $diskconfigs - 
RecoveryResourceGroupId $RecoveryRG.ResourceId

```

When the start-replication operation succeeds, the VM data is replicated to the recovery region.

You can go to the Azure portal and see the replicated VMs under "replicated items."

The replication process starts by seeding a copy of the replicating disks of the virtual machine in the recovery region. This phase is called the initial-replication phase.

After initial replication finishes, replication moves on to the differential-synchronization phase. At this point, the virtual machine is protected. Select the protected virtual machine to see if any disks are excluded.

Next steps

Learn about [running a test failover](#).

Reprotect failed over Azure VMs to the primary region

2/14/2020 • 5 minutes to read • [Edit Online](#)

When you [fail over](#) Azure VMs from one region to another using [Azure Site Recovery](#), the VMs boot up in the secondary region, in an **unprotected** state. If you want to fail back the VMs to the primary region, do the following tasks:

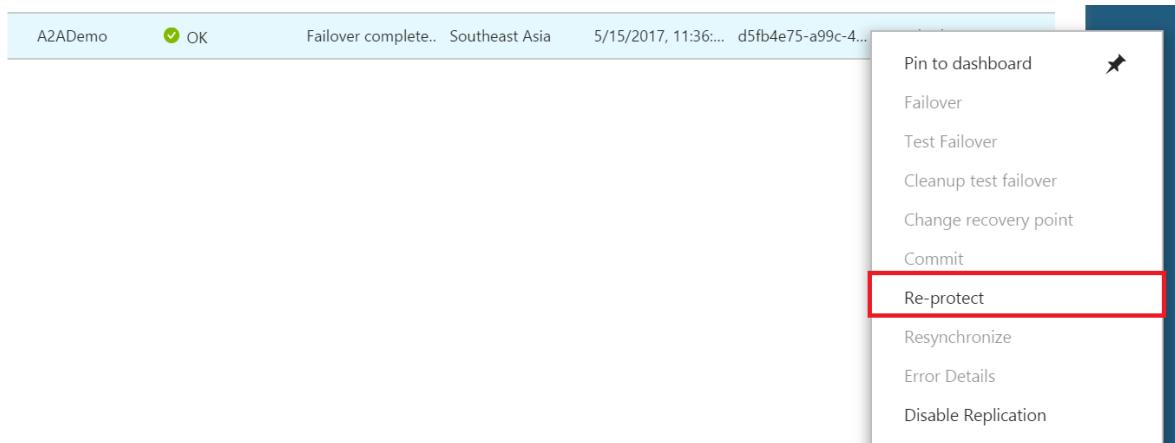
1. Reprotect the VMs in the secondary region, so that they start to replicate to the primary region.
2. After reprottection completes and the VMs are replicating, you can fail over from the secondary to primary region.

Prerequisites

- The VM failover from the primary to secondary region must be committed.
- The primary target site should be available, and you should be able to access or create resources in that region.

Reprotect a VM

1. In **Vault > Replicated items**, right-click the failed over VM, and select **Re-Protect**. The reprottection direction should show from secondary to primary.



2. Review the resource group, network, storage, and availability sets. Then click **OK**. If there are any resources marked as new, they're created as part of the reprottection process.
3. The reprottection job seeds the target site with the latest data. After the job finishes, delta replication takes place. Then, you can fail over back to the primary site. You can select the storage account or the network you want to use during reprottection, using the customize option.

Resource group, Network, Storage and Availability sets

 [Customize](#)

By default, Site Recovery will pick the original source resource group, virtual network, storage accounts and availability sets as below. Click 'Customize' above to change the configuration. The resources created are appended with "asr" suffix.

Target resource group

root2

Target virtual network

RDSRD-vnet

Cache storage accounts

a2aencryptedrgdcacheasr1

Target storage accounts

a2aencryptedrgdisks723

Target availability sets

Not Applicable

Customize reprotect settings

You can customize the following properties of the target VM during reprottection.

Customize target settings



By default Site Recovery will mirror the source site configuration to target site by creating/using the required resource groups, storage accounts, virtual network and availability sets. You can change the settings below.

General settings

Target resource group

Target virtual network

VM settings

VM NAME	SOURCE STORAGE	TARGET STORAGE	CACHE STORAGE	TARGET AVAILABILITY SET
A2ADemo	a2aencryptedrgdisks7asr	<input type="text" value="a2aencryptedrgdisk..."/>	<input type="text" value="a2aencryptedrgdcac.."/>	

PROPERTY	NOTES
Target resource group	Modify the target resource group in which the VM is created. As the part of reprotect, the target VM is deleted. You can choose a new resource group under which to create the VM after failover.
Target virtual network	The target network can't be changed during the reprotect job. To change the network, redo the network mapping.
Target storage (Secondary VM doesn't use managed disks)	You can change the storage account that the VM uses after failover.
Replica managed disks (Secondary VM uses managed disks)	Site Recovery creates replica managed disks in the primary region to mirror the secondary VM's managed disks.

PROPERTY	NOTES
Cache storage	You can specify a cache storage account to be used during replication. By default, a new cache storage account is created, if it doesn't exist.
Availability set	If the VM in the secondary region is part of an availability set, you can choose an availability set for the target VM in the primary region. By default, Site Recovery tries to find the existing availability set in the primary region, and use it. During customization, you can specify a new availability set.

What happens during reprottection?

By default, the following occurs:

1. A cache storage account is created in the region where the failed over VM is running.
2. If the target storage account (the original storage account in the primary region) doesn't exist, a new one is created. The assigned storage account name is the name of the storage account used by the secondary VM, suffixed with `asr`.
3. If your VM uses managed disks, replica managed disks are created in the primary region to store the data replicated from the secondary VM's disks.
4. If the target availability set doesn't exist, a new one is created as part of the reprotect job if necessary. If you've customized the reprottection settings, then the selected set is used.

When you trigger a reprotect job, and the target VM exists, the following occurs:

1. The target side VM is turned off if it's running.
2. If the VM is using managed disks, a copy of the original disk is created with an `-ASRReplica` suffix. The original disks are deleted. The `-ASRReplica` copies are used for replication.
3. If the VM is using unmanaged disks, the target VM's data disks are detached and used for replication. A copy of the OS disk is created and attached on the VM. The original OS disk is detached and used for replication.
4. Only changes between the source disk and the target disk are synchronized. The differentials are computed by comparing both the disks and then transferred. Check below to find the estimated time to complete the reprottection.
5. After the synchronization completes, the delta replication begins, and a recovery point is created in line with the replication policy.

When you trigger a reprotect job, and the target VM and disks don't exist, the following occurs:

1. If the VM is using managed disks, replica disks are created with `-ASRReplica` suffix. The `-ASRReplica` copies are used for replication.
2. If the VM is using unmanaged disks, replica disks are created in the target storage account.
3. The entire disks are copied from the failed over region to the new target region.
4. After the synchronization completes, the delta replication begins, and a recovery point is created in line with the replication policy.

Estimated time to do the reprottection

In most cases, Azure Site Recovery doesn't replicate the complete data to the source region. The following conditions determine how much data is replicated:

1. If the source VM data is deleted, corrupted, or inaccessible for some reason, such as a resource group change/delete, then during reprottection a complete initial replication will happen because there's no data available on the source region to use.
2. If the source VM data is accessible, then only differentials are computed by comparing both the disks and then

transferred. Check the table below to get the estimated time.

EXAMPLE SITUATION	TIME TAKEN TO REPROTECT
Source region has 1 VM with 1 TB standard disk. Only 127 GB data is used, and the rest of the disk is empty. Disk type is standard with 60 MiB/S throughput. No data change after failover.	Approximate time: 45 minutes – 1.5 hours. During reprottection, Site Recovery will populate the checksum of all data that will take 127 GB/ 45 MBs, approximately 45 minutes. Some overhead time is required for Site Recovery to auto scale, approximately 20-30 minutes. No Egress charges.
Source region has 1 VM with 1 TB standard disk. Only 127 GB data is used and rest of the disk is empty. Disk type is standard with 60 MiB/S throughput. 45 GB data changes after failover.	Approximate time: 1 hour – 2 hours. During reprottection, Site Recovery will populate the checksum of all data that will take 127 GB/ 45 MBs, approximately 45 minutes. Transfer time to apply changes of 45 GB that is 45 GB/ 45 MBps, approximately 17 minutes. Egress charges would be for 45 GB data changes, not for the checksum.

Next steps

After the VM is protected, you can initiate a failover. The failover shuts down the VM in the secondary region and creates and boots the VM in the primary region, with brief downtime during this process. We recommend you choose an appropriate time for this process and that you run a test failover before initiating a full failover to the primary site. [Learn more](#) about Azure Site Recovery failover.

Set up disaster recovery for Azure VMs after migration to Azure

11/18/2019 • 2 minutes to read • [Edit Online](#)

Follow this article if you've [migrated on-premises machines to Azure VMs](#) using the [Site Recovery](#) service, and you now want to get the VMs set up for disaster recovery to a secondary Azure region. The article describes how to ensure that the Azure VM agent is installed on migrated VMs, and how to remove the Site Recovery Mobility service that's no longer needed after migration.

Verify migration

Before you set up disaster recovery, make sure that migration has completed as expected. To complete a migration successfully, after the failover, you should select the **Complete Migration** option, for each machine you want to migrate.

Verify the Azure VM agent

Each Azure VM must have the [Azure VM agent](#) installed. To replicate Azure VMs, Site Recovery installs an extension on the agent.

- If the machine is running version 9.7.0.0 or later of the Site Recovery Mobility service, the Azure VM agent is automatically installed by the Mobility service on Windows VMs. On earlier versions of the Mobility service, you'll install the agent manually.
- For Linux VMs, you must install the Azure VM agent manually. You only need to install the Azure VM agent if the Mobility service installed on the migrated machine is v9.6 or earlier.

Install the agent on Windows VMs

If you're running a version of the Site Recovery mobility service earlier than 9.7.0.0, or you have some other need to install the agent manually, do the following:

1. Ensure you have admin permissions on the VM.
2. Download the [VM Agent installer](#).
3. Run the installer file.

Validate the installation

To check that the agent is installed:

1. On the Azure VM, in the C:\WindowsAzure\Packages folder, you should see the WaAppAgent.exe file.
2. Right-click the file, and in **Properties**, select the **Details** tab.
3. Verify that the **Product Version** field shows 2.6.1198.718 or higher.

[Learn more](#) about agent installation for Windows.

Install the agent on Linux VMs

Install the [Azure Linux VM](#) agent manually as follows:

1. Make sure you have admin permissions on the machine.
2. We strongly recommend that you install the Linux VM agent using an RPM or a DEB package from your distribution's package repository. All the [endorsed distribution providers](#) integrate the Azure Linux agent package into their images and repositories.

- We strongly recommend that you update the agent only through a distribution repository.
- We don't recommend installing the Linux VM agent directly from GitHub and updating it.
- If the latest agent for your distribution is not available, contact distribution support for instructions on how to install it.

Validate the installation

1. Run this command: **ps -e** to ensure that the Azure agent is running on the Linux VM.

2. If the process isn't running, restart it by using the following commands:

- For Ubuntu: **service walinuxagent start**
- For other distributions: **service waagent start**

Uninstall the Mobility service

1. Manually uninstall the Mobility service from the Azure VM, using one of the following methods.

- For Windows, in the Control Panel > **Add/Remove Programs**, uninstall **Microsoft Azure Site Recovery Mobility Service/Master Target server**. At an elevated command prompt, run:

```
MsiExec.exe /qn /x {275197FC-14FD-4560-A5EB-38217F80CBD1} /L+*V  
"C:\ProgramData\ASRSetupLogs\UnifiedAgentMSIUninstall.log"
```

- For Linux, sign in as a root user. In a terminal, go to **/user/local/ASR**, and run the following command:

```
./uninstall.sh -Y
```

2. Restart the VM before you configure replication.

Next steps

Review [troubleshooting](#) for the Site Recovery extension on the Azure VM agent. [Quickly replicate an Azure VM to a secondary region](#).

Automatic update of the Mobility service in Azure-to-Azure replication

12/11/2019 • 11 minutes to read • [Edit Online](#)

Azure Site Recovery uses a monthly release cadence to fix any issues and enhance existing features or add new ones. To remain current with the service, you must plan for patch deployment each month. To avoid overhead associated with each upgrade, you can instead allow Site Recovery to manage component updates.

As mentioned in [Azure-to-Azure disaster recovery architecture](#), the Mobility service is installed on all Azure virtual machines (VMs) for which replication is enabled, while replicating VMs from one Azure region to another. When you use automatic updates, each new release updates the Mobility service extension.

NOTE

This article has been updated to use the new Azure PowerShell Az module. You can still use the AzureRM module, which will continue to receive bug fixes until at least December 2020. To learn more about the new Az module and AzureRM compatibility, see [Introducing the new Azure PowerShell Az module](#). For Az module installation instructions, see [Install Azure PowerShell](#).

How automatic updates work

When you use Site Recovery to manage updates, it deploys a global runbook (used by Azure services) via an automation account, created in the same subscription as the vault. Each vault uses one automation account. The runbook checks for each VM in a vault for active auto-updates and upgrades the Mobility service extension if a newer version is available.

The default runbook schedule recurs daily at 12:00 AM in the time zone of the replicated VM's geo. You can also change the runbook schedule via the automation account.

NOTE

Starting with Update Rollup 35, you can choose an existing automation account to use for updates. Prior to this update, Site Recovery created this account by default. Note that you can only select this option when you enable replication for a VM. It isn't available for a replicating VM. The setting you select will apply for all Azure VMs protected in the same vault.

Turning on automatic updates doesn't require a restart of your Azure VMs or affect ongoing replication.

Job billing in the automation account is based on the number of job runtime minutes used in a month. By default, 500 minutes are included as free units for an automation account. Job execution takes a few seconds to about a minute each day and is covered as free units.

FREE UNITS INCLUDED (EACH MONTH)	PRICE
Job runtime 500 minutes	₹0.14/minute

Enable automatic updates

You can allow Site Recovery to manage updates in the following ways.

Manage as part of the enable replication step

When you enable replication for a VM either starting [from the VM view](#) or [from the recovery services vault](#), you can either allow Site Recovery to manage updates for the Site Recovery extension or manage it manually.

Configure disaster recovery - PREVIEW
ad-primary-dc

 **Welcome to Azure Site Recovery**
You can replicate your virtual machines to another Azure region for business continuity and disaster recovery needs. You can conduct periodic DR drills to ensure you meet the compliance needs. The VM will be replicated with the specified settings to the selected region so that you can recover your applications in the event of outages in source region. [Learn more about Azure Site Recovery.](#)

* Target region
Central US

Target settings

SOURCE	TARGET
VM resource group	MercuryPMDemo (new) MercuryPMDemo-asr
Availability set	ADAVALABILITYSET (new) ADAVALABILITYSET-asr
Virtual network	autohaVNETz3l3b (new) autohaVNETz3l3b-asr

Storage settings [\[+\] Show details](#)
1 new target storage account(s), 1 new cache storage accounts(s) will be created.

Replication settings [\[+\] Show details](#)
An existing recovery services vault will be used and a new replication policy will be created.

Extension settings [\[-\] Hide details](#)

Update settings	Allow ASR to manage
Automation account	igniteoff-asr-automationaccount

Enable replication

Toggle the extension update settings inside the vault

1. Inside the vault, go to **Manage > Site Recovery Infrastructure**.
2. Under **For Azure Virtual Machines > Extension Update Settings**, turn on the **Allow Site Recovery to manage** toggle. To manage manually, turn it off.
3. Select **Save**.

The screenshot shows the Azure Recovery Services vault interface. On the left, there's a navigation pane with sections like 'Locks', 'Automation script', 'GETTING STARTED', 'Backup', 'Site Recovery', 'MONITORING AND REPORTS', 'Jobs', 'Alerts and Events', 'Backup Reports', 'POLICIES', 'Backup policies', 'PROTECTED ITEMS', 'Backup items', 'Replicated items', 'MANAGE', and 'Site Recovery Infrastructure' (which is highlighted with a red box). On the right, there's a 'Extension update settings' page with a 'FOR AZURE VIRTUAL MACHINES' section containing 'Network Mapping' and 'Replication Policies' (both with arrows), and 'Extension Update Settings' (also with an arrow and highlighted with a red box). Below that are sections for 'FOR SYSTEM CENTER VMM', 'FOR VMWARE & PHYSICAL MACHINES', and 'FOR HYPER-V SITES'. At the bottom right is a 'Save' button and a note about Site Recovery leveraging an automation account to manage extensions.

IMPORTANT

When you choose **Allow Site Recovery to manage**, the setting is applied to all VMs in the corresponding vault.

NOTE

Either option notifies you of the automation account used for managing updates. If you're using this feature in a vault for the first time, a new automation account is created by default. Alternately, you can customize the setting, and choose an existing automation account. All subsequent enable replications in the same vault use the previously created one. Currently the drop-down will only list Automation accounts that are in the same Resource Group as the vault.

IMPORTANT

The below script needs to be run in the context of an automation account For a custom automation account, use the following script:

```
param(
    [Parameter(Mandatory=$true)]
    [String] $VaultResourceId,
    [Parameter(Mandatory=$true)]
    [ValidateSet("Enabled",'Disabled')]
    [Alias("Enabled or Disabled")]
    [String] $AutoUpdateAction,
    [Parameter(Mandatory=$false)]
    [String] $AutomationAccountArmId
)
```

```

$SiteRecoveryRunbookName = "Modify-AutoUpdateForVaultForPatner"
$TaskId = [guid]::NewGuid().ToString()
$SubscriptionId = "00000000-0000-0000-0000-000000000000"
$AsrApiVersion = "2018-01-10"
$RunAsConnectionName = "AzureRunAsConnection"
$ArmEndPoint = "https://management.azure.com"
$AadAuthority = "https://login.windows.net/"
$AadAudience = "https://management.core.windows.net/"
$AzureEnvironment = "AzureCloud"
$Timeout = "160"

function Throw-TerminatingErrorMessage
{
    Param
    (
        [Parameter(Mandatory=$true)]
        [String]
        $Message
    )

    throw ("Message: {0}, TaskId: {1}.") -f $Message, $TaskId
}

function Write-Tracing
{
    Param
    (
        [Parameter(Mandatory=$true)]
        [ValidateSet("Informational", "Warning", "ErrorLevel", "Succeeded", IgnoreCase = $true)]
        [String]
        $Level,
        [Parameter(Mandatory=$true)]
        [String]
        $Message,
        [Switch]
        $DisplayMessageToUser
    )

    Write-Output $Message
}

function Write-InformationTracing
{
    Param
    (
        [Parameter(Mandatory=$true)]
        [String]
        $Message
    )

    Write-Tracing -Message $Message -Level Informational -DisplayMessageToUser
}

function ValidateInput()
{
    try
    {
        if(!$VaultResourceId.StartsWith("/subscriptions", [System.StringComparison]::OrdinalIgnoreCase))
        {
            $ErrorMessage = "The vault resource id should start with /subscriptions."
            throw $ErrorMessage
        }

        $Tokens = $VaultResourceId.SubString(1).Split("/")
        if(!($Tokens.Count % 2 -eq 0))
        {

```

```

        $ErrorMessage = ("Odd Number of tokens: {0}." -f $Tokens.Count)
        throw $ErrorMessage
    }

    if(!$Tokens.Count/2 -eq 4))
    {
        $ErrorMessage = ("Invalid number of resource in vault ARM id expected:4, actual:{0}." -f
($Tokens.Count/2))
        throw $ErrorMessage
    }

    if($AutoUpdateAction -ieq "Enabled" -and [string]::IsNullOrEmpty($AutomationAccountArmId))
    {
        $ErrorMessage = ("The automation account ARM id should not be null or empty when AutoUpdateAction
is enabled.")
        throw $ErrorMessage
    }
}
catch
{
    $ErrorMessage = ("ValidateInput failed with [Exception: {0}]." -f $_.Exception)
    Write-Tracing -Level ErrorLevel -Message $ErrorMessage -DisplayMessageToUser
    Throw-TerminatingErrorMessage -Message $ErrorMessage
}
}

function Initialize-SubscriptionId()
{
    try
    {
        $Tokens = $VaultResourceId.SubString(1).Split("/")

        $Count = 0
        $ArmResources = @{}
        while($Count -lt $Tokens.Count)
        {
            $ArmResources[$Tokens[$Count]] = $Tokens[$Count+1]
            $Count = $Count + 2
        }

        return $ArmResources["subscriptions"]
    }
    catch
    {
        Write-Tracing -Level ErrorLevel -Message ("Initialize-SubscriptionId: failed with [Exception: {0}]." -
f $_.Exception) -DisplayMessageToUser
        throw
    }
}

function Invoke-InternalRestMethod($Uri, $Headers, [ref]$Result)
{
    $RetryCount = 0
    $MaxRetry = 3
    do
    {
        try
        {
            $ResultObject = Invoke-RestMethod -Uri $Uri -Headers $Headers
            ($Result.Value) += ($ResultObject)
            break
        }
        catch
        {
            Write-InformationTracing ("Retry Count: {0}, Exception: {1}." -f $RetryCount, $_.Exception)
            $RetryCount++
            if(!$RetryCount -le $MaxRetry)
            {
                throw
            }
        }
    }
}

```

```

        }

        Start-Sleep -Milliseconds 2000
    }
}while($true)
}

function Invoke-InternalWebRequest($Uri, $Headers, $Method, $Body, $ContentType, [ref]$Result)
{
    $RetryCount = 0
    $MaxRetry = 3
    do
    {
        try
        {
            $ResultObject = Invoke-WebRequest -Uri $UpdateUrl -Headers $Header -Method 'PATCH' `

                -Body $InputJson -ContentType "application/json" -UseBasicParsing
            ($Result.Value) += ($ResultObject)
            break
        }
        catch
        {
            Write-InformationTracing ("Retry Count: {0}, Exception: {1}." -f $RetryCount, $_.Exception)
            $RetryCount++
            if(!$RetryCount -le $MaxRetry)
            {
                throw
            }
        }

        Start-Sleep -Milliseconds 2000
    }
}while($true)
}

function Get-Header([ref]$Header, $AadAudience, $AadAuthority, $RunAsConnectionName){
try
{
    $RunAsConnection = Get-AutomationConnection -Name $RunAsConnectionName
    $TenantId = $RunAsConnection.TenantId
    $ApplicationId = $RunAsConnection.ApplicationId
    $CertificateThumbprint = $RunAsConnection.CertificateThumbprint
    $Path = "cert:\CurrentUser\My\{0}" -f $CertificateThumbprint
    $Secret = Get-ChildItem -Path $Path
    $ClientCredential = New-Object
    Microsoft.IdentityModel.Clients.ActiveDirectory.ClientAssertionCertificate(
        $ApplicationId,
        $Secret)

    # Trim the forward slash from the AadAuthority if it exist.
    $AadAuthority = $AadAuthority.TrimEnd("/")
    $AuthContext = New-Object Microsoft.IdentityModel.Clients.ActiveDirectory.AuthenticationContext(
        "{0}/{1}" -f $AadAuthority, $TenantId )
    $AuthenticationResult = $AuthContext.AcquireToken($AadAudience, $ClientCredential)
    $Header.Value['Content-Type'] = 'application\json'
    $Header.Value['Authorization'] = $AuthenticationResult.CreateAuthorizationHeader()
    $Header.Value["x-ms-client-request-id"] = $TaskId + "/" + (New-Guid).ToString() + "-" + (Get-
Date).ToString("u")
    }
    catch
    {
        $ErrorMessage = ("Get-BearerToken: failed with [Exception: {0}]." -f $_.Exception)
        Write-Tracing -Level ErrorLevel -Message $ErrorMessage -DisplayMessageToUser
        Throw-TerminatingErrorMessage -Message $ErrorMessage
    }
}

function Get-ProtectionContainerToBeModified([ref] $ContainerMappingList)
{

```

```

try
{
    Write-InformationTracing ("Get protection container mappings : {0}." -f $VaultResourceId)
    $ContainerMappingListUrl = $ArmEndPoint + $VaultResourceId + "/replicationProtectionContainerMappings"
    + "?api-version=" + $AsrApiVersion

    Write-InformationTracing ("Getting the bearer token and the header.")
    Get-Header ([ref]$Header) $AadAudience $AadAuthority $RunAsConnectionName

    $Result = @()
    Invoke-InternalRestMethod -Uri $ContainerMappingListUrl -Headers $header -Result ([ref]$Result)
    $ContainerMappings = $Result[0]

    Write-InformationTracing ("Total retrieved container mappings: {0}." -f
$ContainerMappings.Value.Count)
    foreach($Mapping in $ContainerMappings.Value)
    {
        if(($Mapping.properties.providerSpecificDetails -eq $null) -or
($Mapping.properties.providerSpecificDetails.instanceType -ine "A2A"))
        {
            Write-InformationTracing ("Mapping properties: {0}." -f ($Mapping.properties))
            Write-InformationTracing ("Ignoring container mapping: {0} as the provider does not match." -f
($Mapping.Id))
            continue;
        }

        if($Mapping.Properties.State -ine "Paired")
        {
            Write-InformationTracing ("Ignoring container mapping: {0} as the state is not paired." -f
($Mapping.Id))
            continue;
        }

        Write-InformationTracing ("Provider specific details {0}." -f
($Mapping.properties.providerSpecificDetails))
        $MappingAutoUpdateStatus = $Mapping.properties.providerSpecificDetails.agentAutoUpdateStatus
        $MappingAutomationAccountArmId =
$Mapping.properties.providerSpecificDetails.automationAccountArmId
        $MappingHealthErrorCount = $Mapping.properties.HealthErrorDetails.Count

        if($AutoUpdateAction -ieq "Enabled" -and
            ($MappingAutoUpdateStatus -ieq "Enabled") -and
            ($MappingAutomationAccountArmId -ieq $AutomationAccountArmId) -and
            ($MappingHealthErrorCount -eq 0))
        {
            Write-InformationTracing ("Provider specific details {0}." -f ($Mapping.properties))
            Write-InformationTracing ("Ignoring container mapping: {0} as the auto update is already
enabled and is healthy." -f ($Mapping.Id))
            continue;
        }

        ($ContainerMappingList.Value).Add($Mapping.id)
    }
}
catch
{
    $ErrorMessage = ("Get-ProtectionContainerToBeModified: failed with [Exception: {0}]." -f $_.Exception)
    Write-Tracing -Level ErrorLevel -Message $ErrorMessage -DisplayMessageToUser
    Throw-TerminatingErrorMessage -Message $ErrorMessage
}

$OperationStartTime = Get-Date
$ContainerMappingList = New-Object System.Collections.Generic.List[System.String]
$JobsInProgressList = @()
$JobsCompletedSuccessList = @()
$JobsCompletedFailedList = @()
$JobsFailedToStart = 0
$JobsTimedOut = 0

```

```

$header = @{}

$AzureRMPProfile = Get-Module -ListAvailable -Name AzureRM.Profile | Select Name, Version, Path
$AzureRmProfileModulePath = Split-Path -Parent $AzureRMPProfile.Path
Add-Type -Path (Join-Path $AzureRmProfileModulePath "Microsoft.IdentityModel.Clients.ActiveDirectory.dll")

$Inputs = ("Tracing inputs VaultResourceId: {0}, Timeout: {1}, AutoUpdateAction: {2}, AutomationAccountArmId: {3}." -f $VaultResourceId, $Timeout, $AutoUpdateAction, $AutomationAccountArmId)
Write-Tracing -Message $Inputs -Level Informational -DisplayMessageToUser
$CloudConfig = ("Tracing cloud configuration ArmEndPoint: {0}, AadAuthority: {1}, AadAudience: {2}." -f $ArmEndPoint, $AadAuthority, $AadAudience)
Write-Tracing -Message $CloudConfig -Level Informational -DisplayMessageToUser
$AutomationConfig = ("Tracing automation configuration RunAsConnectionName: {0}." -f $RunAsConnectionName)
Write-Tracing -Message $AutomationConfig -Level Informational -DisplayMessageToUser

ValidateInput
$SubscriptionId = Initialize-SubscriptionId
Get-ProtectionContainerToBeModified ([ref]$ContainerMappingList)

$input = @{
    "properties" = @{
        "providerSpecificInput" = @{
            "instanceType" = "A2A"
            "agentAutoUpdateStatus" = $AutoUpdateAction
            "automationAccountArmId" = $AutomationAccountArmId
        }
    }
}
$inputJson = $input | ConvertTo-Json

if ($ContainerMappingList.Count -eq 0)
{
    Write-Tracing -Level Succeeded -Message ("Exiting as there are no container mappings to be modified.") -DisplayMessageToUser
    exit
}

Write-InformationTracing ("Container mappings to be updated has been retrieved with count: {0}." -f $ContainerMappingList.Count)

try
{
    Write-InformationTracing ("Start the modify container mapping jobs.")
    ForEach($Mapping in $ContainerMappingList)
    {
        try {
            $updateUrl = $ArmEndPoint + $Mapping + "?api-version=" + $AsrApiVersion
            Get-Header ([ref]$header) $AadAudience $AadAuthority $RunAsConnectionName

            $result = @()
            Invoke-InternalWebRequest -Uri $updateUrl -Headers $header -Method 'PATCH' ` 
                -Body $inputJson -ContentType "application/json" -Result ([ref]$result)
            $result = $result[0]

            $jobAsyncUrl = $result.Headers['Azure-AsyncOperation']
            Write-InformationTracing ("The modify container mapping job invoked with async url: {0}." -f $jobAsyncUrl)
            $jobsInProgressList += $jobAsyncUrl;

            # Rate controlling the set calls to maximum 60 calls per minute.
            # ASR throttling for set calls is 200 in 1 minute.
            Start-Sleep -Milliseconds 1000
        }
        catch{
            Write-InformationTracing ("The modify container mappings job creation failed for: {0}." -f $ru)
            Write-InformationTracing $_
            $jobsFailedToStart++
        }
    }
}

```

```

        Write-InformationTracing ("Total modify container mappings has been initiated: {0}." -f
        $JobsInProgressList.Count)
    }
    catch
    {
        $ErrorMessage = ("Modify container mapping jobs failed with [Exception: {0}]." -f $_.Exception)
        Write-Tracing -Level ErrorLevel -Message $ErrorMessage -DisplayMessageToUser
        Throw-TerminatingErrorMessage -Message $ErrorMessage
    }

    try
    {
        while($JobsInProgressList.Count -ne 0)
        {
            Sleep -Seconds 30
            $JobsInProgressListInternal = @()
            ForEach($JobAsyncUrl in $JobsInProgressList)
            {
                try
                {
                    Get-Header ([ref]$Header) $AadAudience $AadAuthority $RunAsConnectionName
                    $Result = Invoke-RestMethod -Uri $JobAsyncUrl -Headers $header
                    $JobState = $Result.Status
                    if($JobState -ieq "InProgress")
                    {
                        $JobsInProgressListInternal += $JobAsyncUrl
                    }
                    elseif($JobState -ieq "Succeeded" -or `
                            $JobState -ieq "PartiallySucceeded" -or `
                            $JobState -ieq "CompletedWithInformation")
                    {
                        Write-InformationTracing ("Jobs succeeded with state: {0}." -f $JobState)
                        $JobsCompletedSuccessList += $JobAsyncUrl
                    }
                    else
                    {
                        Write-InformationTracing ("Jobs failed with state: {0}." -f $JobState)
                        $JobsCompletedFailedList += $JobAsyncUrl
                    }
                }
                catch
                {
                    Write-InformationTracing ("The get job failed with: {0}. Ignoring the exception and retrying
                    the next job." -f $_.Exception)

                    # The job on which the tracking failed, will be considered in progress and tried again later.
                    $JobsInProgressListInternal += $JobAsyncUrl
                }
            }

            # Rate controlling the get calls to maximum 120 calls each minute.
            # ASR throttling for get calls is 10000 in 60 minutes.
            Start-Sleep -Milliseconds 500
        }

        Write-InformationTracing ("Jobs remaining {0}." -f $JobsInProgressListInternal.Count)

        $CurrentTime = Get-Date
        if($CurrentTime -gt $OperationStartTime.AddMinutes($Timeout))
        {
            Write-InformationTracing ("Tracing modify cloud pairing jobs has timed out.")
            $JobsTimedOut = $JobsInProgressListInternal.Count
            $JobsInProgressListInternal = @()
        }

        $JobsInProgressList = $JobsInProgressListInternal
    }
}
catch
{

```

```

{
    $ErrorMessage = ("Tracking modify cloud pairing jobs failed with [Exception: {0}]." -f $_.Exception)
    Write-Tracing -Level ErrorLevel -Message $ErrorMessage -DisplayMessageToUser
    Throw-TerminatingErrorMessage -Message $ErrorMessage
}

Write-InformationTracing ("Tracking modify cloud pairing jobs completed.")
Write-InformationTracing ("Modify cloud pairing jobs success: {0}." -f $JobsCompletedSuccessList.Count)
Write-InformationTracing ("Modify cloud pairing jobs failed: {0}." -f $JobsCompletedFailedList.Count)
Write-InformationTracing ("Modify cloud pairing jobs failed to start: {0}." -f $JobsFailedToStart)
Write-InformationTracing ("Modify cloud pairing jobs timedout: {0}." -f $JobsTimedOut)

if($JobsTimedOut -gt 0)
{
    $ErrorMessage = "One or more modify cloud pairing jobs has timedout."
    Write-Tracing -Level ErrorLevel -Message ($ErrorMessage)
    Throw-TerminatingErrorMessage -Message $ErrorMessage
}
elseif($JobsCompletedSuccessList.Count -ne $ContainerMappingList.Count)
{
    $ErrorMessage = "One or more modify cloud pairing jobs failed."
    Write-Tracing -Level ErrorLevel -Message ($ErrorMessage)
    Throw-TerminatingErrorMessage -Message $ErrorMessage
}

Write-Tracing -Level Succeeded -Message ("Modify cloud pairing completed.") -DisplayMessageToUser

```

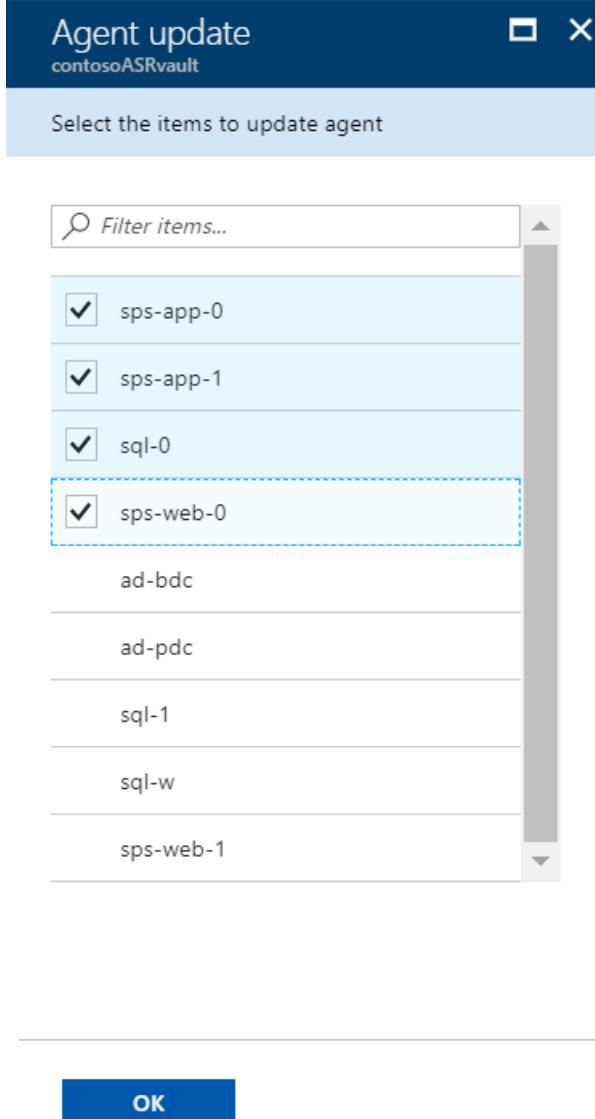
Manage updates manually

- If there are new updates for the Mobility service installed on your VMs, you'll see the following notification: "New Site Recovery replication agent update is available. Click to install"

The screenshot shows a user interface for managing Site Recovery replication agents. At the top, there are navigation buttons: Refresh, Replicate, Columns, and Filter. A prominent yellow notification bar at the top states: "⚠ New Mobility Service Update is available. Push install latest update on every physical and virtual machine →". Below this, a message says "Last refreshed at: 11/14/2019, 9:34:41 AM". A progress bar indicates "Finished loading data from service." A search bar labeled "Filter items..." is present. A table below lists replication agents with columns: Name, Replication Health, Status, Active location, and an ellipsis (...). One row is shown with the name "VM1", replication health as "Healthy", status as "Protected", active location as "Datacenter", and a three-dot menu icon.

Name	Replication Health	Status	Active location	...
VM1	Healthy	Protected	Datacenter	...

- Select the notification to open the VM selection page.
- Choose the VMs you want to upgrade, and then select **OK**. The Update Mobility service will start for each selected VM.



Common issues and troubleshooting

If there's an issue with the automatic updates, you'll see an error notification under **Configuration issues** in the vault dashboard.

If you couldn't enable automatic updates, see the following common errors and recommended actions:

- **Error:** You do not have permissions to create an Azure Run As account (service principal) and grant the Contributor role to the service principal.

Recommended action: Make sure that the signed-in account is assigned as Contributor and try again. Refer to the required permissions section in [Use the portal to create an Azure AD application and service principal that can access resources](#) for more information about assigning permissions.

To fix most issues after you enable automatic updates, select **Repair**. If the repair button isn't available, see the error message displayed in the extension update settings pane.

The screenshot shows the Azure Site Recovery Infrastructure extension update settings. The left pane is a navigation menu with various sections like 'SETTINGS', 'GETTING STARTED', 'MONITORING AND REPORTS', 'POLICIES', 'PROTECTED ITEMS', 'MANAGE', and 'SUPPORT + TROUBLESHOOTING'. The 'Site Recovery Infrastructure' option under 'MANAGE' is selected. The right pane shows 'Extension update settings' with a status message: 'Auto update settings is un-healthy'. A red box highlights this message, and a 'Repair' button is visible next to it.

- **Error:** The Run As account does not have the permission to access the recovery services resource.

Recommended action: Delete and then [re-create the Run As account](#). Or, make sure that the Automation Run As account's Azure Active Directory application has access to the recovery services resource.

- **Error:** Run As account is not found. Either one of these was deleted or not created - Azure Active Directory Application, Service Principal, Role, Automation Certificate asset, Automation Connection asset - or the Thumbprint is not identical between Certificate and Connection.

Recommended action: Delete and then [re-create the Run As account](#).

- **Error:** The Azure Run as Certificate used by the automation account is about to expire.

The self-signed certificate that is created for the Run As account expires one year from the date of creation. You can renew it at any time before it expires. If you have signed up for email notifications, you will also receive emails when an action is required from your side. This error will be shown two months prior to the expiry date, and will change to a critical error if the certificate has expired. Once the certificate has expired, auto update will not be functional until you renew the same.

Recommended action: Click on 'Repair' and then 'Renew Certificate' to resolve this issue.

Azure Run As... Properties

Renew certificate... Delete

Azure Active Directory Application ⓘ

Display Name
TestAutomationAcct_KCulYt0ehOmNcWC

Certificate ⓘ

Name
AzureRunAsCertificate

Expiration
30/01/2018 19:00

NOTE

Once you renew the certificate, please refresh the page so that the current status is updated.

Service updates in Site Recovery

9/11/2019 • 4 minutes to read • [Edit Online](#)

This article provides an overview of [Azure Site Recovery](#) updates, and describes how to upgrade Site Recovery components.

Site Recovery publishes service updates on a regular basis. Updates include new features, support improvements, component updates, and bug fixes. In order to take advantage of the latest features and fixes, we recommend running the latest versions of Site Recovery components.

Updates support

Support statement for Azure Site Recovery

We recommend always upgrading to the latest component versions:

With every new version 'N' of an Azure Site Recovery component that's released, all versions below 'N-4' are considered to be out of support.

IMPORTANT

Official support is for upgrading from > N-4 version to N version. For example, if you're running you are on N-6, you need to first upgrade to N-4, and then upgrade to N.

Links to currently supported update rollups

Review the latest update rollup (version N) in [this article](#). Remember that Site Recovery provides support for N-4 versions.

Component expiry

Site Recovery notifies you of expired components (or nearing expiry) by email (if you subscribed to email notifications), or on the vault dashboard in the portal.

- In addition, when updates are available, in the infrastructure view for your scenario in the portal, an **Update available** button appears next to the component. This button redirects you to a link for downloading the latest component version.
- Vaults dashboard notifications aren't available if you're replicating Hyper-V VMs.

Emails notifications are sent as follows.

TIME	FREQUENCY
60 days before component expiry	Once bi-weekly
Next 53 days	Once a week
Last 7 days	Once a day
After expiry	Once bi-weekly

Upgrading outside official support

If the difference between your component version and the latest release version is greater than four, this is considered out of support. In this case, upgrade as follows:

1. Upgrade the currently installed component to your current version plus four. For example, if your version is 9.16, then upgrade to 9.20.
2. Then, upgrade to the next compatible version. So in our example, after upgrading 9.16 to 9.20, upgrade to 9.24.

Follow the same process for all relevant components.

Support for latest operating systems/kernels

NOTE

If you have a maintenance window scheduled, and a reboot is included in it, we recommend that you first upgrade Site Recovery components, and then proceed with the rest of the scheduled activities in the maintenance window.

1. Before upgrading operating system/kernel versions, verify if the target version is supported Site Recovery.
 - Azure VM support.
 - VMware/physical server support
 - Hyper-V support.
2. Review [available updates](#) to find out what you want to upgrade.
3. Upgrade to the latest Site Recovery version.
4. Upgrade the operating system/kernel to the required versions.
5. Reboot.

This process ensures that the machine operating system/kernel is upgraded to the latest version, and that the latest Site Recovery changes needed to support the new version are loaded on to the machine.

Azure VM disaster recovery to Azure

In this scenario, we strongly recommend that you [enable automatic updates](#). You can allow Site Recovery to manage updates as follows:

- During the enable replication process.
- By setting the extension update settings inside the vault.

If you want to manually manage updates, do the following:

1. In the vault > **Replicated Items**, click this notification at the top of the screen:
New Site Recovery replication agent update is available. Click to install ->
2. Select the VMs for which you want to apply the update, and then click **OK**.

VMware VM/physical server disaster recovery to Azure

1. Based on your current version and the [support statement](#), install the update first on the on-premises configuration server, using [these instructions](#).
2. If you have scale-out process servers, update them next, using [these instructions](#).
3. To update the Mobility agent on each protected machine, refer to [this article](#).

Reboot after Mobility service upgrade

A reboot is recommended after every upgrade of the Mobility service, to ensure that all the latest changes are

loaded on the source machine.

A reboot isn't mandatory, unless the difference between the agent version during last reboot, and the current version, is greater than four.

The example in the table shows how this works.

AGENT VERSION (LAST REBOOT)	UPGRADE TO	MANDATORY REBOOT?
9.16	9.18	Not mandatory
9.16	9.19	Not mandatory
9.16	9.20	Not mandatory
9.16	9.21	Mandatory. Upgrade to 9.20, then reboot before upgrading to 9.21.

Hyper-V VM disaster recovery to Azure

Between a Hyper-V site and Azure

1. Download the update for the Microsoft Azure Site Recovery Provider.
2. Install the Provider on each Hyper-V server registered in Site Recovery. If you're running a cluster, upgrade on all cluster nodes.

Between an on-premises VMM site and Azure

1. Download the update for the Microsoft Azure Site Recovery Provider.
2. Install the Provider on the VMM server. If VMM is deployed in a cluster, install the Provider on all cluster nodes.
3. Install the latest Microsoft Azure Recovery Services agent on all Hyper-V hosts or cluster nodes.

Between two on-premises VMM sites

1. Download the latest update for the Microsoft Azure Site Recovery Provider.
2. Install the latest Provider on the VMM server managing the secondary recovery site. If VMM is deployed in a cluster, install the Provider on all cluster nodes.
3. After the recovery site is updated, install the Provider on the VMM server that's managing the primary site.

Next steps

Follow our [Azure Updates](#) page to track new updates and releases.

Remove servers and disable protection

7/14/2019 • 8 minutes to read • [Edit Online](#)

This article describes how to unregister servers from a Recovery Services vault, and how to disable protection for machines protected by Site Recovery.

Unregister a configuration server

If you replicate VMware VMs or Windows/Linux physical servers to Azure, you can unregister an unconnected configuration server from a vault as follows:

1. [Disable protection of virtual machines](#).
2. [Disassociate or delete replication policies](#).
3. [Delete the configuration server](#)

Unregister a VMM server

1. Stop replicating virtual machines in clouds on the VMM server you want to remove.
2. Delete any network mappings used by clouds on the VMM server that you want to delete. In **Site Recovery Infrastructure > For System Center VMM > Network Mapping**, right-click the network mapping > **Delete**.
3. Note the ID of the VMM server.
4. Disassociate replication policies from clouds on the VMM server you want to remove. In **Site Recovery Infrastructure > For System Center VMM > Replication Policies**, double-click the associated policy. Right-click the cloud > **Disassociate**.
5. Delete the VMM server or active node. In **Site Recovery Infrastructure > For System Center VMM > VMM Servers**, right-click the server > **Delete**.
6. If your VMM server was in a Disconnected state, then download and run the [cleanup script](#) on the VMM server. Open PowerShell with the **Run as Administrator** option, to change the execution policy for the default (LocalMachine) scope. In the script, specify the ID of the VMM server you want to remove. The script removes registration and cloud pairing information from the server.
7. Run the cleanup script on any secondary VMM server.
8. Run the cleanup script on any other passive VMM cluster nodes that have the Provider installed.
9. Uninstall the Provider manually on the VMM server. If you have a cluster, remove from all nodes.
10. If your virtual machines were replicating to Azure, you need to uninstall the Microsoft Recovery Services agent from Hyper-V hosts in the deleted clouds.

Unregister a Hyper-V host in a Hyper-V Site

Hyper-V hosts that aren't managed by VMM are gathered into a Hyper-V site. Remove a host in a Hyper-V site as follows:

1. Disable replication for Hyper-V VMs located on the host.
2. Disassociate policies for the Hyper-V site. In **Site Recovery Infrastructure > For Hyper-V Sites > Replication Policies**, double-click the associated policy. Right-click the site > **Disassociate**.
3. Delete Hyper-V hosts. In **Site Recovery Infrastructure > For Hyper-V Sites > Hyper-V Hosts**, right-click the server > **Delete**.
4. Delete the Hyper-V site after all hosts have been removed from it. In **Site Recovery Infrastructure > For Hyper-V Sites > Hyper-V Sites**, right-click the site > **Delete**.

5. If your Hyper-V host was in a **Disconnected** state, then run the following script on each Hyper-V host that you removed. The script cleans up settings on the server, and unregisters it from the vault.

```

pushd .
try
{
    $windowsIdentity=[System.Security.Principal.WindowsIdentity]::GetCurrent()
    $principal=new-object System.Security.Principal.WindowsPrincipal($windowsIdentity)
    $administrators=[System.Security.Principal.WindowsBuiltInRole]::Administrator
    $isAdmin=$principal.IsInRole($administrators)
    if (!$isAdmin)
    {
        "Please run the script as an administrator in elevated mode."
        $choice = Read-Host
        return;
    }

    $error.Clear()
    "This script will remove the old Azure Site Recovery Provider related properties. Do you want to
continue (Y/N) ?"
    $choice = Read-Host

    if (!($choice -eq 'Y' -or $choice -eq 'y'))
    {
        "Stopping cleanup."
        return;
    }

    $serviceName = "dra"
    $service = Get-Service -Name $serviceName
    if ($service.Status -eq "Running")
    {
        "Stopping the Azure Site Recovery service..."
        net stop $serviceName
    }

    $asrHivePath = "HKLM:\SOFTWARE\Microsoft\Azure Site Recovery"
    $registrationPath = $asrHivePath + '\Registration'
    $proxySettingsPath = $asrHivePath + '\ProxySettings'
    $draIdvalue = 'DraID'
    $idMgmtCloudContainerId='IdMgmtCloudContainerId'

    if (Test-Path $asrHivePath)
    {
        if (Test-Path $registrationPath)
        {
            "Removing registration related registry keys."
            Remove-Item -Recurse -Path $registrationPath
        }

        if (Test-Path $proxySettingsPath)
        {
            "Removing proxy settings"
            Remove-Item -Recurse -Path $proxySettingsPath
        }

        $regNode = Get-ItemProperty -Path $asrHivePath
        if($regNode.DraID -ne $null)
        {
            "Removing DraId"
            Remove-ItemProperty -Path $asrHivePath -Name $draIdValue
        }
        if($regNode.IdMgmtCloudContainerId -ne $null)
        {
            "Removing IdMgmtCloudContainerId"
            Remove-ItemProperty -Path $asrHivePath -Name $idMgmtCloudContainerId
        }
    }
}

```

```

        }
        "Registry keys removed."
    }

    # First retrieve all the certificates to be deleted
    $ASRcerts = Get-ChildItem -Path cert:\localmachine\my | where-object
    {$_.friendlyname.startswith('ASR_SRSAUTH_CERT_KEY_CONTAINER') -or
    $_.friendlyname.startswith('ASR_HYPER_V_HOST_CERT_KEY_CONTAINER')}
    # Open a cert store object
    $store = New-Object System.Security.Cryptography.X509Certificates.X509Store("My", "LocalMachine")
    $store.Open('ReadWrite')
    # Delete the certs
    "Removing all related certificates"
    foreach ($cert in $ASRcerts)
    {
        $store.Remove($cert)
    }
}catch
{
    [system.exception]
    Write-Host "Error occurred" -ForegroundColor "Red"
    $error[0]
    Write-Host "FAILED" -ForegroundColor "Red"
}
popd

```

Disable protection for a VMware VM or physical server (VMware to Azure)

1. In **Protected Items > Replicated Items**, right-click the machine > **Disable replication**.
2. In **Disable replication** page, select one of these options:
 - **Disable replication and remove (recommended)** - This option removes the replicated item from Azure Site Recovery and the replication for the machine is stopped. Replication configuration on Configuration Server is cleaned up and Site Recovery billing for this protected server is stopped. Note that this option can only be used when Configuration Server is in connected state.
 - **Remove** - This option is supposed to be used only if the source environment is deleted or not accessible (not connected). This removes the replicated item from Azure Site Recovery (billing is stopped). Replication configuration on the Configuration Server **will not** be cleaned up.

NOTE

In both the options mobility service will not be uninstalled from the protected servers, you need to uninstall it manually. If you plan to protect the server again using the same Configuration server, you can skip uninstalling the mobility service.

NOTE

If you have already failed over a VM and it is running in Azure, note that disable protection doesn't remove / affect the failed over VM.

Disable protection for a Azure VM (Azure to Azure)

- In **Protected Items > Replicated Items**, right-click the machine > **Disable replication**.

NOTE

mobility service will not be uninstalled from the protected servers, you need to uninstall it manually. If you plan to protect the server again, you can skip uninstalling the mobility service.

Disable protection for a Hyper-V virtual machine (Hyper-V to Azure)

NOTE

Use this procedure if you're replicating Hyper-V VMs to Azure without a VMM server. If you are replicating your virtual machines using the **System Center VMM to Azure** scenario, then follow the instructions Disable protection for a Hyper-V virtual machine replicating using the System Center VMM to Azure scenario

1. In **Protected Items > Replicated Items**, right-click the machine > **Disable replication**.

2. In **Disable replication**, you can select the following options:

- **Disable replication and remove (recommended)** - This option removes the replicated item from Azure Site Recovery and the replication for the machine is stopped. Replication configuration on the on-premises virtual machine will be cleaned up and Site Recovery billing for this protected server is stopped.
- **Remove** - This option is supposed to be used only if the source environment is deleted or not accessible (not connected). This removes the replicated item from Azure Site Recovery (billing is stopped). Replication configuration on the on-premises virtual machine **will not** be cleaned up.

NOTE

> If you chose the **Remove** option then run the following set of scripts to clean up the replication settings on-premises Hyper-V Server.

NOTE

If you have already failed over a VM and it is running in Azure, note that disable protection doesn't remove / affect the failed over VM.

1. On the source Hyper-V host server, to remove replication for the virtual machine. Replace SQLVM1 with the name of your virtual machine and run the script from an administrative PowerShell

```
$vmName = "SQLVM1"
$vm = Get-WmiObject -Namespace "root\virtualization\v2" -Query "Select * From MsVm_ComputerSystem Where ElementName = '$vmName'"
$replicationService = Get-WmiObject -Namespace "root\virtualization\v2" -Query "Select * From MsVm_ReplicationService"
$replicationService.RemoveReplicationRelationship($vm.__PATH)
```

Disable protection for a Hyper-V virtual machine replicating to Azure using the System Center VMM to Azure scenario

1. In **Protected Items > Replicated Items**, right-click the machine > **Disable replication**.

2. In **Disable replication**, select one of these options:

- **Disable replication and remove (recommended)** - This option remove the replicated item from Azure Site Recovery and the replication for the machine is stopped. Replication configuration on the on-premises virtual machine is cleaned up and Site Recovery billing for this protected server is stopped.
- **Remove** - This option is supposed to be used only if the source environment is deleted or not accessible (not connected). This removes the replicated item from Azure Site Recovery (billing is stopped). Replication configuration on the on-premises virtual machine **will not** be cleaned up.

NOTE

If you chose the **Remove** option, then run the following scripts to clean up the replication settings on-premises VMM Server.

3. Run this script on the source VMM server, using PowerShell (administrator privileges required) from the VMM console. Replace the placeholder **SQLVM1** with the name of your virtual machine.

```
$vm = get-scvirtualmachine -Name "SQLVM1"
Set-SCVirtualMachine -VM $vm -ClearDRProtection
```

4. The above steps clear the replication settings on the VMM server. To stop replication for the virtual machine running on the Hyper-V host server, run this script. Replace SQLVM1 with the name of your virtual machine, and host01.contoso.com with the name of the Hyper-V host server.

```
$vmName = "SQLVM1"
$hostName = "host01.contoso.com"
$vm = Get-WmiObject -Namespace "root\virtualization\v2" -Query "Select * From MsVm_ComputerSystem Where ElementName = '$vmName'" -computername $hostName
$replicationService = Get-WmiObject -Namespace "root\virtualization\v2" -Query "Select * From MsVm_ReplicationService" -computername $hostName
$replicationService.RemoveReplicationRelationship($vm.__PATH)
```

Disable protection for a Hyper-V virtual machine replicating to secondary VMM Server using the System Center VMM to VMM scenario

1. In **Protected Items > Replicated Items**, right-click the machine > **Disable replication**.
2. In **Disable replication**, select one of these options:
 - **Disable replication and remove (recommended)** - This option remove the replicated item from Azure Site Recovery and the replication for the machine is stopped. Replication configuration on the on-premises virtual machine is cleaned up and Site Recovery billing for this protected server is stopped.
 - **Remove** - This option is supposed to be used only if the source environment is deleted or not accessible (not connected). This removes the replicated item from Azure Site Recovery (billing is stopped). Replication configuration on the on-premises virtual machine **will not** be cleaned up. Run the following set of scripts to clean up the replication settings on-premises virtual machines.

NOTE

If you chose the **Remove** option, then run the following scripts to clean up the replication settings on-premises VMM Server.

3. Run this script on the source VMM server, using PowerShell (administrator privileges required) from the VMM console. Replace the placeholder **SQLVM1** with the name of your virtual machine.

```
$vm = get-scvirtualmachine -Name "SQLVM1"  
Set-SCVirtualMachine -VM $vm -ClearDRProtection
```

4. On the secondary VMM server, run this script to clean up the settings for the secondary virtual machine:

```
$vm = get-scvirtualmachine -Name "SQLVM1"  
Remove-SCVirtualMachine -VM $vm -Force
```

5. On the secondary VMM server, refresh the virtual machines on the Hyper-V host server, so that the secondary VM gets detected again in the VMM console.
6. The above steps clear up the replication settings on the VMM server. If you want to stop replication for the virtual machine, run the following script on the primary and secondary VMs. Replace SQLVM1 with the name of your virtual machine.

```
Remove-VMReplication -VMName "SQLVM1"
```

Delete a Site Recovery Services vault

1/10/2020 • 2 minutes to read • [Edit Online](#)

This article describes how to delete a Recovery Services vault for Site Recovery. To delete a vault used in Azure Backup, see [Delete a Backup vault in Azure](#).

NOTE

This article has been updated to use the new Azure PowerShell Az module. You can still use the AzureRM module, which will continue to receive bug fixes until at least December 2020. To learn more about the new Az module and AzureRM compatibility, see [Introducing the new Azure PowerShell Az module](#). For Az module installation instructions, see [Install Azure PowerShell](#).

Before you start

Before you can delete a vault you must remove registered servers, and items in the vault. What you need to remove depends on the replication scenarios you've deployed.

Delete a vault-Azure VM to Azure

1. Follow [these instructions](#) to delete all protected VMs.
2. Then, delete the vault.

Delete a vault-VMware VM to Azure

1. Follow [these instructions](#) to delete all protected VMs.
2. Follow [these steps](#) to delete all replication policies.
3. Delete references to vCenter using [these steps](#).
4. Follow [these instructions](#) to decommission a configuration server.
5. Then, delete the vault.

Delete a vault-Hyper-V VM (with VMM) to Azure

1. Follow [these steps](#) to delete Hyper-V VMs managed by System Center VMM.
2. Disassociate and delete all replication policies. Do this in your vault > **Site Recovery Infrastructure > For System Center VMM > Replication Policies**.
3. Follow [these steps](#) to unregister a connected VMM server.
4. Then, delete the vault.

Delete a vault-Hyper-V VM to Azure

1. Follow [these steps](#) to delete all protected VMs.
2. Disassociate and delete all replication policies. Do this in your vault > **Site Recovery Infrastructure > For Hyper-V Sites > Replication Policies**.
3. Follow [these instructions](#) to unregister a Hyper-V host.
4. Delete the Hyper-V site.
5. Then, delete the vault.

Use PowerShell to force delete the vault

IMPORTANT

If you're testing the product and aren't concerned about data loss, use the force delete method to rapidly remove the vault and all its dependencies. The PowerShell command deletes all the contents of the vault and is **not reversible**.

To delete the Site Recovery vault even if there are protected items, use these commands:

```
Connect-AzAccount  
  
Select-AzSubscription -SubscriptionName "XXXXX"  
  
$vault = Get-AzRecoveryServicesVault -Name "vaultname"  
  
Remove-AzRecoveryServicesVault -Vault $vault
```

Learn more about [Get-AzRecoveryServicesVault](#), and [Remove-AzRecoveryServicesVault](#).

Set up disaster recovery at scale for VMware VMs/physical servers

1/10/2020 • 10 minutes to read • [Edit Online](#)

This article describes how to set up disaster recovery to Azure for large numbers (> 1000) of on-premises VMware VMs or physical servers in your production environment, using the [Azure Site Recovery](#) service.

Define your BCDR strategy

As part of your business continuity and disaster recovery (BCDR) strategy, you define recovery point objectives (RPOs) and recovery time objectives (RTOs) for your business apps and workloads. RTO measures the duration of time and service level within which a business app or process must be restored and available, in order to avoid continuity issues.

- Site Recovery provides continuous replication for VMware VMs and physical servers, and an [SLA](#) for RTO.
- As you plan for large-scale disaster recovery for VMware VMs and figure out the Azure resources you need, you can specify an RTO value that will be used for capacity calculations.

Best practices

Some general best practices for large-scale disaster recovery. These best practices are discussed in more detail in the next sections of the document.

- **Identify target requirements:** Estimate out capacity and resource needs in Azure before you set up disaster recovery.
- **Plan for Site Recovery components:** Figure out what Site Recovery components (configuration server, process servers) you need to meet your estimated capacity.
- **Set up one or more scale-out process servers:** Don't use the process server that's running by default on the configuration server.
- **Run the latest updates:** The Site Recovery team releases new versions of Site Recovery components on a regular basis, and you should make sure you're running the latest versions. To help with that, track [what's new](#) for updates, and [enable and install updates](#) as they release.
- **Monitor proactively:** As you get disaster recovery up and running, you should proactively monitor the status and health of replicated machines, and infrastructure resources.
- **Disaster recovery drills:** You should run disaster recovery drills on a regular basis. These don't impact on your production environment, but do help ensure that failover to Azure will work as expected when needed.

Gather capacity planning information

Gather information about your on-premises environment, to help assess and estimate your target (Azure) capacity needs.

- For VMware, run the Deployment Planner for VMware VMs to do this.
- For physical servers, gather the information manually.

Run the Deployment Planner for VMware VMs

The Deployment Planner helps you to gather information about your VMware on-premises environment.

- Run the Deployment Planner during a period that represents typical churn for your VMs. This will generate

more accurate estimates and recommendations.

- We recommend that you run the Deployment Planner on the configuration server machine, since the Planner calculates throughput from the server on which it's running. [Learn more](#) about measuring throughput.
- If you don't yet have a configuration server set up:
 - [Get an overview](#) of Site Recovery components.
 - [Set up a configuration server](#), in order to run the Deployment Planner on it.

Then run the Planner as follows:

1. [Learn about](#) the Deployment Planner. You can download the latest version from the portal, or [download it directly](#).
2. Review the [prerequisites](#) and [latest updates](#) for the Deployment Planner, and [download and extract](#) the tool.
3. [Run the Deployment Planner](#) on the configuration server.
4. [Generate a report](#) to summarize estimations and recommendations.
5. Analyze the [report recommendations](#) and [cost estimations](#).

NOTE

By default, the tool is configured to profile and generates report for up to 1000 VMs. You can change this limit by increasing the MaxVMsSupported key value in the ASRDeploymentPlanner.exe.config file.

Plan target (Azure) requirements and capacity

Using your gathered estimations and recommendations, you can plan for target resources and capacity. If you ran the Deployment Planner for VMware VMs, you can use a number of the [report recommendations](#) to help you.

- **Compatible VMs:** Use this number to identify the number of VMs that are ready for disaster recovery to Azure. Recommendations about network bandwidth and Azure cores are based on this number.
- **Required network bandwidth:** Note the bandwidth you need for delta replication of compatible VMs.
 - When you run the Planner you specify the desired RPO in minutes. The recommendations show you the bandwidth needed to meet that RPO 100% and 90% of the time.
 - The network bandwidth recommendations take into account the bandwidth needed for total number of configuration servers and process servers recommended in the Planner.
- **Required Azure cores:** Note the number of cores you need in the target Azure region, based on the number of compatible VMs. If you don't have enough cores, at failover Site Recovery won't be able to create the required Azure VMs.
- **Recommended VM batch size:** The recommended batch size is based on the ability to finish initial replication for the batch within 72 hours by default, while meeting an RPO of 100%. The hour value can be modified.

You can use these recommendations to plan for Azure resources, network bandwidth, and VM batching.

Plan Azure subscriptions and quotas

We want to make sure that available quotas in the target subscription are sufficient to handle failover.

TASK	DETAILS	ACTION

TASK	DETAILS	ACTION
Check cores	If cores in the available quota don't equal or exceed the total target count at the time of failover, failovers will fail.	<p>For VMware VMs, check you have enough cores in the target subscription to meet the Deployment Planner core recommendation.</p> <p>For physical servers, check that Azure cores meet your manual estimations.</p> <p>To check quotas, in the Azure portal > Subscription, click Usage + quotas.</p> <p>Learn more about increasing quotas.</p>
Check failover limits	The number of failovers mustn't exceed Site Recovery failover limits.	If failovers exceed the limits, you can add subscriptions, and fail over to multiple subscriptions, or increase quota for a subscription.

Failover limits

The limits indicate the number of failovers that are supported by Site Recovery within one hour, assuming three disks per machine.

What does comply mean? To start an Azure VM, Azure requires some drivers to be in boot start state, and services like DHCP to be set to start automatically.

- Machines that comply will already have these settings in place.
- For machines running Windows, you can proactively check compliance, and make them compliant if needed. [Learn more](#).
- Linux machines are only brought into compliance at the time of failover.

MACHINE COMPLIES WITH AZURE?	AZURE VM LIMITS (MANAGED DISK FAILOVER)
Yes	2000
No	1000

- Limits assume that minimal other jobs are in progress in the target region for the subscription.
- Some Azure regions are smaller, and might have slightly lower limits.

Plan infrastructure and VM connectivity

After failover to Azure you need your workloads to operate as they did on-premises, and to enable users to access workloads running on the Azure VMs.

- [Learn more](#) about failing over your Active Directory or DNS on-premises infrastructure to Azure.
- [Learn more](#) about preparing to connect to Azure VMs after failover.

Plan for source capacity and requirements

It's important that you have sufficient configuration servers and scale-out process servers to meet capacity requirements. As you begin your large-scale deployment, start off with a single configuration server, and a single scale-out process server. As you reach the prescribed limits, add additional servers.

NOTE

For VMware VMs, the Deployment Planner makes some recommendations about the configuration and process servers you need. We recommend that you use the tables included in the following procedures, instead of following the Deployment Planner recommendation.

Set up a configuration server

Configuration server capacity is affected by the number of machines replicating, and not by data churn rate. To figure out whether you need additional configuration servers, use these defined VM limits.

CPU	MEMORY	CACHE DISK	REPLICATED MACHINE LIMIT
8 vCPUs 2 sockets * 4 cores @ 2.5 Ghz	16 GB	600 GB	Up to 550 machines Assumes that each machine has three disks of 100 GB each.

- These limits are based on a configuration server set up using an OVF template.
- The limits assume that you're not using the process server that's running by default on the configuration server.

If you need to add a new configuration server, follow these instructions:

- [Set up a configuration server](#) for VMware VM disaster recovery, using an OVF template.
- [Set up a configuration server](#) manually for physical servers, or for VMware deployments that can't use an OVF template.

As you set up a configuration server, note that:

- When you set up a configuration server, it's important to consider the subscription and vault within which it resides, since these shouldn't be changed after setup. If you do need to change the vault, you have to disassociate the configuration server from the vault, and reregister it. This stops replication of VMs in the vault.
- If you want to set up a configuration server with multiple network adapters, you should do this during set up. You can't do this after the registering the configuration server in the vault.

Set up a process server

Process server capacity is affected by data churn rates, and not by the number of machines enabled for replication.

- For large deployments you should always have at least one scale-out process server.
- To figure out whether you need additional servers, use the following table.
- We recommend that you add a server with the highest spec.

CPU	MEMORY	CACHE DISK	CHURN RATE
12 vCPUs 2 sockets*6 cores @ 2.5 Ghz	24 GB	1 GB	Up to 2 TB a day

Set up the process server as follows:

1. Review the [prerequisites](#).
2. Install the server in the [portal](#), or from the [command line](#).
3. Configure replicated machines to use the new server. If you already have machines replicating:
 - You can [move](#) an entire process server workload to the new process server.

- Alternatively, you can [move](#) specific VMs to the new process server.

Enable large-scale replication

After planning capacity and deploying the required components and infrastructure, enable replication for large numbers of VMs.

1. Sort machines into batches. You enable replication for VMs within a batch, and then move on to the next batch.
 - For VMware VMs, you can use the [recommended VM batch size](#) in the Deployment Planner report.
 - For physical machines, we recommend you identify batches based on machines that have a similar size and amount of data, and on available network throughput. The aim is to batch machines that are likely to finish their initial replication in around the same amount of time.
2. If disk churn for a machine is high, or exceeds limits in Deployment thePlanner, you can move non-critical files you don't need to replicate (such as log dumps or temp files) off the machine. For VMware VMs, you can move these files to a separate disk, and then [exclude that disk](#) from replication.
3. Before you enable replication, check that machines meet [replication requirements](#).
4. Configure a replication policy for [VMware VMs](#) or [physical servers](#).
5. Enable replication for [VMware VMs](#) or [physical servers](#). This kicks off the initial replication for the selected machines.

Monitor your deployment

After you kick off replication for the first batch of VMs, start monitoring your deployment as follows:

1. Assign a disaster recovery administrator to monitor the health status of replicated machines.
2. [Monitor events](#) for replicated items and the infrastructure.
3. [Monitor the health](#) of your scale-out process servers.
4. Sign up to get [email notifications](#) for events, for easier monitoring.
5. Conduct regular [disaster recovery drills](#), to ensure that everything's working as expected.

Plan for large-scale failovers

In an event of disaster, you might need to fail over a large number of machines/workloads to Azure. Prepare for this type of event as follows.

You can prepare in advance for failover as follows:

- [Prepare your infrastructure and VMs](#) so that your workloads will be available after failover, and so that users can access the Azure VMs.
- Note the [failover limits](#) earlier in this document. Make sure your failovers will fall within these limits.
- Run regular [disaster recovery drills](#). Drills help to:
 - Find gaps in your deployment before failover.
 - Estimate end-to-end RTO for your apps.
 - Estimate end-to-end RPO for your workloads.
 - Identify IP address range conflicts.
 - As you run drills, we recommend that you don't use production networks for drills, avoid using the same subnet names in production and test networks, and clean up test failovers after every drill.

To run a large-scale failover, we recommend the following:

1. Create recovery plans for workload failover.
 - Each recovery plan can trigger failover of up to 50 machines.
 - [Learn more](#) about recovery plans.
2. Add Azure Automation runbook scripts to recovery plans, to automate any manual tasks on Azure. Typical tasks include configuring load balancers, updating DNS etc. [Learn more](#)
3. Before failover, prepare Windows machines so that they comply with the Azure environment. [Failover limits](#) are higher for machines that comply. [Learn more](#) about runbooks.
4. Trigger failover with the [Start-AzRecoveryServicesAsrPlannedFailoverJob](#) PowerShell cmdlet, together with a recovery plan.

Next steps

[Monitor Site Recovery](#)

Manage VM network interfaces for on-premises disaster recovery to Azure

11/12/2019 • 2 minutes to read • [Edit Online](#)

A virtual machine (VM) in Azure must have at least one network interface attached to it. It can have as many network interfaces attached to it as the VM size supports.

By default, the first network interface attached to an Azure virtual machine is defined as the primary network interface. All other network interfaces in the virtual machine are secondary network interfaces. Also by default, all outbound traffic from the virtual machine is sent out the IP address that's assigned to the primary IP configuration of the primary network interface.

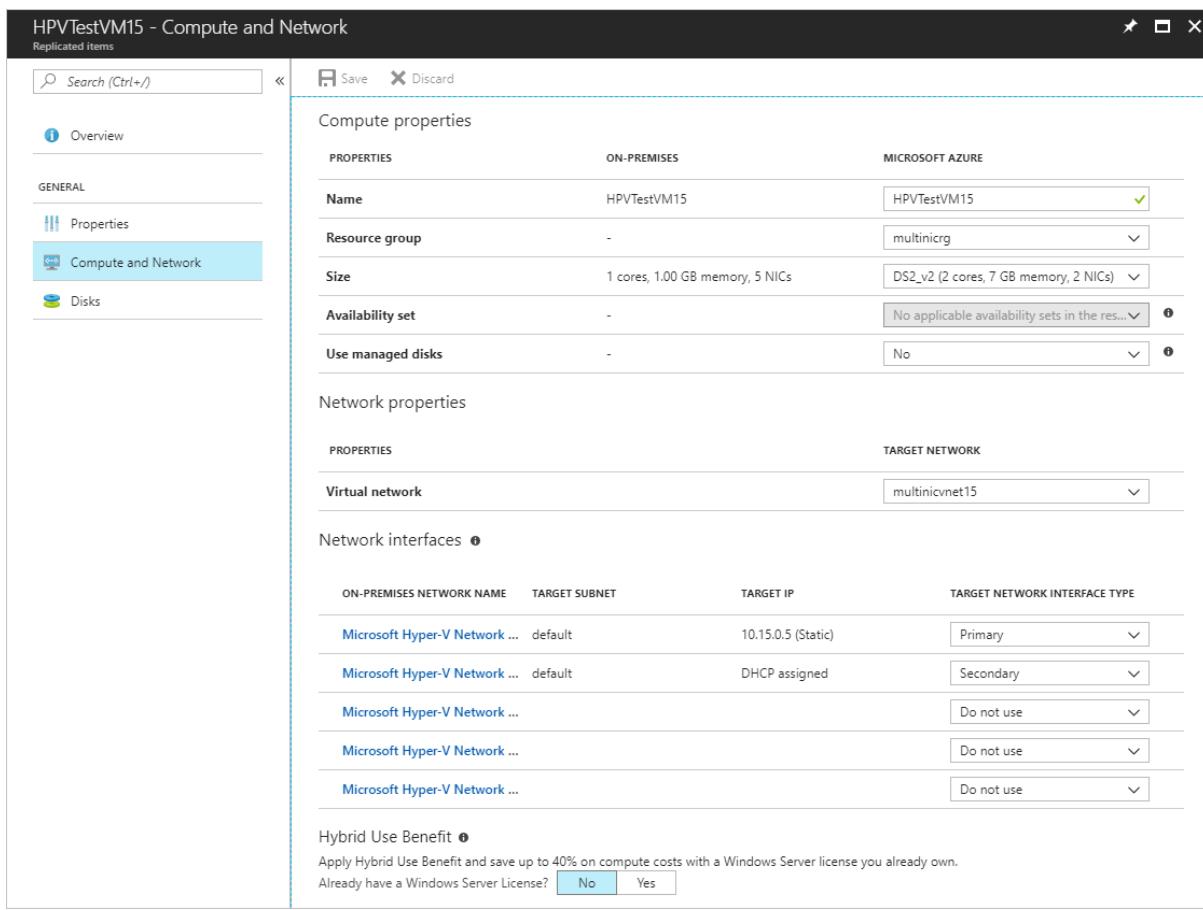
In an on-premises environment, virtual machines or servers can have multiple network interfaces for different networks within the environment. Different networks are typically used for performing specific operations such as upgrades, maintenance, and internet access. When you're migrating or failover to Azure from an on-premises environment, keep in mind that network interfaces in the same virtual machine must all be connected to the same virtual network.

By default, Azure Site Recovery creates as many network interfaces on an Azure virtual machine as are connected to the on-premises server. You can avoid creating redundant network interfaces during migration or failover by editing the network interface settings under the settings for the replicated virtual machine.

Select the target network

For VMware and physical machines, and for Hyper-V (without System Center Virtual Machine Manager) virtual machines, you can specify the target virtual network for individual virtual machines. For Hyper-V virtual machines managed with Virtual Machine Manager, use [network mapping](#) to map VM networks on a source Virtual Machine Manager server and target Azure networks.

1. Under **Replicated items** in a Recovery Services vault, select any replicated item to access the settings for that replicated item.
2. Select the **Compute and Network** tab to access the network settings for the replicated item.
3. Under **Network properties**, choose a virtual network from the list of available network interfaces.



Modifying the target network affects all network interfaces for that specific virtual machine.

For Virtual Machine Manager clouds, modifying network mapping affects all virtual machines and their network interfaces.

Select the target interface type

Under the **Network interfaces** section of the **Compute and Network** pane, you can view and edit network interface settings. You can also specify the target network interface type.

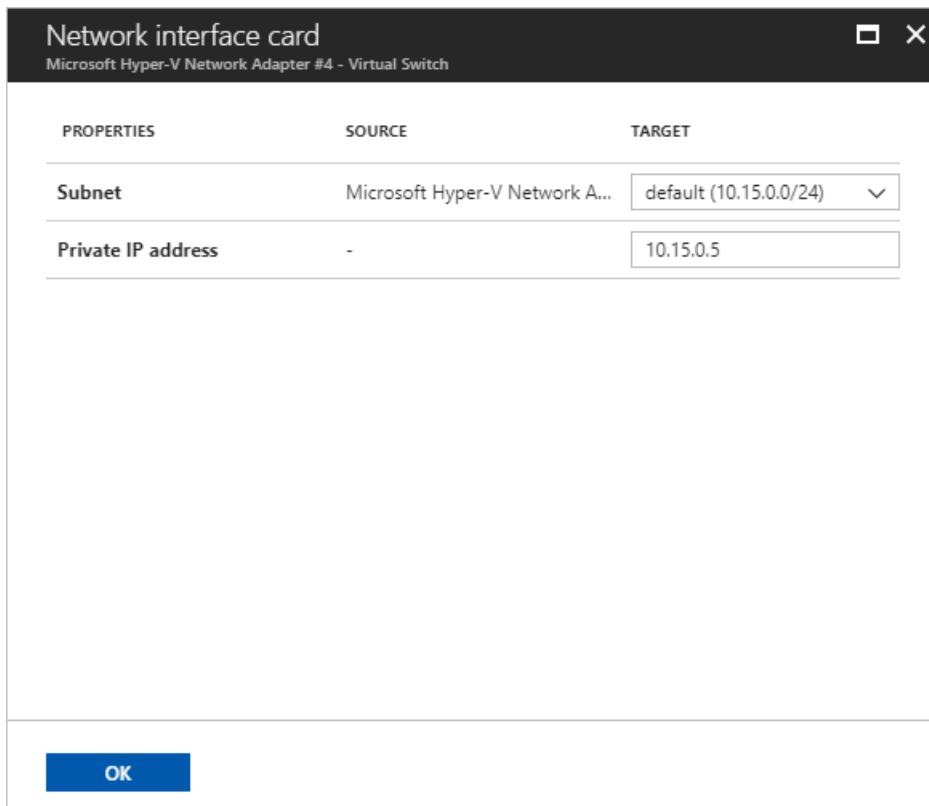
- A **Primary** network interface is required for failover.
- All other selected network interfaces, if any, are **Secondary** network interfaces.
- Select **Do not use** to exclude a network interface from creation at failover.

By default, when you're enabling replication, Site Recovery selects all detected network interfaces on the on-premises server. It marks one as **Primary** and all others as **Secondary**. Any subsequent interfaces added on the on-premises server are marked **Do not use** by default. When you're adding more network interfaces, ensure that the correct Azure virtual machine target size is selected to accommodate all required network interfaces.

Modify network interface settings

You can modify the subnet and IP address for a replicated item's network interfaces. If an IP address is not specified, Site Recovery will assign the next available IP address from the subnet to the network interface at failover.

1. Select any available network interface to open the network interface settings.
2. Choose the desired subnet from the list of available subnets.
3. Enter the desired IP address (as required).



4. Select **OK** to finish editing and return to the **Compute and Network** pane.
5. Repeat steps 1-4 for other network interfaces.
6. Select **Save** to save all changes.

Next steps

[Learn more](#) about network interfaces for Azure virtual machines.

Connect to Azure VMs after failover from on-premises

11/14/2019 • 6 minutes to read • [Edit Online](#)

This article describes how to set up connectivity so that you can successfully connect to Azure VMs after failover.

When you set up disaster recovery of on-premises virtual machines (VMs) and physical servers to Azure, [Azure Site Recovery](#) starts replicating machines to Azure. Then, when outages occur, you can fail over to Azure from your on-premises site. When failover occurs, Site Recovery creates Azure VMs, using replicated on-premises data. As part of disaster recovery planning, you need to figure out how to connect to apps running on these Azure VMs after failover.

In this article you learn how to:

- Prepare on-premises machines before failover.
- Prepare Azure VMs after failover.
- Retain IP addresses on Azure VMs after failover.
- Assign new IP addresses to Azure VMs after failover.

Prepare on-premises machines

To ensure connectivity to Azure VMs, prepare your on-premises machines before failover.

Prepare Windows machines

On on-premises Windows machines, do the following:

1. Configure Windows settings. These include removing any static persistent routes or WinHTTP proxy, and setting the disk SAN policy to **OnlineAll**. [Follow](#) these instructions.
2. Make sure [these services](#) are running.
3. Enable remote desktop (RDP) to allow remote connections to the on-premises machine. [Learn how](#) to enable RDP with PowerShell.
4. To access an Azure VM over the internet after failover, in Windows Firewall on the on-premises machine, allow TCP and UDP in the Public profile, and set RDP as an allowed app for all profiles.
5. If you want to access an Azure VM over a site-to-site VPN after failover, in Windows Firewall on the on-premises machine, allow RDP for the Domain and Private profiles. [Learn](#) how to allow RDP traffic.
6. Make sure that there are no Windows updates pending on the on-premises VM when you trigger a failover. If there are, updates might start installing on the Azure VM after failover, and you won't be able to sign into the VM until updates finish.

Prepare Linux machines

On on-premises Linux machines, do the following:

1. Check that the Secure Shell service is set to start automatically on system boot.
2. Check that firewall rules allow an SSH connection.

Configure Azure VMs after failover

After failover, do the following on the Azure VMs that are created.

1. To connect to the VM over the internet, assign a public IP address to the VM. You can't use the same public IP address for the Azure VM that you used for your on-premises machine. [Learn more](#)
2. Check that network security group (NSG) rules on the VM allow incoming connections to the RDP or SSH port.
3. Check [Boot diagnostics](#) to view the VM.

NOTE

The Azure Bastion service offers private RDP and SSH access to Azure VMs. [Learn more](#) about this service.

Set a public IP address

As an alternative to assigning a public IP address manually to an Azure VM, you can assign the address during failover using a script or Azure automation runbook in a Site Recovery [recovery plan](#), or you can set up DNS-level routing using Azure Traffic Manager. [Learn more](#) about setting up a public address.

Assign an internal address

To set the internal IP address of an Azure VM after failover, you have a couple of options:

- **Retain same IP address:** You can use the same IP address on the Azure VM as the one allocated to the on-premises machine.
- **Use different IP address:** You can use a different IP address for the Azure VM.

Retain IP addresses

Site Recovery lets you retain the same IP addresses when failing over to Azure. Retaining the same IP address avoids potential network issues after failover, but does introduce some complexity.

- If the target Azure VM uses the same IP address/subnet as your on-premises site, you can't connect between them using a site-to-site VPN connection or ExpressRoute, because of the address overlap. Subnets must be unique.
- You need a connection from on-premises to Azure after failover, so that apps are available on Azure VMs. Azure doesn't support stretched VLANs, so if you want to retain IP addresses you need to take the IP space over to Azure by failing over the entire subnet, in addition to the on-premises machine.
- Subnet failover ensures that a specific subnet isn't available simultaneously on-premises and in Azure.

Retaining IP addresses requires the following steps:

- In the Compute & Network properties of the replicated item, set network and IP addressing for the target Azure VM to mirror the on-premises setting.
- Subnets must be managed as part of the disaster recovery process. You need an Azure VNet to match the on-premises network, and after failover network routes must be modified to reflect that the subnet has moved to Azure, and new IP address locations.

Failover example

Let's look at an example.

- The fictitious company Woodgrove Bank hosts their business apps on-premises. They host their mobile apps in Azure.
- They connect from on-premises to Azure over site-to-site VPN.
- Woodgrove is using Site Recovery to replicate on-premises machines to Azure.
- Their on-premises apps use hard-coded IP addresses, so they want to retain the same IP addresses in Azure.

- On-premises the machines running the apps are running in three subnets:
 - 192.168.1.0/24.
 - 192.168.2.0/24
 - 192.168.3.0/24
- Their apps running in Azure are located in the Azure VNet **Azure Network** in two subnets:
 - 172.16.1.0/24
 - 172.16.2.0/24.

In order to retain the addresses, here's what they do.

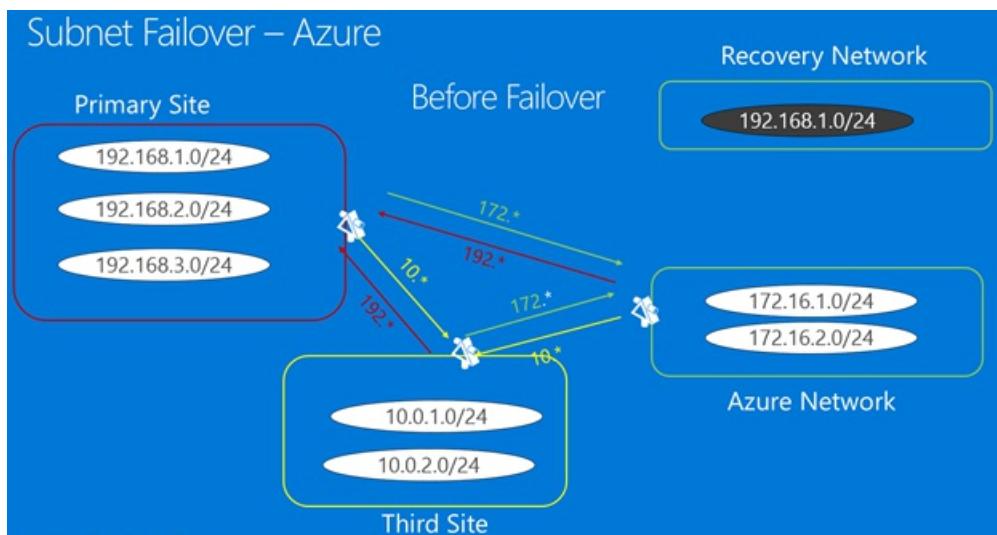
- When they enable replication, they specify that machines should replicate to the **Azure Network**.
- They create **Recovery Network** in Azure. This VNet mirrors the 192.168.1.0/24 subnet in their on-premises network.
- Woodgrove sets up a [VNet-to-VNet connection](#) between the two networks.

NOTE

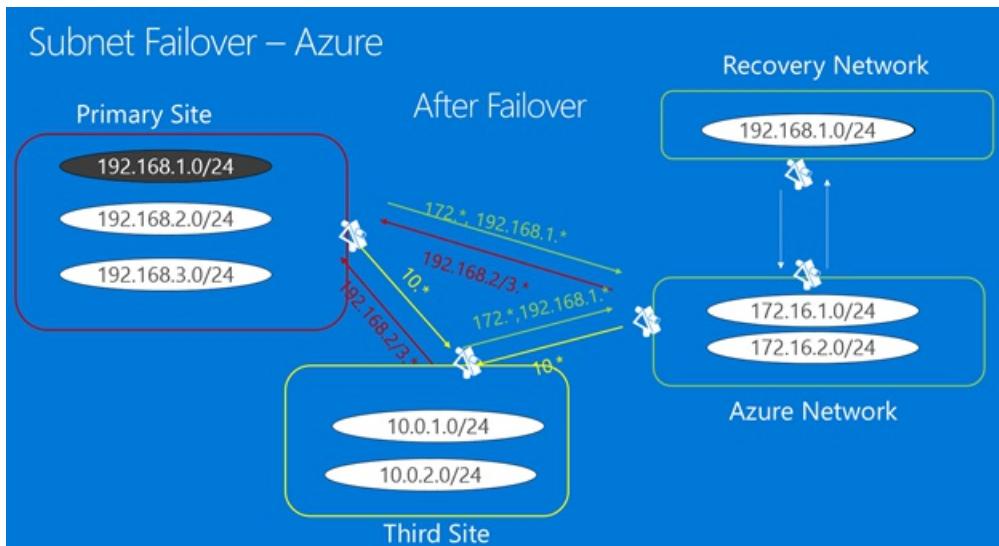
Depending on application requirements, a VNet-to-VNet connection could be set up before failover, as a manual step/scripted step/Azure automation runbook in a Site Recovery [recovery plan](#), or after failover is complete.

- Before failover, on the machine properties in Site Recovery, they set the target IP address to the address of the on-premises machine, as described in the next procedure.
- After failover, the Azure VMs are created with the same IP address. Woodgrove connects from **Azure Network** to **Recovery Network** VNet using VNet peering (with transit connectivity enabled).
- On-premises, Woodgrove needs to make network changes, including modifying routes to reflect that 192.168.1.0/24 has moved to Azure.

Infrastructure before failover



Infrastructure after failover



Set target network settings

Before failover, specify the network settings and IP address for the target Azure VM.

1. In the Recovery Services vault -> **Replicated items**, select the on-premises machine.
2. In the **Compute and Network** page for the machine, click **Edit**, to configure network and adapter settings for the target Azure VM.
3. In **Network properties**, select the target network in which the Azure VM will be located when it's created after failover.
4. In **Network interfaces**, configure the network adapters in the target network. By default Site Recovery shows all detected NICs on the on-premises machine.
 - In **Target network interface type** you can set each NIC as **Primary**, **Secondary**, or **Do not create** if you don't need that specific NIC in the target network. One network adapter must be set as primary for failover. Note that modifying the target network affects all NICs for the Azure VM.
 - Click the NIC name to specify the subnet in which the Azure VM will be deployed.
 - Overwrite **Dynamic** with the private IP address you want to assign to target Azure VM. If an IP address isn't specified Site Recovery will assign the next available IP address in the subnet to the NIC at failover.
 - [Learn more](#) about managing NICs for on-premises failover to Azure.

Get new IP addresses

In this scenario, the Azure VM gets a new IP address after failover. A DNS update to update records for failed over machines to point to the IP address of the Azure VM.

Next steps

[Learn about](#) replicating on-premises Active Directory and DNS to Azure.

Plan capacity and scaling for VMware disaster recovery to Azure

11/12/2019 • 9 minutes to read • [Edit Online](#)

Use this article to plan for capacity and scaling when you replicate on-premises VMware VMs and physical servers to Azure by using [Azure Site Recovery](#).

How do I start capacity planning?

To learn about Azure Site Recovery infrastructure requirements, gather information about your replication environment by running [Azure Site Recovery Deployment Planner](#) for VMware replication. For more information, see [About Site Recovery Deployment Planner for VMware to Azure](#).

Site Recovery Deployment Planner provides a report that has complete information about compatible and incompatible VMs, disks per VM, and data churn per disk. The tool also summarizes network bandwidth requirements to meet target RPO and the Azure infrastructure that's required for successful replication and test failover.

Capacity considerations

COMPONENT	DETAILS
Replication	<p>Maximum daily change rate: A protected machine can use only one process server. A single process server can handle a daily change rate up to 2 TB. So, 2 TB is the maximum daily data change rate that's supported for a protected machine.</p> <p>Maximum throughput: A replicated machine can belong to one storage account in Azure. A standard Azure Storage account can handle a maximum of 20,000 requests per second. We recommend that you limit the number of input/output operations per second (IOPS) across a source machine to 20,000. For example, if you have a source machine that has five disks and each disk generates 120 IOPS (8 K in size) on the source machine, the source machine is within the Azure per-disk IOPS limit of 500. (The number of storage accounts required is equal to the total source machine IOPS divided by 20,000.)</p>
Configuration server	<p>The configuration server must be able to handle the daily change rate capacity across all workloads running on protected machines. The configuration machine must have sufficient bandwidth to continuously replicate data to Azure Storage.</p> <p>A best practice is to place the configuration server on the same network and LAN segment as the machines that you want to protect. You can place the configuration server on a different network, but machines that you want to protect should have layer 3 network visibility.</p> <p>Size recommendations for the configuration server are summarized in the table in the following section.</p>

COMPONENT	DETAILS
Process server	<p>The first process server is installed by default on the configuration server. You can deploy additional process servers to scale your environment.</p> <p>The process server receives replication data from protected machines. The process server optimizes data by using caching, compression, and encryption. Then, the process server sends the data to Azure. The process server machine must have sufficient resources to perform these tasks.</p> <p>The process server uses a disk-based cache. Use a separate cache disk of 600 GB or more to handle data changes that are stored if a network bottleneck or outage occurs.</p>

Size recommendations for the configuration server and inbuilt process server

A configuration server that uses an inbuilt process server to protect the workload can handle up to 200 virtual machines based on the following configurations:

CPU	MEMORY	CACHE DISK SIZE	DATA CHANGE RATE	PROTECTED MACHINES
8 vCPUs (2 sockets * 4 cores @ 2.5 GHz)	16 GB	300 GB	500 GB or less	Use to replicate fewer than 100 machines.
12 vCPUs (2 sockets * 6 cores @ 2.5 GHz)	18 GB	600 GB	501 GB to 1 TB	Use to replicate 100 to 150 machines.
16 vCPUs (2 sockets * 8 cores @ 2.5 GHz)	32 GB	1 TB	>1 TB to 2 TB	Use to replicate 151 to 200 machines.
Deploy another configuration server by using an OVF template .				Deploy a new configuration server if you're replicating more than 200 machines.
Deploy another process server .			>2 TB	Deploy a new scale-out process server if the overall daily data change rate is greater than 2 TB.

In these configurations:

- Each source machine has three disks of 100 GB each.
- We used benchmarking storage of eight shared access signature drives of 10 K RPM with RAID 10 for cache disk measurements.

Size recommendations for the process server

The process server is the component that handles data replication in Azure Site Recovery. If the daily change rate is greater than 2 TB, you must add scale-out process servers to handle the replication load. To scale out, you can:

- Increase the number of configuration servers by deploying by using an [OVF template](#). For example, you can

protect up to 400 machines by using two configuration servers.

- Add [scale-out process servers](#). Use the scale-out process servers to handle replication traffic instead of (or in addition to) the configuration server.

The following table describes this scenario:

- You set up a scale-out process server.
- You configured protected virtual machines to use the scale-out process server.
- Each protected source machine has three disks of 100 GB each.

ADDITIONAL PROCESS SERVER	CACHE DISK SIZE	DATA CHANGE RATE	PROTECTED MACHINES
4 vCPUs (2 sockets * 2 cores @ 2.5 GHz), 8 GB of memory	300 GB	250 GB or less	Use to replicate 85 or fewer machines.
8 vCPUs (2 sockets * 4 cores @ 2.5 GHz), 12 GB of memory	600 GB	251 GB to 1 TB	Use to replicate 86 to 150 machines.
12 vCPUs (2 sockets * 6 cores @ 2.5 GHz) 24 GB of memory	1 TB	>1 TB to 2 TB	Use to replicate 151 to 225 machines.

How you scale your servers depends on your preference for a scale-up or scale-out model. To scale up, deploy a few high-end configuration servers and process servers. To scale out, deploy more servers that have fewer resources. For example, if you want to protect 200 machines with an overall daily data change rate of 1.5 TB, you could take one of the following actions:

- Set up a single process server (16 vCPU, 24 GB of RAM).
- Set up two process servers (2 x 8 vCPU, 2* 12 GB of RAM).

Control network bandwidth

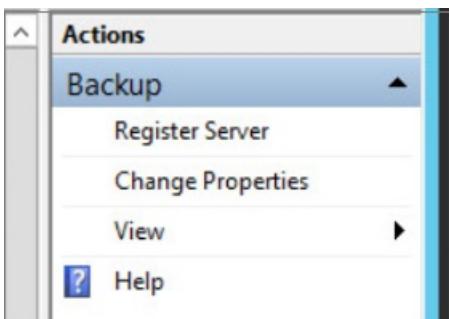
After you use [Site Recovery Deployment Planner](#) to calculate the bandwidth you need for replication (initial replication and then the delta), you have a couple of options for controlling the amount of bandwidth that's used for replication:

- **Throttle bandwidth:** VMware traffic that replicates to Azure goes through a specific process server. You can throttle bandwidth on the machines that are running as process servers.
- **Influence bandwidth:** You can influence the bandwidth that's used for replication by using a couple of registry keys:
 - The **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Azure Backup\Replication\UploadThreadsPerVM** registry value specifies the number of threads that are used for data transfer (initial or delta replication) of a disk. A higher value increases the network bandwidth that's used for replication.
 - The **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Azure Backup\Replication\DownloadThreadsPerVM** registry value specifies the number of threads that are used for data transfer during failback.

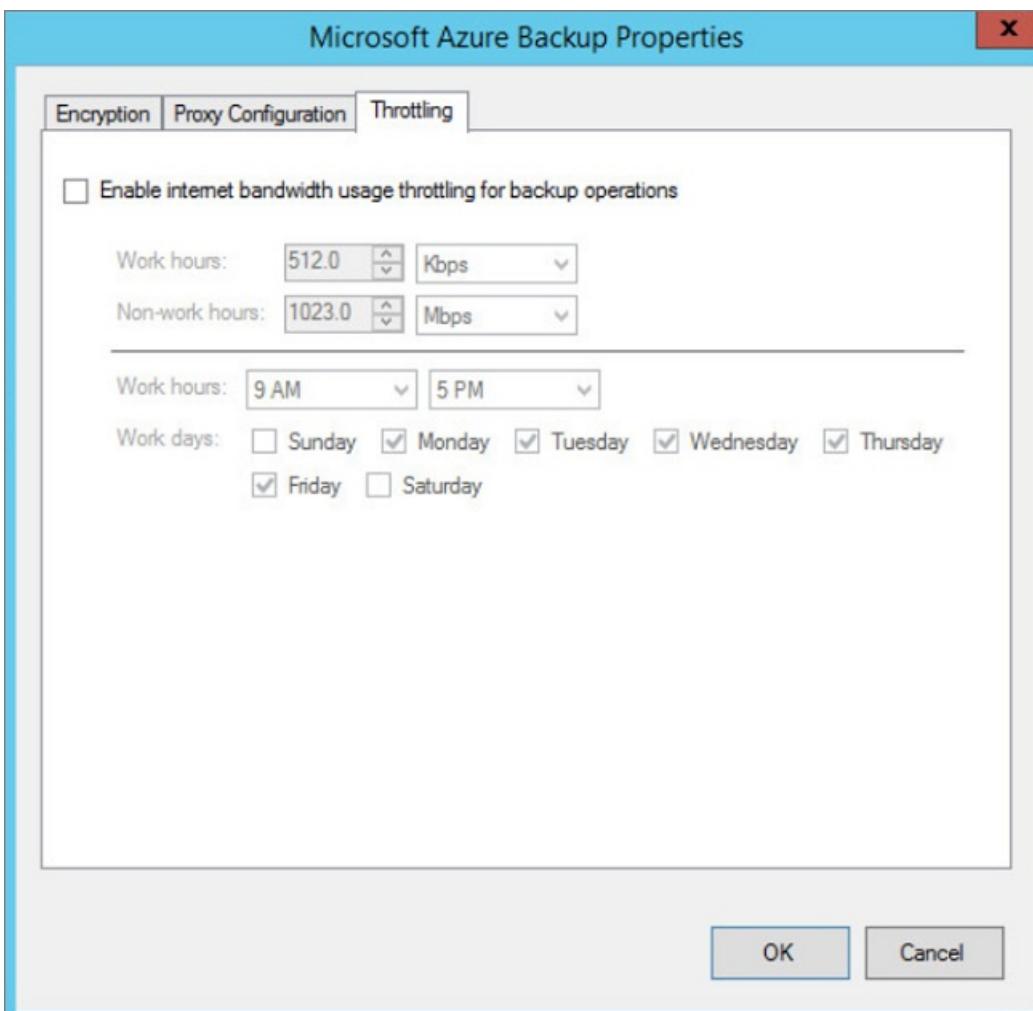
Throttle bandwidth

1. Open the Azure Backup MMC snap-in on the machine you use as the process server. By default, a shortcut for Backup is available on the desktop or in the following folder: C:\Program Files\Microsoft Azure Recovery Services Agent\bin.

2. In the snap-in, select **Change Properties**.



3. On the **Throttling** tab, select **Enable internet bandwidth usage throttling for backup operations**. Set the limits for work and non-work hours. Valid ranges are from 512 Kbps to 1,023 Mbps.



You can also use the [Set-OBMachineSetting](#) cmdlet to set throttling. Here's an example:

```
$mon = [System.DayOfWeek]::Monday
$tue = [System.DayOfWeek]::Tuesday
Set-OBMachineSetting -WorkDay $mon, $tue -StartWorkHour "9:00:00" -EndWorkHour "18:00:00" -WorkHourBandwidth
(512*1024) -NonWorkHourBandwidth (2048*1024)
```

Set-OBMachineSetting -NoThrottle indicates that no throttling is required.

Alter the network bandwidth for a VM

1. In the VM's registry, go to **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Azure**

Backup\Replication.

- To alter the bandwidth traffic on a replicating disk, modify the value of **UploadThreadsPerVM**. Create

the key if it doesn't exist.

- To alter the bandwidth for failback traffic from Azure, modify the value of **DownloadThreadsPerVM**.
2. The default value for each key is **4**. In an "overprovisioned" network, these registry keys should be changed from the default values. The maximum value you can use is **32**. Monitor traffic to optimize the value.

Set up the Site Recovery infrastructure to protect more than 500 VMs

Before you set up the Site Recovery infrastructure, access the environment to measure the following factors: compatible virtual machines, the daily data change rate, the required network bandwidth for the RPO you want to achieve, the number of Site Recovery components that are required, and the time it takes to complete the initial replication. Complete the following steps to gather the required information:

1. To measure these parameters, run Site Recovery Deployment Planner on your environment. For helpful guidelines, see [About Site Recovery Deployment Planner for VMware to Azure](#).
2. Deploy a configuration server that meets the [size recommendations for the configuration server](#). If your production workload exceeds 650 virtual machines, deploy another configuration server.
3. Based on the measured daily data change rate, deploy [scale-out process servers](#) with the help of [size guidelines](#).
4. If you expect the data change rate for a disk virtual machine to exceed 2 MBps, ensure that you use premium managed disks. Site Recovery Deployment Planner runs for a specific time period. Peaks in the data change rate at other times might not be captured in the report.
5. [Set the network bandwidth](#) based on the RPO you want to achieve.
6. When the infrastructure is set up, enable disaster recovery for your workload. To learn how, see [Set up the source environment for VMware to Azure replication](#).

Deploy additional process servers

If you scale out your deployment beyond 200 source machines or if you have a total daily churn rate of more than 2 TB, you must add process servers to handle the traffic volume. We have enhanced the product in 9.24 version to provide [process server alerts](#) on when to set up a scale-out process server. [Set up the process server](#) to protect new source machines or [balance the load](#).

Migrate machines to use the new process server

1. Select **Settings > Site Recovery servers**. Select the configuration server, and then expand **Process servers**.

Process Server
PREVIEW

* Server type ⓘ
Process Server (On-Premise)

Install process server
On-premises

1. Download Process server installer
2. Install the process server

Register process server
On-premises

1. Register the process server to configuration server following the guide lines mentioned here [Learn More](#)

2. Right-click the process server currently in use, and then select **Switch**.

MVA-ASR-1
Configuration server - PREVIEW

+ vCenter + Process Server + Master Target ... Refresh Server Error Details Delete

Essentials ^

Recovery Services vault ASR-MVA-DEMO	Connection status Connected
IP address 10.150.105.29	Last heartbeat at 2/3/2016, 2:45:56 PM
Configuration Server version 9.0.0.0	Provider version 5.1.1400.0
Connected agents 4	Server ID aeb87d90ecf9c6b3e26b43cbc0f4b00cb454...
Protected items 3	

Associated Servers

NAME	STATUS	SERVER ROLE	AGENT VERSION	LAST HEART BEAT
▼ Process Serv...	...			
MVA-ASR...	Connected	Process Server(...)	9.0.0.0	2/3/2016, 2:29:...

More options for MVA-ASR...:

- Pin to dashboard
- Load balance
- Switch
- Error Details

3. In **Select target process server**, select the new process server you want to use. Then, select the virtual machines that the server will handle. To get information about the server, select the information icon. To help you make load decisions, the average space that's required to replicate each selected virtual machine to the new process server is shown. Select the check mark to begin replicating to the new process server.

Deploy additional master target servers

In the following scenarios, more than one master target server is required:

- You want to protect a Linux-based virtual machine.
- The master target server available on the configuration server doesn't have access to the datastore of the VM.
- The total number of disks on the master target server (the number of local disks on server plus the number of disks to be protected) is greater than 60 disks.

To learn how to add a master target server for a Linux-based virtual machine, see [Install a Linux master target server for failback](#).

To add a master target server for a Windows-based virtual machine:

1. Go to **Recovery Services Vault > Site Recovery Infrastructure > Configuration servers**.

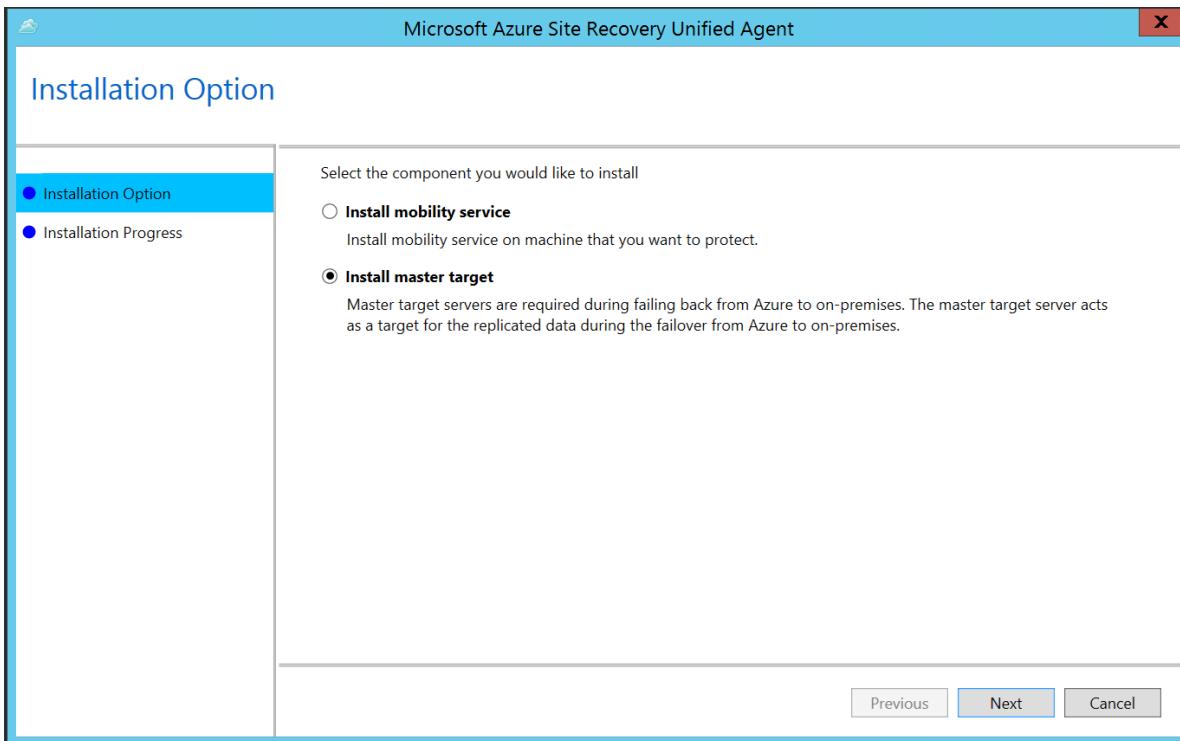
2. Select the required configuration server, and then select **Master Target Server**.

The screenshot shows the 'Configuration Server' interface for 'CS1'. At the top, there are tabs for 'vCenter', 'Process Server', and 'Master Target Server', with 'Master Target Server' highlighted by a red box. Below the tabs, there's a section titled 'Essentials' with a dashed blue box around it. The main content area displays various server details in a two-column format:

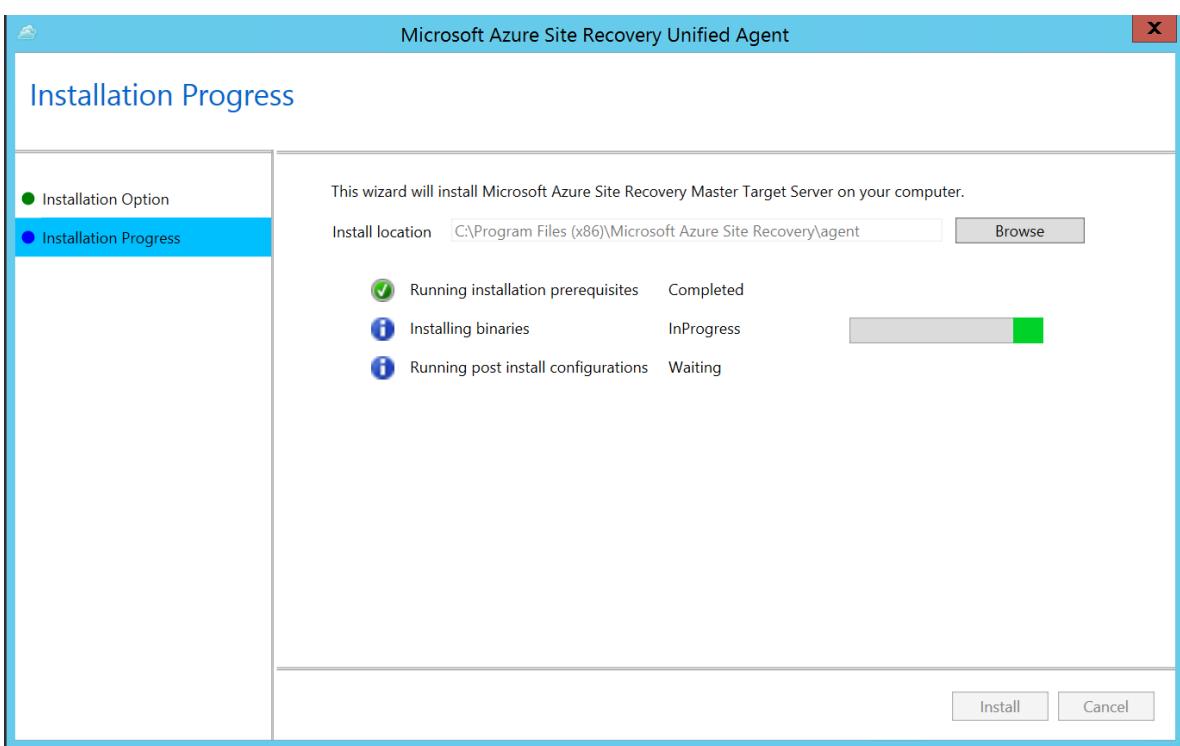
Recovery Services vault	Connection status
CS1	Connected
IP address	Last heartbeat at 6/26/2018 5:24:14 PM
Configuration Server version	Provider version
9.17.0.0	5.1.3400.0
Connected agents	Server ID
5	[Redacted]
Protected items	
3	

3. Download the unified setup file, and then run the file on the VM to set up the master target server.

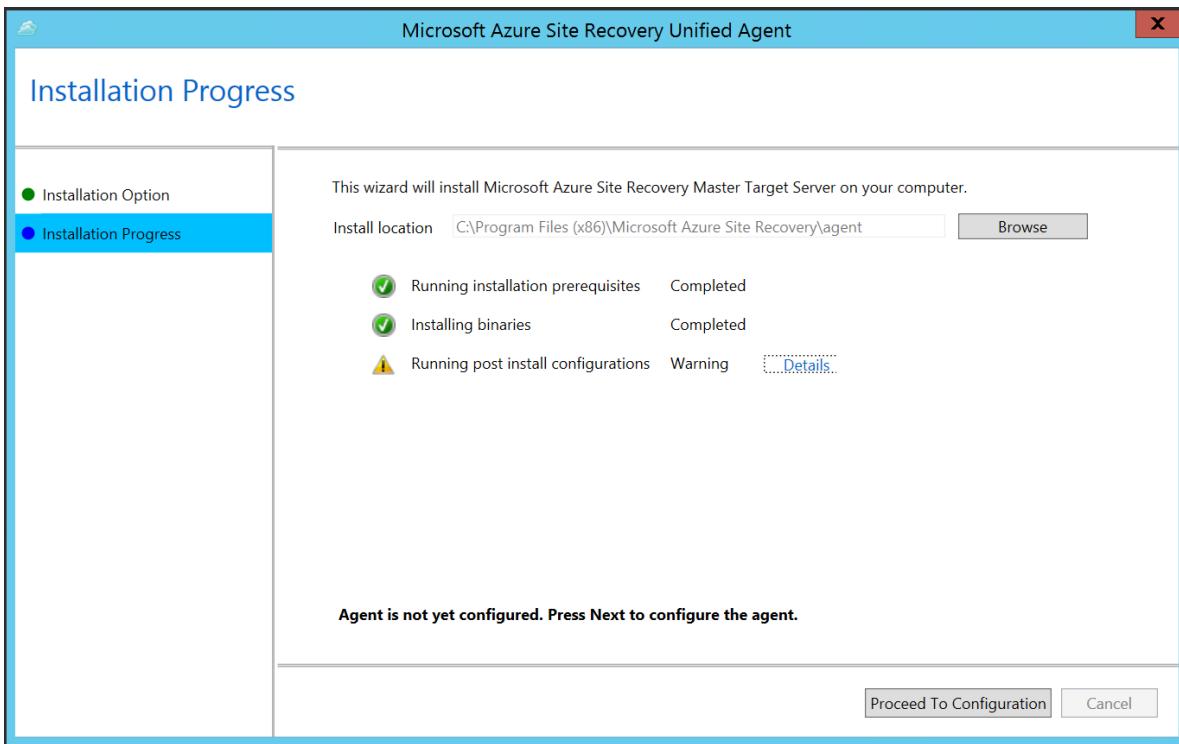
4. Select **Install master target > Next**.



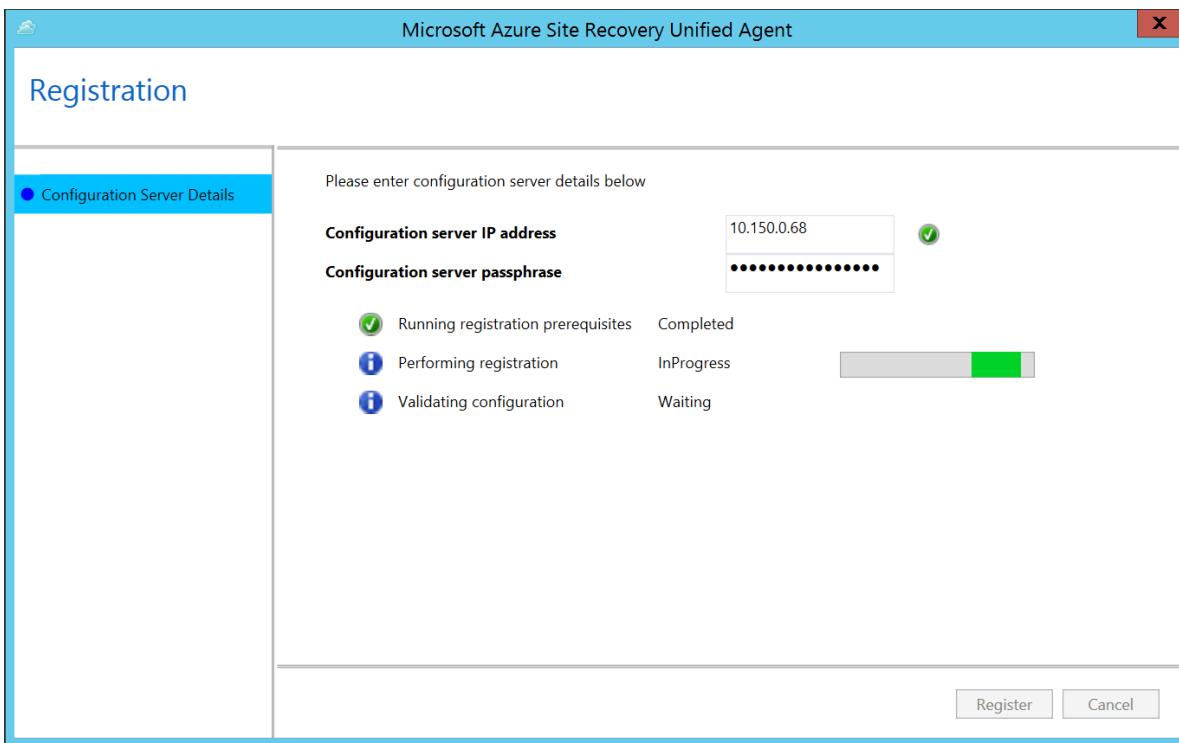
5. Select the default installation location, and then select **Install**.



6. To register the master target with the configuration server, select **Proceed To Configuration**.



7. Enter the IP address of the configuration server, and then enter the passphrase. To learn how to generate a passphrase, see [Generate a configuration server passphrase](#).



8. Select **Register**. When registration is finished, select **Finish**.

When registration finishes successfully, the server is listed in the Azure portal at **Recovery Services Vault > Site Recovery Infrastructure > Configuration servers**, in the master target servers of the configuration server.

NOTE

Download the latest version of the [master target server unified setup file for Windows](#).

Next steps

Download and run [Site Recovery Deployment Planner](#).

About the Azure Site Recovery Deployment Planner for VMware to Azure

11/14/2019 • 7 minutes to read • [Edit Online](#)

This article is the Azure Site Recovery Deployment Planner user guide for VMware to Azure production deployments.

Overview

Before you begin to protect any VMware virtual machines (VMs) by using Azure Site Recovery, allocate sufficient bandwidth, based on your daily data-change rate, to meet your desired recovery point objective (RPO). Be sure to deploy the right number of configuration servers and process servers on-premises.

You also need to create the right type and number of target Azure Storage accounts. You create either standard or premium storage accounts, factoring in growth on your source production servers because of increased usage over time. You choose the storage type per VM, based on workload characteristics (for example, read/write I/O operations per second [IOPS] or data churn) and Site Recovery limits.

Site Recovery Deployment Planner is a command-line tool for both Hyper-V to Azure and VMware to Azure disaster recovery scenarios. You can remotely profile your VMware VMs by using this tool (with no production impact whatsoever) to understand the bandwidth and storage requirements for successful replication and test failover. You can run the tool without installing any Site Recovery components on-premises. To get accurate achieved throughput results, run the planner on a Windows Server that meets the minimum requirements of the Site Recovery configuration server that you eventually need to deploy as one of the first steps in production deployment.

The tool provides the following details:

Compatibility assessment

- VM eligibility assessment, based on number of disks, disk size, IOPS, churn, boot type (EFI/BIOS), and OS version

Network bandwidth need versus RPO assessment

- Estimated network bandwidth that's required for delta replication
- Throughput that Site Recovery can get from on-premises to Azure
- Number of VMs to batch, based on the estimated bandwidth to complete initial replication in a given amount of time
- RPO that can be achieved for a given bandwidth
- Impact on the desired RPO if lower bandwidth is provisioned

Azure infrastructure requirements

- Storage type (standard or premium storage) requirement for each VM
- Total number of standard and premium storage accounts to be set up for replication (Includes cache storage accounts)
- Storage-account naming suggestions, based on Storage guidance
- Number of Azure cores to be set up before test failover or failover on the subscription
- Azure VM-recommended size for each on-premises VM

On-premises infrastructure requirements

- Required number of configuration servers and process servers to be deployed on-premises

Estimated disaster recovery cost to Azure

- Estimated total disaster recovery cost to Azure: compute, storage, network, and Site Recovery license cost
- Detail cost analysis per VM

IMPORTANT

Because usage is likely to increase over time, all the preceding tool calculations are performed assuming a 30 percent growth factor in workload characteristics. The calculations also use a 95th percentile value of all the profiling metrics, such as read/write IOPS and churn. Both growth factor and percentile calculation are configurable. To learn more about growth factor, see the "Growth-factor considerations" section. To learn more about percentile value, see the "Percentile value used for the calculation" section.

Support matrix

	VMWARE TO AZURE	HYPER-V TO AZURE	AZURE TO AZURE	HYPER-V TO SECONDARY SITE	VMWARE TO SECONDARY SITE
Supported scenarios	Yes	Yes	No	Yes*	No
Supported version	vCenter 6.7, 6.5, 6.0 or 5.5	Windows Server 2016, Windows Server 2012 R2	NA	Windows Server 2016, Windows Server 2012 R2	NA
Supported configuration	vCenter, ESXi	Hyper-V cluster, Hyper-V host	NA	Hyper-V cluster, Hyper-V host	NA
Number of servers that can be profiled per running instance of Site Recovery Deployment Planner	Single (VMs belonging to one vCenter Server or one ESXi server can be profiled at a time)	Multiple (VMs across multiple hosts or host clusters can be profiled at a time)	NA	Multiple (VMs across multiple hosts or host clusters can be profiled at a time)	NA

*The tool is primarily for the Hyper-V to Azure disaster recovery scenario. For Hyper-V to secondary site disaster recovery, it can be used only to understand source-side recommendations like required network bandwidth, required free storage space on each of the source Hyper-V servers, and initial replication batching numbers and batch definitions. Ignore the Azure recommendations and costs from the report. Also, the Get Throughput operation is not applicable for the Hyper-V-to-secondary-site disaster recovery scenario.

Prerequisites

The tool has two main phases: profiling and report generation. There is also a third option to calculate throughput only. The requirements for the server from which the profiling and throughput measurement is initiated are presented in the following table.

SERVER REQUIREMENT	DESCRIPTION

Server requirement	Description
Profiling and throughput measurement	<ul style="list-style-type: none"> Operating system: Windows Server 2016 or Windows Server 2012 R2 (ideally matching at least the size recommendations for the configuration server) Machine configuration: 8 vCPUs, 16 GB RAM, 300 GB HDD .NET Framework 4.5 VMware vSphere PowerCLI 6.0 R3 Visual C++ Redistributable for Visual Studio 2012 Internet access to Azure from this server Azure storage account Administrator access on the server Minimum 100 GB of free disk space (assuming 1,000 VMs with an average of three disks each, profiled for 30 days) VMware vCenter statistics level settings can be 1 or higher level Allow vCenter port (default 443): Site Recovery Deployment Planner uses this port to connect to the vCenter server/ESXi host
Report generation	<p>A Windows PC or Windows Server with Excel 2013 or later.</p> <ul style="list-style-type: none"> .NET Framework 4.5 Visual C++ Redistributable for Visual Studio 2012 VMware vSphere PowerCLI 6.0 R3 is required only when you pass -User option in the report generation command to fetch the latest VM configuration information of the VMs. The Deployment Planner connects to vCenter server. Allow vCenter port (default 443) port to connect to vCenter server.
User permissions	Read-only permission for the user account that's used to access the VMware vCenter server/VMware vSphere ESXi host during profiling

NOTE

The tool can profile only VMs with VMDK and RDM disks. It can't profile VMs with iSCSI or NFS disks. Site Recovery does support iSCSI and NFS disks for VMware servers. Because the deployment planner isn't inside the guest and it profiles only by using vCenter performance counters, the tool doesn't have visibility into these disk types.

Download and extract the deployment planner tool

- Download the latest version of [Site Recovery Deployment Planner](#). The tool is packaged in a .zip folder. The current version of the tool supports only the VMware to Azure scenario.
- Copy the .zip folder to the Windows server from which you want to run the tool. You can run the tool from Windows Server 2012 R2 if the server has network access to connect to the vCenter server/vSphere ESXi host that holds the VMs to be profiled. However, we recommend that you run the tool on a server whose hardware configuration meets the [configuration server sizing guidelines](#). If you already deployed Site Recovery components on-premises, run the tool from the configuration server.

We recommend that you have the same hardware configuration as the configuration server (which has an in-built process server) on the server where you run the tool. Such a configuration ensures that the

achieved throughput that the tool reports matches the actual throughput that Site Recovery can achieve during replication. The throughput calculation depends on available network bandwidth on the server and hardware configuration (such as CPU and storage) of the server. If you run the tool from any other server, the throughput is calculated from that server to Azure. Also, because the hardware configuration of the server might differ from that of the configuration server, the achieved throughput that the tool reports might be inaccurate.

3. Extract the .zip folder. The folder contains multiple files and subfolders. The executable file is ASRDeploymentPlanner.exe in the parent folder.

Example: Copy the .zip file to E:\ drive and extract it. E:\ASR Deployment Planner_v2.3.zip

E:\ASR Deployment Planner_v2.3\ASRDeploymentPlanner.exe

Update to the latest version of Deployment Planner

The latest updates are summarized in the Deployment Planner [version history](#).

If you have a previous version of Deployment Planner, do either of the following:

- If the latest version doesn't contain a profiling fix and profiling is already in progress on your current version of the planner, continue the profiling.
- If the latest version does contain a profiling fix, we recommend that you stop profiling on your current version and restart the profiling with the new version.

NOTE

When you start profiling with the new version, pass the same output directory path so that the tool appends profile data on the existing files. A complete set of profiled data is used to generate the report. If you pass a different output directory, new files are created and old profiled data isn't used to generate the report.

Each new Deployment Planner version is a cumulative update of the .zip file. You don't need to copy the newest files to the previous folder. You can create and use a new folder.

Version history

The latest Site Recovery Deployment Planner tool version is 2.5. See the [Site Recovery Deployment Planner version history](#) page for the fixes that are added in each update.

Next steps

[Run Site Recovery Deployment Planner](#)

Azure Site Recovery Deployment Planner Version History

10/16/2019 • 4 minutes to read • [Edit Online](#)

This article provides history of all versions of Azure Site Recovery Deployment Planner along with the fixes, known limitations in each and their release dates.

Version 2.51

Release Date: August 22, 2019

Fixes:

- Fixed the cost recommendation issue with Deployment Planner version 2.5

Version 2.5

Release Date: July 29, 2019

Fixes:

- For VMware virtual machines and physical machines, recommendation is updated to be based on replication to Managed Disks.
- Added support for Windows 10 (x64), Windows 8.1 (x64), Windows 8 (x64), Windows 7 (x64) SP1 or later

Version 2.4

Release Date: April 17, 2019

Fixes:

- Improved operating system compatibility, specifically when handling localization-based errors.
- Added VMs with up to 20 Mbps of data change rate (churn) to the compatibility checklist.
- Improved error messages
- Added support for vCenter 6.7.
- Added support for Windows Server 2019 and Red Hat Enterprise Linux (RHEL) workstation.

Version 2.3

Release Date: December 3, 2018

Fixes:

- Fixed an issue that prevented the Deployment Planner from generating a report with the provided target location and subscription.

Version 2.2

Release Date: April 25, 2018

Fixes:

- GetVMList operations:
 - Fixed an issue that caused GetVMList to fail if the specified folder doesn't exist. It now either creates the default directory, or creates the directory specified in the outputfile parameter.
 - Added more detailed failure reasons for GetVMList.
- Added VM type information as a column in the compatible VMs sheet of the Deployment Planner report.
- Hyper-V to Azure disaster recovery:
 - Excluded VMs with shared VHDs and PassThrough disks from profiling. The Startprofiling operation shows the list of excluded VMs in the console.
 - Added VMs with more than 64 disks to the list of incompatible VMs.
 - Updated the initial replication (IR) and delta replication (DR) compression factor.
 - Added limited support for SMB storage.

Version 2.1

Release Date: January 3, 2018

Fixes:

- Updated the Excel report.
- Fixed bugs in the GetThroughput operation.
- Added option to limit the number of VMs to profile or generate the report. The default limit is 1,000 VMs.
- VMware to Azure disaster recovery:
 - Fixed an issue of Windows Server 2016 VM going into the incompatible table.
 - Updated compatibility messages for Extensible Firmware Interface (EFI) Windows VMs.
- Updated the VMware to Azure and Hyper-V to Azure, VM data churn limit per VM.
- Improved reliability of VM list file parsing.

Version 2.0.1

Release Date: December 7, 2017

Fixes:

- Added recommendation to optimize the network bandwidth.

Version 2.0

Release Date: November 28, 2017

Fixes:

- Added support for Hyper-V to Azure disaster recovery.
- Added cost calculator.
- Added OS version check for VMware to Azure disaster recovery to determine if the VM is compatible or incompatible for the protection. The tool uses the OS version string that is returned by the vCenter server for that VM. It's the guest operating system version that user has selected while creating the VM in VMware.

Known limitations:

- For Hyper-V to Azure disaster recovery, VM with name containing the characters like: , " , [,] , and \ aren't supported. If profiled, report generation will fail or will have an incorrect result.
- For VMware to Azure disaster recovery, VM with name containing comma isn't supported. If profiled, report generation fails or will have an incorrect result.

Version 1.3.1

Release Date: July 19, 2017

Fixes:

- Added support for large disks (> 1 TB) in report generation. Now you can use Deployment Planner to plan replication for virtual machines that have disk sizes greater than 1 TB (up to 4095 GB). Read more about [Large disk support in Azure Site Recovery](#)

Version 1.3

Release Date: May 9, 2017

Fixes:

- Added support for managed disk in report generation. The number of VMs that can be placed to a single storage account is calculated based on if the managed disk is selected for Failover/Test Failover.

Version 1.2

Release Date: April 7, 2017

Fixes:

- Added boot type (BIOS or EFI) checks for each VM to determine if the VM is compatible or incompatible for the protection.
- Added OS type information for each virtual machine in the compatible VMs and incompatible VMs worksheets.
- Added support for GetThroughput operation for the US Government and China Microsoft Azure regions.
- Added few more prerequisite checks for vCenter and ESXi Server.
- Fixed an issue of incorrect report getting generated when locale settings are set to non-English.

Version 1.1

Release Date: March 9, 2017

Fixes:

- Fixed an issue that prevented profiling VMs when there are two or more VMs with the same name or IP address across various vCenter ESXi hosts.
- Fixed an issue that caused copy and search to be disabled for the compatible VMs and incompatible VMs worksheets.

Version 1.0

Release Date: February 23, 2017

Known limitations:

- Supports only for VMware to Azure disaster recovery scenarios. For Hyper-V to Azure disaster recovery scenarios, use the [Hyper-V capacity planner tool](#).
- Doesn't support the GetThroughput operation for the US Government and China Microsoft Azure regions.
- The tool can't profile VMs if the vCenter server has two or more VMs with the same name or IP address across various ESXi hosts. In this version, the tool skips profiling for duplicate VM names or IP addresses in the VMListFile. The workaround is to profile the VMs by using an ESXi host instead of the vCenter server. Ensure to run one instance for each ESXi host.

Run the Deployment Planner for VMware disaster recovery

11/12/2019 • 18 minutes to read • [Edit Online](#)

This article is the Azure Site Recovery Deployment Planner user guide for VMware-to-Azure production deployments.

Modes of running deployment planner

You can run the command-line tool (ASRDeploymentPlanner.exe) in any of the following three modes:

1. [Profiling](#)
2. [Report generation](#)
3. [Get throughput](#)

First, run the tool in profiling mode to gather VM data churn and IOPS. Next, run the tool to generate the report to find the network bandwidth, storage requirements and DR cost.

Profile VMware VMs

In profiling mode, the deployment planner tool connects to the vCenter server/vSphere ESXi host to collect performance data about the VM.

- Profiling does not affect the performance of the production VMs, because no direct connection is made to them. All performance data is collected from the vCenter server/vSphere ESXi host.
- To ensure that there is a negligible impact on the server because of profiling, the tool queries the vCenter server/vSphere ESXi host once every 15 minutes. This query interval does not compromise profiling accuracy, because the tool stores every minute's performance counter data.

Create a list of VMs to profile

First, you need a list of the VMs to be profiled. You can get all the names of VMs on a vCenter server/vSphere ESXi host by using the VMware vSphere PowerCLI commands in the following procedure. Alternatively, you can list in a file the friendly names or IP addresses of the VMs that you want to profile manually.

1. Sign in to the VM that VMware vSphere PowerCLI is installed in.
2. Open the VMware vSphere PowerCLI console.
3. Ensure that the execution policy is enabled for the script. If it is disabled, launch the VMware vSphere PowerCLI console in administrator mode, and then enable it by running the following command:

```
Set-ExecutionPolicy -ExecutionPolicy AllSigned
```

4. You may optionally need to run the following command if Connect-VIServer is not recognized as the name of cmdlet.

```
Add-PSSnapin VMware.VimAutomation.Core
```

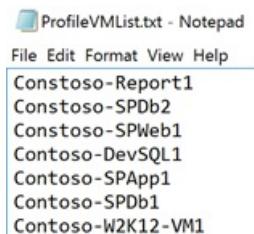
5. To get all the names of VMs on a vCenter server/vSphere ESXi host and store the list in a .txt file, run the two commands listed here. Replace <server name>, <user name>, <password>, <outputfile.txt> with your inputs.

```

Connect-VIServer -Server <server name> -User <user name> -Password <password>
Get-VM | Select Name | Sort-Object -Property Name > <outputfile.txt>

```

6. Open the output file in Notepad, and then copy the names of all VMs that you want to profile to another file (for example, ProfileVMList.txt), one VM name per line. This file is used as input to the *-VMListFile* parameter of the command-line tool.



The screenshot shows a Notepad window with the title 'ProfileVMList.txt - Notepad'. The menu bar includes File, Edit, Format, View, and Help. The main content area contains the following list of VM names:

```

Constoso-Report1
Constoso-SPDb2
Constoso-SPWeb1
Contoso-DevSQL1
Contoso-SPApp1
Contoso-SPDb1
Contoso-W2K12-VM1

```

Start profiling

After you have the list of VMs to be profiled, you can run the tool in profiling mode. Here is the list of mandatory and optional parameters of the tool to run in profiling mode.

```
ASRDeploymentPlanner.exe -Operation StartProfiling /?
```

PARAMETER NAME	DESCRIPTION
-Operation	StartProfiling
-Server	The fully qualified domain name or IP address of the vCenter server/vSphere ESXi host whose VMs are to be profiled.
-User	The user name to connect to the vCenter server/vSphere ESXi host. The user needs to have read-only access, at minimum.
-VMListFile	The file that contains the list of VMs to be profiled. The file path can be absolute or relative. The file should contain one VM name/IP address per line. Virtual machine name specified in the file should be the same as the VM name on the vCenter server/vSphere ESXi host. For example, the file VMList.txt contains the following VMs: <ul style="list-style-type: none"> • virtual_machine_A • 10.150.29.110 • virtual_machine_B
-NoOfMinutesToProfile	The number of minutes for which profiling is to be run. Minimum is 30 minutes.
-NoOfHoursToProfile	The number of hours for which profiling is to be run.
-NoOfDaysToProfile	The number of days for which profiling is to be run. We recommend that you run profiling for more than 7 days to ensure that the workload pattern in your environment over the specified period is observed and used to provide an accurate recommendation.
-Virtualization	Specify the virtualization type (VMware or Hyper-V).

PARAMETER NAME	DESCRIPTION
-Directory	(Optional) The universal naming convention (UNC) or local directory path to store profiling data generated during profiling. If a directory name is not given, the directory named 'ProfiledData' under the current path will be used as the default directory.
-Password	(Optional) The password to use to connect to the vCenter server/vSphere ESXi host. If you do not specify one now, you will be prompted for it when the command is executed.
-Port	(Optional) Port number to connect to vCenter/ESXi host. Default port is 443.
-Protocol	(Optional) Specified the protocol either 'http' or 'https' to connect to vCenter. Default protocol is https.
-StorageAccountName	(Optional) The storage-account name that's used to find the throughput achievable for replication of data from on-premises to Azure. The tool uploads test data to this storage account to calculate throughput. The storage account must be General-purpose v1 (GPv1) type.
-StorageAccountKey	(Optional) The storage-account key that's used to access the storage account. Go to the Azure portal > Storage accounts > <Storage account name> > Settings > Access Keys > Key1.
-Environment	(optional) This is your target Azure Storage account environment. This can be one of three values - AzureCloud,AzureUSGovernment, AzureChinaCloud. Default is AzureCloud. Use the parameter when your target Azure region is either Azure US Government or Azure China 21Vianet.

We recommend that you profile your VMs for more than 7 days. If churn pattern varies in a month, we recommend to profile during the week when you see the maximum churn. The best way is to profile for 31 days to get better recommendation. During the profiling period, ASRDeploymentPlanner.exe keeps running. The tool takes profiling time input in days. For a quick test of the tool or for proof of concept you can profile for few hours or minutes. The minimum allowed profiling time is 30 minutes.

During profiling, you can optionally pass a storage-account name and key to find the throughput that Site Recovery can achieve at the time of replication from the configuration server or process server to Azure. If the storage-account name and key are not passed during profiling, the tool does not calculate achievable throughput.

You can run multiple instances of the tool for various sets of VMs. Ensure that the VM names are not repeated in any of the profiling sets. For example, if you have profiled ten VMs (VM1 through VM10) and after few days you want to profile another five VMs (VM11 through VM15), you can run the tool from another command-line console for the second set of VMs (VM11 through VM15). Ensure that the second set of VMs do not have any VM names from the first profiling instance or you use a different output directory for the second run. If two instances of the tool are used for profiling the same VMs and use the same output directory, the generated report will be incorrect.

By default, the tool is configured to profile and generate report up to 1000 VMs. You can change limit by changing MaxVMsSupported key value in *ASRDeploymentPlanner.exe.config* file.

```
<!-- Maximum number of vms supported-->
<add key="MaxVmsSupported" value="1000"/>
```

With the default settings, to profile say 1500 VMs, create two VMList.txt files. One with 1000 VMs and other with 500 VM list. Run the two instances of Azure Site Recovery Deployment Planner, one with VMList1.txt and other with VMList2.txt. You can use the same directory path to store the profiled data of both the VMList VMs.

We have seen that based on the hardware configuration especially RAM size of the server from where the tool is run to generate the report, the operation may fail with insufficient memory. If you have good hardware, you can change the MaxVMsSupported any higher value.

If you have multiple vCenter servers, you need to run one instance of ASRDeploymentPlanner for each vCenter server for profiling.

VM configurations are captured once at the beginning of the profiling operation and stored in a file called VMdetailList.xml. This information is used when the report is generated. Any change in VM configuration (for example, an increased number of cores, disks, or NICs) from the beginning to the end of profiling is not captured. If a profiled VM configuration has changed during the course of profiling, in the public preview, here is the workaround to get latest VM details when generating the report:

- Back up VMdetailList.xml, and delete the file from its current location.
- Pass -User and -Password arguments at the time of report generation.

The profiling command generates several files in the profiling directory. Do not delete any of the files, because doing so affects report generation.

Example 1: Profile VMs for 30 days, and find the throughput from on-premises to Azure

```
ASRDeploymentPlanner.exe -Operation StartProfiling -Virtualization VMware -Directory
"E:\vCenter1_ProfiledData" -Server vCenter1.contoso.com -VMListFile
"E:\vCenter1_ProfiledData\ProfileVMList1.txt" -NoOfDaysToProfile 30 -User vCenterUser1 -StorageAccountName
asrspfarm1 -StorageAccountKey
Eby8vdM02xN0cqFlqUwJPLlmEt1CDXJ10UzFT50uSRZ6IFsuFq2UVErCz4I6tq/K1SZFPT0tr/KBHBeksoGMGw==
```

Example 2: Profile VMs for 15 days

```
ASRDeploymentPlanner.exe -Operation StartProfiling -Virtualization VMware -Directory
"E:\vCenter1_ProfiledData" -Server vCenter1.contoso.com -VMListFile
"E:\vCenter1_ProfiledData\ProfileVMList1.txt" -NoOfDaysToProfile 15 -User vCenterUser1
```

Example 3: Profile VMs for 60 minutes for a quick test of the tool

```
ASRDeploymentPlanner.exe -Operation StartProfiling -Virtualization VMware -Directory
"E:\vCenter1_ProfiledData" -Server vCenter1.contoso.com -VMListFile
"E:\vCenter1_ProfiledData\ProfileVMList1.txt" -NoOfMinutesToProfile 60 -User vCenterUser1
```

Example 4: Profile VMs for 2 hours for a proof of concept

```
ASRDeploymentPlanner.exe -Operation StartProfiling -Virtualization VMware -Directory
"E:\vCenter1_ProfiledData" -Server vCenter1.contoso.com -VMListFile
"E:\vCenter1_ProfiledData\ProfileVMList1.txt" -NoOfHoursToProfile 2 -User vCenterUser1
```

NOTE

- If the server that the tool is running on is rebooted or has crashed, or if you close the tool by using Ctrl + C, the profiled data is preserved. However, there is a chance of missing the last 15 minutes of profiled data. In such an instance, rerun the tool in profiling mode after the server restarts.
- When the storage-account name and key are passed, the tool measures the throughput at the last step of profiling. If the tool is closed before profiling is completed, the throughput is not calculated. To find the throughput before generating the report, you can run the GetThroughput operation from the command-line console. Otherwise, the generated report will not contain the throughput information.

Generate report

The tool generates a macro-enabled Microsoft Excel file (XLSM file) as the report output, which summarizes all the deployment recommendations. The report is named

`DeploymentPlannerReport_<unique numeric identifier>.xslm` and placed in the specified directory.

NOTE

The report generation requires a Windows PC or Windows Server with Excel 2013 or later. The decimal symbol on this machine should be configured as "." to produce the cost estimates. In case you have setup "," as decimal symbol, please go to "Change date, time or number formats" in Control Panel and go to "Additional Settings" to change the decimal symbol to ":".

After profiling is complete, you can run the tool in report-generation mode. The following table contains a list of mandatory and optional tool parameters to run in report-generation mode.

`ASRDeploymentPlanner.exe -Operation GenerateReport /?`

PARAMETER NAME	DESCRIPTION
-Operation	GenerateReport
-Server	The vCenter/vSphere server fully qualified domain name or IP address (use the same name or IP address that you used at the time of profiling) where the profiled VMs whose report is to be generated are located. Note that if you used a vCenter server at the time of profiling, you cannot use a vSphere server for report generation, and vice-versa.
-VMListFile	The file that contains the list of profiled VMs that the report is to be generated for. The file path can be absolute or relative. The file should contain one VM name or IP address per line. The VM names that are specified in the file should be the same as the VM names on the vCenter server/vSphere ESXi host, and match what was used during profiling.
-Virtualization	Specify the virtualization type (VMware or Hyper-V).
-Directory	(Optional) The UNC or local directory path where the profiled data (files generated during profiling) is stored. This data is required for generating the report. If a name isn't specified, 'ProfiledData' directory will be used.

PARAMETER NAME	DESCRIPTION
-GoalToCompleteIR	(Optional) The number of hours in which the initial replication of the profiled VMs needs to be completed. The generated report provides the number of VMs for which initial replication can be completed in the specified time. The default is 72 hours.
-User	(Optional) The user name to use to connect to the vCenter/vSphere server. The name is used to fetch the latest configuration information of the VMs, such as the number of disks, number of cores, and number of NICs, to use in the report. If the name isn't provided, the configuration information collected at the beginning of the profiling kickoff is used.
-Password	(Optional) The password to use to connect to the vCenter server/vSphere ESXi host. If the password isn't specified as a parameter, you will be prompted for it later when the command is executed.
-Port	(Optional) Port number to connect to vCenter/ESXi host. Default port is 443.
-Protocol	(Optional) Specified the protocol either 'http' or 'https' to connect to vCenter. Default protocol is https.
-DesiredRPO	(Optional) The desired recovery point objective, in minutes. The default is 15 minutes.
-Bandwidth	Bandwidth in Mbps. The parameter to use to calculate the RPO that can be achieved for the specified bandwidth.
-StartDate	(Optional) The start date and time in MM-DD-YYYY:HH:MM (24-hour format). <i>StartDate</i> must be specified along with <i>EndDate</i> . When <i>StartDate</i> is specified, the report is generated for the profiled data that's collected between <i>StartDate</i> and <i>EndDate</i> .
-EndDate	(Optional) The end date and time in MM-DD-YYYY:HH:MM (24-hour format). <i>EndDate</i> must be specified along with <i>StartDate</i> . When <i>EndDate</i> is specified, the report is generated for the profiled data that's collected between <i>StartDate</i> and <i>EndDate</i> .
-GrowthFactor	(Optional) The growth factor, expressed as a percentage. The default is 30 percent.
-UseManagedDisks	(Optional) UseManagedDisks - Yes/No. Default is Yes. The number of virtual machines that can be placed into a single storage account is calculated considering whether Failover/Test failover of virtual machines is done on managed disk instead of unmanaged disk.

PARAMETER NAME	DESCRIPTION
-SubscriptionId	(Optional) The subscription GUID. Note that this parameter is required when you need to generate the cost estimation report with the latest price based on your subscription, the offer that is associated with your subscription and for your specific target Azure region in the specified currency .
-TargetRegion	(Optional) The Azure region where replication is targeted. Since Azure has different costs per region, to generate report with specific target Azure region use this parameter. Default is WestUS2 or the last used target region. Refer to the list of supported target regions .
-OfferId	(Optional) The offer associated with the give subscription. Default is MS-AZR-0003P (Pay-As-You-Go).
-Currency	(Optional) The currency in which cost is shown in the generated report. Default is US Dollar (\$) or the last used currency. Refer to the list of supported currencies .

By default, the tool is configured to profile and generate report up to 1000 VMs. You can change limit by changing MaxVmsSupported key value in *ASRDeploymentPlanner.exe.config* file.

```
<!-- Maximum number of vms supported-->
<add key="MaxVmsSupported" value="1000"/>
```

Example 1: Generate a report with default values when the profiled data is on the local drive

```
ASRDeploymentPlanner.exe -Operation GenerateReport -Virtualization VMware -Server vCenter1.contoso.com -
Directory "E:\vCenter1_ProfiledData" -VMListFile "E:\vCenter1_ProfiledData\ProfileVMList1.txt"
```

Example 2: Generate a report when the profiled data is on a remote server

You should have read/write access on the remote directory.

```
ASRDeploymentPlanner.exe -Operation GenerateReport -Virtualization VMware -Server vCenter1.contoso.com -
Directory "\\\PS1-W2K12R2\vCenter1_ProfiledData" -VMListFile "\\\PS1-
W2K12R2\vCenter1_ProfiledData\ProfileVMList1.txt"
```

Example 3: Generate a report with a specific bandwidth and goal to complete IR within specified time

```
ASRDeploymentPlanner.exe -Operation GenerateReport -Virtualization VMware -Server vCenter1.contoso.com -
Directory "E:\vCenter1_ProfiledData" -VMListFile "E:\vCenter1_ProfiledData\ProfileVMList1.txt" -Bandwidth 100
-GoalToCompleteIR 24
```

Example 4: Generate a report with a 5 percent growth factor instead of the default 30 percent

```
ASRDeploymentPlanner.exe -Operation GenerateReport -Virtualization VMware -Server vCenter1.contoso.com -
Directory "E:\vCenter1_ProfiledData" -VMListFile "E:\vCenter1_ProfiledData\ProfileVMList1.txt" -GrowthFactor 5
```

Example 5: Generate a report with a subset of profiled data

For example, you have 30 days of profiled data and want to generate a report for only 20 days.

```
ASRDeploymentPlanner.exe -Operation GenerateReport -Virtualization VMware -Server vCenter1.contoso.com -  
Directory "E:\vCenter1_ProfiledData" -VMListFile "E:\vCenter1_ProfiledData\ProfileVMList1.txt" -StartDate 01-  
10-2017:12:30 -EndDate 01-19-2017:12:30
```

Example 6: Generate a report for 5-minute RPO

```
ASRDeploymentPlanner.exe -Operation GenerateReport -Virtualization VMware -Server vCenter1.contoso.com -  
Directory "E:\vCenter1_ProfiledData" -VMListFile "E:\vCenter1_ProfiledData\ProfileVMList1.txt" -DesiredRPO 5
```

Example 7: Generate a report for South India Azure region with Indian Rupee and specific offer ID

Note that the subscription ID is required to generate cost report in a specific currency.

```
ASRDeploymentPlanner.exe -Operation GenerateReport -Virtualization VMware -Directory  
"E:\vCenter1_ProfiledData" -VMListFile "E:\vCenter1_ProfiledData\ProfileVMList1.txt" -SubscriptionID  
4d19f16b-3e00-4b89-a2ba-8645edf42fe5 -OfferID MS-AZR-0148P -TargetRegion southindia -Currency INR
```

Percentile value used for the calculation

What default percentile value of the performance metrics collected during profiling does the tool use when it generates a report?

The tool defaults to the 95th percentile values of read/write IOPS, write IOPS, and data churn that are collected during profiling of all the VMs. This metric ensures that the 100th percentile spike your VMs might see because of temporary events is not used to determine your target storage-account and source-bandwidth requirements. For example, a temporary event might be a backup job running once a day, a periodic database indexing or analytics report-generation activity, or other similar short-lived, point-in-time events.

Using 95th percentile values gives a true picture of real workload characteristics, and it gives you the best performance when the workloads are running on Azure. We do not anticipate that you would need to change this number. If you do change the value (to the 90th percentile, for example), you can update the configuration file *ASRDeploymentPlanner.exe.config* in the default folder and save it to generate a new report on the existing profiled data.

```
<add key="WriteIOPSPercentile" value="95" />  
<add key="ReadWriteIOPSPercentile" value="95" />  
<add key="DataChurnPercentile" value="95" />
```

Growth-factor considerations

Why should I consider growth factor when I plan deployments?

It is critical to account for growth in your workload characteristics, assuming a potential increase in usage over time. After protection is in place, if your workload characteristics change, you cannot switch to a different storage account for protection without disabling and re-enabling the protection.

For example, let's say that today your VM fits in a standard storage replication account. Over the next three months, several changes are likely to occur:

- The number of users of the application that runs on the VM will increase.
- The resulting increased churn on the VM will require the VM to go to premium storage so that Site Recovery replication can keep pace.
- Consequently, you will have to disable and re-enable protection to a premium storage account.

We strongly recommend that you plan for growth during deployment planning and while the default value is 30

percent. You are the expert on your application usage pattern and growth projections, and you can change this number accordingly while generating a report. Moreover, you can generate multiple reports with various growth factors with the same profiled data and determine what target storage and source bandwidth recommendations work best for you.

The generated Microsoft Excel report contains the following information:

- [On-premises Summary](#)
- [Recommendations](#)
- [VM<->Storage Placement](#)
- [Compatible VMs](#)
- [Incompatible VMs](#)
- [Cost Estimation](#)


Microsoft Azure Site Recovery Deployment Planner

Recommendations for VMware to Azure

Profiled data period: 10 days (11/1/2017 - 11/10/2017) Server Name: vCenter1.contoso.com Desired RPO: 15

Profiling Overview

110
 Total Profiled Virtual Machines

107
 Virtual Machines Compatible
 (Click for details)

3
 Virtual Machines Incompatible
 (Click for details)

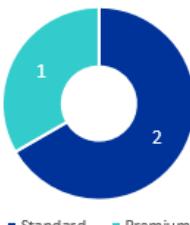
15
 Desired RPO (minutes)

Required Network Bandwidth (Mbps) For Delta Replication

Achieved Throughput	230
To meet RPO 90% of the time	570
To meet RPO 100% of the time	704

[Recommendation: Use ExpressRoute](#)

Required Azure Storage Accounts Total: 3



[Recommended VM placement plan](#)

Required Number of Azure Cores

 **610**

[Learn more about Azure subscription limits](#)

Required On-Premises Infrastructure

 **1** Configuration Servers  **0** Additional Process Servers

[Learn more about configuring these servers](#)

What if you provision lower bandwidth (Mbps): 570

If the bandwidth provided **570 Mbps** you can achieve **15** minutes RPO for **90%** of the time and you will have **22** RPO violations

RPO Violations over Profiling Period

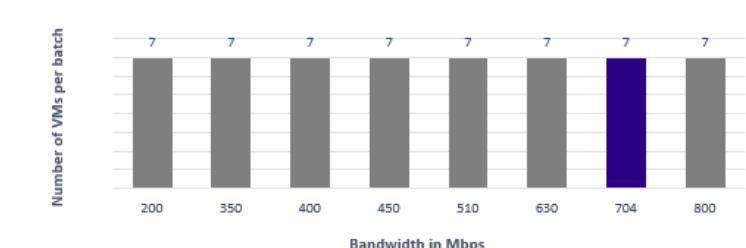


Recommended VM Batch Size for Initial Replication

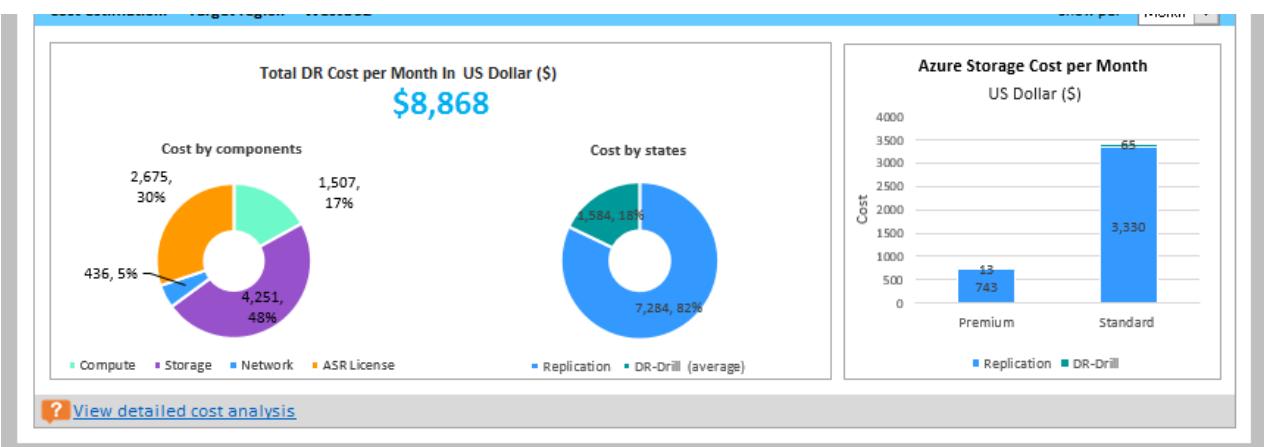
IR of batch of **7 VMs** will complete within **72 hours** with allocated bandwidth of **704 Mbps**

Recommended VM Batch Size for Initial Replication to Complete in (Hours): 72

Average detected VM size (GB): **672**



Cost estimation: Target region - WestUS2 Show per Month



Growth factor considered for all virtual machines (%): 30 [Learn more](#)

Max value of IOPS and data churn of the profiled data considered for calculating bandwidth and Azure storage type: [Learn more](#)

Write IOPS percentile: 95

Read/Write IOPS percentile: 95

Data churn percentile: 95

Note:

- Recommended network bandwidth should be dedicated for Azure Site Recovery replication
- Desired RPO implies acceptable delay of data transfer from on-premises to Azure
- Number of RPO violations identified are spread across the total duration of profiling days and not just for one day
- There may be multiple RPO violations occurred on a day - the RPO violations graph shows the peak RPO hit every day

On-Premises Summary | **Recommendations** | VM<->Storage Placement | Compatible VMs | Incompatible VMs | ... | [+](#)

Get throughput

To estimate the throughput that Site Recovery can achieve from on-premises to Azure during replication, run the tool in GetThroughput mode. The tool calculates the throughput from the server that the tool is running on. Ideally, this server is based on the configuration server sizing guide. If you have already deployed Site Recovery infrastructure components on-premises, run the tool on the configuration server.

Open a command-line console, and go to the Site Recovery deployment planning tool folder. Run ASRDeploymentPlanner.exe with following parameters.

```
ASRDeploymentPlanner.exe -Operation GetThroughput /?
```

PARAMETER NAME	DESCRIPTION
-Operation	GetThroughput
-Virtualization	Specify the virtualization type (VMware or Hyper-V).
-Directory	(Optional) The UNC or local directory path where the profiled data (files generated during profiling) is stored. This data is required for generating the report. If a directory name is not specified, 'ProfiledData' directory is used.
-StorageAccountName	The storage-account name that's used to find the bandwidth consumed for replication of data from on-premises to Azure. The tool uploads test data to this storage account to find the bandwidth consumed. The storage account must be either General-purpose v1 (GPv1) type.
-StorageAccountKey	The storage-account key that's used to access the storage account. Go to the Azure portal > Storage accounts > <Storage account name> > Settings > Access Keys > Key1 (or a primary access key for a classic storage account).

PARAMETER NAME	DESCRIPTION
-VMListFile	<p>The file that contains the list of VMs to be profiled for calculating the bandwidth consumed. The file path can be absolute or relative. The file should contain one VM name/IP address per line. The VM names specified in the file should be the same as the VM names on the vCenter server/vSphere ESXi host.</p> <p>For example, the file VMList.txt contains the following VMs:</p> <ul style="list-style-type: none"> • VM_A • 10.150.29.110 • VM_B
-Environment	<p>(optional) This is your target Azure Storage account environment. This can be one of three values - AzureCloud,AzureUSGovernment, AzureChinaCloud. Default is AzureCloud. Use the parameter when your target Azure region is either Azure US Government or Azure China 21Vianet.</p>

The tool creates several 64-MB asrvhdfile<#>.vhf files (where "#" is the number of files) on the specified directory. The tool uploads the files to the storage account to find the throughput. After the throughput is measured, the tool deletes all the files from the storage account and from the local server. If the tool is terminated for any reason while it is calculating throughput, it doesn't delete the files from the storage or from the local server. You will have to delete them manually.

The throughput is measured at a specified point in time, and it is the maximum throughput that Site Recovery can achieve during replication, provided that all other factors remain the same. For example, if any application starts consuming more bandwidth on the same network, the actual throughput varies during replication. If you are running the GetThroughput command from a configuration server, the tool is unaware of any protected VMs and ongoing replication. The result of the measured throughput is different if the GetThroughput operation is run when the protected VMs have high data churn. We recommend that you run the tool at various points in time during profiling to understand what throughput levels can be achieved at various times. In the report, the tool shows the last measured throughput.

Example

```
ASRDeploymentPlanner.exe -Operation GetThroughput -Directory E:\vCenter1_ProfiledData -Virtualization VMware
-VMListFile E:\vCenter1_ProfiledData\ProfileVMList1.txt -StorageAccountName asrspfarm1 -StorageAccountKey
by8vdM02xN0cqFlqUwJPL1mEt1CDXJ10UzFT50uSRZ6IFsuFq2UVErCz4I6tq/K1SZFPT0tr/KBHbeksoGMGw==
```

NOTE

Run the tool on a server that has the same storage and CPU characteristics as the configuration server.

For replication, set the recommended bandwidth to meet the RPO 100 percent of the time. After you set the right bandwidth, if you don't see an increase in the achieved throughput reported by the tool, do the following:

1. Check to determine whether there is any network Quality of Service (QoS) that is limiting Site Recovery throughput.
2. Check to determine whether your Site Recovery vault is in the nearest physically supported Microsoft Azure region to minimize network latency.
3. Check your local storage characteristics to determine whether you can improve the hardware (for example, HDD to SSD).
4. Change the Site Recovery settings in the process server to [increase the amount of network bandwidth used for replication](#).

Next steps

- [Analyze the generated report](#).

Analyze the Deployment Planner report for VMware disaster recovery to Azure

12/26/2019 • 18 minutes to read • [Edit Online](#)

The generated Microsoft Excel report contains the following sheets:

On-premises summary

The On-premises summary worksheet provides an overview of the profiled VMware environment.



Microsoft Azure Site Recovery Deployment Planner Report

Profiled Report for	VMware to Azure
Start date	11/1/2017
End date	11/10/2017
Total number of profiling days	10

Source Environment Summary

Deployment planning recommendation has been generated based on following source environment details and desired replication inputs

Total number of profiled virtual machines	110
Number of compatible virtual machines	107
Total number of disks across all compatible virtual machines	310
Average number of disks per compatible virtual machine	2.90
Average disk size (GB)	232
Total data to be replicated for initial replication (GB)	71,920
Desired RPO (minutes)	15
Desired bandwidth (Mbps)	NA
Observed typical data churn per day (GB)	2,010

Start Date and End Date: The start and end dates of the profiling data considered for report generation. By default, the start date is the date when profiling starts, and the end date is the date when profiling stops. This can be the 'StartDate' and 'EndDate' values if the report is generated with these parameters.

Total number of profiling days: The total number of days of profiling between the start and end dates for which the report is generated.

Number of compatible virtual machines: The total number of compatible VMs for which the required network bandwidth, required number of storage accounts, Microsoft Azure cores, configuration servers and additional process servers are calculated.

Total number of disks across all compatible virtual machines: The number that's used as one of the inputs to decide the number of configuration servers and additional process servers to be used in the deployment.

Average number of disks per compatible virtual machine: The average number of disks calculated across all compatible VMs.

Average disk size (GB): The average disk size calculated across all compatible VMs.

Desired RPO (minutes): Either the default recovery point objective or the value passed for the 'DesiredRPO' parameter at the time of report generation to estimate required bandwidth.

Desired bandwidth (Mbps): The value that you have passed for the 'Bandwidth' parameter at the time of report

generation to estimate achievable RPO.

Observed typical data churn per day (GB): The average data churn observed across all profiling days. This number is used as one of the inputs to decide the number of configuration servers and additional process servers to be used in the deployment.

Recommendations

The recommendations sheet of the VMware to Azure report has the following details as per the selected desired RPO:

Microsoft Azure Site Recovery Deployment Planner

Recommendations for VMware to Azure

Profiled data period: 10 days (11/1/2017 - 11/10/2017) Server Name: vCenter1.contoso.com Desired RPO: 15

Profiling Overview

110 Total Profiled Virtual Machines	107 Virtual Machines Compatible (Click for details)	3 Virtual Machines Incompatible (Click for details)	15 Desired RPO (minutes)
---	--	--	------------------------------------

Required Network Bandwidth (Mbps) For Delta Replication

Achieved Throughput: 230	To meet RPO 90% of the time: 570	To meet RPO 100% of the time: 704
--------------------------	----------------------------------	-----------------------------------

Recommendation: Use ExpressRoute

Required Azure Storage Accounts Total: 3

Recommended VM placement plan

Required Number of Azure Cores

610

[Learn more about Azure subscription limits](#)

Required On-Premises Infrastructure

1 Configuration Servers **0 Additional Process Servers**

[Learn more about configuring these servers](#)

What if you provision lower bandwidth (Mbps): 570

If the bandwidth provided 570 Mbps you can achieve 15 minutes RPO for 90% of the time and you will have 22 RPO violations	RPO Violations over Profiling Period Peak RPO per day
---	---

Recommended VM Batch Size for Initial Replication

IR of batch of **7 VMs** will complete within **72 hours** with allocated bandwidth of **704 Mbps**

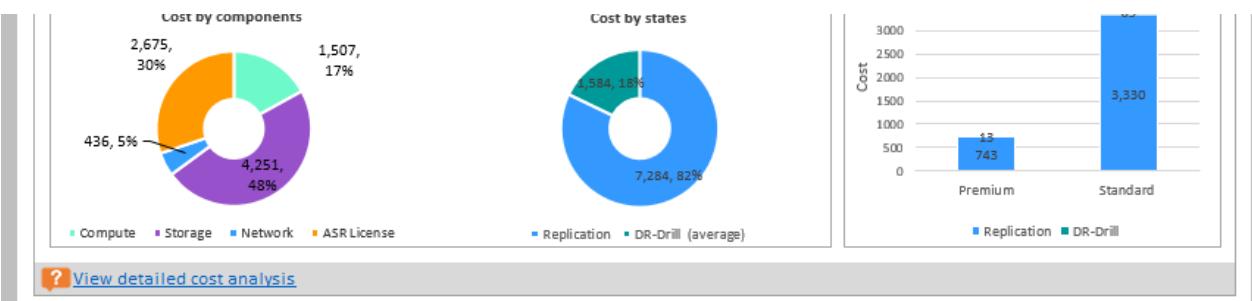
Recommended VM Batch Size for Initial Replication to Complete in (Hours): 72

Average detected VM size (GB): **672**

Cost estimation: Target region - WestUS2

Show per Month

Total DR Cost per Month In US Dollar (\$) \$8,868	Azure Storage Cost per Month US Dollar (\$)
---	--



Growth factor considered for all virtual machines (%): 30 [Learn more](#)

Max value of IOPS and data churn of the profiled data considered for calculating bandwidth and Azure storage type: [Learn more](#)

Write IOPS percentile: 95

Read/Write IOPS percentile: 95

Data churn percentile: 95

Note:

- Recommended network bandwidth should be dedicated for Azure Site Recovery replication
- Desired RPO implies acceptable delay of data transfer from on-premises to Azure
- Number of RPO violations identified are spread across the total duration of profiling days and not just for one day
- There may be multiple RPO violations occurred on a day - the RPO violations graph shows the peak RPO hit every day



Profiled data

Microsoft Azure Site Recovery Deployment Planner

Recommendations for VMware to Azure

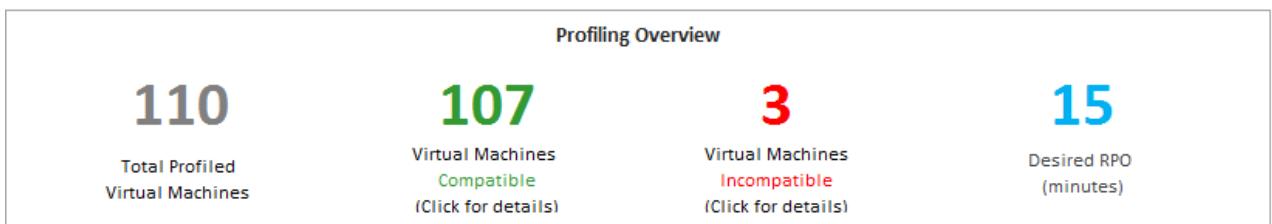
Profiled data period: 10 days (11/1/2017 - 11/10/2017) Server Name: vCenter1.contoso.com Desired RPO: 15

Profiled data period: The period during which the profiling was run. By default, the tool includes all profiled data in the calculation, unless it generates the report for a specific period by using StartDate and EndDate options during report generation.

Server Name: The name or IP address of the VMware vCenter or ESXi host whose VMs' report is generated.

Desired RPO: The recovery point objective for your deployment. By default, the required network bandwidth is calculated for RPO values of 15, 30, and 60 minutes. Based on the selection, the affected values are updated on the sheet. If you have used the *DesiredRPOinMin* parameter while generating the report, that value is shown in the Desired RPO result.

Profiling overview



Total Profiled Virtual Machines: The total number of VMs whose profiled data is available. If the VMListFile has names of any VMs which were not profiled, those VMs are not considered in the report generation and are excluded from the total profiled VMs count.

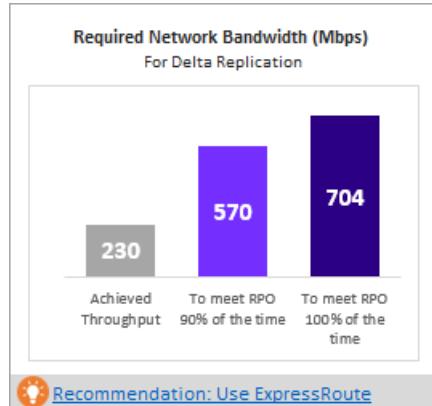
Compatible Virtual Machines: The number of VMs that can be protected to Azure by using Site Recovery. It is the total number of compatible VMs for which the required network bandwidth, number of storage accounts, number of Azure cores, and number of configuration servers and additional process servers are calculated. The details of every compatible VM are available in the "Compatible VMs" section.

Incompatible Virtual Machines: The number of profiled VMs that are incompatible for protection with Site Recovery. The reasons for incompatibility are noted in the "Incompatible VMs" section. If the VMListFile has

names of any VMs that were not profiled, those VMs are excluded from the incompatible VMs count. These VMs are listed as "Data not found" at the end of the "Incompatible VMs" section.

Desired RPO: Your desired recovery point objective, in minutes. The report is generated for three RPO values: 15 (default), 30, and 60 minutes. The bandwidth recommendation in the report is changed based on your selection in the Desired RPO drop-down list at the top right of the sheet. If you have generated the report by using the `-DesiredRPO` parameter with a custom value, this custom value will show as the default in the Desired RPO drop-down list.

Required network bandwidth (Mbps)



To meet RPO 100 percent of the time: The recommended bandwidth in Mbps to be allocated to meet your desired RPO 100 percent of the time. This amount of bandwidth must be dedicated for steady-state delta replication of all your compatible VMs to avoid any RPO violations.

To meet RPO 90 percent of the time: Because of broadband pricing or for any other reason, if you cannot set the bandwidth needed to meet your desired RPO 100 percent of the time, you can choose to go with a lower bandwidth setting that can meet your desired RPO 90 percent of the time. To understand the implications of setting this lower bandwidth, the report provides a what-if analysis on the number and duration of RPO violations to expect.

Achieved Throughput: The throughput from the server on which you have run the GetThroughput command to the Microsoft Azure region where the storage account is located. This throughput number indicates the estimated level that you can achieve when you protect the compatible VMs by using Site Recovery, provided that your configuration server or process server storage and network characteristics remain the same as that of the server from which you have run the tool.

For replication, you should set the recommended bandwidth to meet the RPO 100 percent of the time. After you set the bandwidth, if you don't see any increase in the achieved throughput, as reported by the tool, do the following:

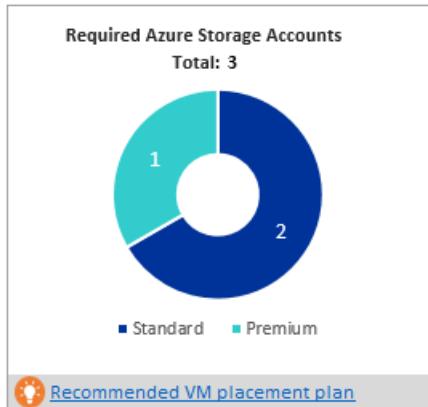
1. Check to see whether there is any network Quality of Service (QoS) that is limiting Site Recovery throughput.
2. Check to see whether your Site Recovery vault is in the nearest physically supported Microsoft Azure region to minimize network latency.
3. Check your local storage characteristics to determine whether you can improve the hardware (for example, HDD to SSD).
4. Change the Site Recovery settings in the process server to [increase the amount network bandwidth used for replication](#).

If you are running the tool on a configuration server or process server that already has protected VMs, run the tool a few times. The achieved throughput number changes depending on the amount of churn being processed at that point in time.

For all enterprise Site Recovery deployments, we recommend that you use [ExpressRoute](#).

Required storage accounts

The following chart shows the total number of storage accounts (standard and premium) that are required to protect all the compatible VMs. To learn which storage account to use for each VM, see the "VM-storage placement" section. If you are using v2.5 of Deployment Planner, this recommendation only shows the number of standard cache storage accounts which are needed for replication since the data is being directly written to Managed Disks.



Required number of Azure cores

This result is the total number of cores to be set up before failover or test failover of all the compatible VMs. If too few cores are available in the subscription, Site Recovery fails to create VMs at the time of test failover or failover.



Required on-premises infrastructure

This figure is the total number of configuration servers and additional process servers to be configured that would suffice to protect all the compatible VMs. Depending on the supported [size recommendations for the configuration server](#), the tool might recommend additional servers. The recommendation is based on the larger of either the per-day churn or the maximum number of protected VMs (assuming an average of three disks per VM), whichever is hit first on the configuration server or the additional process server. You'll find the details of total churn per day and total number of protected disks in the "On-premises summary" section.



What-if analysis

This analysis outlines how many violations could occur during the profiling period when you set a lower bandwidth for the desired RPO to be met only 90 percent of the time. One or more RPO violations can occur on any given day. The graph shows the peak RPO of the day. Based on this analysis, you can decide if the number of RPO violations across all days and peak RPO hit per day is acceptable with the specified lower bandwidth. If it is acceptable, you can allocate the lower bandwidth for replication, else allocate the higher bandwidth as suggested to meet the desired RPO 100 percent of the time.

What if you provision lower bandwidth (Mbps): 570

If the bandwidth provided
570 Mbps
you can achieve
15 minutes RPO
for
90% of the time
and you will have
22 RPO violations

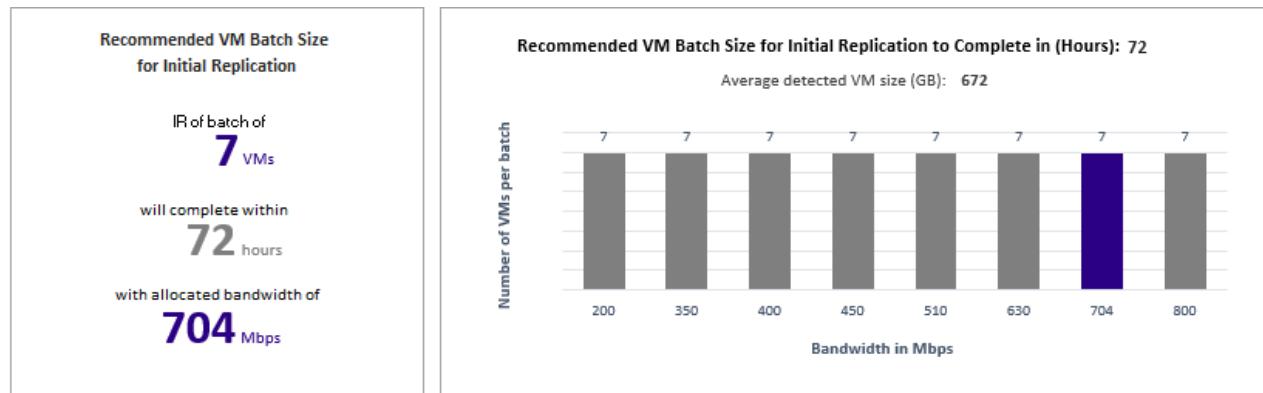


Recommended VM batch size for initial replication

In this section, we recommend the number of VMs that can be protected in parallel to complete the initial replication within 72 hours with the suggested bandwidth to meet desired RPO 100 percent of the time being set. This value is configurable value. To change it at report-generation time, use the *GoalToCompleteIR* parameter.

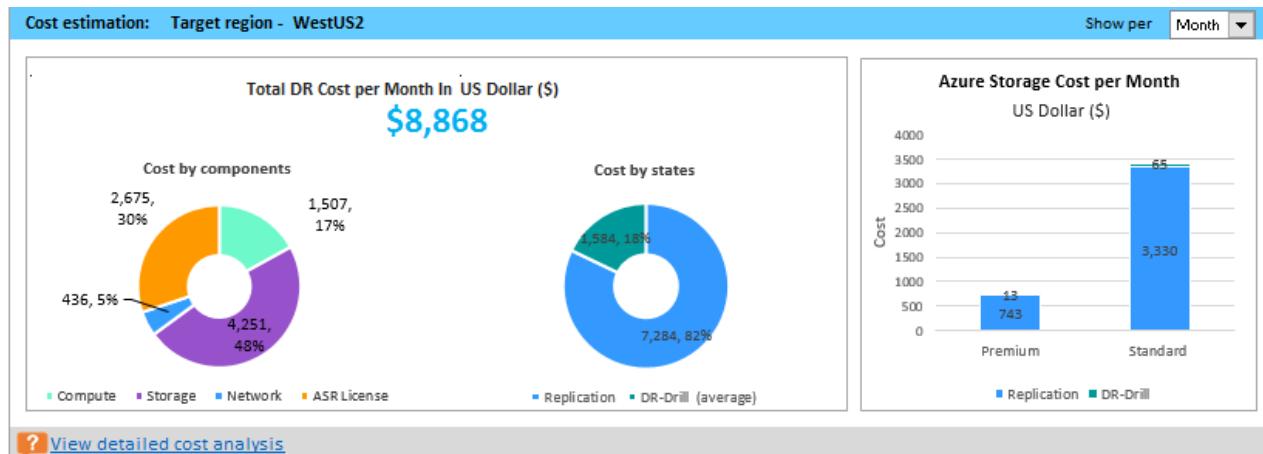
The graph here shows a range of bandwidth values and a calculated VM batch size count to complete initial replication in 72 hours, based on the average detected VM size across all the compatible VMs.

In the public preview, the report does not specify which VMs should be included in a batch. You can use the disk size shown in the "Compatible VMs" section to find each VM's size and select them for a batch, or you can select the VMs based on known workload characteristics. The completion time of the initial replication changes proportionally, based on the actual VM disk size, used disk space, and available network throughput.



Cost estimation

The graph shows the summary view of the estimated total disaster recovery (DR) cost to Azure of your chosen target region and the currency that you have specified for report generation.



The summary helps you to understand the cost that you need to pay for storage, compute, network, and license when you protect all your compatible VMs to Azure using Azure Site Recovery. The cost is calculated on for compatible VMs and not on all the profiled VMs.

You can view the cost either monthly or yearly. Learn more about [supported target regions](#) and [supported currencies](#).

Cost by components The total DR cost is divided into four components: Compute, Storage, Network, and Azure Site Recovery license cost. The cost is calculated based on the consumption that will be incurred during replication and at DR drill time for compute, storage (premium and standard), ExpressRoute/VPN that is configured between the on-premises site and Azure, and Azure Site Recovery license.

Cost by states The total disaster recovery (DR) cost is categories based on two different states - Replication and DR drill.

Replication cost: The cost that will be incurred during replication. It covers the cost of storage, network, and Azure Site Recovery license.

DR-Drill cost: The cost that will be incurred during test failovers. Azure Site Recovery spins up VMs during test failover. The DR drill cost covers the running VMs' compute and storage cost.

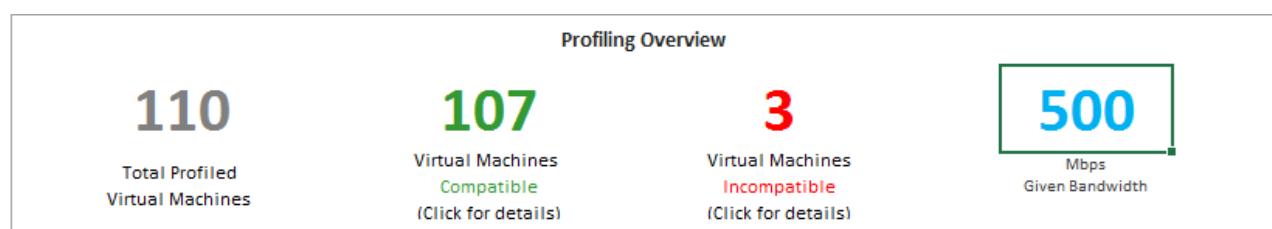
Azure storage cost per Month/Year It shows the total storage cost that will be incurred for premium and standard storage for replication and DR drill. You can view detailed cost analysis per VM in the [Cost Estimation](#) sheet.

Growth factor and percentile values used

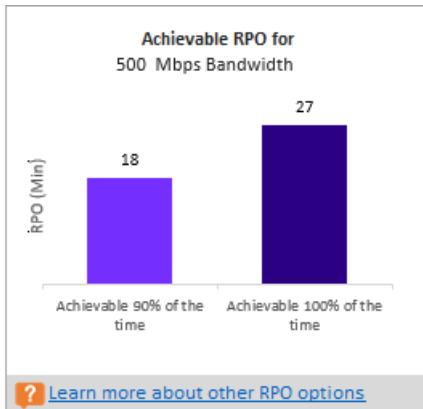
This section at the bottom of the sheet shows the percentile value used for all the performance counters of the profiled VMs (default is 95th percentile), and the growth factor (default is 30 percent) that's used in all the calculations.

Growth factor considered for all virtual machines (%):	30	Learn more
Max value of IOPS and data churn of the profiled data considered for calculating bandwidth and Azure storage type:		Learn more
Write IOPS percentile:	95	
Read/Write IOPS percentile	95	
Data churn percentile:	95	
Note:		
• Recommended network bandwidth should be dedicated for Azure Site Recovery replication		
• Desired RPO implies acceptable delay of data transfer from on-premises to Azure		
• Number of RPO violations identified are spread across the total duration of profiling days and not just for one day		
• There may be multiple RPO violations occurred on a day - the RPO violations graph shows the peak RPO hit every day		

Recommendations with available bandwidth as input



You might have a situation where you know that you cannot set a bandwidth of more than x Mbps for Site Recovery replication. The tool allows you to input available bandwidth (using the -Bandwidth parameter during report generation) and get the achievable RPO in minutes. With this achievable RPO value, you can decide whether you need to set up additional bandwidth or you are OK with having a disaster recovery solution with this RPO.



VM-storage placement

NOTE

Deployment Planner v2.5 onwards recommends the storage placement for machines which will replicate directly to managed disks.

Replication Storage Type (Managed Disk Type)	Log Storage Account Type	Suggested Prefix for Storage account	Suggested Log Account Name	Placement Summary	Vms to Place
Standard HDD	Standard	mum	mum<standard>		
Premium SSD	Standard	mum	mum<standard>		

Replication Storage Type: Either a standard or premium managed disk, which is used to replicate all the corresponding VMs mentioned in the **VMs to Place** column.

Log Storage Account Type: All the replication logs are stored in a standard storage account.

Suggested Prefix for Storage Account: The suggested three-character prefix that can be used for naming the cache storage account. You can use your own prefix, but the tool's suggestion follows the [partition naming convention for storage accounts](#).

Suggested Log Account Name: The storage-account name after you include the suggested prefix. Replace the name within the angle brackets (< and >) with your custom input.

Placement Summary: A summary of the disks needed to protect VMs by storage type. It includes the total number of VMs, total provisioned size across all disks, and total number of disks.

Virtual Machines to Place: A list of all the VMs that should be placed on the given storage account for optimal performance and use.

Compatible VMs

VM Name	VM Compatibility	Storage Type	asrseeddisk (Managed Disk) created for replication	Peak R/W IOPS (with Growth Factor)	Peak Data Churn (Mbps) (with Growth Factor)	Azure VM Size	Number of Disks	Disk Size (GB)	Cores	Memory (MB)	NICs	Boot Type	OS Type
an-mt01 (10.150.8.10)	Yes	Standard		6	0.06	Standard_A4	2	340	8	8192	1	BIOS	Microsoft Windows Server 2012 (64-bit)
scsi0:1 Hard disk 2		\$20	asrseeddisk-scsi0:1{GUID}	0	0.00			300					
scsi0:0 Hard disk 1		\$6	asrseeddisk-scsi0:0{GUID}	6	0.06			40					
an-mt02 (10.150.8.16)	Yes	Standard		3	0.02	Standard_A4	2	340	8	8192	1	BIOS	Microsoft Windows Server 2012 (64-bit)
scsi0:0 Hard disk 1		\$6		3	0.02			40					
scsi0:1 Hard disk 2		\$20		0	0.00			300					
an-mt03 (10.150.8.17)	Yes	Standard		3	0.02	Standard_A4	2	380	8	8192	1	BIOS	Microsoft Windows Server 2012 (64-bit)
scsi0:1 Hard disk 2		\$20		0	0.00			300					
scsi0:0 Hard disk 1		\$10		3	0.02			80					
ashmad (10.150.8.10)	Yes	Standard		15	0.11	Standard_A3	3	100	4	2048	1	BIOS	Microsoft Windows Server 2012 (64-bit)
scsi0:2 Hard disk 3		\$4		0	0.00			20					
scsi0:1 Hard disk 2		\$6		0	0.00			40					
scsi0:0 Hard disk 1		\$6		12	0.07			40					
ashwd (10.150.8.10)	Yes	Standard		15	0.25	Standard_A2_v2	2	80	2	4096	1	BIOS	Microsoft Windows Server 2012 (64-bit)
scsi0:1 Hard disk 2		\$6		0	0.00			40					
scsi0:0 Hard disk 1		\$6		13	0.20			40					

VM Name: The VM name or IP address that's used in the VMListFile when a report is generated. This column also lists the disks (VMDKs) that are attached to the VMs. To distinguish vCenter VMs with duplicate names or IP addresses, the names include the ESXi host name. The listed ESXi host is the one where the VM was placed when the tool discovered during the profiling period.

VM Compatibility: Values are **Yes** and **Yes***. **Yes*** is for instances in which the VM is a fit for [premium SSDs](#). Here, the profiled high-churn or IOPS disk fits in the P20 or P30 category, but the size of the disk causes it to be mapped down to a P10 or P20. The storage account decides which premium storage disk type to map a disk to, based on its size. For example:

- <128 GB is a P10.
- 128 GB to 256 GB is a P15
- 256 GB to 512 GB is a P20.
- 512 GB to 1024 GB is a P30.
- 1025 GB to 2048 GB is a P40.
- 2049 GB to 4095 GB is a P50.

For example, if the workload characteristics of a disk put it in the P20 or P30 category, but the size maps it down to a lower premium storage disk type, the tool marks that VM as **Yes***. The tool also recommends that you either change the source disk size to fit into the recommended premium storage disk type or change the target disk type post-failover.

Storage Type: Standard or premium.

Asrseeddisk (Managed Disk) created for replication: The name of the disk that is created when you enable replication. It stores the data and its snapshots in Azure.

Peak R/W IOPS (with Growth Factor): The peak workload read/write IOPS on the disk (default is 95th percentile), including the future growth factor (default is 30 percent). Note that the total read/write IOPS of a VM is not always the sum of the VM's individual disks' read/write IOPS, because the peak read/write IOPS of the VM is the peak of the sum of its individual disks' read/write IOPS during every minute of the profiling period.

Peak Data Churn in Mbps (with Growth Factor): The peak churn rate on the disk (default is 95th percentile), including the future growth factor (default is 30 percent). Note that the total data churn of the VM is not always the sum of the VM's individual disks' data churn, because the peak data churn of the VM is the peak of the sum of its individual disks' churn during every minute of the profiling period.

Azure VM Size: The ideal mapped Azure Cloud Services virtual-machine size for this on-premises VM. The mapping is based on the on-premises VM's memory, number of disks/cores/NICs, and read/write IOPS. The recommendation is always the lowest Azure VM size that matches all of the on-premises VM characteristics.

Number of Disks: The total number of virtual machine disks (VMDKs) on the VM.

Disk size (GB): The total setup size of all disks of the VM. The tool also shows the disk size for the individual disks in the VM.

Cores: The number of CPU cores on the VM.

Memory (MB): The RAM on the VM.

NICs: The number of NICs on the VM.

Boot Type: Boot type of the VM. It can be either BIOS or EFI. Currently Azure Site Recovery supports Windows Server EFI VMs (Windows Server 2012, 2012 R2 and 2016) provided the number of partitions in the boot disk is less than 4 and boot sector size is 512 bytes. To protect EFI VMs, Azure Site Recovery mobility service version must be 9.13 or above. Only failover is supported for EFI VMs. Fallback is not supported.

OS Type: It is OS type of the VM. It can be either Windows or Linux or other based on the chosen template from VMware vSphere while creating the VM.

Incompatible VMs

VM Name	VM Compatibility	Peak R/W IOPS (with Growth Factor)	Peak Data Churn (MBps) (with Growth Factor)	Number of Disks	Disk Size (GB)	Cores	Memory (MB)	NICs	Boot Type	OS Type
Windows Server 2008 (32-bit) is not supported.	Operating system Microsoft Windows Server 2008 (32-bit) is not supported.	2	0.01	1	500	4	8192	1	BIOS	Microsoft Windows Server 2008 (32-bit)
scsi0:0 Hard disk 1		2	0.01		500					
Windows Server 2012 (64-bit) is not supported.	No	79	0.34	4	780	1	2048	1	BIOS	Microsoft Windows Server 2012 (64-bit)
scsi0:2 Hard disk 2		0	0.00		120					
scsi0:3 Hard disk 3		20	0.14		120					
scsi0:0 Hard disk 1	Not supported (Average effective write IOPS exceeds supported ASR IOPS limit (840))	52	0.23		500					
scsi0:4 Hard disk 4		0	0.00		40					
Linux (64-bit) is not supported.	No Not Supported (Disk size > 4095 GB)	85	0.67	3	6500	2	1024	1	BIOS	Other Linux (64-bit)
scsi0:2 Hard disk 3		6	0.19		5500					
scsi0:0 Hard disk 1		84	0.63		400					
scsi0:1 Hard disk 2		0	0.00		600					

VM Name: The VM name or IP address that's used in the VMListFile when a report is generated. This column also lists the VMDKs that are attached to the VMs. To distinguish vCenter VMs with duplicate names or IP addresses, the names include the ESXi host name. The listed ESXi host is the one where the VM was placed when the tool discovered during the profiling period.

VM Compatibility: Indicates why the given VM is incompatible for use with Site Recovery. The reasons are described for each incompatible disk of the VM and, based on published [storage limits](#), can be any of the following:

- Wrong data disk size or wrong OS disk size. [Review](#) the support limits.
- Total VM size (replication + TFO) exceeds the supported storage-account size limit (35 TB). This incompatibility usually occurs when a single disk in the VM has a performance characteristic that exceeds the maximum supported Azure or Site Recovery limits for standard storage. Such an instance pushes the VM into the premium storage zone. However, the maximum supported size of a premium storage account is 35 TB, and a single protected VM cannot be protected across multiple storage accounts. Also note that when a test failover is executed on a protected VM, it runs in the same storage account where replication is progressing. In this instance, set up 2x the size of the disk for replication to progress and test failover to succeed in parallel.
- Source IOPS exceeds supported storage IOPS limit of 7500 per disk.
- Source IOPS exceeds supported storage IOPS limit of 80,000 per VM.
- Average data churn exceeds supported Site Recovery data churn limit of 20 MB/s for average I/O size for the disk.
- Peak data churn across all disks on the VM exceeds the maximum supported Site Recovery peak data churn limit of 54 MB/s per VM.
- Average effective write IOPS exceeds the supported Site Recovery IOPS limit of 840 for disk.

- Calculated snapshot storage exceeds the supported snapshot storage limit of 10 TB.
- Total data churn per day exceeds supported churn per day limit of 2 TB by a Process Server.

Peak R/W IOPS (with Growth Factor): The peak workload IOPS on the disk (default is 95th percentile), including the future growth factor (default is 30 percent). Note that the total read/write IOPS of the VM is not always the sum of the VM's individual disks' read/write IOPS, because the peak read/write IOPS of the VM is the peak of the sum of its individual disks' read/write IOPS during every minute of the profiling period.

Peak Data Churn in Mbps (with Growth Factor): The peak churn rate on the disk (default 95th percentile) including the future growth factor (default 30 percent). Note that the total data churn of the VM is not always the sum of the VM's individual disks' data churn, because the peak data churn of the VM is the peak of the sum of its individual disks' churn during every minute of the profiling period.

Number of Disks: The total number of VMDKs on the VM.

Disk size (GB): The total setup size of all disks of the VM. The tool also shows the disk size for the individual disks in the VM.

Cores: The number of CPU cores on the VM.

Memory (MB): The amount of RAM on the VM.

NICs: The number of NICs on the VM.

Boot Type: Boot type of the VM. It can be either BIOS or EFI. Currently Azure Site Recovery supports Windows Server EFI VMs (Windows Server 2012, 2012 R2 and 2016) provided the number of partitions in the boot disk is less than 4 and boot sector size is 512 bytes. To protect EFI VMs, Azure Site Recovery mobility service version must be 9.13 or above. Only failover is supported for EFI VMs. Fallback is not supported.

OS Type: It is OS type of the VM. It can be either Windows or Linux or other based on the chosen template from VMware vSphere while creating the VM.

Azure Site Recovery limits

The following table provides the Azure Site Recovery limits. These limits are based on our tests, but they cannot cover all possible application I/O combinations. Actual results can vary based on your application I/O mix. For best results, even after deployment planning, we always recommend that you perform extensive application testing by issuing a test failover to get the true performance picture of the application.

REPLICATION STORAGE TARGET	AVERAGE SOURCE DISK I/O SIZE	AVERAGE SOURCE DISK DATA CHURN	TOTAL SOURCE DISK DATA CHURN PER DAY
Standard storage	8 KB	2 MB/s	168 GB per disk
Premium P10 or P15 disk	8 KB	2 MB/s	168 GB per disk
Premium P10 or P15 disk	16 KB	4 MB/s	336 GB per disk
Premium P10 or P15 disk	32 KB or greater	8 MB/s	672 GB per disk
Premium P20 or P30 or P40 or P50 disk	8 KB	5 MB/s	421 GB per disk
Premium P20 or P30 or P40 or P50 disk	16 KB or greater	20 MB/s	1684 GB per disk

SOURCE DATA CHURN	MAXIMUM LIMIT
Peak data churn across all disks on a VM	54 MB/s
Maximum data churn per day supported by a Process Server	2 TB

These are average numbers assuming a 30 percent I/O overlap. Site Recovery is capable of handling higher throughput based on overlap ratio, larger write sizes, and actual workload I/O behavior. The preceding numbers assume a typical backlog of approximately five minutes. That is, after data is uploaded, it is processed and a recovery point is created within five minutes.

Cost estimation

Learn more about [cost estimation](#).

Next steps

Learn more about [cost estimation](#).

Review cost estimations in the VMware Deployment Planner

11/12/2019 • 9 minutes to read • [Edit Online](#)

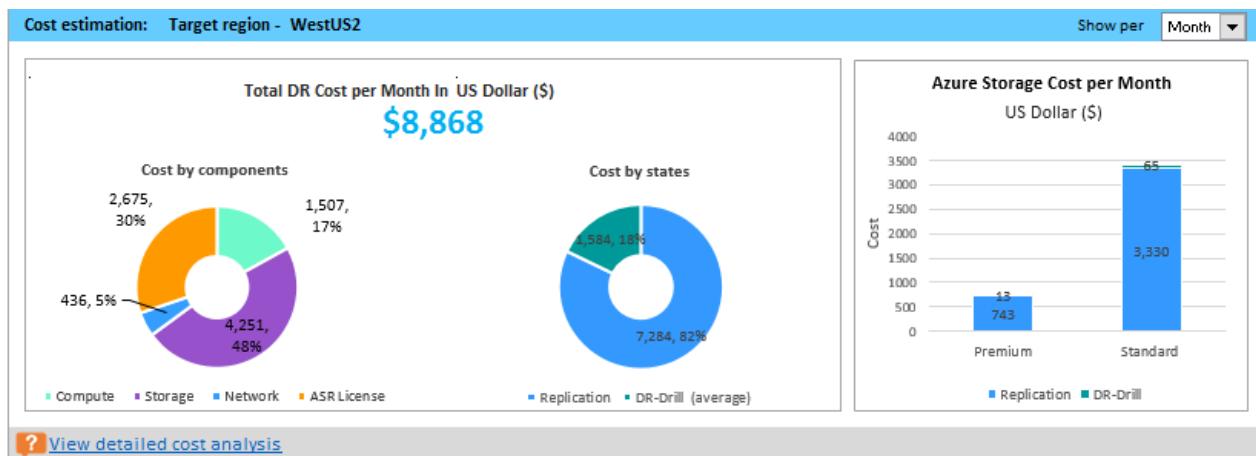
The deployment planner report provides the cost estimation summary in [Recommendations](#) sheets and detailed cost analysis in Cost Estimation sheet. It has the detailed cost analysis per VM.

NOTE

The current version of Deployment planner tool v2.5 provides cost estimation for VMs replicating to Managed Disks.

Cost estimation summary

The graph shows the summary view of the estimated total disaster recovery (DR) cost to Azure of your chosen target region and the currency that you have specified for report generation. Cost estimation summary



The summary helps you to understand the cost that you need to pay for storage, compute, network, and license when you protect all your compatible VMs to Azure using Azure Site Recovery. The cost is calculated on for compatible VMs and not on all the profiled VMs.

You can view the cost either monthly or yearly. Learn more about [supported target regions](#) and [supported currencies](#).

Cost by components The total DR cost is divided into four components: Compute, Storage, Network, and Azure Site Recovery license cost. The cost is calculated based on the consumption that will be incurred during replication and at DR drill time for compute, storage (premium and standard), ExpressRoute/VPN that is configured between the on-premises site and Azure, and Azure Site Recovery license.

Cost by states The total disaster recovery (DR) cost is categories based on two different states - Replication and DR drill.

Replication cost: The cost that will be incurred during replication. It covers the cost of storage, network, and Azure Site Recovery license.

DR-Drill cost: The cost that will be incurred during test failovers. Azure Site Recovery spins up VMs during test failover. The DR drill cost covers the running VMs' compute and storage cost.

Azure storage cost per Month/Year It shows the total storage cost that will be incurred for premium and standard storage for replication and DR drill.

Detailed cost analysis

Azure prices for compute, storage, network, etc. varies across Azure regions. You can generate a cost estimation report with the latest Azure prices based on your subscription, the offer that is associated with your subscription and for the specified target Azure region in the specified currency. By default, the tool uses West US 2 Azure region and US dollar (USD) currency. If you have used any other region and currency, the next time when you generate a report without subscription ID, offer ID, target region, and currency, it will use prices of the last used target region and last used currency for cost estimation. This section shows the subscription ID and offer ID that you have used for report generation. If not used, it is blank.

In the whole report, the cells marked in gray are read only. Cells in white can be modified per your requirements.

Overall DR costs by components			Overall DR costs by States		
	Month	Year		Month	Year
Compute	\$3,995	\$47,939	Replication (ASR License + Storage + Network)	\$9,772	\$117,262
Storage	\$6,870	\$82,435	DR-Drill (average) (Compute + Storage)	\$4,590	\$55,076
Network	\$872	\$10,464	Total	\$14,362	\$172,338
ASR License	\$2,625	\$31,500			
Total	\$14,362	\$172,338			
Storage cost - Year (without discount)			Storage cost - Year (with discount)		
Premium		Replication	Replication		Replication
Premium	\$34,025	DR-Drill	\$34,025	DR-Drill	DR-Drill
Standard	\$40,073	\$3,847	\$3,847	\$2,835	\$321
Total	\$74,098	\$3,290	\$3,290	\$3,339	\$274
Site to Azure Network			Number of virtual machines type and compute cost (per year)		
ExpressRoute	ExpressRoute - 2 Gbps (Metered)		OS type	Number of VMs	DR-Drill compute cost
VPN Gateway type	NA		Windows	105	\$47,939
Target region	WestUS2		Non-Windows	0	\$0
VM running on Azure			Settings		
Domain controller/DNS	Number of VMs	IaaS size	Using Managed disk	Yes	
SQL Always On	0	Standard_D3	Currency	US Dollar (\$)	
			Cost duration	Year	
Apply overall discount if applicable					
Discount in (%)	0				

Detailed cost analysis

The below table lists cost breakup for each compatible VM of the profiled virtual machines.

You can also use this table to get estimated Azure DR cost of non-profiled virtual machines by manually adding virtual machines.

To manually add virtual machines:

- Click on 'Insert row' button below to insert a new row between Start and End rows
- Fill the following columns based on approximate virtual machine size and number of virtual machines that match this configuration - Number of VMs, IaaS size (Your selection), Storage T VM total storage size (GB), Number of DR-Drills in a year, Each DR-Drill duration (Days), OS Type, Data redundancy and Azure Hybrid Use Benefit
- You can apply the same value to all the virtual machines in the table by clicking 'Apply to all' button for Number of DR-Drills in a year, Each DR-Drill duration (Days), Data redundancy and
- Click 'Re-calculate cost' to update cost

[Learn more about cost estimation](#)

Insert row	Re-calculate cost	IaaS characteristics							
VM Name	Number of VMs	IaaS size (Recommended)	IaaS size (Your selection)	Storage type Standard/Premium	VM total storage size (GB) (Replication)	Number of DR-Drills in a year	Each DR-Drill duration (Days)	Cost duration	
START:INSERT A ROW BELOW TO ADD A NEW ENTRY									
co1magicsql1 (CO1-CU-SV-EB001)	1	Standard_DS5_v2	Standard_DS5_v2	Premium	2949.00	4	Apply to all	7	
colecitweb05 (CO1-CU-SV-EB003)	1	Standard_DS3_v2	Standard_DS3_v2	Premium	652.00	4		7	
colecitweb07 (CO1-CU-SV-EB004)	1	Standard_A3	Standard_A3	Standard	652.00	4		7	
colpiappsm02 (CO1-CU-SV-EB004)	1	Standard_A2	Standard_A2	Standard	200.00	4		7	
colsu1407 (CO1-CU-SV-EB004)	1	Standard_A4	Standard_A4	Standard	300.00	4		7	
col1xitexsqla (CO1-CU-SV-EB004)	1	Standard_D5_v2	Standard_D5_v2	Standard	1194.00	4		7	
col1bmsspolp01 (CO1-CU-SV-EB00)	1	Standard_A4	Standard_A4	Standard	550.00	4		7	

Overall DR cost by components

The first section shows the overall DR cost by components and DR cost by states.

Compute: Cost of IaaS VMs that run on Azure for DR needs. It includes VMs that are created by Azure Site Recovery during DR-drills (test failovers) and VMs running on Azure like SQL Server with Always On Availability Groups and domain controllers / Domain Name Servers.

Storage: Cost of Azure storage consumption for DR needs. It includes storage consumption for replication and during DR drills. Network: ExpressRoute and Site to Site VPN cost for DR needs.

ASR license: Azure Site Recovery license cost for all compatible VMs. If you have manually entered a VM in the detailed cost analysis table, Azure Site Recovery license cost is also included for that VM.

Overall DR cost by states

The total DR cost is categorized based on two different states - replication and DR-Drill.

Replication cost: The cost incurs at the time of replication. It covers the cost of storage, network, and Azure Site Recovery license.

DR-Drill cost: The cost incurs at the time of DR drills. Azure Site Recovery spins up VMs during DR drills. The DR drill cost covers compute and storage cost of the running VMs. Total DR drill duration in a year = Number of DR drills x Each DR drill duration (days) Average DR drill cost (per month) = Total DR drill cost / 12

Storage cost table:

This table shows premium and standard storage cost incur for replication and DR drills with and without discount.

Site to Azure network

Select the appropriate setting as per your requirements.

ExpressRoute: By default, the tool selects the nearest ExpressRoute plan that matches with the required network bandwidth for delta replication. You can change the plan as per your requirements.

VPN Gateway: Select the VPN Gateway if you have any in your environment. By default, it is NA.

Target Region: Specified Azure region for DR. The price used in the report for compute, storage, network, and license is based on the Azure pricing for that region.

VM running on Azure

If you have any domain controller or DNS VM or SQL Server VM with Always On Availability Groups running on Azure for DR, you can provide the number of VMs and the size to consider their computing cost in the total DR cost.

Apply overall discount if applicable

If you are an Azure partner or a customer and are entitled to any discount on overall Azure pricing, you can use this field. The tool applies the discount (in %) on all components.

Number of virtual machines type and compute cost (per year)

This table shows the number of Windows and non-Windows VMs and DR drill compute cost for them.

Settings

Currency: The currency in which the report is generated. Cost duration: You can view all costs either for the month or for the whole year.

Detailed cost analysis table

Detailed cost analysis														
The below table lists cost breakup for each compatible VM of the profiled virtual machines. You can also use this table to get estimated Azure DR cost of non-profiled virtual machines by manually adding virtual machines. To add new row: 1. Click on the 'New' button below to insert a new row between Start and End rows. 2. Fill the following columns based on approximate virtual machine size and number of virtual machines that match this configuration - Number of VMs, IaaS size (Your selection), Storage Type (Standard/Premium), VM total storage size (GB), Number of DR-Drills in a year, Each DR-Drill duration (Days), OS Type, Data redundancy and Azure Hybrid Use Benefit 3. You can apply the same value to all the virtual machines in the table by clicking 'Apply to all' button for Number of DR-Drills in a year, Each DR-Drill duration (Days), Data redundancy and Azure Hybrid Use Benefit 4. Click 'Re-calculate cost' to update cost.														
Learn more about cost estimation														
Insert row	Re-calculate cost	IaaS characteristics	Cost breakup											
VM Name	Number of VMs	IaaS size (Recommended)	IaaS size (Your selection)	Storage type Standard/Premium	VM total storage size (GB) (Replication)	Number of DR-Drills in a year	Each DR-Drill duration (Days)	OS Type	Data redundancy	Azure Hybrid Use Benefit	Total Azure consumption per Year (Compute + Storage + License)	Steady state replication cost per Year (Storage)	Total DR-Drill cost per Year (Compute + Storage)	
START INDEX & COUNT BELOW TO ADD A NEW ENTRY														
colemagics1 (C01-CU-SV-E000)	1	Standard_D5_v2	Premium	Standard	2949.00	4	Apply to all	Windows	LRS	Apply to all	\$5,462	\$4,454	\$6,048	
colechicweb05 (C01-CU-SV-E000)	1	Standard_D5_v2	Premium	Standard	652.00	4	7	Windows	LRS	Yes	\$1,577	\$1,095	\$181	
colechicweb07 (C01-CU-SV-E004)	1	Standard_A3	Standard	652.00	4	7	Windows	LRS	Yes	\$855	\$391	\$164		
colelapgsm02 (C01-CU-SV-E000)	1	Standard_A2	Standard	200.00	4	7	Windows	LRS	Yes	\$444	\$120	\$24		
colelapgsm03 (C01-CU-SV-E000)	1	Standard_A2	Standard	300.00	4	7	Windows	LRS	Yes	\$707	\$180	\$287		
colenterstola (C01-CU-SV-E004)	1	Standard_D5_v2	Standard	300.00	4	7	Windows	LRS	Yes	\$1,209	\$716	\$149		
coleimspms01 (C01-CU-SV-E001)	1	Standard_A4	Standard	550.00	4	7	Windows	LRS	Yes	\$928	\$330	\$298		
coleimssrd01 (C01-CU-SV-E004)	1	Standard_A2_v2	Standard	541.00	4	7	Windows	LRS	Yes	\$660	\$225	\$35		
coleictive17 (C01-CU-SV-E004)	1	Standard_A3	Standard	650.00	4	7	Windows	LRS	Yes	\$854	\$390	\$164		
colelemw10 (C01-CU-SV-E004)	1	Standard_G5	Standard	1221.00	4	7	Windows	LRS	Yes	\$8,391	\$733	\$5,358		
colelmpsymweb10 (C01-CU-SV-E5)	1	Standard_G5	Standard	200.00	4	7	Windows	LRS	Yes	\$5,701	\$120	\$5,281		

The table lists the cost breakup for each compatible VM. You can also use this table to get estimated Azure DR

cost of non-profiled VMs by manually adding VMs. It is useful in cases where you need to estimate Azure costs for a new disaster recovery deployment without detailed profiling being done. To manually add VMs:

1. Click on the 'Insert row' button to insert a new row between the Start and End rows.
2. Fill the following columns based on approximate VM size and number of VMs that match this configuration:

- Number of VMs, IaaS size (Your selection)
- Storage Type (Standard/Premium)
- VM total storage size (GB) of the source machine
- Number of DR drills in a year
- Each DR drill duration (Days)
- OS Type
- Data redundancy
- Azure Hybrid Benefit

1. You can apply the same value to all VMs in the table by clicking the 'Apply to all' button for Number of DR-Drills in a year, Each DR-Drill duration (Days), Data redundancy, and Azure Hybrid Use Benefit.

2. Click 'Re-calculate cost' to update cost.

VM Name: The name of the VM.

Number of VMs: The number of VMs that match the configuration. You can update the number of the existing VMs if similar configuration VMs are not profiled but will be protected.

IaaS size (Recommendation): It is the VM role size of the compatible VM that the tool recommends.

IaaS size (Your selection): By default, it is the same as recommended VM role size. You can change the role based on your requirement. Compute cost is based on your selected VM role size.

Storage type: The type of the storage that is used by the VM. It is either standard or premium storage.

VM total storage size (GB): The total storage of the source VM.

Number of DR-Drills in a year: The number of times you perform DR-Drills in a year. By default, it is 4 times in a year. You can modify the period for specific VMs or apply the new value to all VMs by entering the new value on the top row and clicking the 'Apply to all' button. Based on number of DR-Drills in a year and each DR-Drill duration period, the total DR-Drill cost is calculated.

Each DR-Drill duration (Days): The duration of each DR-Drill. By default, it is 7 days every 90 days as per the [Disaster Recovery Software Assurance benefit](#). You can modify the period for specific VMs or you can apply a new value to all VMs by entering new value on the top row and clicking the 'Apply to all' button. The total DR-Drill cost is calculated based on number of DR-Drills in a year and each DR-Drill duration period.

OS Type: The OS type of the VM. It is either Windows or Linux. If the OS type is Windows, then Azure Hybrid Use Benefit can be applied to that VM.

Data redundancy: It can be one of the following - Locally redundant storage (LRS), Geo-redundant storage (GRS) or Read-access geo-redundant storage (RA-GRS). Default is LRS. You can change the type based on your storage account for specific VMs or you can apply the new type to all VMs by changing the type of the top row and clicking 'Apply to all' button. The cost of storage for replication is calculated based on the price of data redundancy that you have selected.

Azure Hybrid Benefit: You can apply Azure Hybrid Benefit to Windows VMs if applicable. Default is Yes. You can change the setting for specific VMs or update all VMs by clicking the 'Apply to all' button.

Total Azure consumption: It includes compute, storage, and Azure Site Recovery license cost for your DR. Based on your selection it shows the cost either monthly or yearly.

Steady state replication cost: It includes storage cost for replication.

Total DR-Drill cost (average): It includes compute and storage cost for DR-Drill.

ASR license cost: Azure Site Recovery license cost.

Supported target regions

The Azure Site Recovery deployment planner provides cost estimation for the following Azure regions. If your region is not listed below, you can use any of the following regions whose pricing is nearest to your region.

eastus, eastus2, westus, centralus, northcentralus, southcentralus, northeurope, westeurope, eastasia, southeastasia, japaneast, japanwest, australiaeast, australiasoutheast, brazilsouth, southindia, centralindia, westindia, canadacentral, canadaeast, westus2, westcentralus, uksouth, ukwest, koreacentral, koreasouth

Supported currencies

The Azure Site Recovery Deployment Planner can generate the cost report with any of the following currencies.

CURRENCY	NAME	CURRENCY	NAME	CURRENCY	NAME
ARS	Argentine Peso (\$)	AUD	Australian Dollar (\$)	BRL	Brazilian Real (R\$)
CAD	Canadian Dollar (\$)	CHF	Swiss Franc. (chf)	DKK	Danish Krone (kr)
EUR	Euro (€)	GBP	British Pound (£)	HKD	Hong Kong Dollar (HK\$)
IDR	Indonesia rupiah (Rp)	INR	Indian Rupee (₹)	JPY	Japanese Yen (¥)
KRW	Korean Won (₩)	MXN	Mexican Peso (MX\$)	MYR	Malaysian Ringgit (RM\$)
NOK	Norwegian Krone (kr)	NZD	New Zealand Dollar (\$)	RUB	Russian Ruble (py6)
SAR	Saudi Riyal (SR)	SEK	Swedish Krona (kr)	TWD	Taiwanese Dollar (NT\$)
TRY	Turkish Lira (TL)	USD	US Dollar (\$)	ZAR	South African Rand (R)

Next steps

Learn more about protecting [VMware VMs to Azure using Azure Site Recovery](#).

Scale with additional process servers

4/29/2019 • 8 minutes to read • [Edit Online](#)

By default, when you're replicating VMware VMs or physical servers to Azure using [Site Recovery](#), a process server is installed on the configuration server machine, and is used to coordinate data transfer between Site Recovery and your on-premises infrastructure. To increase capacity and scale out your replication deployment, you can add additional standalone process servers. This article describes how to setup a scale-out process server.

Before you start

Capacity planning

Make sure you've performed [capacity planning](#) for VMware replication. This helps you to identify how and when you should deploy additional process servers.

From 9.24 version, guidance is added during selection of process server for new replications. Process server will be marked Healthy, Warning and Critical based on certain criteria. To understand different scenarios that can influence state of process server, review the [process server alerts](#).

NOTE

Use of a cloned Process Server component is not supported. Follow the steps in this article for each PS scale-out.

Sizing requirements

Verify the sizing requirements summarized in the table. In general, if you have to scale your deployment to more than 200 source machines, or you have a total daily churn rate of more than 2 TB, you need additional process servers to handle the traffic volume.

ADDITIONAL PROCESS SERVER	CACHE DISK SIZE	DATA CHANGE RATE	PROTECTED MACHINES
4 vCPUs (2 sockets * 2 cores @ 2.5 GHz), 8-GB memory	300 GB	250 GB or less	Replicate 85 or less machines.
8 vCPUs (2 sockets * 4 cores @ 2.5 GHz), 12-GB memory	600 GB	250 GB to 1 TB	Replicate between 85-150 machines.
12 vCPUs (2 sockets * 6 cores @ 2.5 GHz) 24-GB memory	1 TB	1 TB to 2 TB	Replicate between 150-225 machines.

Where each protected source machine is configured with 3 disks of 100 GB each.

Prerequisites

The prerequisites for the additional process server are summarized in the following table.

Configuration and process server requirements

Hardware requirements

COMPONENT	REQUIREMENT
CPU cores	8
RAM	16 GB
Number of disks	3, including the OS disk, process server cache disk, and retention drive for failback
Free disk space (process server cache)	600 GB
Free disk space (retention disk)	600 GB

Software requirements

COMPONENT	REQUIREMENT
Operating system	Windows Server 2012 R2 Windows Server 2016
Operating system locale	English (en-us)
Windows Server roles	Don't enable these roles: - Active Directory Domain Services - Internet Information Services - Hyper-V
Group policies	Don't enable these group policies: - Prevent access to the command prompt. - Prevent access to registry editing tools. - Trust logic for file attachments. - Turn on Script Execution. Learn more
IIS	- No pre-existing default website - No pre-existing website/application listening on port 443 - Enable anonymous authentication - Enable FastCGI setting
FIPS (Federal Information Processing Standards)	Do not enable FIPS mode

Network requirements

COMPONENT	REQUIREMENT
IP address type	Static
Ports	443 (Control channel orchestration) 9443 (Data transport)
NIC type	VMXNET3 (if the configuration server is a VMware VM)

COMPONENT	REQUIREMENT
Internet access (the server needs access to the following URLs, directly or via proxy):	
*.backup.windowsazure.com	Used for replicated data transfer and coordination
*.store.core.windows.net	Used for replicated data transfer and coordination
*.blob.core.windows.net	Used to access storage account that stores replicated data
*.hypervrecoverymanager.windowsazure.com	Used for replication management operations and coordination
https://management.azure.com	Used for replication management operations and coordination
*.services.visualstudio.com	Used for telemetry purposes (optional)
time.nist.gov	Used to check time synchronization between system and global time
time.windows.com	Used to check time synchronization between system and global time
<ul style="list-style-type: none"> • https://login.microsoftonline.com • https://secure.aadcdn.microsoftonline-p.com • https://login.live.com • https://graph.windows.net • https://login.windows.net • https://www.live.com • https://www.microsoft.com 	OVF setup needs access to these URLs. They're used for access control and identity management by Azure Active Directory.
https://dev.mysql.com/get/Downloads/MySQLInstaller/mysql-installer-community-5.7.20.0.msi	To complete MySQL download. In a few regions, the download might be redirected to the CDN URL. Ensure that the CDN URL is also whitelisted, if necessary.

Required software

COMPONENT	REQUIREMENT
VMware vSphere PowerCLI	PowerCLI version 6.0 should be installed if the Configuration Server is running on a VMware VM.
MYSQL	MySQL should be installed. You can install manually, or Site Recovery can install it. (Refer to configure settings for more information)

Sizing and capacity requirements

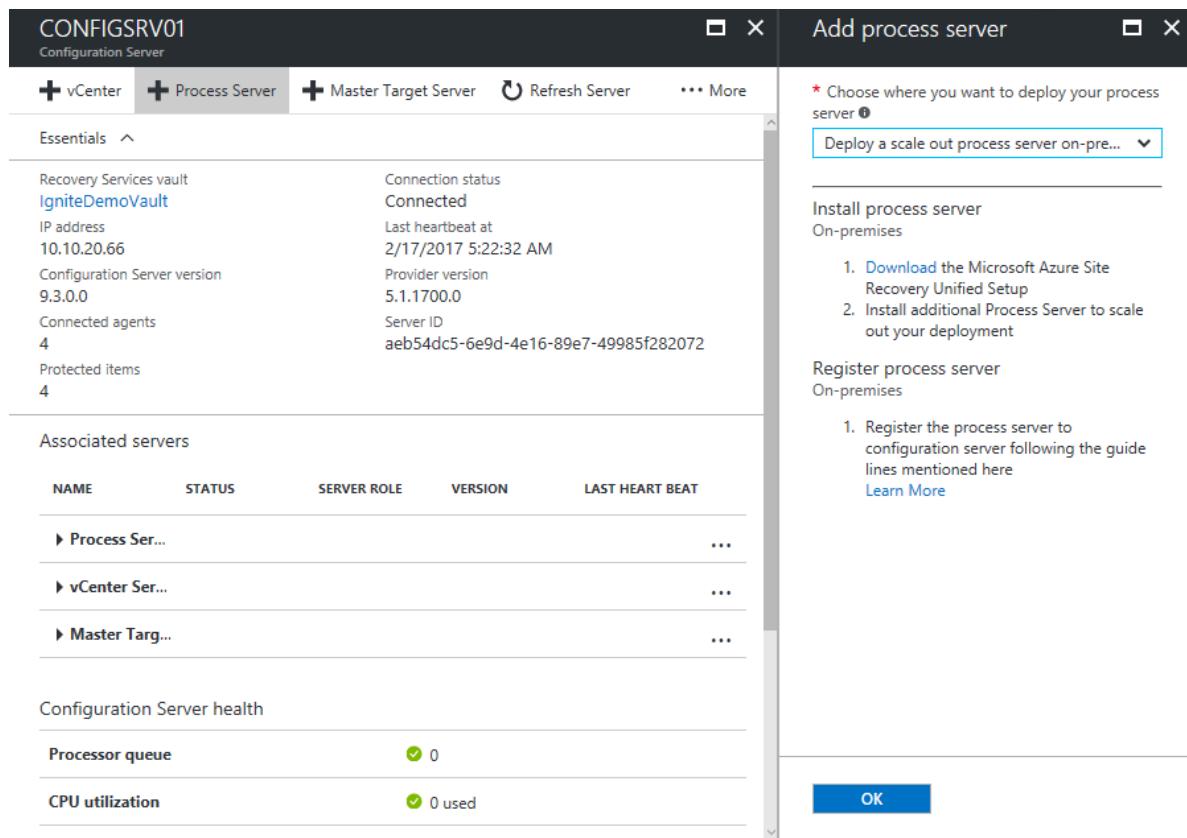
The following table summarizes capacity requirements for the configuration server. If you're replicating multiple VMware VMs, review the [capacity planning considerations](#) and run the [Azure Site Recovery Deployment Planner tool](#).

CPU	MEMORY	CACHE DISK	DATA CHANGE RATE	REPLICATED MACHINES
8 vCPUs 2 sockets * 4 cores @ 2.5 GHz	16 GB	300 GB	500 GB or less	< 100 machines
12 vCPUs 2 socks * 6 cores @ 2.5 GHz	18 GB	600 GB	500 GB-1 TB	100 to 150 machines
16 vCPUs 2 socks * 8 cores @ 2.5 GHz	32 GB	1 TB	1-2 TB	150 -200 machines

Download installation file

Download the installation file for the process server as follows:

1. Sign in to the Azure portal, and browse to your Recovery Services Vault.
2. Open **Site Recovery Infrastructure > VMWare and Physical Machines > Configuration Servers** (under For VMware & Physical Machines).
3. Select the configuration server to drill down into the server details. Then click **+ Process Server**.
4. In **Add Process server > Choose where you want to deploy your process server**, select **Deploy a Scale-out Process Server on-premises**.



5. Click **Download the Microsoft Azure Site Recovery Unified Setup**. This downloads the latest version of the installation file.

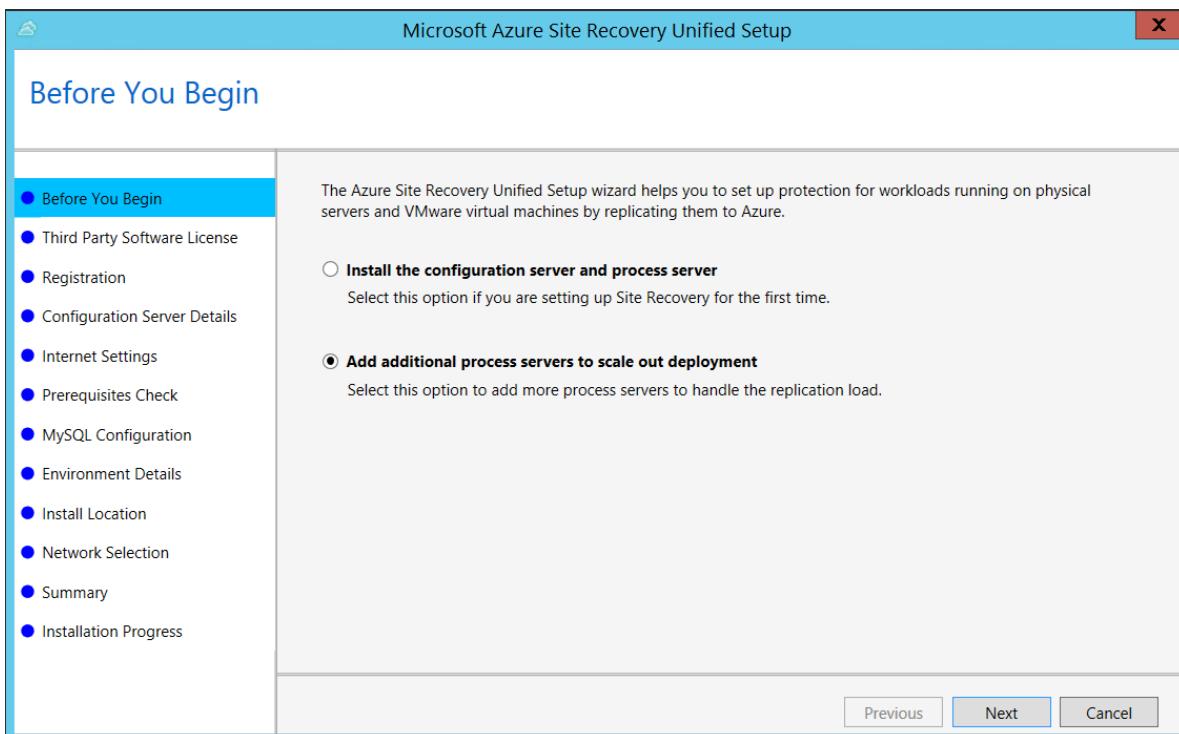
WARNING

The process server installation version should be the same as, or earlier than, the configuration server version you have running. A simple way to ensure version compatibility is to use the same installer, that you most recently used to install or update your configuration server.

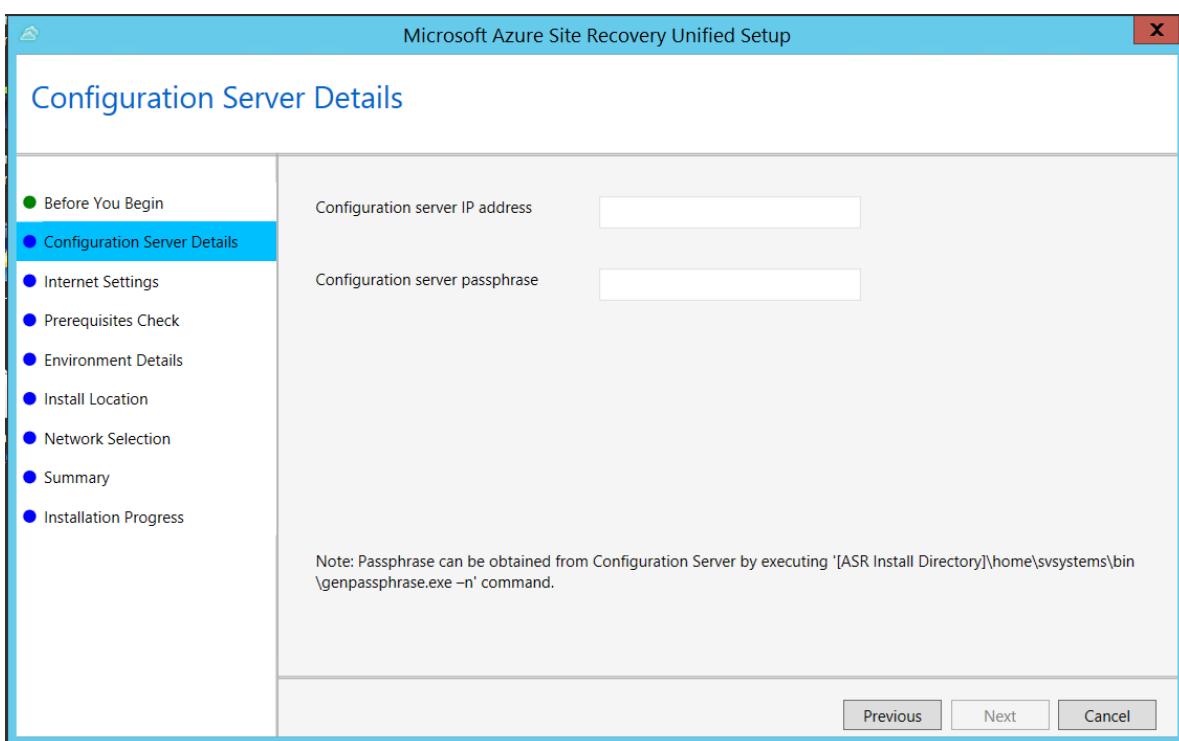
Install from the UI

Install as follows. After setting up the server, you migrate source machines to use it.

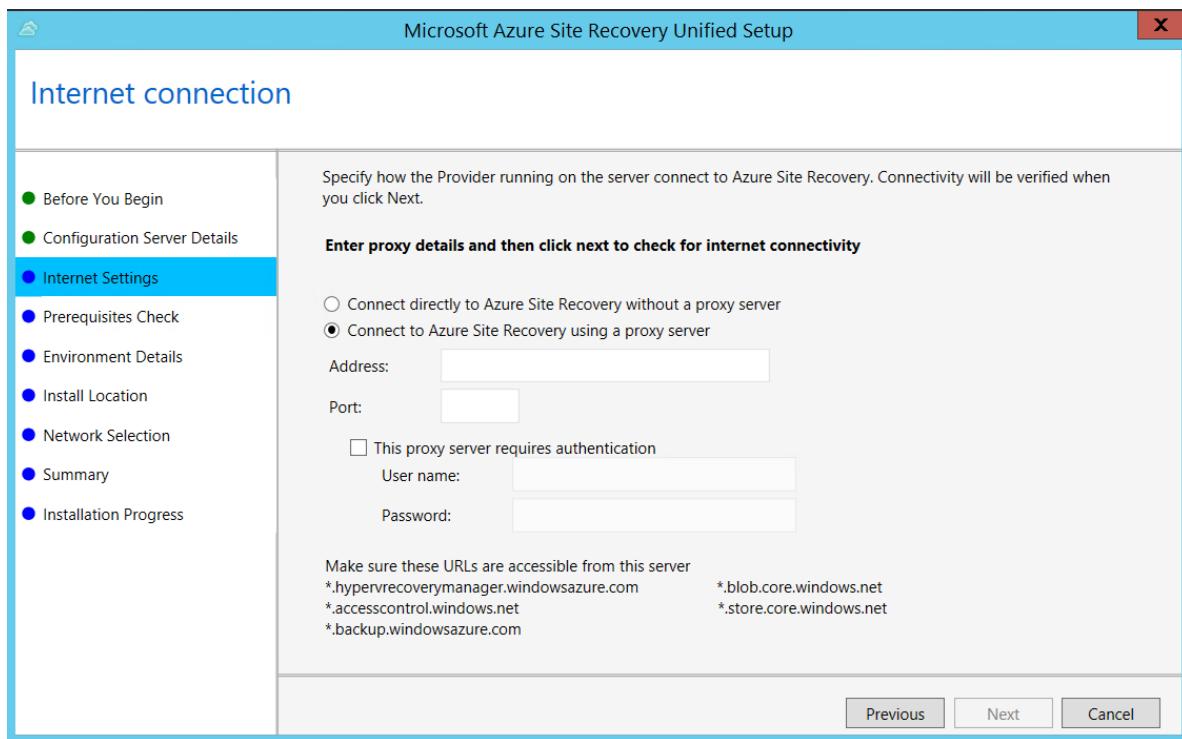
1. Launch the Azure Site Recovery UnifiedSetup.exe
2. In **Before you begin**, select **Add additional process servers to scale out deployment**.



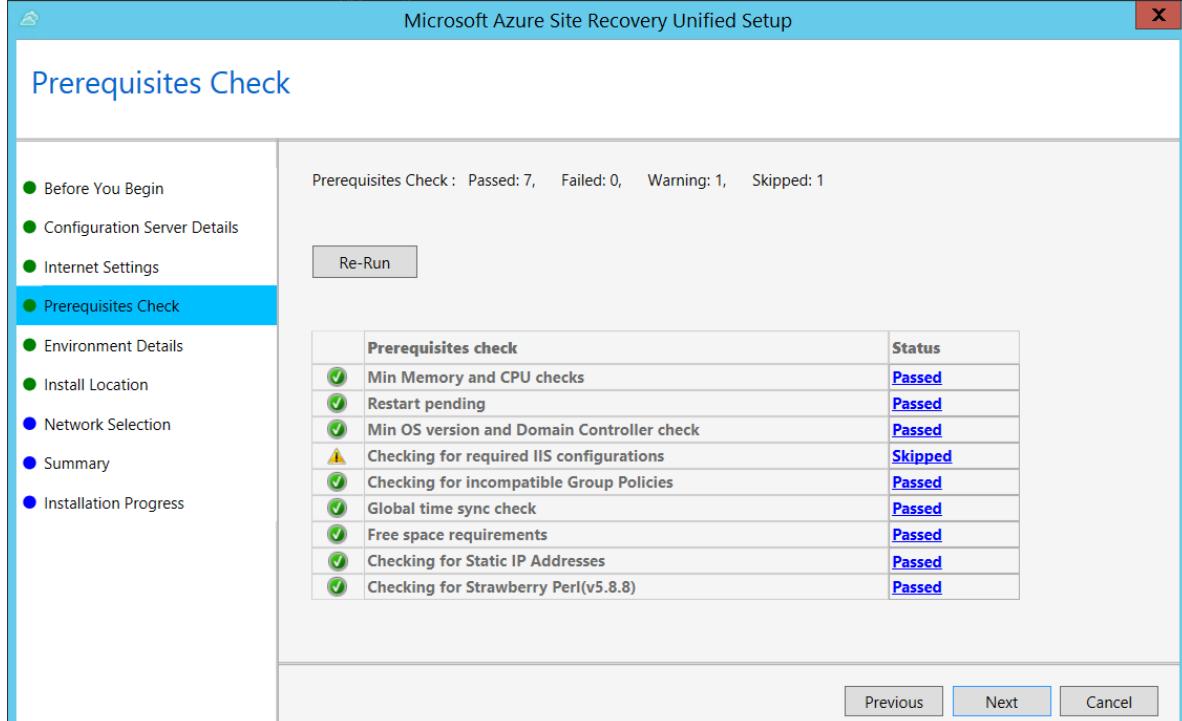
3. In **Configuration Server Details**, specify the IP address of the Configuration Server, and the passphrase.



4. In **Internet Settings**, specify how the Provider running on the Configuration Server connects to Azure Site Recovery over the Internet.

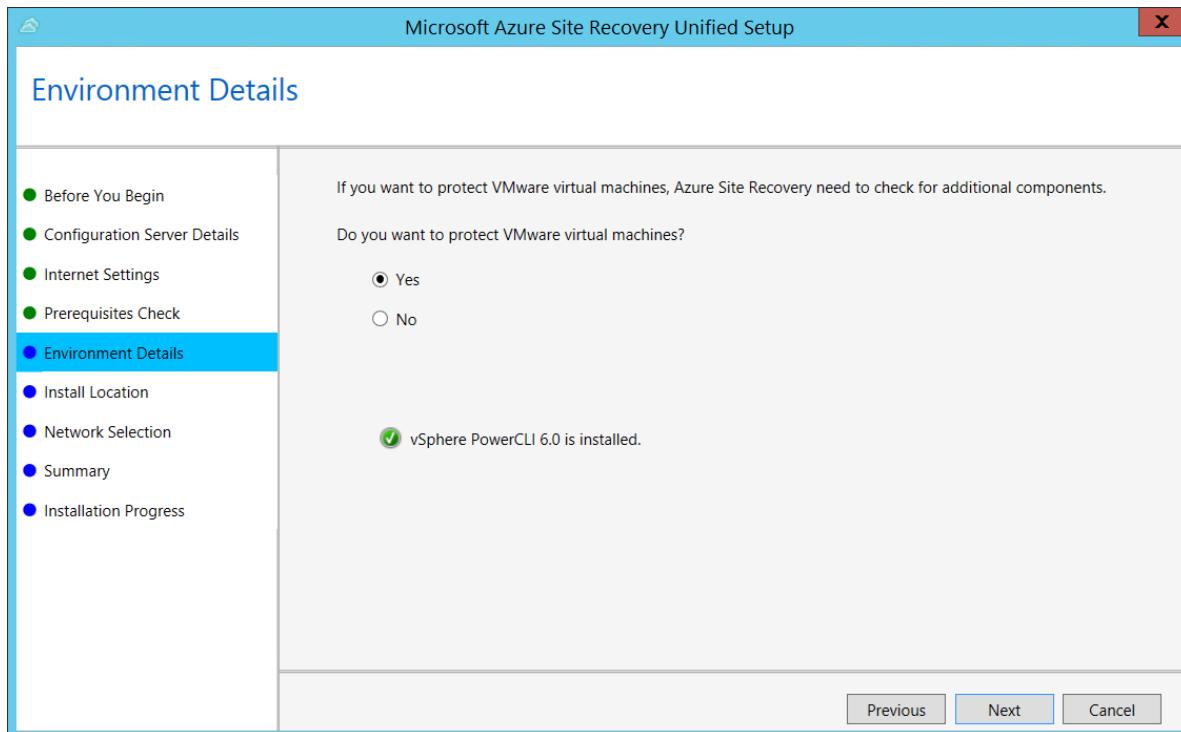


- If you want to connect with the proxy that's currently set up on the machine, select **Connect with existing proxy settings**.
 - If you want the Provider to connect directly, select **Connect directly without a proxy**.
 - If the existing proxy requires authentication, or if you want to use a custom proxy for the Provider connection, select **Connect with custom proxy settings**.
 - If you use a custom proxy, you need to specify the address, port, and credentials.
 - If you're using a proxy, you should have already allowed access to the service urls.
5. In **Prerequisites Check**, Setup runs a check to make sure that installation can run. If a warning appears about the **Global time sync check**, verify that the time on the system clock (**Date and Time** settings) is the same as the time zone.

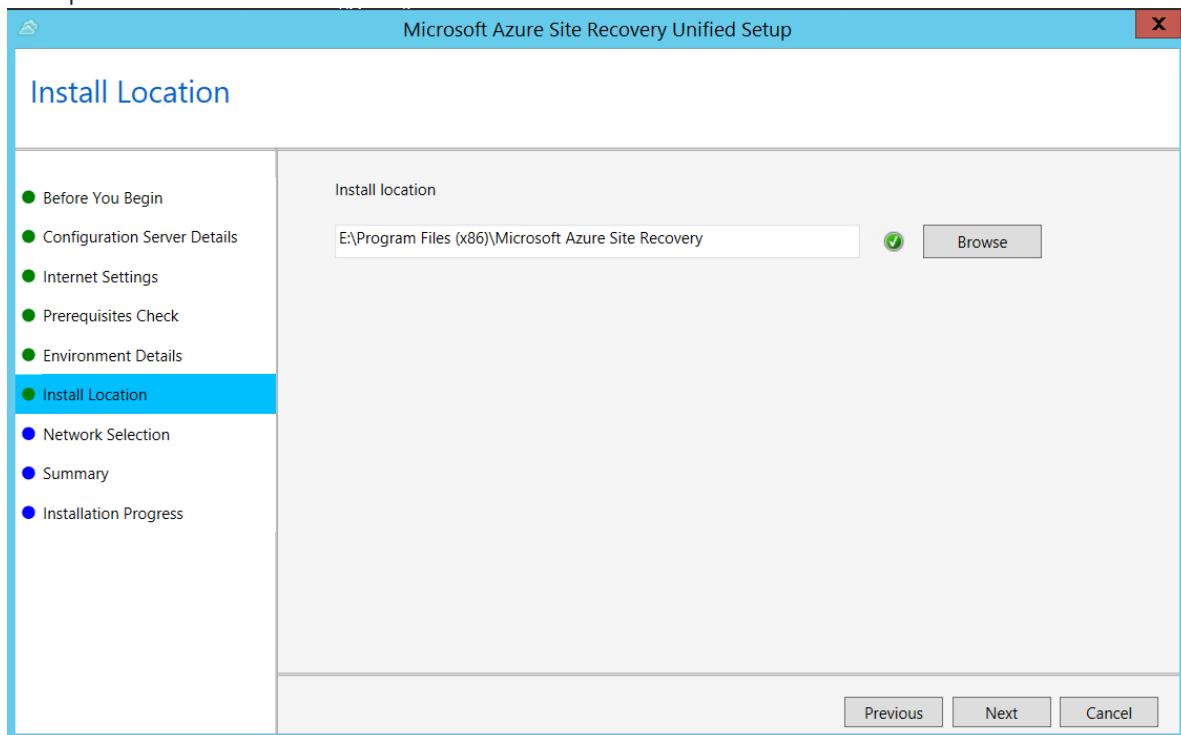


6. In **Environment Details**, select whether you're going to replicate VMware VMs. If you are, then setup

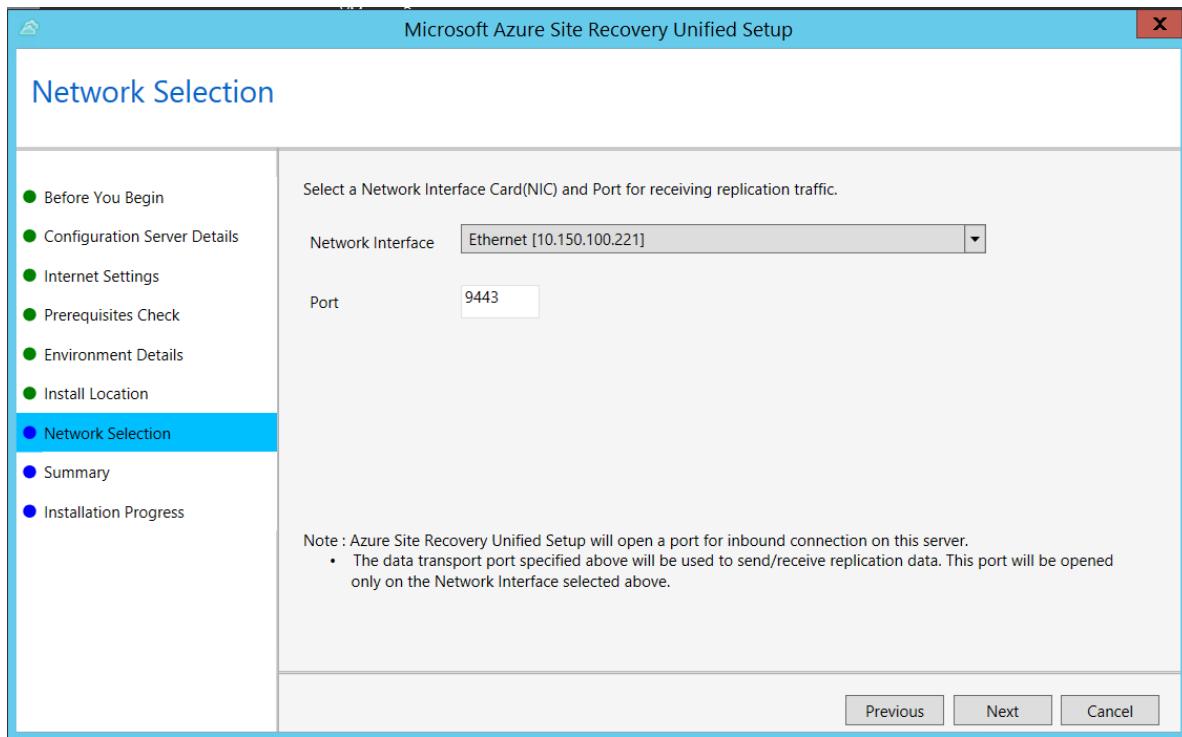
checks that PowerCLI 6.0 is installed.



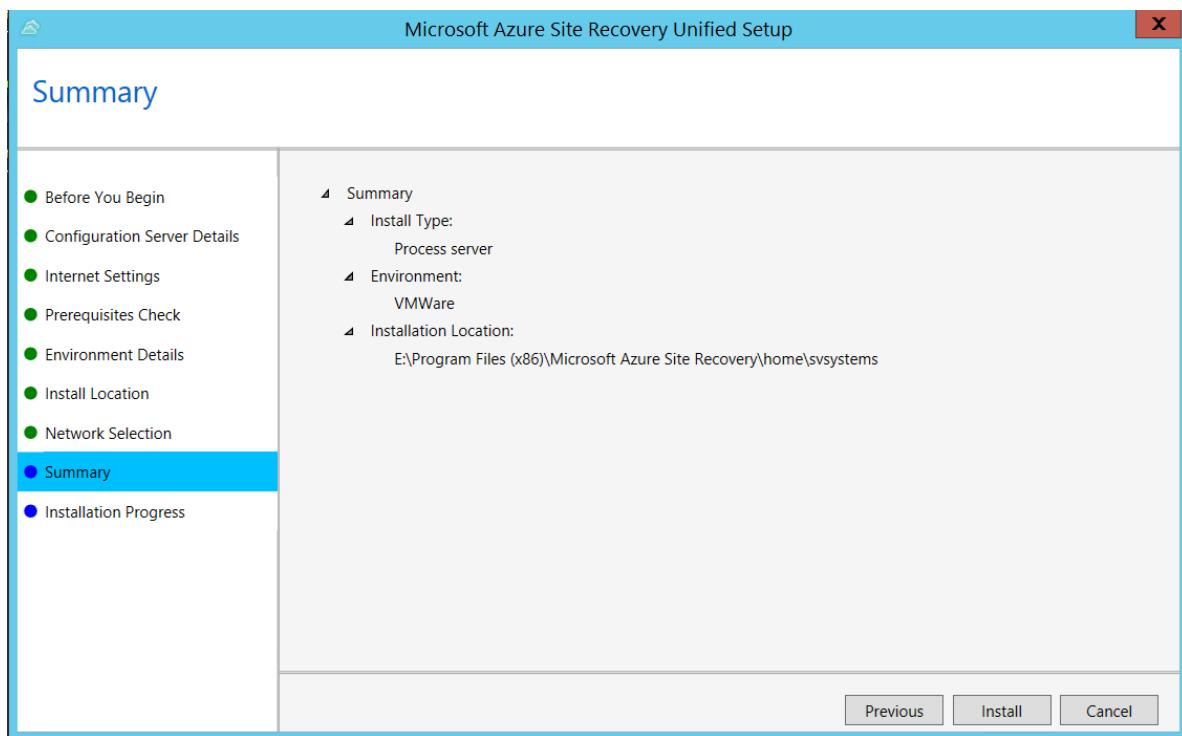
7. In **Install Location**, select where you want to install the binaries and store the cache. The drive you select must have at least 5 GB of disk space available, but we recommend a cache drive with at least 600 GB of free space.



8. In **Network Selection**, specify the listener (network adapter and SSL port) on which the Configuration Server sends and receives replication data. Port 9443 is the default port used for sending and receiving replication traffic, but you can modify this port number to suit your environment's requirements. In addition to the port 9443, we also open port 443, which is used by a web server to orchestrate replication operations. Do not use Port 443 for sending or receiving replication traffic.



9. In **Summary**, review the information and click **Install**. When installation finishes, a passphrase is generated. You will need this when you enable replication, so copy it and keep it in a secure location.



Install from the command line

Install by running the following command:

```
UnifiedSetup.exe [/ServerMode <CS/PS>] [/InstallDrive <DriveLetter>] [/MySQLCredsFilePath <MySQL credentials file path>] [/VaultCredsFilePath <Vault credentials file path>] [/EnvType <VMWare/NonVMWare>] [/PSIP <IP address to be used for data transfer>] [/CSIP <IP address of CS to be registered with>] [/PassphraseFilePath <Passphrase file path>]
```

Where command line parameters are as follows:

PARAMETER NAME	TYPE	DESCRIPTION	POSSIBLE VALUES
/ServerMode	Mandatory	Specifies whether both the configuration and process servers should be installed, or the process server only	CS PS
/InstallLocation	Mandatory	The folder in which the components are installed	Any folder on the computer
/MySQLCredsFilePath	Mandatory	The file path in which the MySQL server credentials are stored	The file should be the format specified below
/VaultCredsFilePath	Mandatory	The path of the vault credentials file	Valid file path
/EnvType	Mandatory	Type of environment that you want to protect	VMware NonVMware
/PSIP	Mandatory	IP address of the NIC to be used for replication data transfer	Any valid IP Address
/CSIP	Mandatory	The IP address of the NIC on which the configuration server is listening on	Any valid IP Address
/PassphraseFilePath	Mandatory	The full path to location of the passphrase file	Valid file path
/BypassProxy	Optional	Specifies that the configuration server connects to Azure without a proxy	To do get this value from Venu
/ProxySettingsFilePath	Optional	Proxy settings (The default proxy requires authentication, or a custom proxy)	The file should be in the format specified below
DataTransferSecurePort	Optional	Port number on the PSIP to be used for replication data	Valid Port Number (default value is 9433)
/SkipSpaceCheck	Optional	Skip space check for cache disk	
/AcceptThirdpartyEULA	Mandatory	Flag implies acceptance of third-party EULA	
/ShowThirdpartyEULA	Optional	Displays third-party EULA. If provided as input all other parameters are ignored	

For example:

```
MicrosoftAzureSiteRecoveryUnifiedSetup.exe /q /x:C:\Temp\Extracted  
cd C:\Temp\Extracted  
UNIFIEDSETUP.EXE /AcceptThirdpartyEULA /servermode "PS" /InstallLocation "D:\" /EnvType "VMWare" /CSIP  
"10.150.24.119" /PassphraseFilePath "C:\Users\Administrator\Desktop\Passphrase.txt" /DataTransferSecurePort  
443
```

Create a proxy settings file

If you need to set up a proxy, the ProxySettingsFilePath parameter takes a file as input. You can create the file as follows, and pass it as input ProxySettingsFilePath parameter.

```
* [ProxySettings]  
* ProxyAuthentication = "Yes/No"  
* Proxy IP = "IP Address"  
* ProxyPort = "Port"  
* ProxyUserName="UserName"  
* ProxyPassword="Password"
```

Next steps

Learn about [managing process server settings](#)

Set up the source environment for VMware to Azure replication

11/5/2019 • 2 minutes to read • [Edit Online](#)

This article describes how to set up your source on-premises environment, to replicate VMware VMs to Azure. The article includes steps for selecting your replication scenario, setting up an on-premises machine as the Site Recovery configuration server, and automatically discovering on-premises VMs.

Prerequisites

The article assumes that you have already:

- Planned your deployment with the help of [Azure Site Recovery Deployment Planner](#). This helps you to allocate sufficient bandwidth, based on your daily data-change rate, to meet your desired recovery point objective (RPO).
- [Set up resources in the Azure portal](#).
- [Set up on-premises VMware](#), including a dedicated account for automatic discovery.

Choose your protection goals

1. In **Recovery Services vaults**, select the vault name. We're using **ContosoVMVault** for this scenario.
2. In **Getting Started**, select Site Recovery. Then select **Prepare Infrastructure**.
3. In **Protection goal > Where are your machines located**, select **On-premises**.
4. In **Where do you want to replicate your machines**, select **To Azure**.
5. In **Are your machines virtualized**, select **Yes, with VMware vSphere Hypervisor**. Then select **OK**.

Set up the configuration server

You can set up the configuration server as an on-premises VMware VM through an Open Virtualization Application (OVA) template. [Learn more](#) about the components that will be installed on the VMware VM.

1. Learn about the [prerequisites](#) for configuration server deployment.
2. [Check capacity numbers](#) for deployment.
3. [Download](#) and [import](#) the OVA template to set up an on-premises VMware VM that runs the configuration server. The license provided with the template is an evaluation license and is valid for 180 days. Post this period, customer needs to activate the windows with a procured license.
4. Turn on the VMware VM, and [register it](#) in the Recovery Services vault.

Azure Site Recovery folder exclusions from Antivirus program

If Antivirus software is active on Source machine

If source machine has an Antivirus software active, installation folder should be excluded. So, exclude folder C:\ProgramData\ASR\agent for smooth replication.

If Antivirus Software is active on Configuration server

Exclude following folders from Antivirus software for smooth replication and to avoid connectivity issues

- C:\Program Files\Microsoft Azure Recovery Services Agent.

- C:\Program Files\Microsoft Azure Site Recovery Provider
- C:\Program Files\Microsoft Azure Site Recovery Configuration Manager
- C:\Program Files\Microsoft Azure Site Recovery Error Collection Tool
 - C:\thirdparty
 - C:\Temp
 - C:\strawberry
 - C:\ProgramData\MySQL
 - C:\Program Files (x86)\MySQL
 - C:\ProgramData\ASR
 - C:\ProgramData\Microsoft Azure Site Recovery
 - C:\ProgramData\ASRLogs
 - C:\ProgramData\ASRSetupLogs
 - C:\ProgramData\LogUploadServiceLogs
 - C:\inetpub
- Site Recovery server installation directory. For example: E:\Program Files (x86)\Microsoft Azure Site Recovery

If Antivirus Software is active on scale-out Process server/Master Target

Exclude following folders from Antivirus software

1. C:\Program Files\Microsoft Azure Recovery Services Agent
2. C:\ProgramData\ASR
3. C:\ProgramData\ASRLogs
4. C:\ProgramData\ASRSetupLogs
5. C:\ProgramData\LogUploadServiceLogs
6. C:\ProgramData\Microsoft Azure Site Recovery
7. Azure Site Recovery load balanced process server installation directory, Example: C:\Program Files (x86)\Microsoft Azure Site Recovery

Next steps

[Set up your target environment](#)

Deploy a configuration server

12/16/2019 • 12 minutes to read • [Edit Online](#)

You deploy an on-premises configuration server when you use [Azure Site Recovery](#) for disaster recovery of VMware VMs and physical servers to Azure. The configuration server coordinates communications between on-premises VMware and Azure. It also manages data replication. This article walks you through the steps needed to deploy the configuration server when you're replicating VMware VMs to Azure. If you need to set up a configuration server for physical server replication, see [Set up the configuration server for disaster recovery of physical servers to Azure](#).

TIP

To learn about the role of a configuration server as part of Azure Site Recovery architecture, see [VMware to Azure disaster recovery architecture](#).

Deploy a configuration server through an OVA template

The configuration server must be set up as a highly available VMware VM with certain minimum hardware and sizing requirements. For convenient and easy deployment, Site Recovery provides a downloadable Open Virtualization Application (OVA) template to set up the configuration server that complies with all the mandated requirements listed here.

Prerequisites

Minimum hardware requirements for a configuration server are summarized in the following sections.

Configuration and process server requirements

Hardware requirements

COMPONENT	REQUIREMENT
CPU cores	8
RAM	16 GB
Number of disks	3, including the OS disk, process server cache disk, and retention drive for failback
Free disk space (process server cache)	600 GB
Free disk space (retention disk)	600 GB

Software requirements

COMPONENT	REQUIREMENT
Operating system	Windows Server 2012 R2 Windows Server 2016
Operating system locale	English (en-us)
Windows Server roles	Don't enable these roles: - Active Directory Domain Services - Internet Information Services - Hyper-V
Group policies	Don't enable these group policies: - Prevent access to the command prompt. - Prevent access to registry editing tools. - Trust logic for file attachments. - Turn on Script Execution. Learn more
IIS	- No pre-existing default website - No pre-existing website/application listening on port 443 - Enable anonymous authentication - Enable FastCGI setting
FIPS (Federal Information Processing Standards)	Do not enable FIPS mode

Network requirements

COMPONENT	REQUIREMENT
IP address type	Static
Ports	443 (Control channel orchestration) 9443 (Data transport)
NIC type	VMXNET3 (if the configuration server is a VMware VM)
Internet access (the server needs access to the following URLs, directly or via proxy):	
*.backup.windowsazure.com	Used for replicated data transfer and coordination
*.store.core.windows.net	Used for replicated data transfer and coordination
*.blob.core.windows.net	Used to access storage account that stores replicated data
*.hypervrecoverymanager.windowsazure.com	Used for replication management operations and coordination
https://management.azure.com	Used for replication management operations and coordination

COMPONENT	REQUIREMENT
*.services.visualstudio.com	Used for telemetry purposes (optional)
time.nist.gov	Used to check time synchronization between system and global time
time.windows.com	Used to check time synchronization between system and global time
<ul style="list-style-type: none"> • https://login.microsoftonline.com • https://secure.aadcdn.microsoftonline-p.com • https://login.live.com • https://graph.windows.net • https://login.windows.net • https://www.live.com • https://www.microsoft.com 	OVF setup needs access to these URLs. They're used for access control and identity management by Azure Active Directory.
https://dev.mysql.com/get/Downloads/MySQLInstaller/mysql-installer-community-5.7.20.0.msi	<p>To complete MySQL download.</p> <p>In a few regions, the download might be redirected to the CDN URL. Ensure that the CDN URL is also whitelisted, if necessary.</p>

Required software

COMPONENT	REQUIREMENT
VMware vSphere PowerCLI	PowerCLI version 6.0 should be installed if the Configuration Server is running on a VMware VM.
MYSQL	MySQL should be installed. You can install manually, or Site Recovery can install it. (Refer to configure settings for more information)

Sizing and capacity requirements

The following table summarizes capacity requirements for the configuration server. If you're replicating multiple VMware VMs, review the [capacity planning considerations](#) and run the [Azure Site Recovery Deployment Planner tool](#).

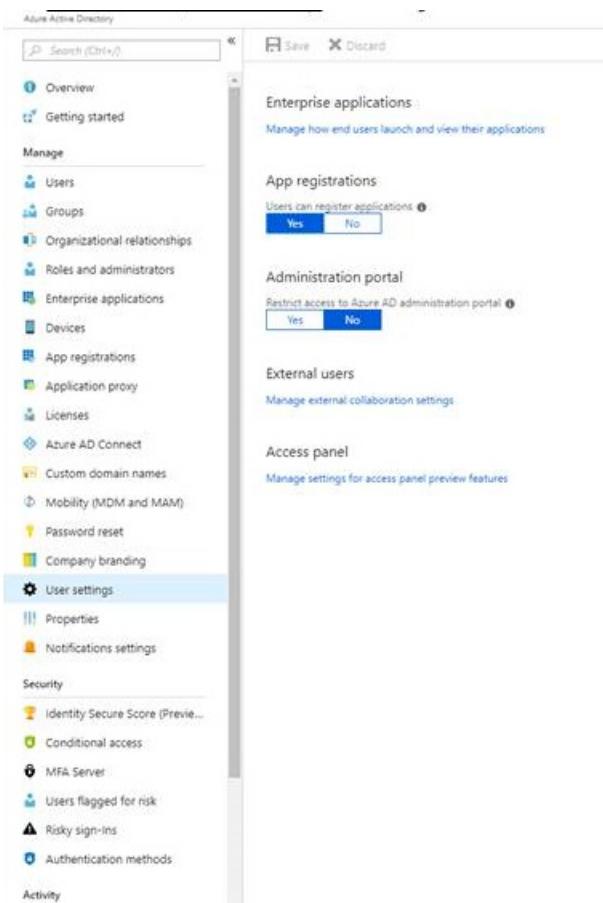
CPU	MEMORY	CACHE DISK	DATA CHANGE RATE	REPLICATED MACHINES
8 vCPUs 2 sockets * 4 cores @ 2.5 GHz	16 GB	300 GB	500 GB or less	< 100 machines
12 vCPUs 2 socks * 6 cores @ 2.5 GHz	18 GB	600 GB	500 GB-1 TB	100 to 150 machines

CPU	MEMORY	CACHE DISK	DATA CHANGE RATE	REPLICATED MACHINES
16 vCPUs 2 socks * 8 cores @ 2.5 GHz	32 GB	1 TB	1-2 TB	150 -200 machines

Azure Active Directory permission requirements

You must have a user with one of the following permissions set in Azure Active Directory (Azure AD) to register the configuration server with Azure Site Recovery services.

1. The user must have an application developer role to create an application.
 - To verify, sign in to the Azure portal.
 - Go to **Azure Active Directory > Roles and administrators**.
 - Verify that the application developer role is assigned to the user. If not, use a user with this permission or contact an [administrator to enable the permission](#).
2. If the application developer role can't be assigned, ensure that the **Users can register applications** flag is set as **true** for the user to create an identity. To enable these permissions:
 - Sign in to the Azure portal.
 - Go to **Azure Active Directory > User settings**.
 - Under **App registrations, Users can register applications**, select **Yes**.



NOTE

Active Directory Federation Services *isn't supported*. Use an account managed through [Azure Active Directory](#).

Download the template

1. In the vault, go to **Prepare Infrastructure > Source**.
2. In **Prepare source**, select **+Configuration server**.
3. In **Add Server**, check that **Configuration server for VMware** appears in **Server type**.
4. Download the OVA template for the configuration server.

TIP

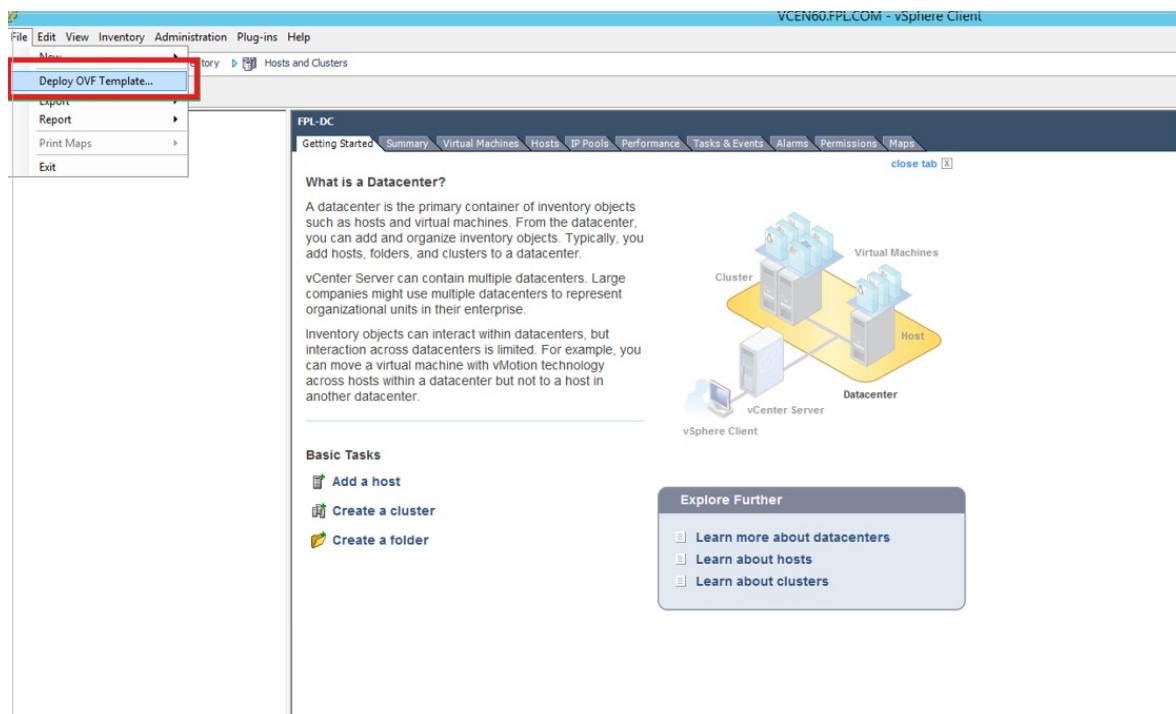
You can also download the latest version of the configuration server template directly from the [Microsoft Download Center](#).

NOTE

The license provided with an OVA template is an evaluation license that's valid for 180 days. After this period, you must procure a license.

Import the template in VMware

1. Sign in to the VMware vCenter server or vSphere ESXi host by using the VMWare vSphere Client.
2. On the **File** menu, select **Deploy OVF Template** to start the **Deploy OVF Template** wizard.



3. On **Select source**, enter the location of the downloaded OVF.
4. On **Review details**, select **Next**.
5. On **Select name and folder** and **Select configuration**, accept the default settings.

6. On **Select storage**, for best performance select **Thick Provision Eager Zeroed** in **Select virtual disk format**. Use of the thin provisioning option might affect the performance of the configuration server.

7. On the rest of the wizard pages, accept the default settings.

8. On **Ready to complete**:

- To set up the VM with the default settings, select **Power on after deployment** > **Finish**.
- To add an additional network interface, clear **Power on after deployment**, and then select **Finish**. By default, the configuration server template is deployed with a single NIC. You can add additional NICs after deployment.

IMPORTANT

Don't change resource configurations, such as memory, cores, and CPU restriction, or modify or delete installed services or files on the configuration server after deployment. These types of changes affect the registration of the configuration server with Azure services and the performance of the configuration server.

Add an additional adapter

NOTE

Two NICs are required if you plan to retain the IP addresses of the source machines on failover and want to fail back to on-premises later. One NIC is connected to source machines, and the other NIC is used for Azure connectivity.

If you want to add an additional NIC to the configuration server, add it before you register the server in the vault. Adding additional adapters isn't supported after registration.

1. In the vSphere Client inventory, right-click the VM and select **Edit Settings**.
2. In **Hardware**, select **Add** > **Ethernet Adapter**. Then select **Next**.
3. Select an adapter type and a network.
4. To connect the virtual NIC when the VM is turned on, select **Connect at power-on**. Then select **Next** > **Finish** > **OK**.

Register the configuration server with Azure Site Recovery services

1. From the VMWare vSphere Client console, turn on the VM.
2. The VM boots up into a Windows Server 2016 installation experience. Accept the license agreement, and enter an administrator password.
3. After the installation finishes, sign in to the VM as the administrator.
4. The first time you sign in, within a few seconds the Azure Site Recovery Configuration tool starts.
5. Enter a name that's used to register the configuration server with Site Recovery. Then select **Next**.
6. The tool checks that the VM can connect to Azure. After the connection is established, select **Sign in** to sign in to your Azure subscription.
 - a. The credentials must have access to the vault in which you want to register the configuration server.
 - b. Ensure that the chosen user account has permission to create an application in Azure. To enable the required permissions, follow the guidelines in the section [Azure Active Directory permission requirements](#).
7. The tool performs some configuration tasks, and then reboots.
8. Sign in to the machine again. The configuration server management wizard starts automatically in a few seconds.

Configure settings

- In the configuration server management wizard, select **Setup connectivity**. From the drop-down boxes, first select the NIC that the in-built process server uses for discovery and push installation of mobility service on source machines. Then select the NIC that the configuration server uses for connectivity with Azure. Select **Save**. You can't change this setting after it's configured. Don't change the IP address of a configuration server. Ensure that the IP assigned to the configuration server is a static IP and not a DHCP IP.
- On **Select Recovery Services vault**, sign in to Microsoft Azure with the credentials used in step 6 of [Register the configuration server with Azure Site Recovery services](#).
- After sign-in, select your Azure subscription and the relevant resource group and vault.

NOTE

After registration, there's no flexibility to change the recovery services vault. Changing a recovery services vault requires disassociation of the configuration server from the current vault, and the replication of all protected virtual machines under the configuration server is stopped. To learn more, see [Manage the configuration server for VMware VM disaster recovery](#).

- On **Install third-party software**:

SCENARIO	STEPS TO FOLLOW
Can I download and install MySQL manually?	Yes. Download the MySQL application, place it in the folder C:\Temp\ASRSetup , and then install manually. After you accept the terms and select Download and install , the portal says <i>Already installed</i> . You can proceed to the next step.
Can I avoid download of MySQL online?	Yes. Place your MySQL installer application in the folder C:\Temp\ASRSetup . Accept the terms, select Download and install , and the portal uses the installer you added to install the application. After installation finishes, proceed to the next step.
I want to download and install MySQL through Azure Site Recovery.	Accept the license agreement, and select Download and install . After installation finishes, proceed to the next step.

- On **Validate appliance configuration**, prerequisites are verified before you continue.
- On **Configure vCenter Server/vSphere ESXi server**, enter the FQDN or IP address of the vCenter server, or vSphere host, where the VMs you want to replicate are located. Enter the port on which the server is listening. Enter a friendly name to be used for the VMware server in the vault.
- Enter credentials to be used by the configuration server to connect to the VMware server. Site Recovery uses these credentials to automatically discover VMware VMs that are available for replication. Select **Add > Continue**. The credentials entered here are locally saved.
- On **Configure virtual machine credentials**, enter the user name and password of virtual machines to automatically install mobility service during replication. For **Windows** machines, the account needs local administrator privileges on the machines you want to replicate. For **Linux**, provide details for the root account.
- Select **Finalize configuration** to complete registration.
- After registration finishes, open the Azure portal and verify that the configuration server and VMware

server are listed on **Recovery Services Vault > Manage > Site Recovery Infrastructure > Configuration Servers**.

Upgrade the configuration server

To upgrade the configuration server to the latest version, see [Manage the configuration server for VMware VM disaster recovery](#). For instructions on how to upgrade all Site Recovery components, see [Service updates in Site Recovery](#).

Manage the configuration server

To avoid interruptions in ongoing replication, ensure that the IP address of the configuration server doesn't change after the configuration server is registered to a vault. To learn more about common configuration server management tasks, see [Manage the configuration server for VMware VM disaster recovery](#).

Troubleshoot deployment issues

Refer to our [troubleshooting article](#) to resolve deployment & connectivity issues.

FAQs

- How long is the license provided on a configuration server deployed through OVF valid? What happens if I don't reactivate the license?

The license provided with an OVA template is an evaluation license valid for 180 days. Before expiration, you need to activate the license. Otherwise, it can result in frequent shutdown of the configuration server and cause a hindrance to replication activities. For more information, see [Manage the configuration server for VMware VM disaster recovery](#).

- Can I use the VM where the configuration server is installed for different purposes?

No. Use the VM for the sole purpose of the configuration server. Ensure that you follow all the specifications mentioned in [Prerequisites](#) for efficient management of disaster recovery.

- Can I switch the vault already registered in the configuration server with a newly created vault?

No. After a vault is registered with the configuration server, it can't be changed.

- Can I use the same configuration server to protect both physical and virtual machines?

Yes. The same configuration server can be used for replicating physical and virtual machines. However, the physical machine can be failed back only to a VMware VM.

- What's the purpose of a configuration server and where is it used?

To learn more about the configuration server and its functionalities, see [VMware to Azure replication architecture](#).

- Where can I find the latest version of the configuration server?

For steps to upgrade the configuration server through the portal, see [Upgrade the configuration server](#). For instructions on how to upgrade all Site Recovery components, see [Service updates in Site Recovery](#).

- Where can I download the passphrase for configuration server?

To download the passphrase, see [Manage the configuration server for VMware VM disaster recovery](#).

- Can I change the passphrase?

No. Don't change the passphrase of the configuration server. A change in the passphrase breaks replication of protected machines and leads to a critical health state.

- Where can I download vault registration keys?

In **Recovery Services Vault**, select **Manage > Site Recovery Infrastructure > Configuration Servers**. In **Servers**, select **Download registration key** to download the vault credentials file.

- Can I clone an existing configuration server and use it for replication orchestration?

No. Use of a cloned configuration server component isn't supported. Cloning of a scale-out process server is also an unsupported scenario. Cloning Site Recovery components affects ongoing replications.

- Can I change the IP of a configuration server?

No. Don't change the IP address of a configuration server. Ensure that all IPs assigned to the configuration server are static IPs and not DHCP IPs.

- Can I set up a configuration server on Azure?

Set up a configuration server in an on-premises environment with a direct line-of-sight with v-Center and to minimize data transfer latencies. You can take scheduled backups of configuration server for [failback purposes](#).

- Can I change cache driver on a configuration server or scale-out process server?

No, Cache driver cannot be changed once set up is complete.

For more FAQs on configuration servers, see [Configuration server common questions](#).

Next steps

Set up disaster recovery of [VMware VMs](#) to Azure.

Prepare the target environment for disaster recovery of VMware VMs or physical servers to Azure

11/6/2019 • 2 minutes to read • [Edit Online](#)

This article describes how to prepare your target Azure environment to start replicating VMware virtual machines or physical servers to Azure.

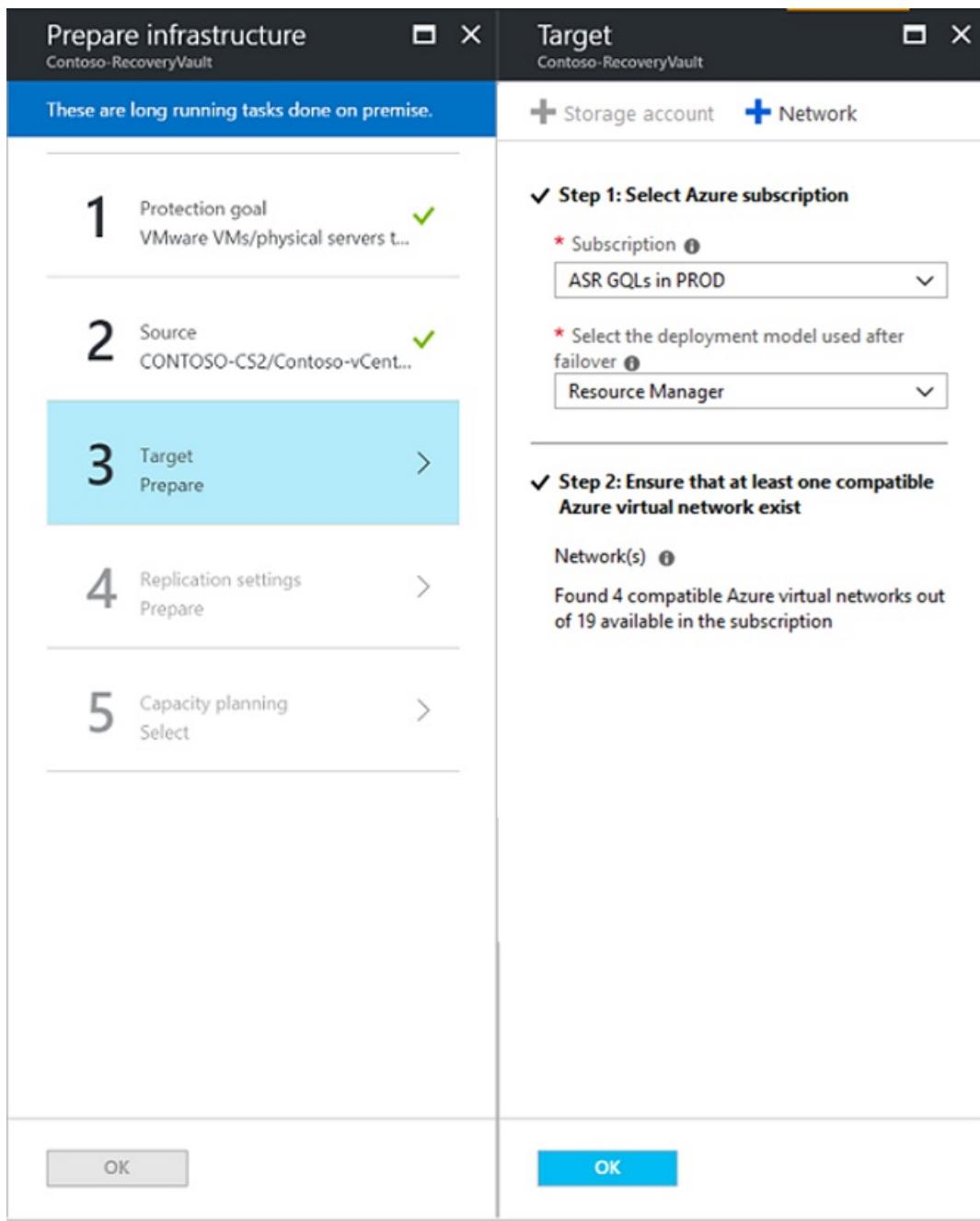
Prerequisites

The article assumes:

- You have created a Recovery Services Vault on [Azure portal](#) to protect your source machines
- You have setup your on-premises environment to replicate the source [VMware virtual machines](#) or [physical servers](#) to Azure.

Prepare target

After completing the **Step 1: Select Protection goal** and **Step 2: Prepare Source**, you are taken to **Step 3: Target**



- Subscription:** From the drop-down menu, select the Subscription that you want to replicate your virtual machines or physical servers to.
- Deployment Model:** Select the deployment model (Classic or Resource Manager)

Based on the chosen deployment model, a validation is run to ensure that you have at least one virtual network in the target subscription to replicate and failover your virtual machine or physical server to.

Once the validations complete successfully, click OK to go to the next step.

If you don't have a virtual network, you can create one by clicking the + Network button at the top of the page.

Next steps

[Configure replication settings.](#)

Configure and manage replication policies for VMware disaster recovery

11/12/2019 • 2 minutes to read • [Edit Online](#)

This article describes how to configure a replication policy when you're replicate VMware VMs to Azure, using [Azure Site Recovery](#).

Create a policy

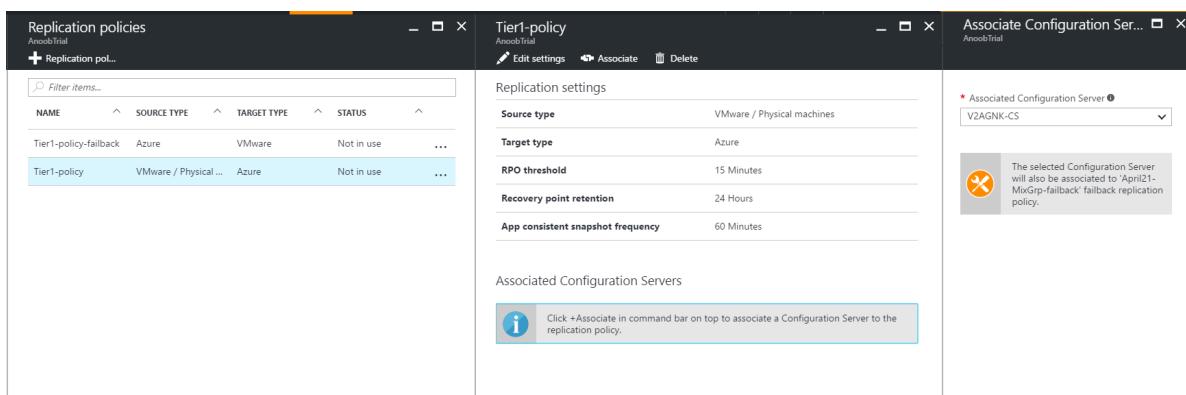
1. Select **Manage > Site Recovery Infrastructure**.
2. In **For VMware and Physical machines**, select **Replication policies**.
3. Click **+Replication policy**, and specify the policy name.
4. In **RPO threshold**, specify the RPO limit. Alerts are generated when continuous replication exceeds this limit.
5. In **Recovery point retention**, specify (in hours) the duration of the retention window for each recovery point. Protected machines can be recovered to any point within a retention window. Up to 24 hours of retention is supported for machines replicated to premium storage. Up to 72 hours is supported for standard storage.
6. In **App-consistent snapshot frequency**, choose from the dropdown how often (in hours) recovery points that contain application-consistent snapshots should be created. If you wish to turn off generation of application consistency points, choose "Off" value in the dropdown.
7. Click **OK**. The policy should be created in 30 to 60 seconds.

When you create a replication policy, a matching failback replication policy is automatically created, with the suffix "failback". After creating the policy, you can edit it by selecting it > **Edit Settings**.

Associate a configuration server

Associate the replication policy with your on-premises configuration server.

1. Click **Associate**, and select the configuration server.



2. Click **OK**. The configuration server should be associated in one to two minutes.

The screenshot shows two overlapping windows from the Azure portal. The left window, titled 'Replication policies', lists existing replication policies. The right window, titled 'Tier1-policy', shows the configuration details for a selected policy.

Replication policies

NAME	SOURCE TYPE	TARGET TYPE	STATUS	...
Tier1-policy-fallback	Azure	VMware	Not in use	...
Tier1-policy	VMware / Physical ...	Azure	Not in use	...

Tier1-policy

Replication settings

Source type	VMware / Physical machines
Target type	Azure
RPO threshold	15 Minutes
Recovery point retention	24 Hours
App consistent snapshot frequency	60 Minutes

Associated Configuration Servers

NAME	ASSOCIATION STATUS	...
V2AGNK-CS	Associated	...

Edit a policy

You can modify a replication policy after creating it.

- Changes in the policy are applied to all machines using the policy.
- If you want to associate replicated machines with a different replication policy, you need to disable and reenable protection for the relevant machines.

Edit a policy as follows:

- Select **Manage > Site Recovery Infrastructure > Replication Policies**.
- Select the replication policy you wish to modify.
- Click **Edit settings**, and update the RPO threshold/recovery point retention hours/app-consistent snapshot frequency fields as required.
- If you wish to turn off generation of application consistency points, choose "Off" value in the dropdown of the field **App-consistent snapshot frequency**.
- Click **Save**. The policy should be updated in 30 to 60 seconds.

Disassociate or delete a replication policy

- Choose the replication policy. a. To dissociate the policy from the configuration server, make sure that no replicated machines are using the policy. Then, click **Dissociate**. b. To delete the policy, make sure it's not associated with a configuration server. Then, click **Delete**. It should take 30-60 seconds to delete.
- Click **OK**.

About the Mobility service for VMware VMs and physical servers

2/21/2020 • 6 minutes to read • [Edit Online](#)

When you set up disaster recovery for VMware VMs and physical servers using [Azure Site Recovery](#), you install the Site Recovery Mobility service on each on-premises VMware VM and physical server. The Mobility service captures data writes on the machine, and forwards them to the Site Recovery process server. You can deploy the Mobility Service using the following methods:

- [Push installation](#): Site Recovery installs mobility agent on the server when protection is enabled via Azure portal.
- Install manually: You can install the Mobility service manually on each machine through [UI](#) or [command prompt](#).
- [Automated deployment](#): You can automate installation with software deployment tools such as Configuration Manager.

NOTE

The Mobility agent uses approximately 6%-10% of memory on source machines for VMware VMs or physical machines.

Anti-virus on replicated machines

If machines you want to replicate have active anti-virus software running, make sure you exclude the Mobility service installation folder from anti-virus operations (`C:\ProgramData\ASR\agent`). This ensures that replication works as expected.

Push installation

Push installation is an integral part of "[Enable Replication](#)" job triggered in the portal. After choosing the set of virtual machines you wish to protect and trigger "[Enable Replication](#)", configuration server pushes mobility agent on to the servers, installs the agent and complete registration of agent with configuration server. For successful completion of this operation,

- Ensure that all push installation [prerequisites](#) are met.
- Ensure that all configurations of servers fall under [support matrix of VMware to Azure DR scenario](#).

Details of push installation workflow has been described in the following sections.

From 9.23 version onwards

During push installation of mobility agent, following steps are performed

1. Pushes agent on to the source machine. Copying the agent on to source machine can fail due to multiple environmental errors. Visit [our guidance](#) to troubleshoot push installation failures.
2. After agent is successfully copied on to the server prerequisite checks are performed on the server. Installation fails if one or more of the [prerequisites](#) are not met. If all prerequisites are met, installation is triggered.
3. Azure Site Recovery VSS provider is installed on the server as part of Mobility agent installation. This provider is used to generate Application consistent points. If installation of VSS provider fails, this step will

be skipped and agent installation will continue.

4. If agent installation succeeds but VSS provider installation fails, then job status is marked as "Warning". This does not impact crash consistency points generation.
 - a. To generate application consistent points, refer to [our guidance](#) to complete installation of Site Recovery VSS provider manually.
 - b. If you do not wish application consistent points to be generated, [modify the replication policy](#) to turn off application consistent points.

Before 9.22 versions

1. Pushes agent on to the source machine. Copying the agent on to source machine can fail due to multiple environmental errors. Visit [our guidance](#) to troubleshoot push installation failures.
2. After agent is successfully copied on to the server prerequisite checks are performed on the server. Installation fails if one or more of the [prerequisites](#) are not met. If all prerequisites are met, installation is triggered.
3. Azure Site Recovery VSS provider is installed on the server as part of Mobility agent installation. This provider is used to generate Application consistent points. If installation of VSS provider fails, then agent installation will fail. To avoid failure of mobility agent installation, use [9.23 version](#) or higher to generate crash consistent points and install VSS provider manually.

Install mobility agent through UI

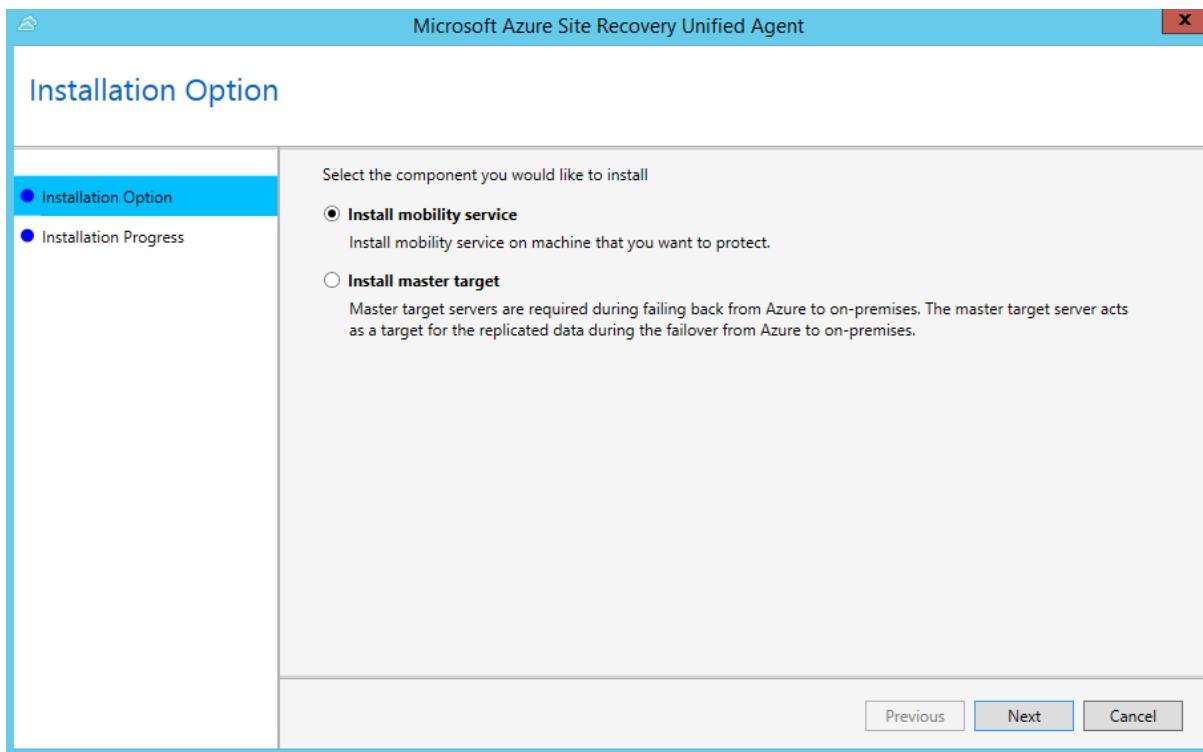
Prerequisite

- Ensure that all configurations of servers fall under [support matrix of VMware to Azure DR scenario](#).
- [Locate the installer](#) based on the operating system of the server.

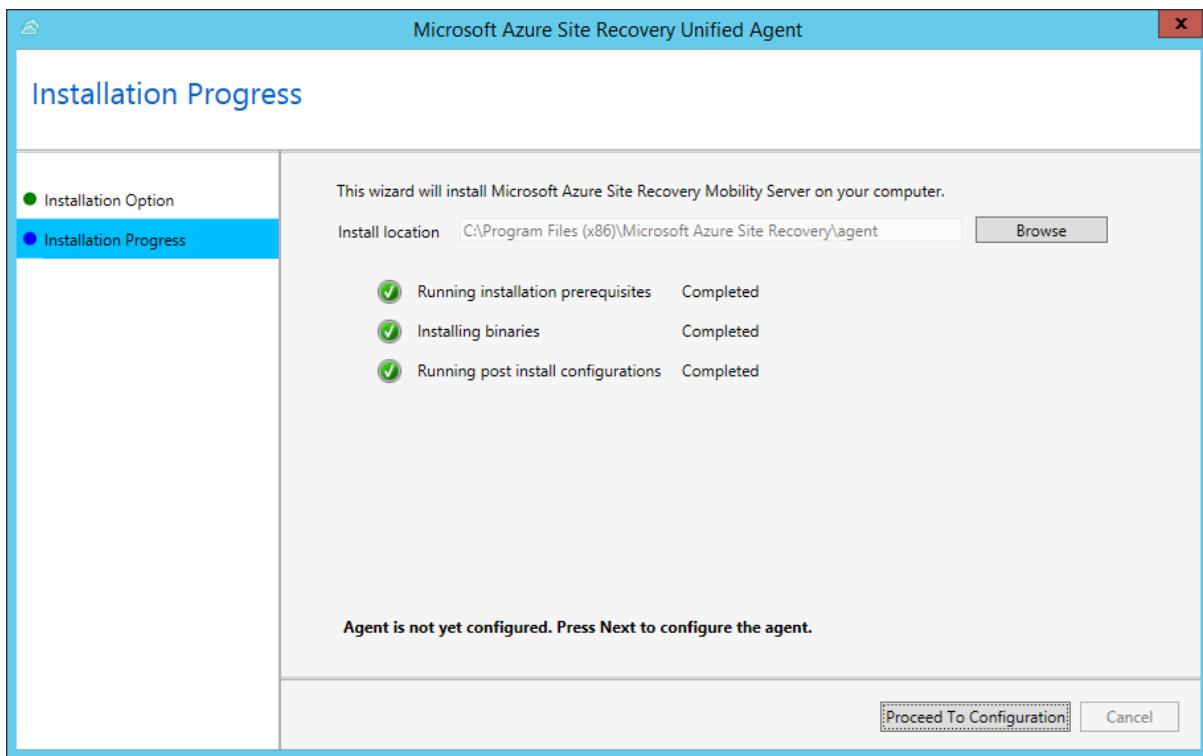
IMPORTANT

If you are replicating Azure IaaS VM from one Azure region to another, don't use this method. Use the command-line-based installation method instead.

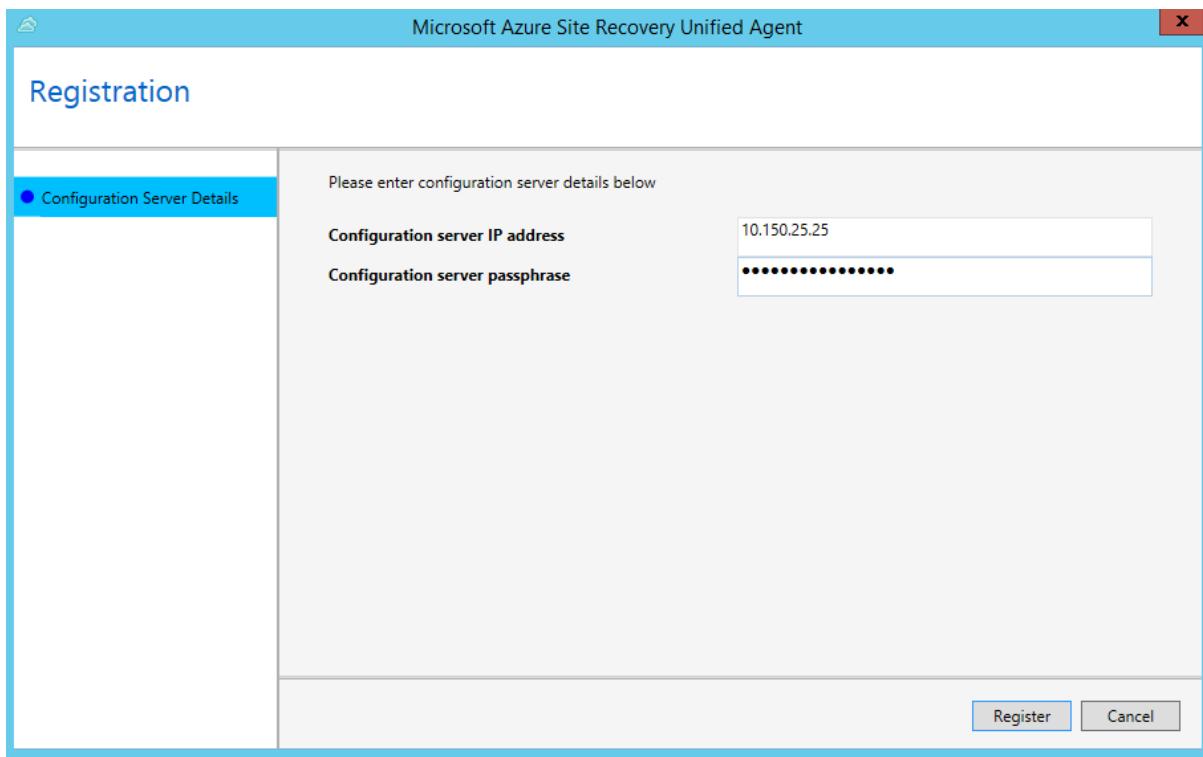
1. Copy the installation file to the machine, and run it.
2. In **Installation Option**, select **Install mobility service**.
3. Select the installation location > **Install**.



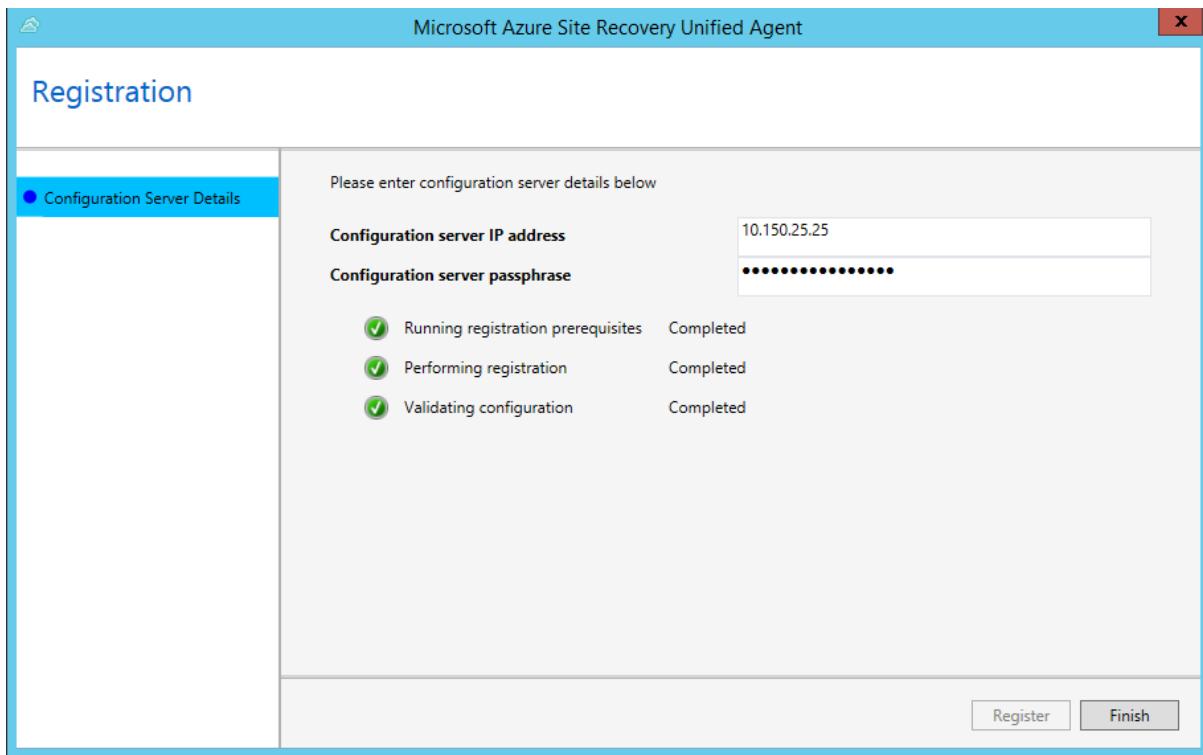
4. Monitor the installation in **Installation Progress**. After the installation is finished, select **Proceed to Configuration** to register the service with the configuration server.



5. In **Configuration Server Details**, specify the IP address and passphrase you configured.



6. Select **Register** to finish the registration.



Install mobility agent through command prompt

Prerequisite

- Ensure that all configurations of servers fall under [support matrix of VMware to Azure DR scenario](#).
- [Locate the installer](#) based on the operating system of the server.

On a Windows machine

- Copy the installer to a local folder (for example, C:\Temp) on the server that you want to protect.

```

cd C:\Temp
ren Microsoft-ASR_UA*Windows*release.exe MobilityServiceInstaller.exe
MobilityServiceInstaller.exe /q /x:C:\Temp\Extracted
cd C:\Temp\Extracted

```

- Install as follows:

```

UnifiedAgent.exe /Role "MS" /InstallLocation "C:\Program Files (x86)\Microsoft Azure Site Recovery"
/Platform "VmWare" /Silent

```

- Register the agent with the configuration server.

```

cd C:\Program Files (x86)\Microsoft Azure Site Recovery\agent
UnifiedAgentConfigurator.exe /CSEndPoint <CSIP> /PassphraseFilePath <PassphraseFilePath>

```

Installation settings

SETTING	DETAILS
Usage	UnifiedAgent.exe /Role <MS/MT> /InstallLocation <Install Location> /Platform "VmWare" /Silent
Setup logs	Under %ProgramData%\ASRSetupLogs\ASRUnifiedAgentInstaller.log.
/Role	Mandatory installation parameter. Specifies whether the Mobility service (MS) or master target (MT) should be installed.
/InstallLocation	Optional parameter. Specifies the Mobility service installation location (any folder).
/Platform	Mandatory. Specifies the platform on which Mobility Service is installed. VMware for VMware VMs/physical servers; Azure for Azure VMs. If you're treating Azure VMs as physical machines, specify VMware .
/Silent	Optional. Specifies whether to run the installer in silent mode.

Registration settings

SETTING	DETAILS
Usage	UnifiedAgentConfigurator.exe /CSEndPoint <CSIP> /PassphraseFilePath <PassphraseFilePath>
Agent configuration logs	Under %ProgramData%\ASRSetupLogs\ASRUnifiedAgentConfigurator.log.
/CSEndPoint	Mandatory parameter. Specifies the IP address of the configuration server. Use any valid IP address.

SETTING	DETAILS
/PassphraseFilePath	Mandatory. Location of the passphrase. Use any valid UNC or local file path.

On a Linux machine

1. Copy the installer to a local folder (for example, /tmp) on the server that you want to protect. In a terminal, run the following commands:

```
cd /tmp ;
tar -xvf Microsoft-ASR_UA*release.tar.gz
```

2. Install as follows:

```
sudo ./install -d <Install Location> -r MS -v VmWare -q
```

3. After installation is finished, Mobility Service must be registered to the configuration server. Run the following command to register Mobility Service with the configuration server:

```
/usr/local/ASR/Vx/bin/UnifiedAgentConfigurator.sh -i <CSIP> -P /var/passphrase.txt
```

Installation settings

SETTING	DETAILS
Usage	./install -d <Install Location> -r <MS/MT> -v VmWare -q
-r	Mandatory installation parameter. Specifies whether the Mobility service (MS) or master target (MT) should be installed.
-d	Optional parameter. Specifies the Mobility service installation location: /usr/local/ASR.
-v	Mandatory. Specifies the platform on which Mobility Service is installed. VMware for VMware VMs/physical servers; Azure for Azure VMs.
-q	Optional. Specifies whether to run the installer in silent mode.

Registration settings

SETTING	DETAILS
Usage	cd /usr/local/ASR/Vx/bin UnifiedAgentConfigurator.sh -i <CSIP> -P <PassphraseFilePath>
-i	Mandatory parameter. Specifies the IP address of the configuration server. Use any valid IP address.
-P	Mandatory. Full file path of the file in which the passphrase is saved. Use any valid folder.

SETTING	DETAILS
---------	---------

Azure Virtual Machine agent

- **Windows VMs:** From version 9.7.0.0 of the Mobility service, the [Azure VM agent](#) is installed by the Mobility service installer. This ensures that when the machine fails over to Azure, the Azure VM meets the agent installation prerequisite for using any Vm extension.
- **Linux VMs:** The [WALinuxAgent](#) must be installed manually on the Azure VM after failover.

Locate installer files

Go to %ProgramData%\ASR\home\svsystems\pushinstallsvc\repository folder on configuration server. Check which installer you need based on operating system. The following table summarizes the installer files for each VMware VM and physical server operating system. You can review [supported operating systems](#) before you start.

INSTALLER FILE	OPERATING SYSTEM (64-BIT ONLY)
Microsoft-ASR_UA*Windows*release.exe	Windows Server 2016; Windows Server 2012 R2; Windows Server 2012; Windows Server 2008 R2 SP1
Microsoft-ASR_UA*RHEL6-64*release.tar.gz	Red Hat Enterprise Linux (RHEL) 6.* CentOS 6.*
Microsoft-ASR_UA*RHEL7-64*release.tar.gz	Red Hat Enterprise Linux (RHEL) 7.* CentOS 7.*
Microsoft-ASR_UA*SLES12-64*release.tar.gz	SUSE Linux Enterprise Server 12 SP1,SP2,SP3
Microsoft-ASR_UA*SLES11-SP3-64*release.tar.gz	SUSE Linux Enterprise Server 11 SP3
Microsoft-ASR_UA*SLES11-SP4-64*release.tar.gz	SUSE Linux Enterprise Server 11 SP4
Microsoft-ASR_UA*OL6-64*release.tar.gz	Oracle Enterprise Linux 6.4, 6.5
Microsoft-ASR_UA*UBUNTU-14.04-64*release.tar.gz	Ubuntu Linux 14.04
Microsoft-ASR_UA*UBUNTU-16.04-64*release.tar.gz	Ubuntu Linux 16.04 LTS server
Microsoft-ASR_UA*DEBIAN7-64*release.tar.gz	Debian 7
Microsoft-ASR_UA*DEBIAN8-64*release.tar.gz	Debian 8

Next steps

[Set up push installation for the Mobility service.](#)

Prepare source machine for push installation of mobility agent

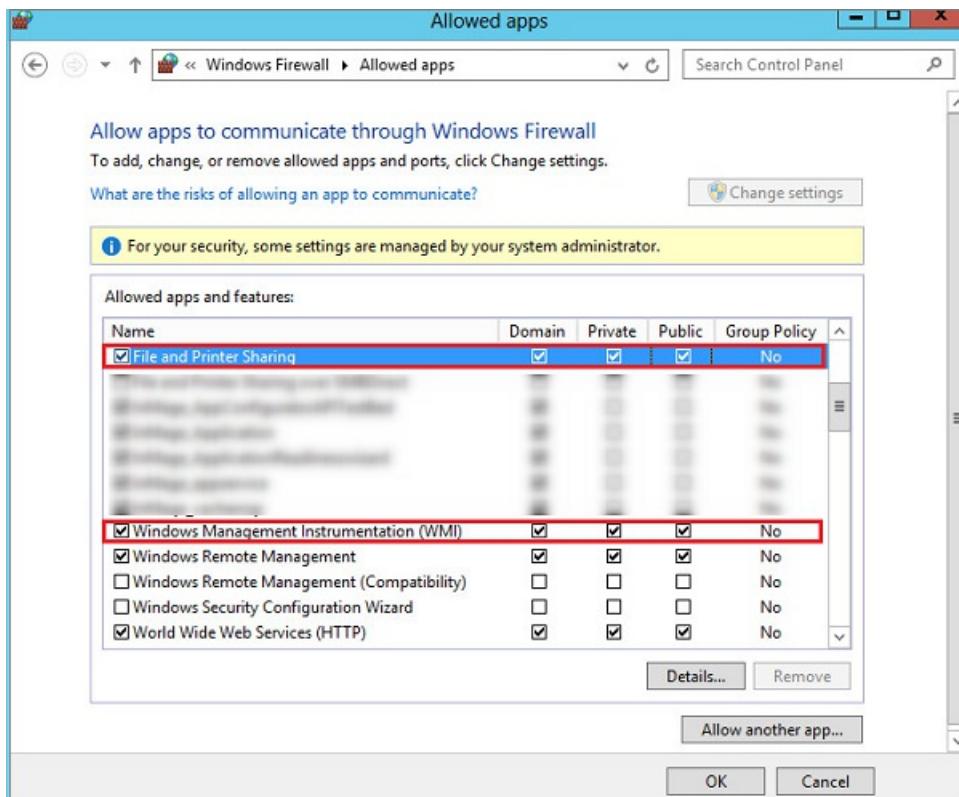
11/19/2019 • 2 minutes to read • [Edit Online](#)

When you set up disaster recovery for VMware VMs and physical servers using [Azure Site Recovery](#), you install the [Site Recovery Mobility service](#) on each on-premises VMware VM and physical server. The Mobility service captures data writes on the machine, and forwards them to the Site Recovery process server.

Install on Windows machine

On each Windows machine you want to protect, do the following:

1. Ensure that there's network connectivity between the machine and the process server. If you haven't set up a separate process server, then by default it's running on the configuration server.
2. Create an account that the process server can use to access the computer. The account should have administrator rights, either local or domain. Use this account only for the push installation and for agent updates.
3. If you don't use a domain account, disable Remote User Access control on the local computer as follows:
 - Under HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System registry key, add a new DWORD: **LocalAccountTokenFilterPolicy**. Set the value to **1**.
 - To do this at a command prompt, run the following command:
`'REG ADD HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v LocalAccountTokenFilterPolicy /t REG_DWORD /d`
4. In Windows Firewall on the machine you want to protect, select **Allow an app or feature through Firewall**. Enable **File and Printer Sharing** and **Windows Management Instrumentation (WMI)**. For computers that belong to a domain, you can configure the firewall settings by using a Group Policy object (GPO).



5. Add the account that you created in CSPSConfigtool. To do this, sign in to your configuration server.
6. Open **cspscfgtool.exe**. It's available as a shortcut on the desktop and in the %ProgramData%\ASR\home\svsystems\bin folder.
7. On the **Manage Accounts** tab, select **Add Account**.
8. Add the account you created.
9. Enter the credentials you use when you enable replication for a computer.

Install on Linux machine

On each Linux machine that you want to protect, do the following:

1. Ensure that there's network connectivity between the Linux machine and the process server.
2. Create an account that the process server can use to access the computer. The account should be a **root** user on the source Linux server. Use this account only for the push installation and for updates.
3. Check that the /etc/hosts file on the source Linux server has entries that map the local hostname to IP addresses associated with all network adapters.
4. Install the latest openssh, openssh-server, and openssl packages on the computer that you want to replicate.
5. Ensure that Secure Shell (SSH) is enabled and running on port 22.
6. Enable SFTP subsystem and password authentication in the sshd_config file. To do this, sign in as **root**.
7. In the **/etc/ssh/sshd_config** file, find the line that begins with **PasswordAuthentication**.
8. Uncomment the line, and change the value to **yes**.
9. Find the line that begins with **Subsystem**, and uncomment the line.

```
# override default of no subsystems
Subsystem      sftp      /usr/libexec/openssh/sftp-server
```

10. Restart the **sshd** service.
11. Add the account that you created in CSPSConfigtool. To do this, sign in to your configuration server.
12. Open **cspconfigtool.exe**. It's available as a shortcut on the desktop and in the %ProgramData%\home\svsystems\bin folder.
13. On the **Manage Accounts** tab, select **Add Account**.
14. Add the account you created.
15. Enter the credentials you use when you enable replication for a computer.

Anti-virus on replicated machines

If machines you want to replicate have active anti-virus software running, make sure you exclude the Mobility service installation folder from anti-virus operations (*C:\ProgramData\ASR\agent*). This ensures that replication works as expected.

Next steps

After the Mobility Service is installed, in the Azure portal, select **+ Replicate** to start protecting these VMs. Learn more about enabling replication for [VMware VMs](#) and [physical servers](#).

Automate Mobility Service installation

2/14/2020 • 10 minutes to read • [Edit Online](#)

This article describes how to automate installation and updates for the Mobility Service agent in [Azure Site Recovery](#).

When you deploy Site Recovery for disaster recovery of on-premises VMware VMs and physical servers to Azure, you install the Mobility Service agent on each machine you want to replicate. The Mobility Service captures data writes on the machine, and forwards them to the Site Recovery process server for replication. You can deploy the Mobility Service in a few ways:

- **Push installation:** Let Site Recovery install the Mobility service agent when you enable replication for a machine in the Azure portal.
- **Manual installation:** Install the Mobility service manually on each machine. [Learn more](#) about push and manual installation.
- **Automated deployment:** Automate installation with software deployment tools such as Microsoft Endpoint Configuration Manager, or third-party tools such as JetPatch.

Automated installation and updating provides a solution if:

- Your organization doesn't allow for push installation on protected servers.
- Your company policy requires passwords to be changed periodically. You have to specify a password for the push installation.
- Your security policy doesn't permit adding firewall exceptions for specific machines.
- You're acting as a hosting service provider and don't want to provide customer machine credentials that are needed for push installation with Site Recovery.
- You need to scale agent installations to lots of servers simultaneously.
- You want to schedule installations and upgrades during planned maintenance windows.

Prerequisites

To automate the installation, you need the following items:

- A deployed software installation solution such as [Configuration Manager](#) or [JetPatch](#).
- Deployment prerequisites in place in [Azure](#) and [on-premises](#) for VMware disaster recovery, or for [physical server](#) disaster recovery. Review the [support requirements](#) for disaster recovery.

Prepare for automated deployment

The following table summarizes tools and processes for automating Mobility Service deployment.

TOOL	DETAILS	INSTRUCTIONS
------	---------	--------------

Tool	Details	Instructions
Configuration Manager	<p>1. Verify that you have the prerequisites listed above in place.</p> <p>2. Deploy disaster recovery by setting up the source environment, including downloading an OVA file to deploy the Site Recovery configuration server as a VMware VM using an OVF template.</p> <p>3. You register the configuration server with the Site Recovery service, set up the target Azure environment, and configure a replication policy.</p> <p>4. For automated Mobility Service deployment, you create a network share containing the configuration server passphrase and Mobility Service installation files.</p> <p>5. You create a Configuration Manager package containing the installation or updates, and prepare for Mobility Service deployment.</p> <p>6. You can then enable replication to Azure for the machines that have the Mobility Service installed.</p>	Automate with Configuration Manager
JetPatch	<p>1. Verify that you have the prerequisites listed above in place.</p> <p>2. Deploy disaster recovery by setting up the source environment, including downloading and deploying JetPatch Agent Manager for Azure Site Recovery in your Site Recovery environment, using an OVF template.</p> <p>3. You register the configuration server with Site Recovery, set up the target Azure environment, and configure a replication policy.</p> <p>4. For automated deployment, initialize and complete the JetPatch Agent Manager configuration.</p> <p>5. In JetPatch you can create a Site Recovery policy to automate deployment and upgrade of the Mobility Service agent.</p> <p>6. You can then enable replication to Azure for the machines that have the Mobility Service installed.</p>	Automate with JetPatch Agent Manager Troubleshoot agent installation in JetPatch

Automate with Configuration Manager

Prepare the installation files

1. Make sure you have the prerequisites in place.
2. Create a secure network file share (SMB share) that can be accessed by the machine running the configuration server.
3. In Configuration Manager, [categorize the servers](#) on which you want to install or update the Mobility Service. One collection should contain all Windows servers, the other all Linux servers.
4. On the network share, create a folder:
 - For installation on Windows machines, create a folder named *MobSvcWindows*.
 - For installation on Linux machines, create a folder named *MobSvcLinux*.
5. Sign in to the configuration server machine.
6. On the configuration server machine, open an administrative command prompt.
7. To generate the passphrase file, run this command:

```
cd %ProgramData%\ASR\home\svsystems\bin
genpassphrase.exe -v > MobSvc.passphrase
```

8. Copy the *MobSvc.passphrase* file to the Windows folder and the Linux folder.
9. To browse to the folder that contains the installation files, run this command:

```
cd %ProgramData%\ASR\home\svsystems\pushinstallsvc\repository
```

10. Copy these installation files to the network share:

- For Windows, copy *Microsoft-ASR_UA_version_Windows_GA_date_Release.exe* to *MobSvcWindows*.
- For Linux, copy the following files to *MobSvcLinux*:
 - *Microsoft-ASR_UARHEL6-64release.tar.gz*
 - *Microsoft-ASR_UARHEL7-64release.tar.gz*
 - *Microsoft-ASR_UASLES11-SP3-64release.tar.gz*
 - *Microsoft-ASR_UASLES11-SP4-64release.tar.gz*
 - *Microsoft-ASR_UAOL6-64release.tar.gz*
 - *Microsoft-ASR_UAUBUNTU-14.04-64release.targz*

11. As described in the following procedures, copy the code to the Windows or Linux folders. We're assuming that:
 - The configuration server's IP address is `192.168.3.121`.
 - The secure network file share is `\ContosoSecureFS\MobilityServiceInstallers`.

Copy code to the Windows folder

Copy the following code:

- Save the code in the *MobSvcWindows* folder as *install.bat*.
- Replace the `[CSIP]` placeholders in this script with the actual values of the IP address of your configuration server.
- The script supports new installations of the Mobility Service agent, and updates to agents that are already installed.

```
Time /t >> C:\Temp\logfile.log
REM =====
REM === Clean up the folders =====
```

```

RMDIR /S /q %temp%\MobSvc
MKDIR %Temp%\MobSvc
MKDIR C:\Temp
REM =====

REM === Copy new files =====
COPY M*.* %Temp%\MobSvc
CD %Temp%\MobSvc
REN Micro*.exe MobSvcInstaller.exe
REM =====

REM === Extract the installer =====
MobSvcInstaller.exe /q /x:%Temp%\MobSvc\Extracted
REM === Wait 10s for extraction to complete =====
TIMEOUT /t 10
REM =====

REM === Perform installation =====
REM =====

CD %Temp%\MobSvc\Extracted
whoami >> C:\Temp\logfile.log
SET PRODKEY=HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall
REG QUERY %PRODKEY%\{275197FC-14FD-4560-A5EB-38217F80CBD1}
IF NOT %ERRORLEVEL% EQU 0 (
    echo "Product is not installed. Goto INSTALL." >> C:\Temp\logfile.log
    GOTO :INSTALL
) ELSE (
    echo "Product is installed." >> C:\Temp\logfile.log

    echo "Checking for Post-install action status." >> C:\Temp\logfile.log
    GOTO :POSTINSTALLCHECK
)

:POSTINSTALLCHECK
REG QUERY "HKLM\SOFTWARE\Wow6432Node\InMage Systems\Installed Products\5" /v "PostInstallActions" | Find
"Succeeded"
If %ERRORLEVEL% EQU 0 (
    echo "Post-install actions succeeded. Checking for Configuration status." >> C:\Temp\logfile.log
    GOTO :CONFIGURATIONCHECK
) ELSE (
    echo "Post-install actions didn't succeed. Goto INSTALL." >> C:\Temp\logfile.log
    GOTO :INSTALL
)

:CONFIGURATIONCHECK
REG QUERY "HKLM\SOFTWARE\Wow6432Node\InMage Systems\Installed Products\5" /v "AgentConfigurationStatus" | Find
"Succeeded"
If %ERRORLEVEL% EQU 0 (
    echo "Configuration has succeeded. Goto UPGRADE." >> C:\Temp\logfile.log
    GOTO :UPGRADE
) ELSE (
    echo "Configuration didn't succeed. Goto CONFIGURE." >> C:\Temp\logfile.log
    GOTO :CONFIGURE
)

:INSTALL
echo "Perform installation." >> C:\Temp\logfile.log
UnifiedAgent.exe /Role MS /InstallLocation "C:\Program Files (x86)\Microsoft Azure Site Recovery" /Platform
"VmWare" /Silent
IF %ERRORLEVEL% EQU 0 (
    echo "Installation has succeeded." >> C:\Temp\logfile.log
    (GOTO :CONFIGURE)
) ELSE (
    echo "Installation has failed." >> C:\Temp\logfile.log
    GOTO :ENDSCRIPT
)

```

```

:CONFIGURE
echo "Perform configuration." >> C:\Temp\logfile.log
cd "C:\Program Files (x86)\Microsoft Azure Site Recovery\agent"
UnifiedAgentConfigurator.exe /CSEndPoint "[CSIP]" /PassphraseFilePath %Temp%\MobSvc\MobSvc.passphrase
IF %ERRORLEVEL% EQU 0 (
    echo "Configuration has succeeded." >> C:\Temp\logfile.log
) ELSE (
    echo "Configuration has failed." >> C:\Temp\logfile.log
)
GOTO :ENDSCRIPT

:UPGRADE
echo "Perform upgrade." >> C:\Temp\logfile.log
UnifiedAgent.exe /Platform "VmWare" /Silent
IF %ERRORLEVEL% EQU 0 (
    echo "Upgrade has succeeded." >> C:\Temp\logfile.log
) ELSE (
    echo "Upgrade has failed." >> C:\Temp\logfile.log
)
GOTO :ENDSCRIPT

:ENDSCRIPT
echo "End of script." >> C:\Temp\logfile.log

```

Copy code to the Linux folder

Copy the following code:

- Save the code in the *MobSvcLinux* folder as *install_linux.sh*.
- Replace the `[CSIP]` placeholders in this script with the actual values of the IP address of your configuration server.
- The script supports new installations of the Mobility Service agent, and updates to agents that are already installed.

```

#!/usr/bin/env bash

rm -rf /tmp/MobSvc
mkdir -p /tmp/MobSvc
INSTALL_DIR='/usr/local/ASR'
VX_VERSION_FILE='/usr/local/.vx_version'

echo "======" >> /tmp/MobSvc/sccm.log
echo `date` >> /tmp/MobSvc/sccm.log
echo "======" >> /tmp/MobSvc/sccm.log

if [ -f /etc/oracle-release ] && [ -f /etc/redhat-release ]; then
    if grep -q 'Oracle Linux Server release 6.*' /etc/oracle-release; then
        if uname -a | grep -q x86_64; then
            OS="OL6-64"
            echo $OS >> /tmp/MobSvc/sccm.log
            cp *OL6*.tar.gz /tmp/MobSvc
        fi
    fi
elif [ -f /etc/redhat-release ]; then
    if grep -q 'Red Hat Enterprise Linux Server release 6.* (Santiago)' /etc/redhat-release || \
       grep -q 'CentOS Linux release 6.* (Final)' /etc/redhat-release || \
       grep -q 'CentOS release 6.* (Final)' /etc/redhat-release; then
        if uname -a | grep -q x86_64; then
            OS="RHEL6-64"
            echo $OS >> /tmp/MobSvc/sccm.log
            cp *RHEL6*.tar.gz /tmp/MobSvc
        fi
    elif grep -q 'Red Hat Enterprise Linux Server release 7.* (Maipo)' /etc/redhat-release || \
          grep -q 'CentOS Linux release 7.* (Core)' /etc/redhat-release; then
        if uname -a | grep -q x86_64; then
            -- -----

```

```

OS="RHEL7-64"
echo $OS >> /tmp/MobSvc/sccm.log
cp *RHEL7*.tar.gz /tmp/MobSvc
fi
fi
elif [ -f /etc/SuSE-release ] && grep -q 'VERSION = 11' /etc/SuSE-release; then
if grep -q "SUSE Linux Enterprise Server 11" /etc/SuSE-release && grep -q 'PATCHLEVEL = 3' /etc/SuSE-
release; then
if uname -a | grep -q x86_64; then
OS="SLES11-SP3-64"
echo $OS >> /tmp/MobSvc/sccm.log
cp *SLES11-SP3*.tar.gz /tmp/MobSvc
fi
fi
elif grep -q "SUSE Linux Enterprise Server 11" /etc/SuSE-release && grep -q 'PATCHLEVEL = 4' /etc/SuSE-
release; then
if uname -a | grep -q x86_64; then
OS="SLES11-SP4-64"
echo $OS >> /tmp/MobSvc/sccm.log
cp *SLES11-SP4*.tar.gz /tmp/MobSvc
fi
fi
fi
elif [ -f /etc/lsb-release ] ; then
if grep -q 'DISTRIB_RELEASE=14.04' /etc/lsb-release ; then
if uname -a | grep -q x86_64; then
OS="UBUNTU-14.04-64"
echo $OS >> /tmp/MobSvc/sccm.log
cp *UBUNTU-14*.tar.gz /tmp/MobSvc
fi
fi
else
exit 1
fi

if [ -z "$OS" ]; then
exit 1
fi

Install()
{
echo "Perform Installation." >> /tmp/MobSvc/sccm.log
./install -q -d ${INSTALL_DIR} -r MS -v VmWare
RET_VAL=$?
echo "Installation Returncode: $RET_VAL" >> /tmp/MobSvc/sccm.log
if [ $RET_VAL -eq 0 ]; then
echo "Installation has succeeded. Proceed to configuration." >> /tmp/MobSvc/sccm.log
Configure
else
echo "Installation has failed." >> /tmp/MobSvc/sccm.log
exit $RET_VAL
fi
}

Configure()
{
echo "Perform configuration." >> /tmp/MobSvc/sccm.log
${INSTALL_DIR}/Vx/bin/UnifiedAgentConfigurator.sh -i [CSIP] -P MobSvc.passphrase
RET_VAL=$?
echo "Configuration Returncode: $RET_VAL" >> /tmp/MobSvc/sccm.log
if [ $RET_VAL -eq 0 ]; then
echo "Configuration has succeeded." >> /tmp/MobSvc/sccm.log
else
echo "Configuration has failed." >> /tmp/MobSvc/sccm.log
exit $RET_VAL
fi
}

Upgrade()
{
echo "Perform Upgrade." >> /tmp/MobSvc/sccm.log

```

```

./install -q -v VmWare
RET_VAL=$?
echo "Upgrade Returncode: $RET_VAL" >> /tmp/MobSvc/sccm.log
if [ $RET_VAL -eq 0 ]; then
    echo "Upgrade has succeeded." >> /tmp/MobSvc/sccm.log
else
    echo "Upgrade has failed." >> /tmp/MobSvc/sccm.log
    exit $RET_VAL
fi
}

cp MobSvc.passphrase /tmp/MobSvc
cd /tmp/MobSvc

tar -zxvf *.tar.gz

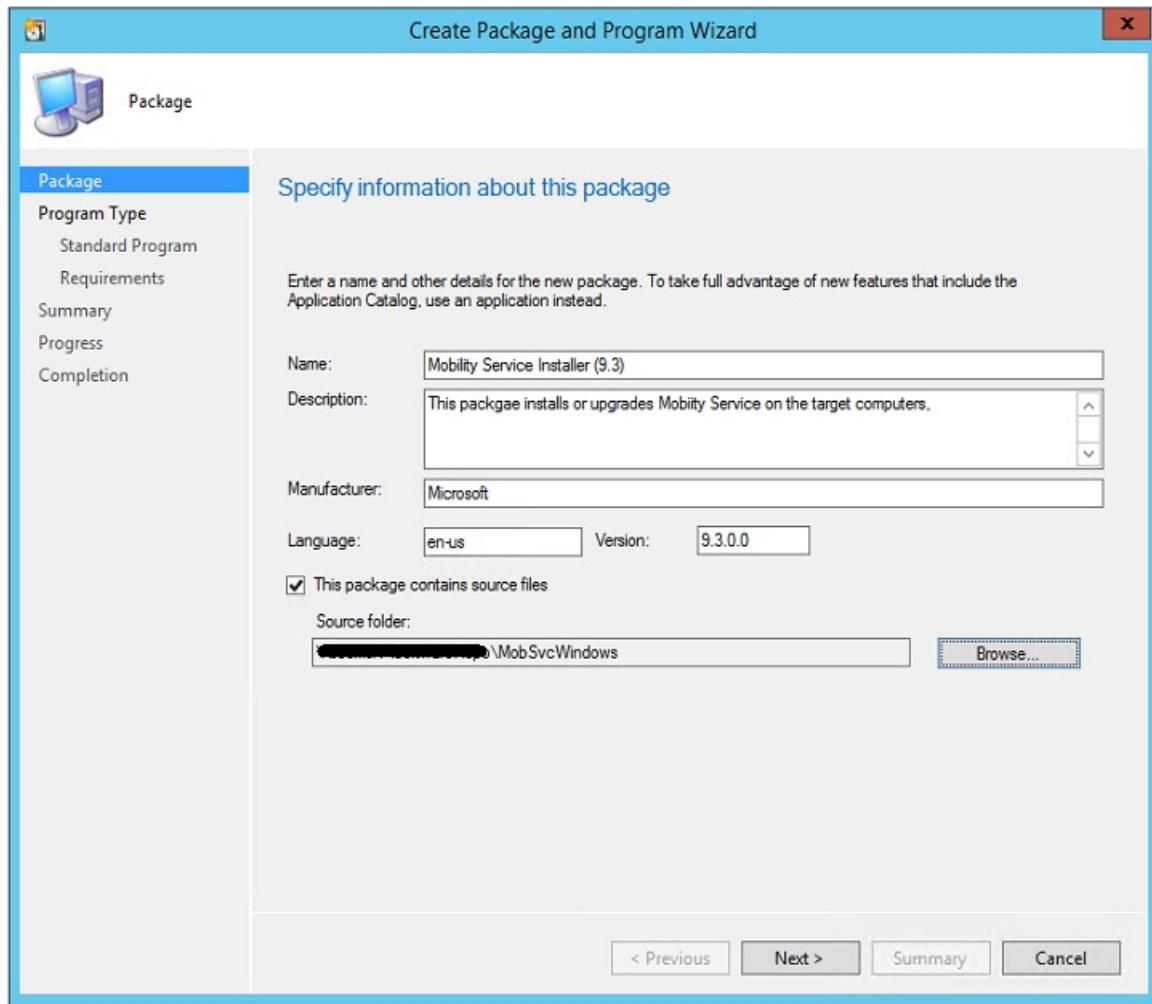
if [ -e ${VX_VERSION_FILE} ]; then
    echo "${VX_VERSION_FILE} exists. Checking for configuration status." >> /tmp/MobSvc/sccm.log
    agent_configuration=$(grep ^AGENT_CONFIGURATION_STATUS "${VX_VERSION_FILE}" | cut -d "=" -f2 | tr -d " ")
    echo "agent_configuration=$agent_configuration" >> /tmp/MobSvc/sccm.log
    if [ "$agent_configuration" == "Succeeded" ]; then
        echo "Agent is already configured. Proceed to Upgrade." >> /tmp/MobSvc/sccm.log
        Upgrade
    else
        echo "Agent is not configured. Proceed to Configure." >> /tmp/MobSvc/sccm.log
        Configure
    fi
else
    Install
fi

cd /tmp

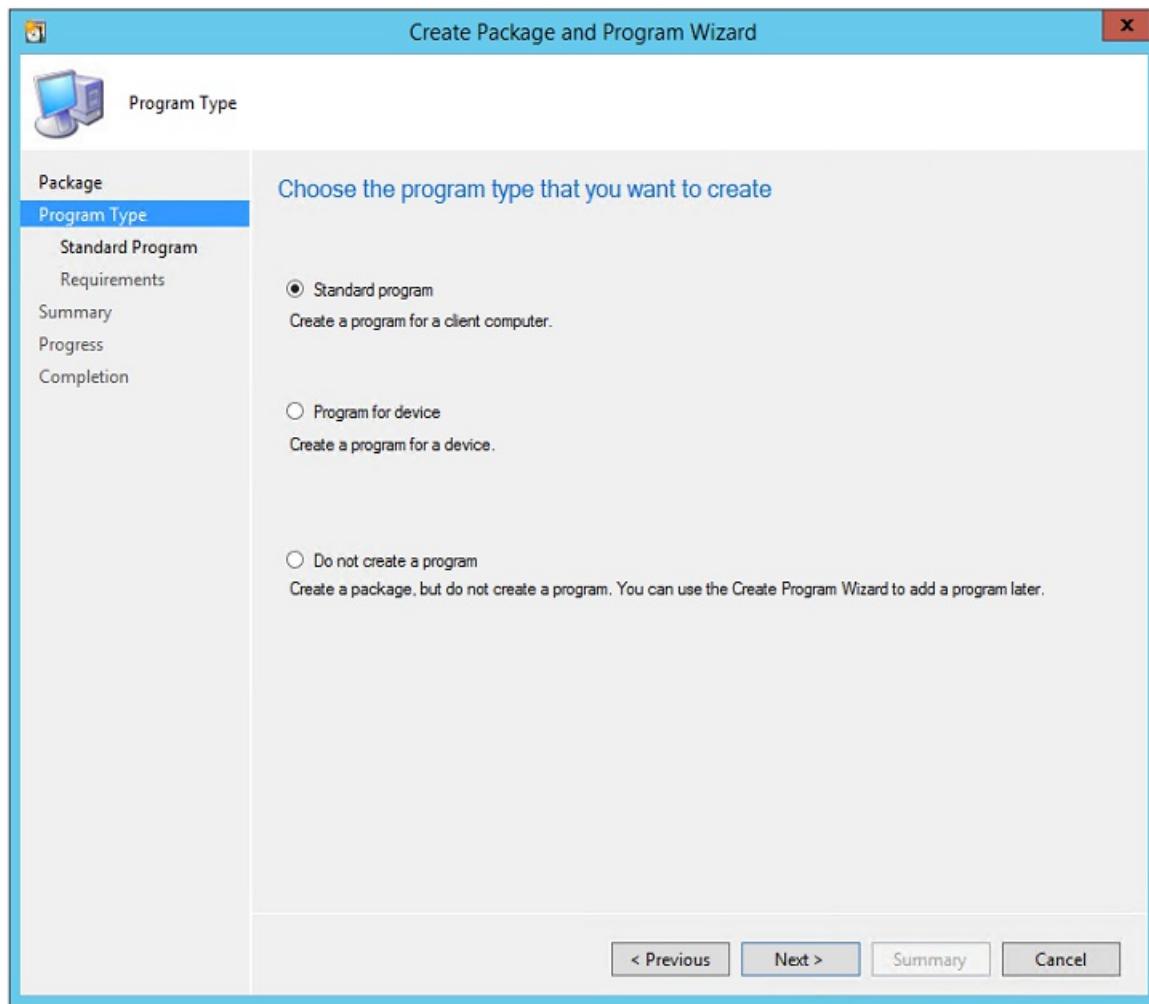
```

Create a package

1. Sign in to the Configuration Manager console and go to **Software Library > Application Management > Packages.**
2. Right-click **Packages > Create Package.**
3. Provide package details including a name, description, manufacturer, language, and version.
4. Select **This package contains source files.**
5. Click **Browse**, and select the network share and folder that contains the relevant installer (*MobSvcWindows* or *MobSvcLinux*). Then, select **Next**.

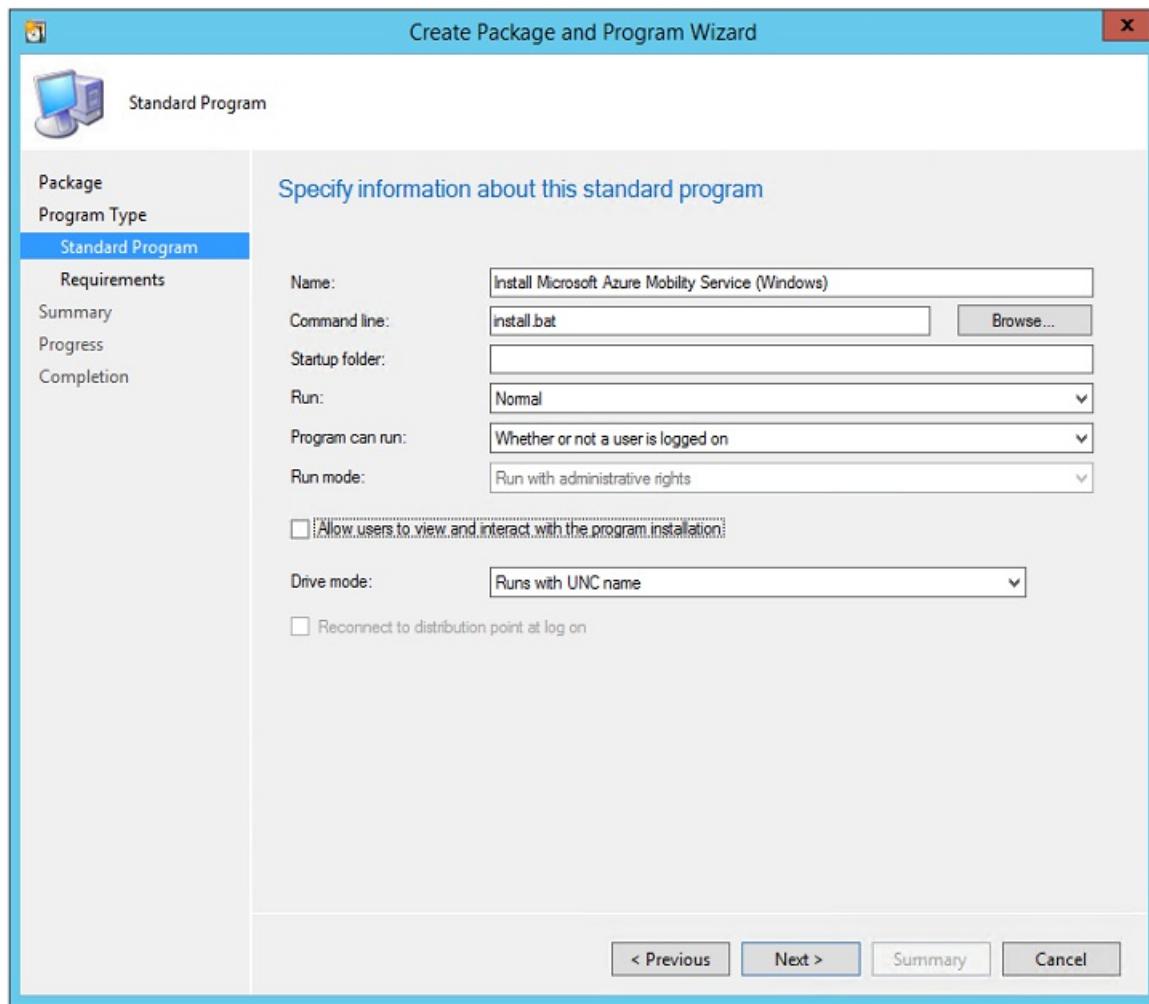


6. In **Choose the program type that you want to create** page, select **Standard Program > Next**.



7. In **Specify information about this standard program** page, specify the following values:

PARAMETER	WINDOWS VALUE	LINUX VALUE
Name	Install Microsoft Azure Mobility Service (Windows)	Install Microsoft Azure Mobility Service (Linux).
Command line	install.bat	./install_linux.sh
Program can run	Whether or not a user is logged on	Whether or not a user is logged on
Other parameters	Use default setting	Use default setting



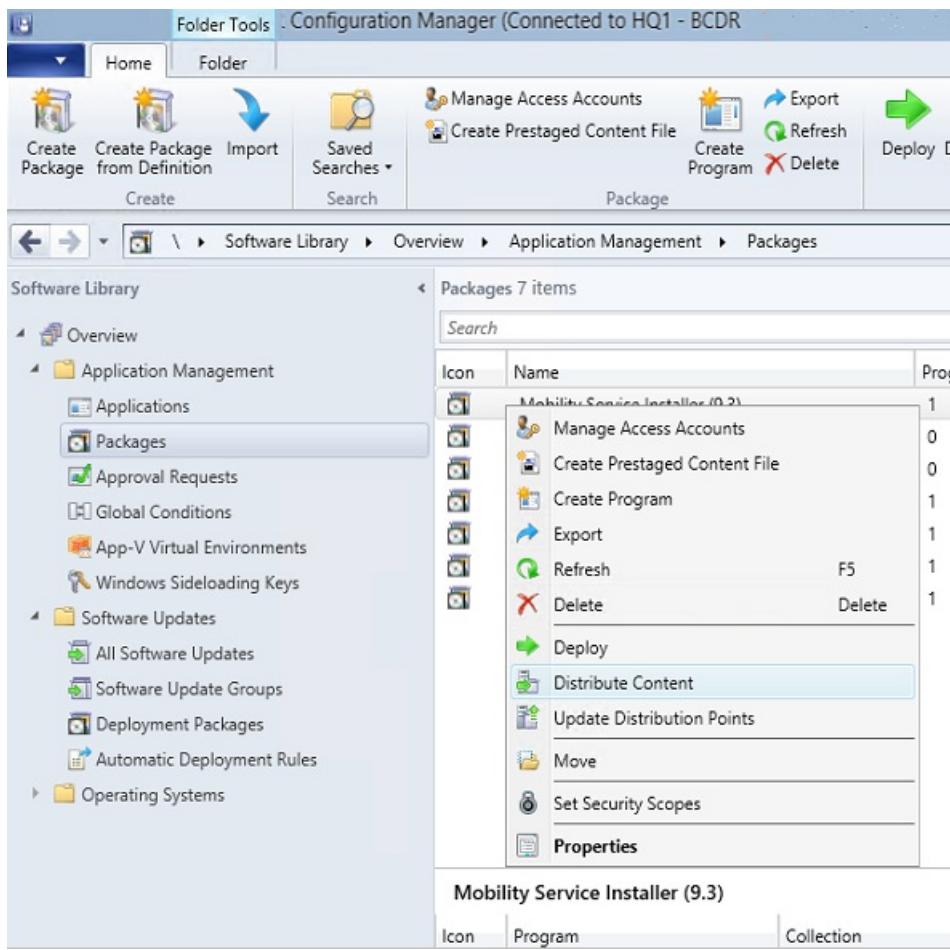
8. In **Specify the requirements for this standard program**, do the following tasks:

- For Windows machines, select **This program can run only on specified platforms**. Then, select the [supported Windows operating systems](#) and select **Next**.
- For Linux machines, select **This program can run on any platform**. Then select **Next**.

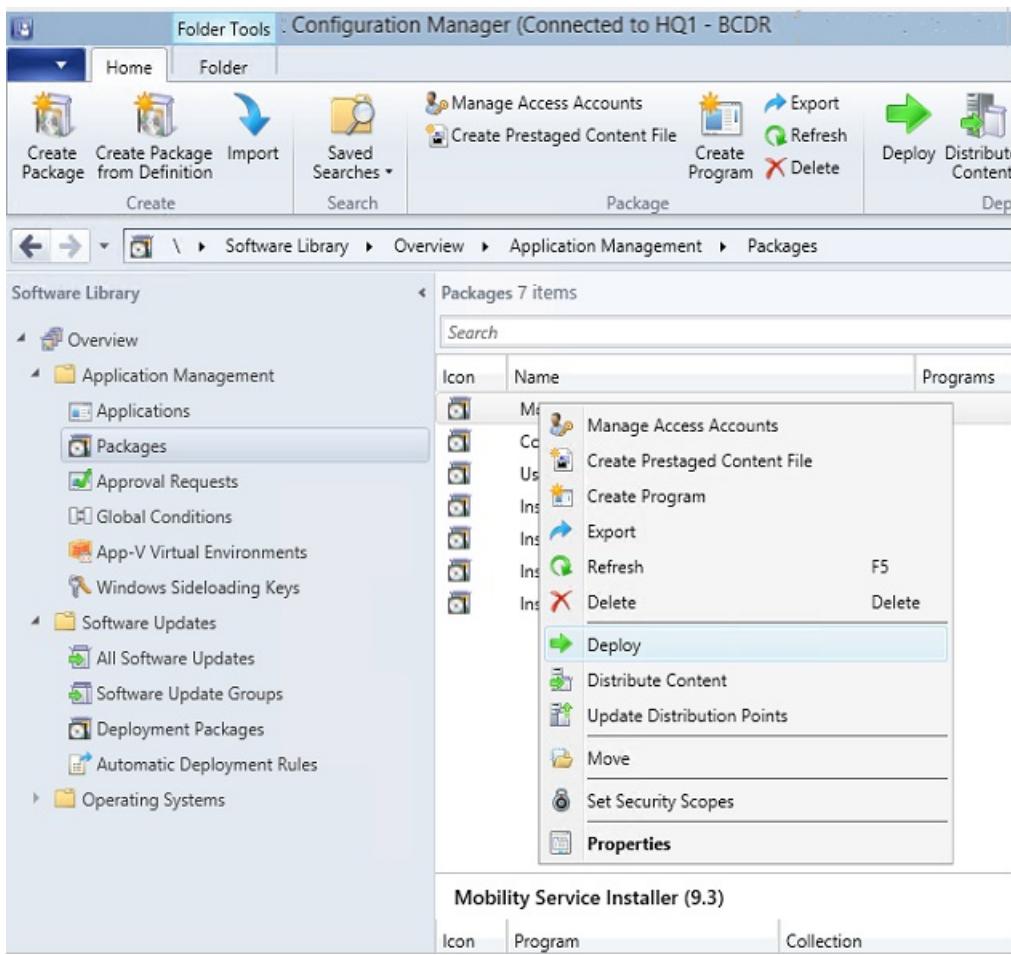
9. Finish the wizard.

Deploy the package

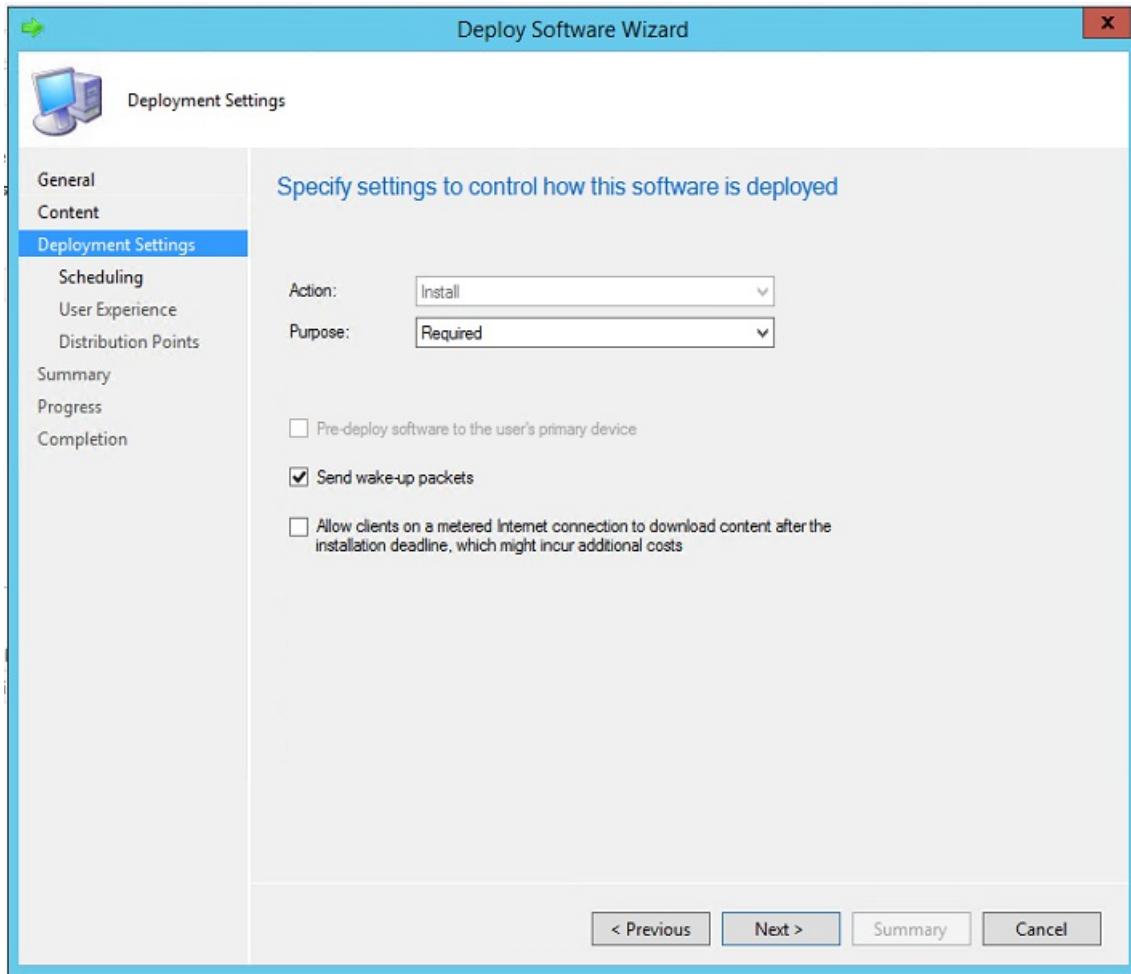
1. In the Configuration Manager console, right-click the package and select **Distribute Content**.



2. Select the distribution points on to which the packages should be copied. [Learn more](#).
3. Complete the wizard. The package then starts replicating to the specified distribution points.
4. After the package distribution finishes, right-click the package > **Deploy**.



5. Select the Windows or Linux device collection you created previously.
6. On the **Specify the content destination** page, select **Distribution Points**.
7. In **Specify settings to control how this software is deployed** page, set **Purpose** to **Required**.



8. In **Specify the schedule for this deployment**, set up a schedule. [Learn more](#).

- The Mobility Service is installed in accordance with the schedule you specify.
- To avoid unnecessary reboots, schedule the package installation during your monthly maintenance window or software updates window.

9. On the **Distribution Points** page, configure settings and finish the wizard.

10. Monitor deployment progress in the Configuration Manager console. Go to **Monitoring > Deployments > <your package name>**.

Uninstall the Mobility Service

You can create Configuration Manager packages to uninstall the Mobility Service. For example, the following script uninstalls the Mobility Service:

```
Time /t >> C:\logfile.log
REM =====
REM === Check if Mob Svc is already installed =====
REM === If not installed no operation required =====
REM === Else run uninstall command =====
REM === {275197FC-14FD-4560-A5EB-38217F80CBD1} is ===
REM === guid for Mob Svc Installer =====
whoami >> C:\logfile.log
NET START | FIND "InMage Scout Application Service"
IF %ERRORLEVEL% EQU 1 (GOTO :INSTALL) ELSE GOTO :UNINSTALL
:NOOPERATION
    echo "No Operation Required." >> c:\logfile.log
    GOTO :ENDSCRIPT
:UNINSTALL
    echo "Uninstall" >> C:\logfile.log
    MsiExec.exe /qn /x {275197FC-14FD-4560-A5EB-38217F80CBD1} /L+*V
"C:\ProgramData\ASRSetupLogs\UnifiedAgentMSIUninstall.log"
:ENDSCRIPT
```

Next steps

[Enable replication for VMs.](#)

Enable replication to Azure for VMware VMs

12/26/2019 • 8 minutes to read • [Edit Online](#)

This article describes how to enable replication of on-premises VMware VMs to Azure.

Resolve common issues

- Each disk should be smaller than 4 TB.
- The OS disk should be a basic disk, not a dynamic disk.
- For generation 2/UEFI-enabled virtual machines, the operating system family should be Windows, and the boot disk should be smaller than 300 GB.

Prerequisites

This article assumes that you have:

- [Set up your on-premises source environment](#).
- [Set up your target environment in Azure](#).
- [Verify requirements and prerequisites](#) before you start. Important things to note include:
 - [Supported operating systems](#) for replicated machines.
 - [Storage/disk support](#).
 - [Azure requirements](#) with which on-premises machines should comply.

Before you start

When you're replicating VMware virtual machines, keep this information in mind:

- Your Azure user account needs to have certain [permissions](#) to enable replication of a new virtual machine to Azure.
- VMware VMs are discovered every 15 minutes. It can take 15 minutes or longer for VMs to appear in the Azure portal after discovery. Likewise, discovery can take 15 minutes or longer when you add a new vCenter server or vSphere host.
- It can take 15 minutes or longer for environment changes on the virtual machine (such as VMware tools installation) to be updated in the portal.
- You can check the last-discovered time for VMware VMs: See the **Last Contact At** field on the [Configuration Servers](#) page for the vCenter server/vSphere host.
- To add virtual machines for replication without waiting for the scheduled discovery, highlight the configuration server (but don't click it), and select **Refresh**.
- When you enable replication, if the virtual machine is prepared, the process server automatically installs the Azure Site Recovery Mobility service on it.

Enable replication

Before you follow the steps in this section, note the following information:

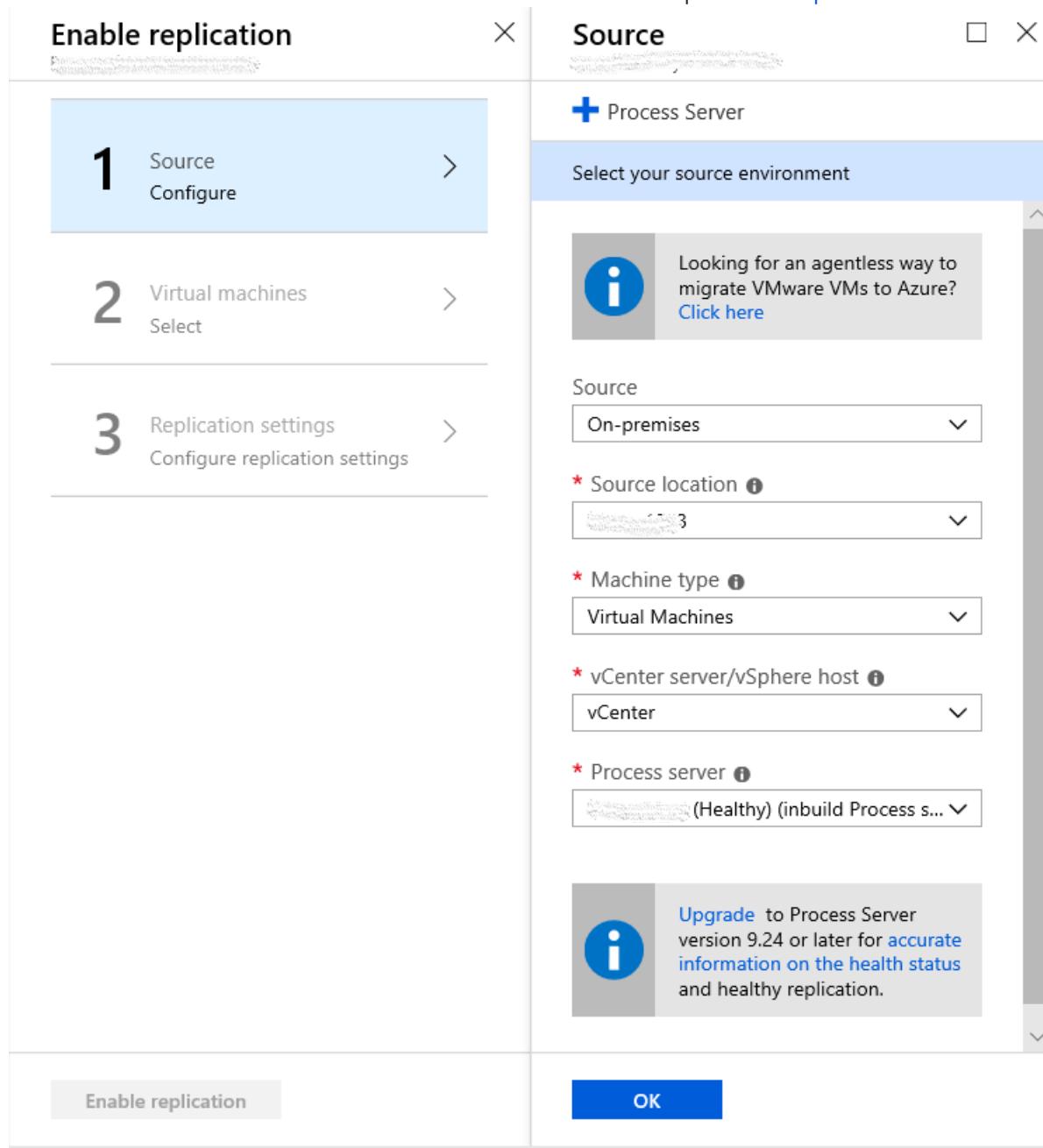
- Azure Site Recovery now replicates directly to managed disks for all new replications. The process server writes replication logs to a cache storage account in the target region. These logs are used to create recovery points in replica managed disks that have naming convention of `asrseeddisk`.
- Powershell support for replicating to managed disks is available from [Az.RecoveryServices module version](#)

2.0.0 onwards

- At the time of failover, the recovery point that you select is used to create the target-managed disk.
- VMs that were previously configured to replicate to target storage accounts aren't affected.
- Replication to storage accounts for a new virtual machine is only available via a Representational State Transfer (REST) API and Powershell. Use Azure REST API version 2016-08-10 or 2018-01-10 for replicating to storage accounts.

Please follow below steps to Enable Replication:

1. Go to **Step 2: Replicate application > Source**. After you enable replication for the first time, select **+Replicate** in the vault to enable replication for additional virtual machines.
2. In the **Source** page > **Source**, select the configuration server.
3. For **Machine type**, select **Virtual Machines** or **Physical Machines**.
4. In **vCenter/vSphere Hypervisor**, select the vCenter server that manages the vSphere host, or select the host. This setting isn't relevant if you're replicating physical computers.
5. Select the process server. If there are no additional process servers created, inbuilt process server of configuration server will be available in the dropdown. Health status of each process server is indicated as per recommended limits and other parameters. Choose a healthy process server. A **critical** process server cannot be chosen. You can either [troubleshoot and resolve](#) the errors **or** set up a scale-out process server.

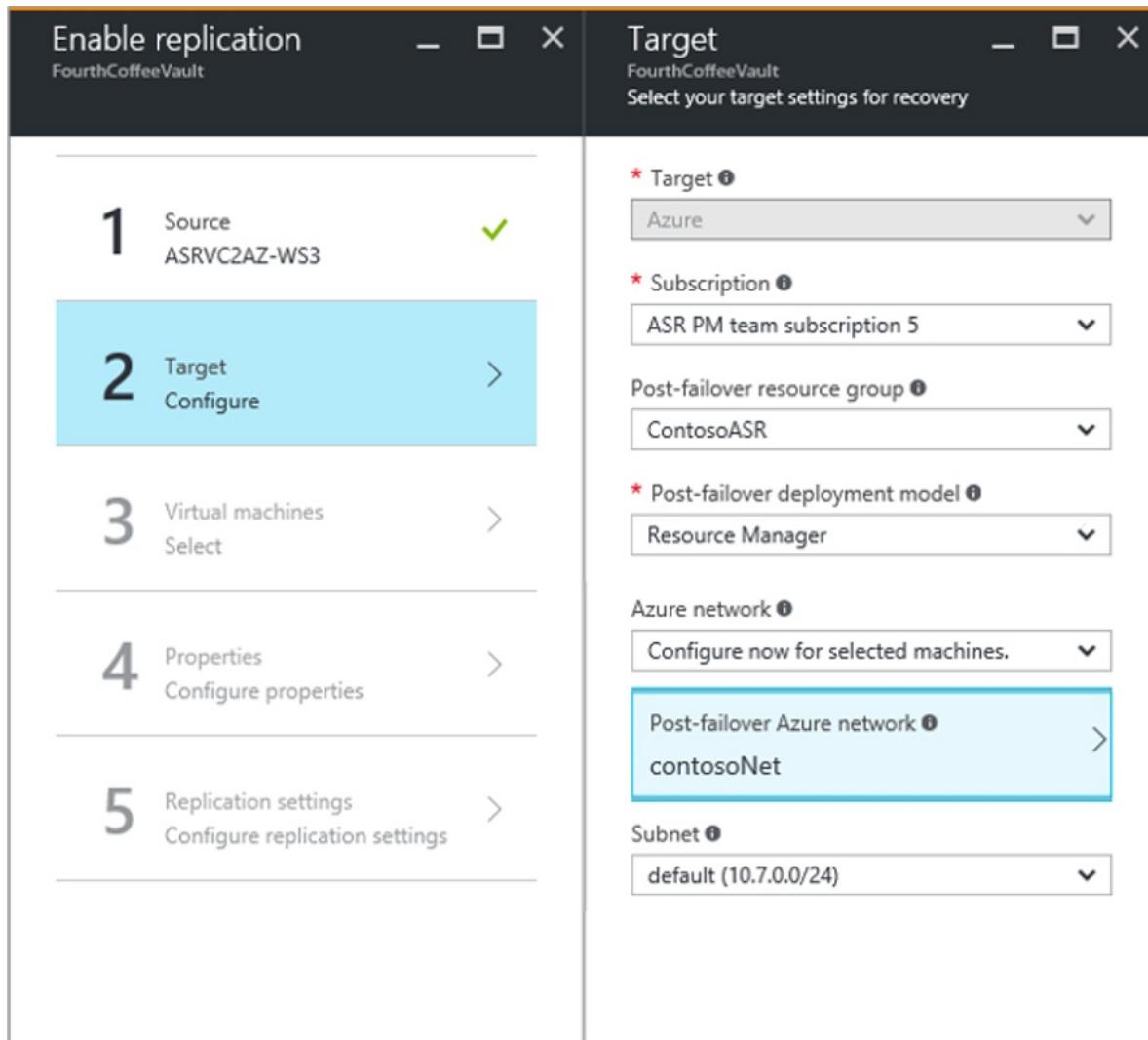


NOTE

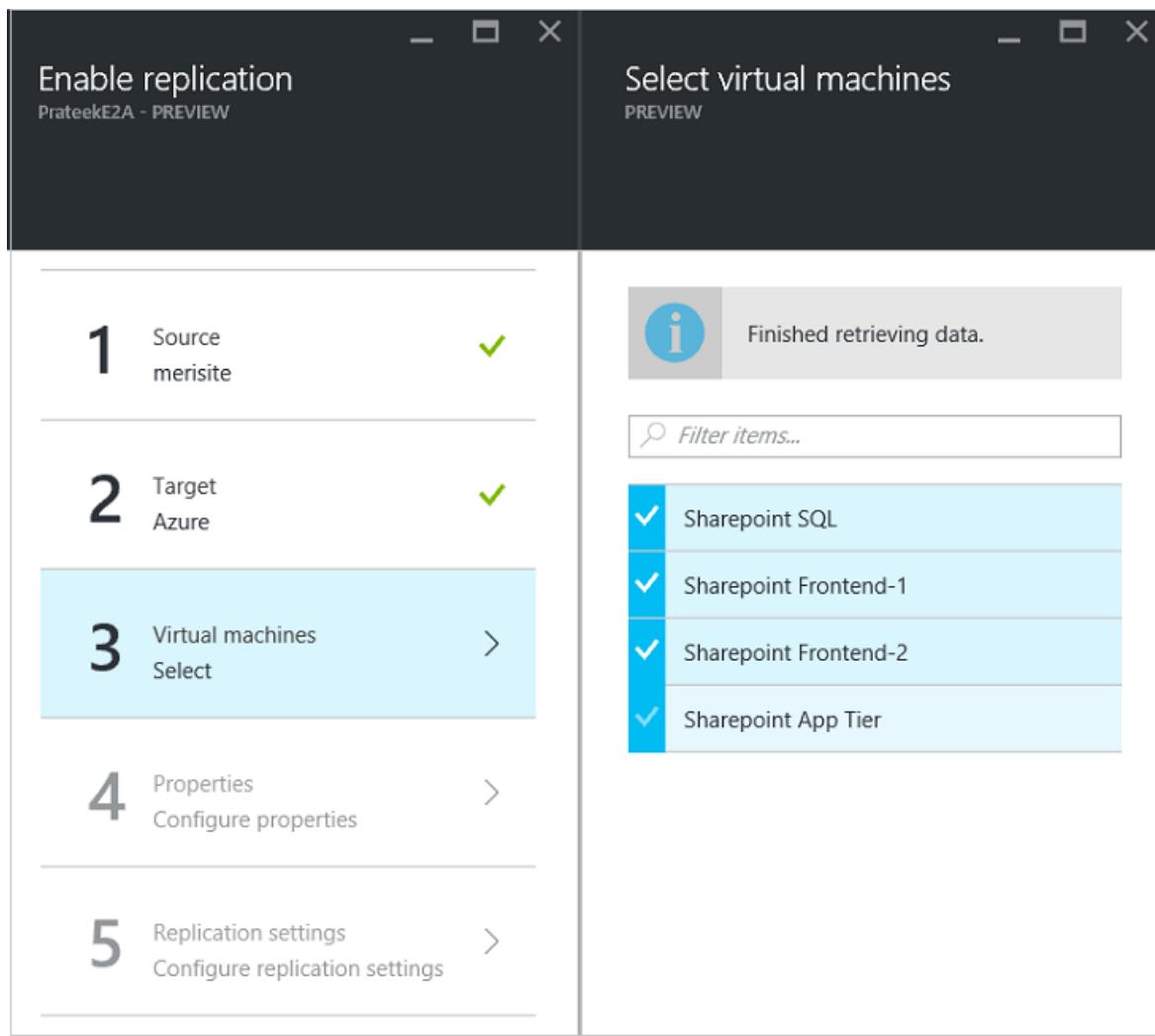
From [9.24 versions](#), additional alerts are introduced to enhance the health alerts of process server. Upgrade Site Recovery components to 9.24 versions or above for all alerts to be generated.

6. For **Target**, select the subscription and resource group where you want to create the failed-over virtual machines. Choose the deployment model that you want to use in Azure for the failed-over VMs.
7. Select the Azure network and subnet that the Azure VMs will connect to after failover. The network must be in the same region as the Site Recovery service vault.

Select **Configure now for selected machines** to apply the network setting to all virtual machines that you select for protection. Select **Configure later** to select the Azure network per virtual machine. If you don't have a network, you need to create one. To create a network by using Azure Resource Manager, select **Create new**. Select a subnet if applicable, and then select **OK**.



8. For **Virtual machines > Select virtual machines**, select each virtual machine that you want to replicate. You can only select virtual machines for which replication can be enabled. Then select **OK**. If you can't see or select any particular virtual machine, see [Source machine isn't listed in the Azure portal](#) to resolve the issue.



9. For **Properties > Configure properties**, select the account that the process server uses to automatically install the Site Recovery Mobility service on the virtual machine. Also, choose the type of target managed disk to replicate to based on your data churn patterns.
10. By default, all the disks of a source virtual machine are replicated. To exclude disks from replication, clear the **Include** check box for any disks that you don't want to replicate. Then select **OK**. You can set additional properties later. Learn more about [excluding disks](#).

Enable replication		Configure properties
wcvusvault		
1	Source ANUTALLUCS	✓
2	Target Azure	✓
3	Virtual machines 3 Selected	✓
4	Properties Configure properties	>
5	Replication settings Configure replication settings	>

Note:

1. Select the user account with accurate credentials and has **administrator** privileges (for Windows) / a **root user** (for Linux) privileges to install mobility agent. The list contains user accounts added during configuration server setup. Click [here](#) to learn more on how to add / modify the accounts.

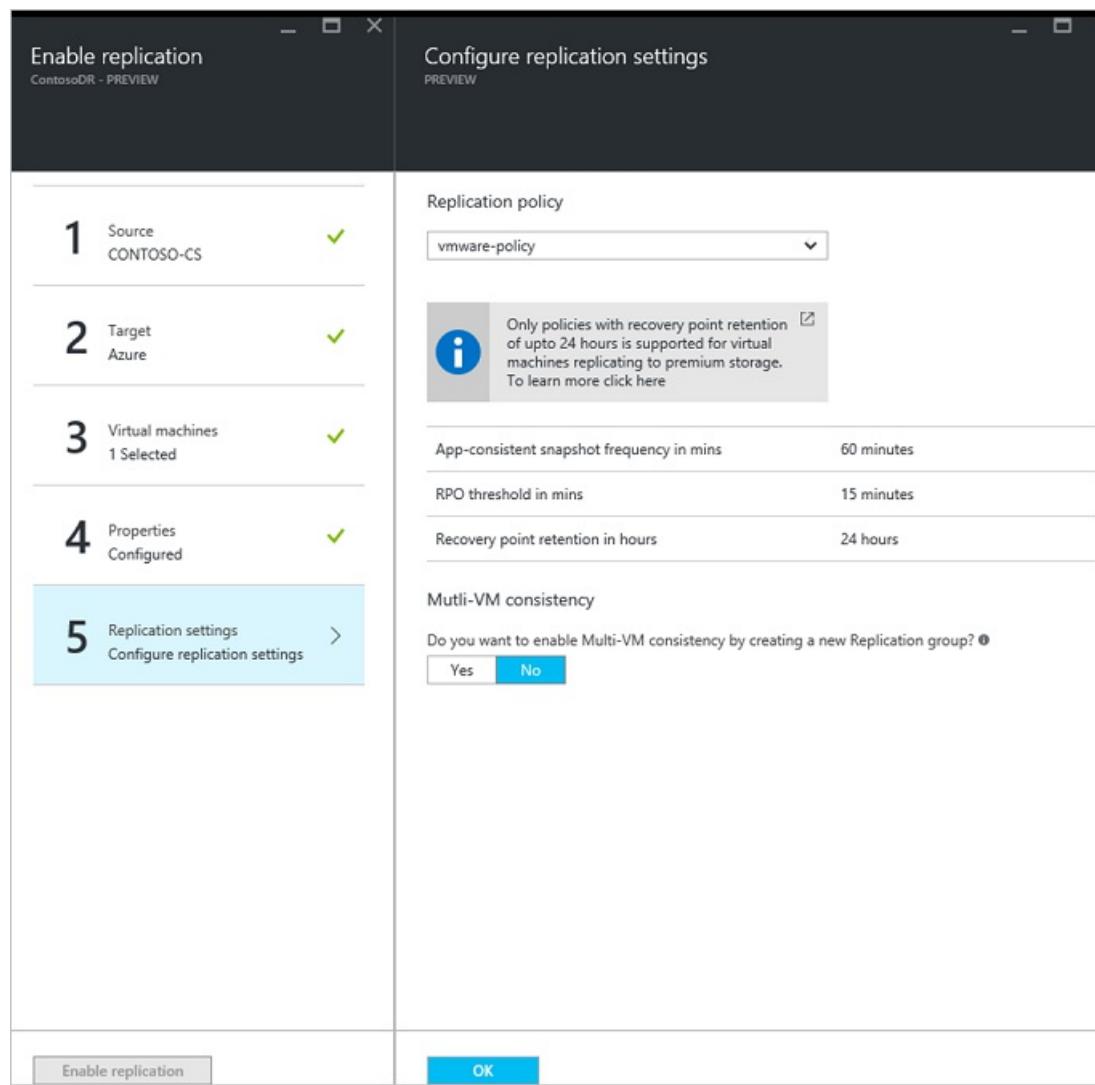
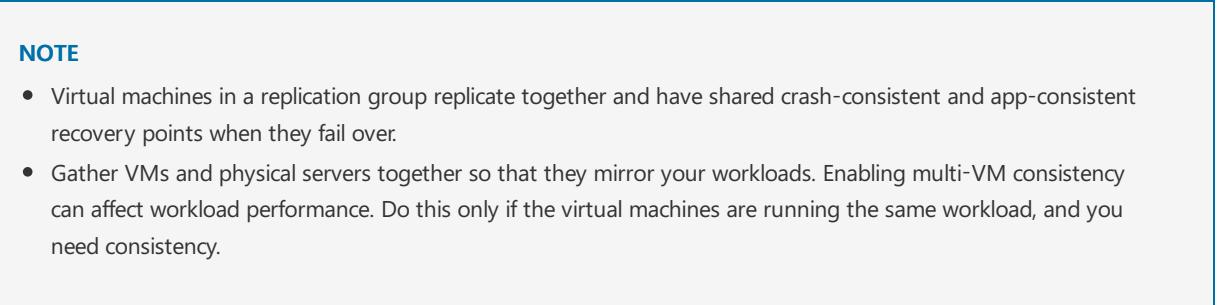
2. The user account selected as *Default user account* will be used to install mobility agent on all the VMs. To change the credentials of a specific VM, change the value in **USER ACCOUNT TO INSTALL MOBILITY SERVICE** field.

VM NAME	MANAGED DISK TY...	CACHE STORAGE A...	USER ACCOUNT TO...	DISKS TO REPLICATE	TARGET NAME
Default user account	Select	Select	Select	Need to select...	Fix per VM
asrdev-lin-12	3 disks	wtskrowcus...			asrdev-lin-12
/dev/sda(Basic) [30.00 GB, /dev...	Select			<input checked="" type="checkbox"/> Include	...
/dev/sdb(Basic) [2.00 GB,]	Select			<input checked="" type="checkbox"/> Include	...
/dev/sdc(Basic) [1.00 GB,]	Select			<input checked="" type="checkbox"/> Include	...
bsiva-W2K12R2	Select	wtskrowcus...	All disks		bsiva-W2K12R2

11. At **Replication settings > Configure replication settings**, verify that the correct replication policy is

selected. You can modify replication policy settings at **Settings > Replication policies > policy name > Edit Settings**. Changes that you apply to a policy also apply to replicating and new virtual machines.

12. Enable **Multi-VM consistency** if you want to gather virtual machines into a replication group. Specify a name for the group, and then select **OK**.



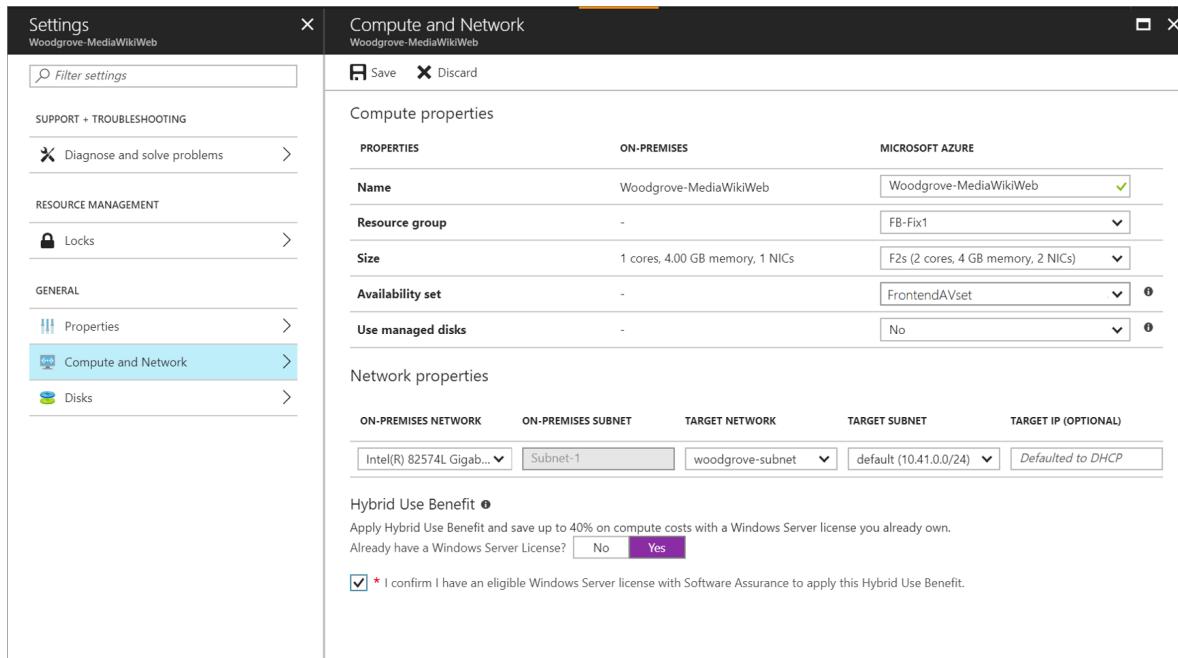
13. Select **Enable Replication**. You can track the progress of the **Enable Protection** job at **Settings > Jobs > Site Recovery Jobs**. After the **Finalize Protection** job runs, the virtual machine is ready for failover.

View and manage VM properties

Next, verify the properties of the source virtual machine. Remember that the Azure VM name needs to conform with [Azure virtual machine requirements](#).

1. Go to **Settings > Replicated items**, and then select the virtual machine. The **Essentials** page shows information about the VM's settings and status.
2. In **Properties**, you can view replication and failover information for the VM.

3. In **Compute and Network > Compute properties**, you can change multiple VM properties.



- Azure VM name: Modify the name to meet Azure requirements, if necessary.
- Target VM size or VM type: The default VM size is chosen based on a few parameters that include Disk count, NIC count, CPU core count, Memory and available VM role sizes in target Azure region. Azure Site Recovery picks the first available VM size which satisfies all the criteria. You can select a different VM size based on your needs at any time before failover. Note that VM disk size is also based on source disk size, and it can only be changed after failover. Learn more about disk sizes and IOPS rates at [Scalability and performance targets for VM disks on Windows](#).
- Resource group: You can select a [resource group](#), from which a virtual machine becomes a part of a post failover. You can change this setting at any time before failover. After failover, if you migrate the virtual machine to a different resource group, the protection settings for that virtual machine break.
- Availability set: You can select an [availability set](#) if your virtual machine needs to be a part of a post failover. When you select an availability set, keep the following information in mind:
 - Only availability sets that belong to the specified resource group are listed.
 - VMs that are on different virtual networks can't be a part of the same availability set.
 - Only virtual machines of the same size can be a part of an availability set.

4. You can also add information about the target network, subnet, and IP address that's assigned to the Azure VM.

5. In **Disks**, you can see the operating system and data disks on the VM that will be replicated.

Configure networks and IP addresses

You can set the target IP address. If you don't provide an address, the failed-over virtual machine uses DHCP. If you set an address that isn't available at failover, the failover doesn't work. If the address is available in the test failover network, you can use the same target IP address for test failover.

The number of network adapters is dictated by the size that you specify for the target virtual machine, as follows:

- If the number of network adapters on the source virtual machine is less than or equal to the number of adapters that are allowed for the target VM's size, the target has the same number of adapters as the source.
- If the number of adapters for the source virtual machine exceeds the number that's allowed for the target VM's size, the target size maximum is used. For example, if a source virtual machine has two network adapters and the target VM's size supports four, the target virtual machine has two adapters. If the source VM

has two adapters but the target size only supports one, the target VM has only one adapter.

- If the virtual machine has multiple network adapters, they all connect to the same network. Also, the first adapter that's shown in the list becomes the *default* network adapter in the Azure virtual machine.

Azure Hybrid Benefit

Microsoft Software Assurance customers can use Azure Hybrid Benefit to save on licensing costs for Windows Server computers that are migrated to Azure. The benefit also applies to Azure disaster recovery. If you're eligible, you can assign the benefit to the virtual machine that Site Recovery creates if there's a failover. To do that, follow these steps:

1. Go to the **Computer and Network properties** of the replicated virtual machine.
2. Answer when asked if you have a Windows Server license that makes you eligible for Azure Hybrid Benefit.
3. Confirm that you have an eligible Windows Server license with Software Assurance that you can use to apply the benefit to the VM that will be created at failover.
4. Save the settings for the replicated virtual machine.

Learn more about [Azure Hybrid Benefit](#).

Next steps

After the virtual machine reaches a protected state, try a [failover](#) to check whether your application appears in Azure.

- Learn how to [clean registration and protection settings](#) to disable replication.
- Learn how to [automate replication for your virtual machines by using Powershell](#).

Exclude disks from VMware VM replication to Azure

12/26/2019 • 2 minutes to read • [Edit Online](#)

This article describes how to exclude disks when replicating VMware VMs to Azure for disaster recovery. You might want to exclude disks from replication for a number of reasons:

- Ensure that unimportant data churned on the excluded disk doesn't get replicated.
- Optimize the consumed replication bandwidth, or the target-side resources, by excluding disks you don't need to replicate.
- Save storage and network resources by not replicating data you don't need.

Before you exclude disks from replication:

- [Learn more](#) about excluding disks.
- Review [typical exclude scenarios](#) and [examples](#) that show how excluding a disk affects replication, failover, and failback.

Before you start

Note the following before you start:

- **Replication:** By default, all disks on a machine are replicated.
- **Disk type:** Only basic disks can be excluded from replication. You can't exclude operating system or dynamic disks.
- **Mobility service:** To exclude a disk from replication, you must manually install the Mobility service on the machine before you enable replication. You can't use the push installation, since this method installs the Mobility service on a VM only after replication is enabled.
- **Add/remove/exclude disks:** After you enable replication, you can't add/remove/exclude disks for replication. If you want to add/remove or exclude disks, you need to disable protection for the machine and then enable it again.
- **Failover:** After failover, if failed over apps need excluded disks in order to work, you need to create those disks manually. Alternatively, you can integrate Azure automation into a recovery plan, to create the disk during failover of the machine.
- **Failback-Windows:** When you fail back to your on-premises site after failover, Windows disks that you create manually in Azure aren't failed back. For example, if you fail over three disks and create two disks directly on Azure VMs, only the three disks that were failed over will be failed back.
- **Failback-Linux:** For failback of Linux machines, disks that you create manually in Azure are failed back. For example, if you fail over three disks and create two disks directly on Azure VMs, all five will be failed back. You can't exclude disks that were created manually in the failback, or in reprotection of VMs.

Exclude disks from replication

1. When you [enable replication](#) for a VMware VM, after selecting the VMs that you want to replicate, in the **Enable replication > Properties > Configure properties** page, review the **Disks to Replicate** column. By default all disks are selected for replication.
2. If you don't want to replicate a specific disk, in **Disks to replicate** clear the selection for any disks you want to exclude.

VM NAME	MANAGED DISK TY...	CACHE STORAGE A...	USER ACCOUNT TO...	DISKS TO REPLICATE	TARGET NAME
Default user account	Select	Select	Select	Need to select ...	Fix per VM
▼ asrdev-lin-12	3 disks	wtskrowcus...			asrdev-lin-12
/dev/sda(Basic) [30.00 GB, /dev...	Select		<input checked="" type="checkbox"/> Include		...
/dev/sdb(Basic) [2.00 GB,]	Select		<input checked="" type="checkbox"/> Include		...
/dev/sdc(Basic) [1.00 GB,]	Select		<input checked="" type="checkbox"/> Include		...
bsiva-W2K12R2	Select	wtskrowcus...	All disks		bsiva-W2K12R2

Next steps

After your deployment is set up and running, [learn more](#) about different types of failover.

Set up VMware disaster recovery in a multi-tenancy environment with the Cloud Solution Provider (CSP) program

12/3/2018 • 4 minutes to read • [Edit Online](#)

The [CSP program](#) fosters better-together stories for Microsoft cloud services, including Office 365, Enterprise Mobility Suite, and Microsoft Azure. With CSP, partners own the end-to-end relationship with customers, and become the primary relationship contact point. Partners can deploy Azure subscriptions for customers, and combine the subscriptions with their own value-added, customized offerings.

With [Azure Site Recovery](#), as partners you can manage disaster recovery for customers directly through CSP. Alternately, you can use CSP to set up Site Recovery environments, and let customers manage their own disaster recovery needs in a self-service manner. In both scenarios, partners are the liaison between Site Recovery and their customers. Partners service the customer relationship, and bill customers for Site Recovery usage.

This article describes how you as a partner can create and manage tenant subscriptions through CSP, for a multi-tenant VMware replication scenario.

Prerequisites

To set up VMware replication, you need to do the following:

- [Prepare](#) Azure resources, including an Azure subscription, an Azure virtual network, and a storage account.
- [Prepare](#) on-premises VMware servers and VMs.
- For each tenant, create a separate management server that can communicate with the tenant VMs, and your vCenter servers. Only you as a partner should have access rights to this management server. Learn more about [multi-tenant environments](#).

Create a tenant account

1. Through [Microsoft Partner Center](#), sign in to your CSP account.
2. On the **Dashboard** menu, select **Customers**.
3. On the page that opens, click the **Add customer** button.
4. In **New Customer** page, fill in the account information details for the tenant.

The screenshot shows the Microsoft Partner Center 'New customer' setup page. On the left, there's a sidebar with 'New customer' and links for 'Account info', 'Subscriptions', 'Review', and 'Confirmation'. Below that is a 'Customers' link. The main area has sections for 'Account info', 'Company', and 'Primary contact'. Under 'Company', there's a 'Country/region' dropdown set to 'United States', a 'Company name' input field containing 'ASRTest', and a 'Primary domain name' input field showing 'asrtestaccount.onmicrosoft.com' with a green checkmark indicating it's available. There are also fields for 'Address line 1' ('1 Microsoft Way'), 'City' ('Redmond'), 'State/Province' ('Washington'), and 'ZIP/Postal code' ('98052'). Under 'Primary contact', there are fields for 'First name' ('ASR'), 'Last name' ('ASR'), 'Email address' ('asrtestaccount@xyz.com'), and 'Phone number' ('8123456789'). At the bottom, there are 'Next: Subscriptions' and 'Cancel' buttons.

5. Then click **Next: Subscriptions**.
6. On the subscriptions selection page, select **Microsoft Azure** check box. You can add other subscriptions now or at any other time.
7. On the **Review** page, confirm the tenant details, and then click **Submit**.
8. After you've created the tenant account, a confirmation page appears, displaying the details of the default account and the password for that subscription. Save the information, and change the password later as necessary, through the Azure portal sign-in page.

You can share this information with the tenant as is, or you can create and share a separate account if necessary.

Access the tenant account

You can access the tenant's subscription through the Microsoft Partner Center Dashboard.

1. On the **Customers** page, click the name of the tenant account.
2. In the **Subscriptions** page of the tenant account, you can monitor the existing account subscriptions and add more subscriptions, as required.
3. To manage the tenant's disaster-recovery operations, select **All resources (Azure portal)**. This grants you access to the tenant's Azure subscriptions.

ASRTest

Subscriptions

Customer insights

Users and licenses

Service management

Account

[← Customers](#)

Subscriptions

Add subscription

License-based subscriptions

This customer doesn't have any license-based subscriptions.

Usage-based subscriptions Report for 11/30/16 5:57 PM

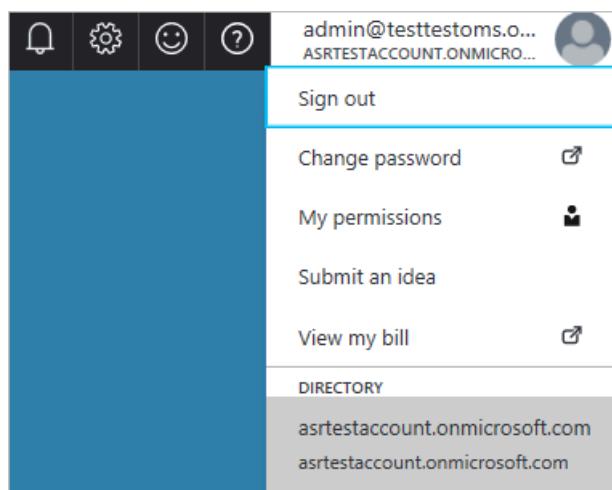
Current estimate Set a budget, and you'll be able to track the usage on the portal if your monthly spending will exceed it.
\$0.00 Apply

Billing period November 1 - November 30. There are 0 days left.

Subscription	Current estimate	% of total	Status
Microsoft Azure	\$0.00	0%	Active

All resources (Azure portal)

4. You can verify access by clicking the Azure Active Directory link on the top right of the Azure portal.



You can now perform and manage all Site Recovery operations for the tenant in the Azure portal. To access the tenant subscription through CSP for managed disaster recovery, follow the previously described process.

Assign tenant access to the subscription

1. Ensure that the disaster recovery infrastructure is set up. Partners access tenant subscriptions through the CSP portal, regardless of whether disaster recovery is managed or self-service. Set up the vault and register infrastructure to the tenant subscriptions.
2. Provide the tenant with the [account you created](#).
3. You can add a new user to the tenant subscription through the CSP portal as follows:
 - a) Go to the tenant's CSP subscription page, and then select the **Users and licenses** option.

- b) Now create a new user by entering the relevant details and selecting permissions, or by uploading the list of users in a CSV file.
- c) After you've created a new user, go back to the Azure portal. In the **Subscription** page, select the relevant subscription.
- d) Select **Access control (IAM)**, and then click **Role assignments**.
- e) Click **Add role assignment** to add a user with the relevant access level. The users that were created through the CSP portal are displayed on the Role assignments tab.

- For most management operations, the *Contributor* role is sufficient. Users with this access level can do everything on a subscription except change access levels (for which *Owner*-level access is required).
- Site Recovery also has three [predefined user roles](#), that can be used to further restrict access levels as required.

Multi-tenant environments

There are three major multi-tenant models:

- Shared Hosting Services Provider (HSP):** The partner owns the physical infrastructure, and uses shared resources (vCenter, datacenters, physical storage, and so on) to host multiple tenant VMs on the same

infrastructure. The partner can provide disaster-recovery management as a managed service, or the tenant can own disaster recovery as a self-service solution.

- **Dedicated Hosting Services Provider:** The partner owns the physical infrastructure, but uses dedicated resources (multiple vCenters, physical datastores, and so on) to host each tenant's VMs on a separate infrastructure. The partner can provide disaster-recovery management as a managed service, or the tenant can own it as a self-service solution.
- **Managed Services Provider (MSP):** The customer owns the physical infrastructure that hosts the VMs, and the partner provides disaster-recovery enablement and management.

By setting up tenant subscriptions as described in this article, you can quickly start enabling customers in any of the relevant multi-tenant models. You can learn more about the different multi-tenant models and enabling on-premises access controls [here](#).

Next steps

- Learn more about [role-based access control](#) to manage Azure Site Recovery deployments.
- Learn more about VMware to Azure [replication architecture](#).
- [Review the tutorial](#) for replicating VMware VMs to Azure. Learn more about [multi-tenant environments](#) for replicating VMware VMs to Azure.

Create and customize recovery plans

1/23/2020 • 4 minutes to read • [Edit Online](#)

This article describes how to create and customize a recovery plan for failover in [Azure Site Recovery](#). Before you start, [learn more](#) about recovery plans.

Create a recovery plan

1. In the Recovery Services vault, select **Recovery Plans (Site Recovery)** > **+Recovery Plan**.
2. In **Create recovery plan**, specify a name for the plan.
3. Choose a source and target based on the machines in the plan, and select **Resource Manager** for the deployment model. The source location must have machines that are enabled for failover and recovery.

FAILOVER	SOURCE	TARGET
Azure to Azure	Select the Azure region	Select the Azure region
VMware to Azure	Select the configuration server	Select Azure
Physical machines to Azure	Select the configuration server	Select Azure
Hyper-V to Azure	Select the Hyper-V site name	Select Azure
Hyper-V (managed by VMM) to Azure	Select the VMM server	Select Azure

Note the following:

- You can only use a recovery plan for failover from the source location to Azure. You can't use a recovery plan for failback from Azure.
 - The source location must have machines that are enabled for failover and recovery.
 - A recovery plan can contain machines with the same source and target.
 - You can include VMware VMs and Hyper-V VMs managed by VMM, in the same plan.
 - VMware VMs and physical servers can be in the same plan.
4. In **Select items virtual machines**, select the machines (or replication group) that you want to add to the plan. Then click **OK**.
 - Machines are added default group (Group 1) in the plan. After failover, all machines in this group start at the same time.
 - You can only select machines are in the source and target locations that you specified.
 5. Click **OK** to create the plan.

Add a group to a plan

You create additional groups, and add machines to different groups so that you can specify different behavior on a group-by-group basis. For example, you can specify when machines in a group should start after failover, or specify customized actions per group.

1. In **Recovery Plans**, right-click the plan > **Customize**. By default, after creating a plan all the machines you

added to it are located in default Group 1.

2. Click **+Group**. By default a new group is numbered in the order in which it's added. You can have up to seven groups.
3. Select the machine you want to move to the new group, click **Change group**, and then select the new group. Alternatively, right-click the group name > **Protected item**, and add machines to the group. A machine or replication group can only belong to one group in a recovery plan.

Add a script or manual action

You can customize a recovery plan by adding a script or manual action. Note that:

- If you're replicating to Azure you can integrate Azure automation runbooks into your recovery plan. [Learn more](#).
- If you're replicating Hyper-V VMs managed by System Center VMM, you can create a script on the on-premises VMM server, and include it in the recovery plan.
- When you add a script, it adds a new set of actions for the group. For example, a set of pre-steps for Group 1 is created with the name *Group 1: pre-steps*. All pre-steps are listed inside this set. You can add a script on the primary site only if you have a VMM server deployed.
- If you add a manual action, when the recovery plan runs, it stops at the point at which you inserted the manual action. A dialog box prompts you to specify that the manual action was completed.
- To create a script on the VMM server, follow the instructions in [this article](#).
- Scripts can be applied during failover to the secondary site, and during fallback from the secondary site to the primary. Support depends on your replication scenario:

SCENARIO	FAILOVER	FAILBACK
Azure to Azure	Runbook	Runbook
VMware to Azure	Runbook	NA
Hyper-V with VMM to Azure	Runbook	Script
Hyper-V site to Azure	Runbook	NA
VMM to secondary VMM	Script	Script

1. In the recovery plan, click the step to which the action should be added, and specify when the action should occur:
 - a. If you want the action to occur before the machines in the group are started after failover, select **Add pre-action**.
 - b. If you want the action to occur after the machines in the group start after failover, select **Add post action**. To move the position of the action, select the **Move Up** or **Move Down** buttons.
2. In **Insert action**, select **Script** or **Manual action**.
3. If you want to add a manual action, do the following:
 - a. Type in a name for the action, and type in action instructions. The person running the failover will see these instructions.
 - b. Specify whether you want to add the manual action for all types of failover (Test, Failover, Planned failover (if relevant)). Then click **OK**.
4. If you want to add a script, do the following:

- a. If you're adding a VMM script, select **Failover to VMM script**, and in **Script Path** type the relative path to the share. For example, if the share is located at \\<VMMServerName>\MSSCVMMLibrary\RPScripts, specify the path: \RPScripts\RPScript.ps1.
 - b. If you're adding an Azure automation run book, specify the **Azure Automation Account** in which the runbook is located, and select the appropriate **Azure Runbook Script**.
5. Run a test failover of the recovery plan to ensure that the script works as expected.

Watch a video

Watch a video that demonstrates how to build a recovery plan.

Next steps

Learn more about [running failovers](#).

Run a test failover (disaster recovery drill) to Azure

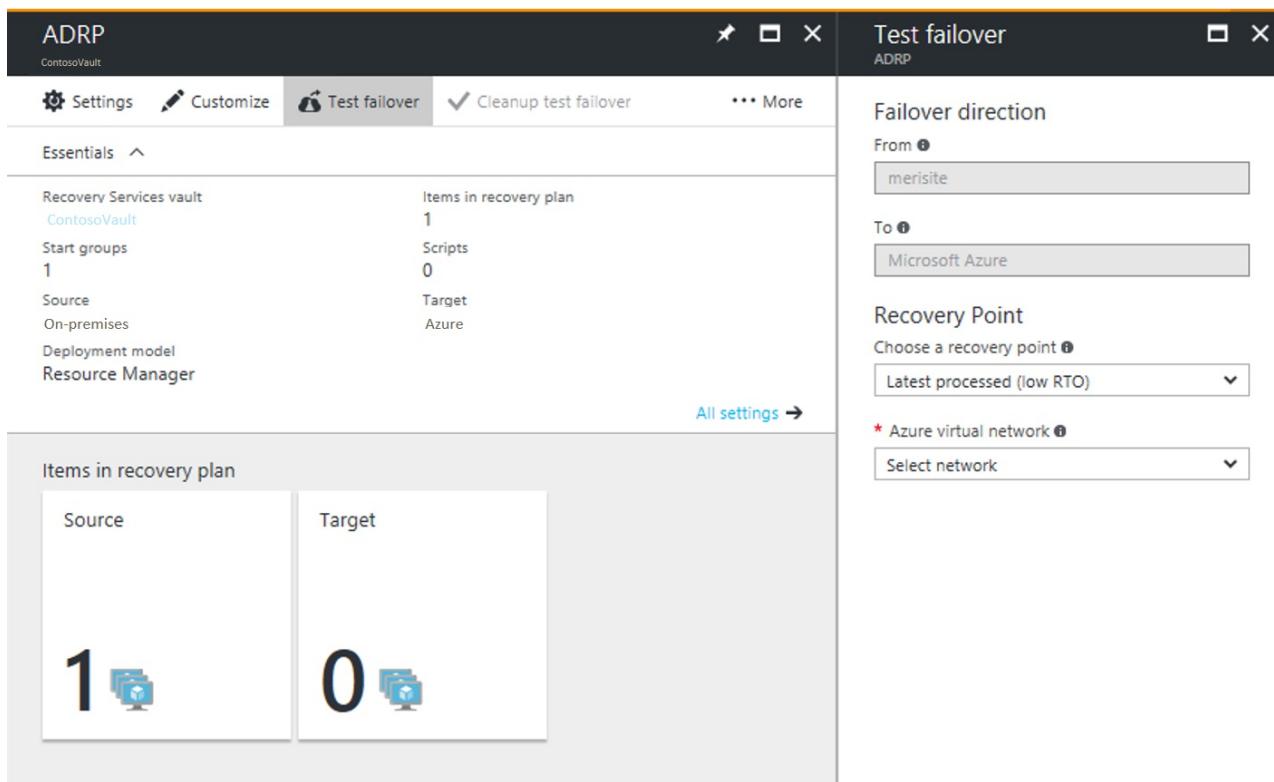
11/14/2019 • 7 minutes to read • [Edit Online](#)

This article describes how to run a disaster recovery drill to Azure, using a Site Recovery test failover.

You run a test failover to validate your replication and disaster recovery strategy, without any data loss or downtime. A test failover doesn't impact ongoing replication, or your production environment. You can run a test failover on a specific virtual machine (VM), or on a [recovery plan](#) containing multiple VMs.

Run a test failover

This procedure describes how to run a test failover for a recovery plan. If you want to run a test failover for a single VM, follow the steps described [here](#).



1. In Site Recovery in the Azure portal, click **Recovery Plans** > *recoveryplan_name* > **Test Failover**.
2. Select a **Recovery Point** to which to fail over. You can use one of the following options:
 - **Latest processed:** This option fails over all VMs in the plan to the latest recovery point processed by Site Recovery. To see the latest recovery point for a specific VM, check **Latest Recovery Points** in the VM settings. This option provides a low RTO (Recovery Time Objective), because no time is spent processing unprocessed data.
 - **Latest app-consistent:** This option fails over all the VMs in the plan to the latest application-consistent recovery point processed by Site Recovery. To see the latest recovery point for a specific VM, check **Latest Recovery Points** in the VM settings.
 - **Latest:** This option first processes all the data that has been sent to Site Recovery service, to create a recovery point for each VM before failing over to it. This option provides the lowest RPO (Recovery Point Objective), because the VM created after failover will have all the data replicated to Site Recovery when the failover was triggered.
 - **Latest multi-VM processed:** This option is available for recovery plans with one or more VMs that have

multi-VM consistency enabled. VMs with the setting enabled fail over to the latest common multi-VM consistent recovery point. Other VMs fail over to the latest processed recovery point.

- **Latest multi-VM app-consistent:** This option is available for recovery plans with one or more VMs that have multi-VM consistency enabled. VMs that are part of a replication group fail over to the latest common multi-VM application-consistent recovery point. Other VMs fail over to their latest application-consistent recovery point.
- **Custom:** Use this option to fail over a specific VM to a particular recovery point.

3. Select an Azure virtual network in which test VMs will be created.

- Site Recovery attempts to create test VMs in a subnet with the same name and same IP address as that provided in the **Compute and Network** settings of the VM.
 - If a subnet with the same name isn't available in the Azure virtual network used for test failover, then the test VM is created in the first subnet alphabetically.
 - If same IP address isn't available in the subnet, then the VM receives another available IP address in the subnet. [Learn more](#).
4. If you're failing over to Azure and data encryption is enabled, in **Encryption Key**, select the certificate that was issued when you enabled encryption during Provider installation. You can ignore this step if encryption isn't enabled.
5. Track failover progress on the **Jobs** tab. You should be able to see the test replica machine in the Azure portal.
6. To initiate an RDP connection to the Azure VM, you need to [add a public IP address](#) on the network interface of the failed over VM.
7. When everything is working as expected, click **Cleanup test failover**. This deletes the VMs that were created during test failover.
8. In **Notes**, record and save any observations associated with the test failover.

Job

NAME	STATUS	START TIME	DURATION	
Prerequisites check for the recovery plan	✔ Successful	5/3/2017 3:48:14 PM	00:00:04	...
Create the test environment	✔ Successful	5/3/2017 3:48:19 PM	00:00:01	...
▼ Recovery plan failover	✔ Successful	5/3/2017 3:48:20 PM	00:01:14	...
SQLServer	✔ Successful	5/3/2017 3:48:20 PM	00:01:14	...
▼ Group 1: Start (1)	✔ Successful	5/3/2017 3:49:35 PM	00:01:40	...
SQLServer	✔ Successful	5/3/2017 3:49:35 PM	00:01:40	...
Finalizing the recovery plan	✔ Successful	5/3/2017 3:51:16 PM	00:00:00	...

When a test failover is triggered, the following occurs:

1. **Prerequisites:** A prerequisites check runs to make sure that all conditions required for failover are met.
2. **Failover:** The failover processes and prepares the data, so that an Azure VM can be created from it.
3. **Latest:** If you have chosen the latest recovery point, a recovery point is created from the data that's been sent to the service.
4. **Start:** This step creates an Azure virtual machine using the data processed in the previous step.

Failover timing

In the following scenarios, failover requires an extra intermediate step that usually takes around 8 to 10 minutes to

complete:

- VMware VMs running a version of the Mobility service older than 9.8
- Physical servers
- VMware Linux VMs
- Hyper-V VM protected as physical servers
- VMware VM where the following drivers aren't boot drivers:
 - storvsc
 - vmbus
 - storflt
 - intelide
 - atapi
- VMware VM that don't have DHCP enabled, irrespective of whether they are using DHCP or static IP addresses.

In all the other cases, no intermediate step is not required, and failover takes significantly less time.

Create a network for test failover

We recommended that for test failover, you choose a network that's isolated from the production recovery site network specific in the **Compute and Network** settings for each VM. By default, when you create an Azure virtual network, it is isolated from other networks. The test network should mimic your production network:

- The test network should have same number of subnets as your production network. Subnets should have the same names.
- The test network should use the same IP address range.
- Update the DNS of the test network with the IP address specified for the DNS VM in **Compute and Network** settings. Read [test failover considerations for Active Directory](#) for more details.

Test failover to a production network in the recovery site

Although we recommended that you use a test network separate from your production network, if you do want to test a disaster recovery drill into your production network, note the following:

- Make sure that the primary VM is shut down when you run the test failover. Otherwise there will be two VMs with the same identity, running in the same network at the same time. This can lead to unexpected consequences.
- Any changes to VMs created for test failover are lost when you clean up the failover. These changes are not replicated back to the primary VM.
- Testing in your production environment leads to a downtime of your production application. Users shouldn't use apps running on VMs when the test failover is in progress.

Prepare Active Directory and DNS

To run a test failover for application testing, you need a copy of your production Active Directory environment in your test environment. Read [test failover considerations for Active Directory](#) to learn more.

Prepare to connect to Azure VMs after failover

If you want to connect to Azure VMs using RDP/SSH after failover, follow the requirements summarized in the table.

FAILOVER	LOCATION	ACTIONS
Azure VM running Windows	On-premises machine before failover	<p>To access the Azure VM over the internet, enable RDP, and make sure that TCP and UDP rules are added for Public, and that RDP is allowed for all profiles in Windows Firewall > Allowed Apps.</p> <p>To access the Azure VM over a site-to-site connection, enable RDP on the machine, and ensure that RDP is allowed in the Windows Firewall -> Allowed apps and features, for Domain and Private networks.</p> <p>Make sure the operating system SAN policy is set to OnlineAll. Learn more.</p> <p>Make sure there are no Windows updates pending on the VM when you trigger a failover. Windows update might start when you fail over, and you won't be able to log onto the VM until the update completes.</p>
Azure VM running Windows	Azure VM after failover	<p>Add a public IP address for the VM.</p> <p>The network security group rules on the failed over VM (and the Azure subnet to which it is connected) need to allow incoming connections to the RDP port.</p> <p>Check Boot diagnostics to verify a screenshot of the VM.</p> <p>If you can't connect, check that the VM is running, and review these troubleshooting tips.</p>
Azure VM running Linux	On-premises machine before failover	<p>Ensure that the Secure Shell service on the VM is set to start automatically on system boot.</p> <p>Check that firewall rules allow an SSH connection to it.</p>
Azure VM running Linux	Azure VM after failover	<p>The network security group rules on the failed over VM (and the Azure subnet to which it is connected) need to allow incoming connections to the SSH port.</p> <p>Add a public IP address for the VM.</p> <p>Check Boot diagnostics for a screenshot of the VM.</p>

Follow the steps described [here](#) to troubleshoot any connectivity issues post failover.

Next steps

After you've completed a disaster recovery drill, learn more about other types of [failover](#).

Run a failover from on-premises to Azure

1/2/2020 • 7 minutes to read • [Edit Online](#)

This article describes how to fail over on-premises machines to Azure in [Azure Site Recovery](#)

Before you start

- [Learn](#) about the failover process in disaster recovery.
- If you want to fail over multiple machines, [learn](#) how to gather machines together in a recovery plan.
- Before you do a full failover, run a [disaster recovery drill](#) to ensure that everything is working as expected.

Prepare to connect after failover

To make sure you can connect to the Azure VMs that are created after failover, here are a number of things you need to do on-premises before failover.

Prepare on-premises to connect after failover

If you want to connect to Azure VMs using RDP/SSH after failover, there are a number of things you need to do on-premises before failover.

AFTER FAILOVER	LOCATION	ACTIONS
Azure VM running Windows	On-premises machine before failover	To access the Azure VM over the internet, enable RDP, and make sure that TCP and UDP rules are added for Public , and that RDP is allowed for all profiles in Windows Firewall > Allowed Apps .
		To access the Azure VM over a site-to-site connection, enable RDP on the machine, and ensure that RDP is allowed in the Windows Firewall -> Allowed apps and features , for Domain and Private networks.
		Remove any static persistent routes and WinHTTP proxy. Make sure the operating system SAN policy is set to OnlineAll . Learn more .
		Make sure there are no Windows updates pending on the VM when you trigger a failover. Windows update might start when you fail over, and you won't be able to log onto the VM until the update completes.

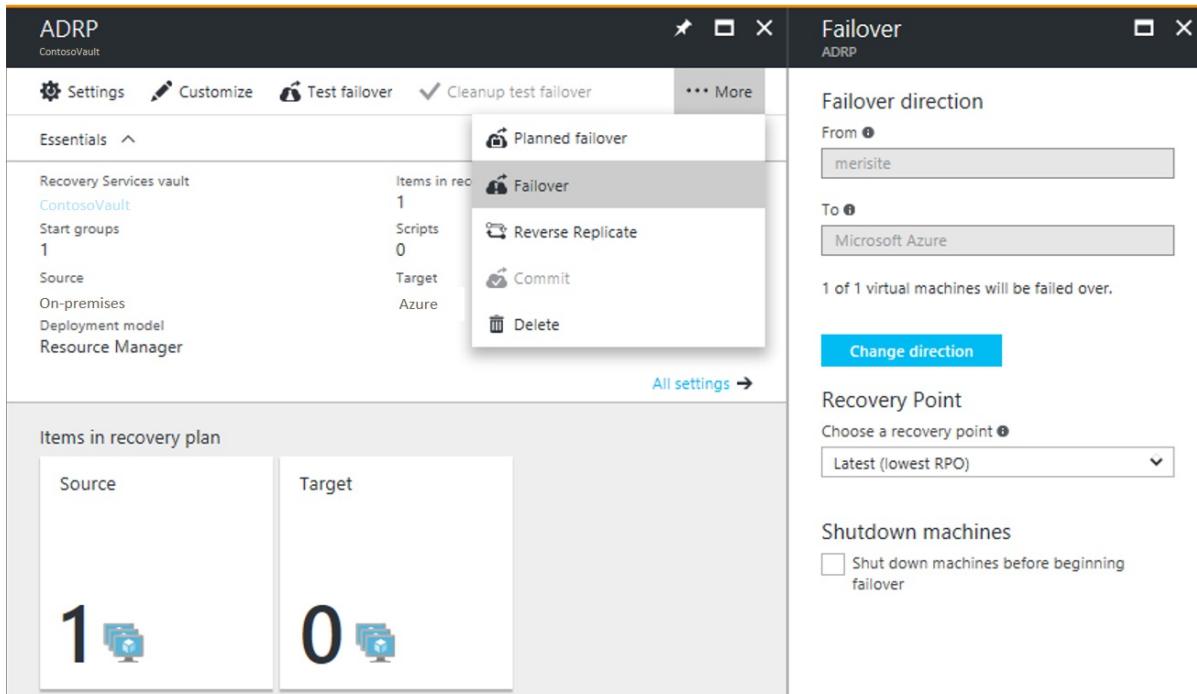
AFTER FAILOVER	LOCATION	ACTIONS
Azure VM running Linux	On-premises machine before failover	<p>Ensure that the Secure Shell service on the VM is set to start automatically on system boot.</p> <p>Check that firewall rules allow an SSH connection to it.</p>

Run a failover

This procedure describes how to run a failover for a [recovery plan](#). If you want to run a failover for a single VM, follow the instructions for a [VMware VM](#), a [physical server](#), or a [Hyper-V VM](#).

Run the recovery plan failover as follows:

1. In the Site Recovery vault, select **Recovery Plans** > *recoveryplan_name*.
2. Click **Failover**.



3. In **Failover > Failover direction**, leave the default if you're replicating to Azure.
4. In **Failover**, select a **Recovery Point** to which to fail over.
 - **Latest:** Use the latest point. This processes all the data that's been sent to Site Recovery service, and creates a recovery point for each machine. This option provides the lowest RPO (Recovery Point Objective) because the VM created after failover has all the data that's been replicated to Site Recovery when the failover was triggered.
 - **Latest processed:** Use this option to fail over VMs to the latest recovery point already processed by Site Recovery. You can see the latest processed recovery point in the VM **Latest Recovery Points**. This option provides a low RTO as no time is spent to processing the unprocessed data.
 - **Latest app-consistent:** Use this option to fail VMs over to the latest application consistent recovery point that's been processed by Site Recovery.
 - **Latest multi-VM processed:** With this option VMs that are part of a replication group failover to the latest common multi-VM consistent recovery point. Other virtual machines fail over to their latest processed recovery point. This option is only for recovery plans that have at least one VM with multi-VM

consistency enabled.

- **Latest multi-VM app-consistent:** With this option VMs that are part of a replication group fail over to the latest common multi-VM application-consistent recovery point. Other virtual machines failover to their latest application-consistent recovery point. Only for recovery plans that have at least one VM with multi-VM consistency enabled.
- **Custom:** Not available for recovery plans. This option is only for failover of individual VMs.

5. Select **Shut-down machine before beginning failover** if you want Site Recovery shut down source VMs before starting the failover. Failover continues even if shutdown fails.

NOTE

If you fail over Hyper-V VMs, shutdown tries to synchronize and replicate the on-premises data that hasn't yet been sent to the service, before triggering the failover.

6. Follow failover progress on the **Jobs** page. Even if errors occurs, the recovery plan runs until it is complete.
7. After the failover, sign into the VM to validate it.
8. If you want to switch to different recovery point to use for the failover, use **Change recovery point**.
9. When you're ready, you can commit the failover. The **Commit** action deletes all the recovery points available with the service. The **Change recovery point** option will no longer be available.

Run a planned failover (Hyper-V)

You can run a planned failover for Hyper-V VMs.

- A planned failover is a zero data loss failover option.
- When a planned failover is triggered, first the source virtual machines are shut-down, the latest data is synchronized and then a failover is triggered.
- You run a planned failover using the **Planned failover** option. It runs in a similar way to a regular failover.

Track failovers

There are a number of jobs associated with failover.

Job

NAME	STATUS	START TIME	DURATION	...
Prerequisites check for the recovery plan	✔ Successful	5/3/2017 4:01:19 PM	00:00:02	...
Create the environment	✔ Successful	5/3/2017 4:01:22 PM	00:00:00	...
▼ All groups shutdown (1)	✔ Successful	5/3/2017 4:01:23 PM	00:01:54	...
Shutdown: Group 1 (1)	✔ Successful	5/3/2017 4:01:23 PM	00:01:54	...
▼ Recovery plan failover	✔ Successful	5/3/2017 4:03:18 PM	00:01:38	...
SQLServer	✔ Successful	5/3/2017 4:03:18 PM	00:01:38	...
▼ Group 1: Start (1)	✔ Successful	5/3/2017 4:04:57 PM	00:01:45	...
SQLServer	✔ Successful	5/3/2017 4:04:57 PM	00:01:45	...
Finalizing the recovery plan	✔ Successful	5/3/2017 4:06:43 PM	00:00:00	...

- **Prerequisites check:** Ensures that all conditions required for failover are met.

- **Failover:** Processes the data so that an Azure VM can be created from it. If you have chosen **Latest** recovery point, a recovery point is created from the data that's been sent to the service.
- **Start:** Creates an Azure VM using the data processed in the previous step.

WARNING

Don't cancel a failover in progress: Before failover is started, replication stops for the VM. If you cancel an in-progress job, failover stops, but the VM will not start to replicate. Replication can't be started again.

Extra failover time

In some cases, VM failover requires intermediate step that usually takes around eight to 10 minutes to complete. These are the machines that are affected by this additional step/time:

- VMware virtual machines running a Mobility service version older than 9.8.
- Physical servers, and Hyper-V VMs protected as physical servers.
- VMware Linux VMs.
- VMware VMs on which these drivers aren't present as boot drivers:
 - storvsc
 - vmbus
 - storflt
 - intelide
 - atapi
- VMware VMs that don't have DHCP enabled, irrespective of whether they're using DHCP or static IP addresses.

Automate actions during failover

You might want to automate actions during failover. To do this, you can use scripts or Azure automation runbooks in recovery plans.

- [Learn](#) about creating and customizing recovery plans, including adding scripts.
- [Learn](#) about adding Azure Automation runbooks to recovery plans.

Configure settings after failover

Retain drive letters after failover

Site Recovery handles retention of drive letters. If you're excluding disks during VM replication, [review an example](#) of how this works.

Prepare in Azure to connect after failover

If you want to connect to Azure VMs that are created after failover using RDP or SSH, follow the requirements summarized in the table.

FAILOVER	LOCATION	ACTIONS
----------	----------	---------

FAILOVER	LOCATION	ACTIONS
Azure VM running Windows	Azure VM after failover	<p>Add a public IP address for the VM.</p> <p>The network security group rules on the failed over VM (and the Azure subnet to which it is connected) need to allow incoming connections to the RDP port.</p> <p>Check Boot diagnostics to verify a screenshot of the VM.</p> <p>If you can't connect, check that the VM is running, and review these troubleshooting tips.</p>
Azure VM running Linux	Azure VM after failover	<p>The network security group rules on the failed over VM (and the Azure subnet to which it is connected) need to allow incoming connections to the SSH port.</p> <p>Add a public IP address for the VM.</p> <p>Check Boot diagnostics for a screenshot of the VM.</p>

Follow the steps described [here](#) to troubleshoot any connectivity issues post failover.

Set up IP addressing

- **Internal IP addresses:** To set the internal IP address of an Azure VM after failover, you have a couple of options:
 - Retain same IP address: You can use the same IP address on the Azure VM as the one allocated to the on-premises machine.
 - Use different IP address: You can use a different IP address for the Azure VM.
 - [Learn more](#) about setting up internal IP addresses.
- **External IP addresses:** You can retain public IP addresses on failover. Azure VMs created as part of the failover process must be assigned an Azure public IP address available in the Azure region. You can assign a public IP address either manually or by automating the process with a recovery plan. [Learn more](#).

Next steps

After you've failed over, you need to reprotect to start replicating the Azure VMs back to the on-premises site. After replication is up and running, you can fail back on-premises when you're ready.

- [Learn more](#) about reprottection and failback.
- [Prepare](#) for VMware reprottection and failback.
- [Fail back](#) Hyper-V VMs.
- [Learn about](#) the failover and failback process for physical servers.

Prepare for reprottection and failback of VMware VMs

12/26/2019 • 6 minutes to read • [Edit Online](#)

After [failover](#) of on-premises VMware VMs or physical servers to Azure, you reprotect the Azure VMs created after failover, so that they replicate back to the on-premises site. With replication from Azure to on-premises in place, you can then fail back by running a failover from Azure to on-premises when you're ready.

Before you continue, get a quick overview with this video about how to fail back from Azure to an on-premises site.

Reprotection/failback components

You need a number of components and settings in place before you can reprotect and fail back from Azure.

DETAILS	
On-premises configuration server	<p>The on-premises configuration server must be running and connected to Azure.</p> <p>The VM you're failing back to must exist in the configuration server database. If disaster affects the configuration server, restore it with the same IP address to ensure that failback works.</p> <p>If IP addresses of replicated machines were retained on failover, site-to-site connectivity (or ExpressRoute connectivity) should be established between Azure VMs machines and the fallback NIC of the configuration server. For retained IP addresses the configuration server needs two NICs - one for source machine connectivity, and one for Azure failback connectivity. This avoids overlap of subnet address ranges for the source and failed over VMs.</p>
Process server in Azure	<p>You need a process server in Azure before you can fail back to your on-premises site.</p> <p>The process server receives data from the protected Azure VM, and sends it to the on-premises site.</p> <p>You need a low-latency network between the process server and the protected VM, so we recommend that you deploy the process server in Azure for higher replication performance.</p> <p>For proof-of-concept, you can use the on-premises process server, and ExpressRoute with private peering.</p> <p>The process server should be in the Azure network in which the failed over VM is located. The process server must also be able to communicate with the on-premises configuration server and master target server.</p>

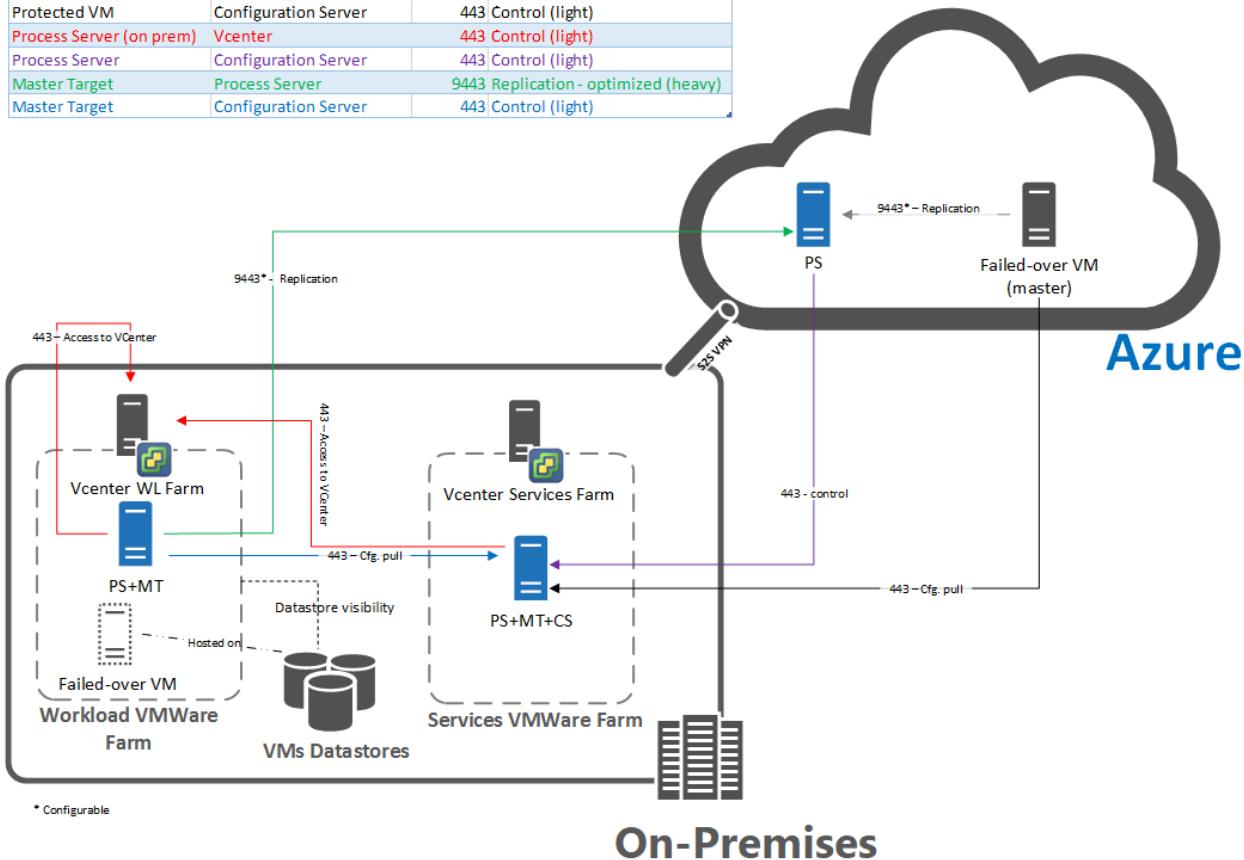
DETAILS

Separate master target server	<p>The master target server receives failback data, and by default a Windows master target server runs on the on-premises configuration server.</p> <p>A master target server can have up to 60 disks attached to it. VMs being failed back have more than a collective total of 60 disks, or if you're failing back large volumes of traffic, create a separate master target server for failback.</p> <p>If machines are gathered into a replication group for multi-VM consistency, the VMs must all be Windows, or must all be Linux. Why? Because all VMs in a replication group must use the same master target server, and the master target server must have same operating system (With the same or a higher version) than those of the replicated machines.</p> <p>The master target server shouldn't have any snapshots on its disks, otherwise reprottection and failback won't work.</p> <p>The master target can't have a Paravirtual SCSI controller. The controller can only be an LSI Logic controller. Without an LSI Logic controller, reprottection fails.</p>
Fallback replication policy	<p>To replicate back to on-premises site, you need a failback policy. This policy is automatically created when you create a replication policy to Azure.</p> <p>The policy is automatically associated with the configuration server. It's set to an RPO threshold of 15 minutes, recovery point retention of 24 hours, and app-consistent snapshot frequency is 60 minutes. The policy can't be edited.</p>
Site-to-site VPN/ExpressRoute private peering	<p>Reprottection and failback needs a site-to-site VPN connection, or ExpressRoute private peering to replicate data.</p>

Ports for reprottection/failback

A number of ports must be open for reprottection/failback. The following graphic illustrates the ports and reprotect/failback flow.

Source	Destination	Port	Traffic (size)
Protected VM	Process Server	9443	Replication (heavy)
Protected VM	Configuration Server	443	Control (light)
Process Server (on prem)	Vcenter	443	Control (light)
Process Server	Configuration Server	443	Control (light)
Master Target	Process Server	9443	Replication - optimized (heavy)
Master Target	Configuration Server	443	Control (light)



Deploy a process server in Azure

1. Set up a process server in Azure for failback.
2. Ensure that Azure VMs can reach the process server.
3. Make sure that the site-to-site VPN connection or ExpressRoute private peering network has enough bandwidth to send data from the process server to the on-premises site.

Deploy a separate master target server

1. Note the master target server [requirements and limitations](#).
2. Create a [Windows](#) or [Linux](#) master target server, to match the operating system of the VMs you want to reprotect and fail back.
3. Make sure you don't use Storage vMotion for the master target server, or failback can fail. The VM machine can't start because the disks aren't available to it.
 - To prevent this, exclude the master target server from your vMotion list.
 - If a master target undergoes a Storage vMotion task after reprottection, the protected VM disks attached to the master target server migrate to the target of the vMotion task. If you try to fail back after this, disk detachment fails because the disks aren't found. It's then hard to find the disks in your storage accounts. If this occurs, find them manually and attach them to the VM. After that, the on-premises VM can be booted.
4. Add a retention drive to the existing Windows master target server. Add a new disk and format the drive. The retention drive is used to stop the points in time when the VM replicates back to the on-premises site. Note these criteria. If they aren't met, the drive isn't listed for the master target server:
 - The volume isn't used for any other purpose, such as a replication target, and it isn't in lock mode.
 - The volume isn't a cache volume. The custom installation volume for the process server and master

target isn't eligible for a retention volume. When the process server and master target are installed on a volume, the volume is a cache volume of the master target.

- The file system type of the volume isn't FAT or FAT32.
 - The volume capacity is nonzero.
 - The default retention volume for Windows is the R volume.
 - The default retention volume for Linux is /mnt/retention.
5. Add a drive if you're using an existing process server. The new drive must meet the requirements in the last step. If the retention drive isn't present, it doesn't appear in the selection drop-down list on the portal. After you add a drive to the on-premises master target, it takes up to 15 minutes for the drive to appear in the selection on the portal. You can refresh the configuration server if the drive doesn't appear after 15 minutes.
6. Install VMware tools or open-vm-tools on the master target server. Without the tools, the datastores on the master target's ESXi host can't be detected.
7. Set the disk.EnableUUID=true setting in the configuration parameters of the master target VM in VMware. If this row doesn't exist, add it. This setting is required to provide a consistent UUID to the VMDK so that it mounts correctly.
8. Check vCenter Server access requirements:
- If the VM to which you're failing back is on an ESXi host managed by VMware vCenter Server, the master target server needs access to the on-premises VM Virtual Machine Disk (VMDK) file, in order to write the replicated data to the virtual machine's disks. Make sure that the on-premises VM datastore is mounted on the master target host with read/write access.
 - If the VM isn't on an ESXi host managed by a VMware vCenter Server, Site Recovery creates a new VM during reprottection. This VM is created on the ESXi host on which you create the master target server VM. Choose the ESXi host carefully, to create the VM on the host that you want. The hard disk of the VM must be in a datastore that's accessible by the host on which the master target server is running.
 - Another option, if the on-premises VM already exists for failback, is to delete it before you do a failback. Failback then creates a new VM on the same host as the master target ESXi host. When you fail back to an alternate location, the data is recovered to the same datastore and the same ESXi host as that used by the on-premises master target server.
9. For physical machines failing back to VMware VMs, you should complete discovery of the host on which the master target server is running, before you can reprotect the machine.
10. Check that the ESXi host on which the master target VM has at least one virtual machine file system (VMFS) datastore attached to it. If no VMFS datastores are attached, the datastore input in the reprottection settings is empty and you can't proceed.

Next steps

[Reprotect](#) a VM.

Reprotect from Azure to on-premises

12/26/2019 • 4 minutes to read • [Edit Online](#)

After [failover](#) of on-premises VMware VMs or physical servers to Azure, the first step in failing back to your on-premises site is to reprotect the Azure VMs that were created during failover. This article describes how to do this.

Before you begin

1. Follow the steps in [this article](#) to prepare for reprottection and failback, including setting up a process server in Azure, and an on-premises master target server, and configuring a site-to-site VPN, or ExpressRoute private peering, for failback.
2. Make sure that the the on-premises configuration server is running and connected to Azure. During failover to Azure, the on-premises site might not be accessible, and the configuration server might be unavailable or shut down. During failback, the VM must exist in the configuration server database. Otherwise, failback is unsuccessful.
3. Delete any snapshots on the on-premises master target server. Reprotection won't work if there are snapshots. The snapshots on the VM are automatically merged during a reprotect job.
4. If you're reprotecting VMs gathered into a replication group for multi-VM consistency, make sure they all have the same operating system (Windows or Linux) and make sure that the master target server you deploy has the same type of operating system. All VMs in a replication group must use the same master target server.
5. Open [the required ports](#) for failback.
6. Ensure that the vCenter Server is connected before failback. Otherwise, disconnecting disks and attaching them back to the virtual machine fails.
7. If a vCenter server manages the VMs to which you'll fail back, make sure that you have the required permissions. If you perform a read-only user vCenter discovery and protect virtual machines, protection succeeds, and failover works. However, during reprottection, failover fails because the datastores can't be discovered, and aren't listed during reprotect. To resolve this problem, you can update the vCenter credentials with an [appropriate account/permissions](#), and then retry the job.
8. If you used a template to create your virtual machines, ensure that each VM has its own UUID for the disks. If the on-premises VM UUID clashes with the UUID of the master target server because both were created from the same template, reprottection fails. Deploy from a different template.
9. If you're failing back to an alternate vCenter Server, make sure that the new vCenter Server and the master target server are discovered. Typically if they're not the datastores aren't accessible, or aren't visible in **Reprotect**.
10. Verify the following scenarios in which you can't fail back:
 - If you're using either the ESXi 5.5 free edition or the vSphere 6 Hypervisor free edition. Upgrade to a different version.
 - If you have a Windows Server 2008 R2 SP1 physical server.
 - VMware VMs can't fail back to Hyper-V.
 - VMs that have [been migrated](#).
 - A VM that's been moved to another resource group.
 - A replica Azure VM that's been deleted.
 - A replica Azure VM that isn't protected (replicating to the on-premises site).
11. [Review the types of failback](#) you can use - original location recovery and alternate location recovery.

Enable reprottection

Enable replication. You can reprotect specific VMs, or a recovery plan:

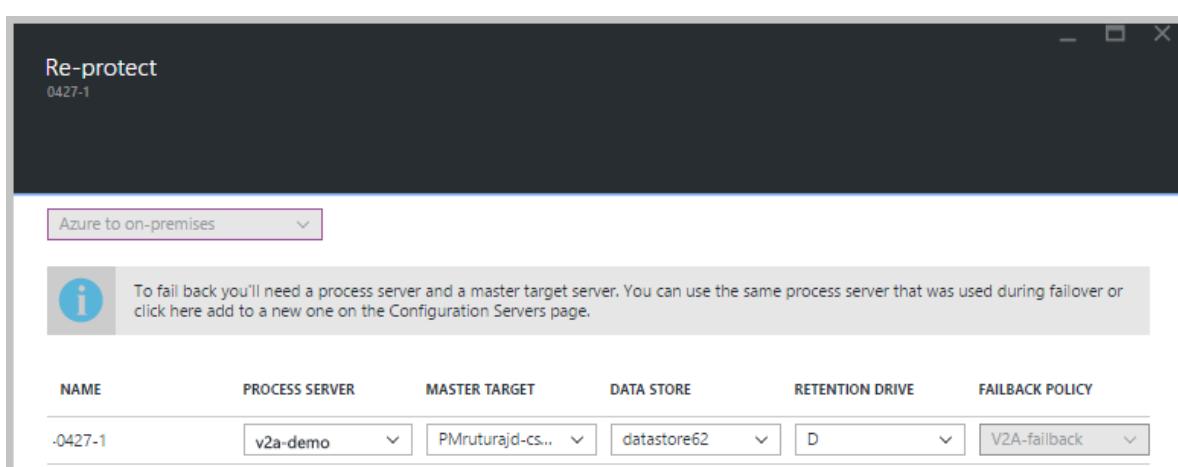
- If you reprotect a recovery plan, you must provide the values for every protected machine.
- If VMs belong to a replication group for multi-VM consistency, they can only be reprotected using a recovery plan. VMs in a replication group must use the same master target server

Before you start

- After a VM boots in Azure after failover, it takes some time for the agent to register back to the configuration server (up to 15 minutes). During this time, you won't be able to reprotect and an error message indicates that the agent isn't installed. If this happens, wait for a few minutes, and then reprotect.
- If you want to fail back the Azure VM to an existing on-premises VM, mount the on-premises VM datastores with read/write access on the master target server's ESXi host.
- If you want to fail back to an alternate location, for example if the on-premises VM doesn't exist, select the retention drive and datastore that are configured for the master target server. When you fail back to the on-premises site, the VMware virtual machines in the fallback protection plan use the same datastore as the master target server. A new VM is then created in vCenter.

Enable reprotection as follows:

1. Select **Vault > Replicated items**. Right-click the virtual machine that failed over, and then select **Re-Protect**. Or, from the command buttons, select the machine, and then select **Re-Protect**.
2. Verify that the **Azure to On-premises** direction of protection is selected.
3. In **Master Target Server** and **Process Server**, select the on-premises master target server and the process server.
4. For **Datastore**, select the datastore to which you want to recover the disks on-premises. This option is used when the on-premises virtual machine is deleted, and you need to create new disks. This option is ignored if the disks already exist. You still need to specify a value.
5. Select the retention drive.
6. The fallback policy is automatically selected.
7. Select **OK** to begin reprottection.



8. A job begins to replicate the Azure VM to the on-premises site. You can track the progress on the **Jobs** tab.
 - When the reprottection succeeds, the VM enters a protected state.
 - The on-premises VM is turned off during reprottection. This helps ensure data consistency during replication.
 - Don't turn on the on-premises VM after reprottection finishes.

Next steps

- If you encounter any issues, review the [troubleshooting article](#).
- After the Azure VMs are protected, you can [run a fallback](#). Fallback shuts down the Azure VM and boots the on-premises VM. Expect some downtime for the application, and choose a fallback time accordingly.

Fail back VMware VMs to on-premises site

12/26/2019 • 2 minutes to read • [Edit Online](#)

This article describes how to fail back Azure VMs to an on-premises site, following [failover](#) of on-premises VMs to Azure with [Azure Site Recovery](#). After failback to on-premises, you enable replication so that the on-premises VMs start replicating to Azure.

Before you start

1. Learn about [VMware failback](#).
2. Make sure you've reviewed and completed the steps to [prepare for failback](#), and that all the required components are deployed. Components include a process server in Azure, an on-premises master target server, and a VPN site-to-site connection (or ExpressRoute private peering) for failback.
3. Make sure you've completed the [requirements](#) for reprottection and failback, and that you've [enabled reprottection](#) of Azure VMs, so that they're replicating from Azure to the on-premises site. VMs must be in a replicated state in order to fail back.

Run a failover to fail back

1. Make sure that Azure VMs are reprotected and replicating to the on-premises site.
 - A VM needs at least one recovery point in order to fail back.
 - If you fail back a recovery plan, then all machines in the plan should have at least one recovery point.
2. In the vault > **Replicated items**, select the VM. Right-click the VM > **Unplanned Failover**.
3. In **Confirm Failover**, verify the failover direction (from Azure).
4. Select the recovery point that you want to use for the failover.
 - We recommend that you use the **Latest** recovery point. The app-consistent point is behind the latest point in time, and causes some data loss.
 - **Latest** is a crash-consistent recovery point.
 - With **Latest**, a VM fails over to its latest available point in time. If you have a replication group for multi-VM consistency within a recovery plan, each VM in the group fails over to its independent latest point in time.
 - If you use an app-consistent recovery point, each VM fails back to its latest available point. If a recovery plan has a replication group, each group recovers to its common available recovery point.
5. Failover begins. Site Recovery shuts down the Azure VMs.
6. After failover completes, check everything's working as expected. Check that the Azure VMs are shut down.
7. With everything verified, right-click the VM > **Commit**, to finish the failover process. Commit removes the failed-over Azure VM.

NOTE

For Windows VMs, Site Recovery disables the VMware tools during failover. During failback of the Windows VM, the VMware tools are enable again.

Reprotect from on-premises to Azure

After committing the failback, the Azure VMs are deleted. The VM is back in the on-premises site, but it isn't protected. To start replicating VMs to Azure again,as follows:

1. In the vault > **Replicated items**, select failed back VMs, and then select **Re-Protect**.
2. Specify the process server that's used to send data back to Azure.
3. Select **OK** to begin the reprotect job.

NOTE

After an on-premises VM starts, it takes up to 15 minutes for the agent to register back to the configuration server. During this time, reprotect fails and returns an error message stating that the agent isn't installed. If this occurs, wait for a few minutes, and reprotect.

Next steps

After the reprotect job finishes, the on-premises VM is replicating to Azure. As needed, you can [run another failover](#) to Azure.

Set up a process server in Azure for failback

11/14/2019 • 2 minutes to read • [Edit Online](#)

After you fail over VMware VMs or physical servers to Azure using [Site Recovery](#), you can fail them back to the on-premises site when it's up and running again. In order to fail back, you need to set up a temporary process server in Azure, to handle replication from Azure to on-premises. You can delete this VM after failback is complete.

Before you start

Learn more about the [reprotection](#) and [failback](#) process.

This article assumes that

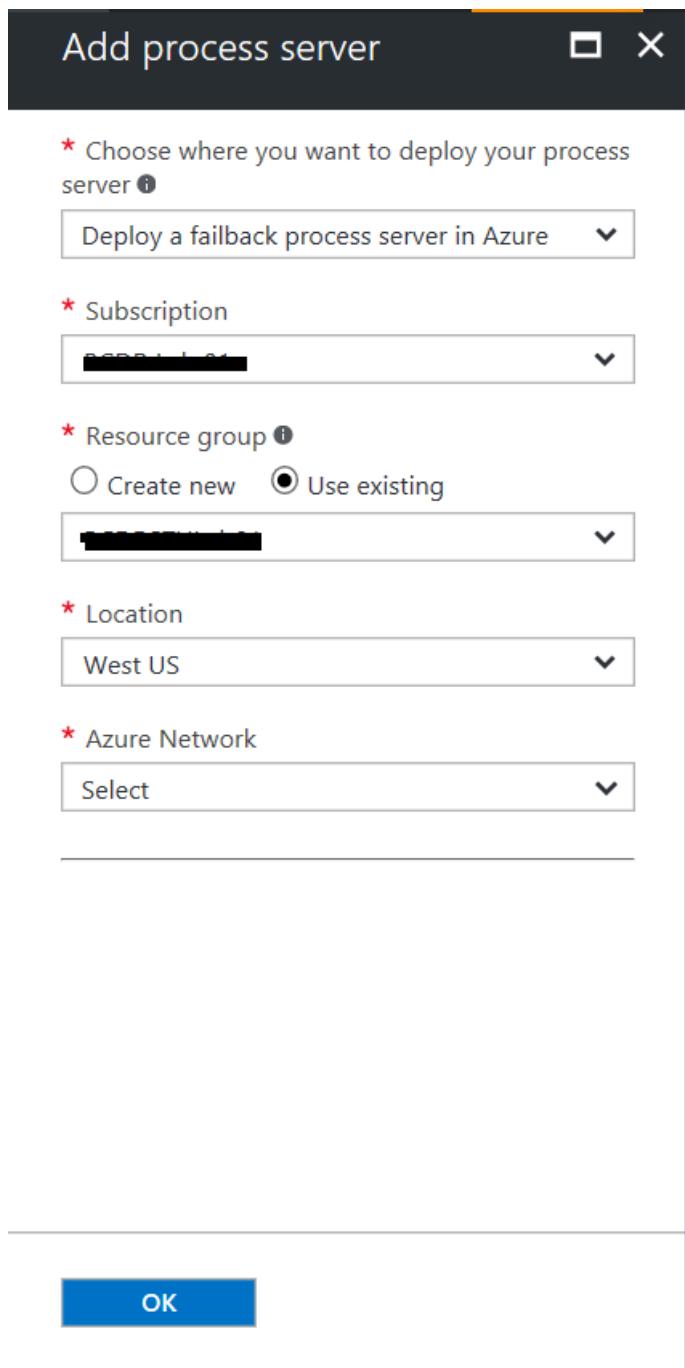
1. A **Site to Site VPN** or an **Express Route** connection between your on-premises network and the Azure Virtual Network has already been established.
2. Your user account has permissions to create a new virtual machine in the Azure Subscription that the virtual machines have been failed over into.
3. Your subscription has a minimum of 8 Cores available to spin up a new Process Server virtual machine.
4. You have the **Configuration Server Passphrase** available.

TIP

Ensure that you are able to connect port 443 of the Configuration Server (running on-premises) from the Azure Virtual Network that the virtual machines have been failed over into.

Deploy a process server in Azure

1. In the vault > **Site Recovery Infrastructure** > **Manage** > **Configuration Servers**, select the configuration server.
2. In the server page, click **+ Process server**
3. In **Add process server** page, and select to deploy the process server in Azure.
4. Specify the Azure settings, including the subscription used for failover, a resource group, the Azure region used for failover, and the virtual network in which the Azure VMs are located. If you used multiple Azure networks, you need a process server in each one.



5. In **Server name**, **User name**, and **Password**, specify a name for the process server, and credentials that will be assigned Admin permissions on the server.
6. Specify a storage account to be used for the server VM disks, the subnet in which the process server VM will be located, and the server IP address that will be assigned when the VM starts.
7. Click **OK** button to start deploying the process server VM. The process server will be deployed on Standard_A8_v2 SKU. Ensure that this VM SKU is available for your subscription.

Registering the process server (running in Azure) to a Configuration Server (running on-premises)

After the process server VM is up and running, you need to register it with the on-premises configuration server, as follows:

1. Establish a Remote Desktop Connection to the machine running the process server.
2. Run `cpsconfigtool.exe` to start the Azure Site Recovery Process Server configuration tool.

- The tool is launched automatically the first time you sign into the process server.
 - If it doesn't open automatically, click its shortcut on the desktop.
3. In **Configuration server FQDN or IP**, specify the name or IP address of the configuration server with which to register the process server.
 4. In **Configuration Server Port**, ensure that 443 is specified. This is the port on which the configuration server listens for requests.
 5. In **Connection Passphrase**, specify the passphrase that you specified when you set up the configuration server. To find the passphrase:

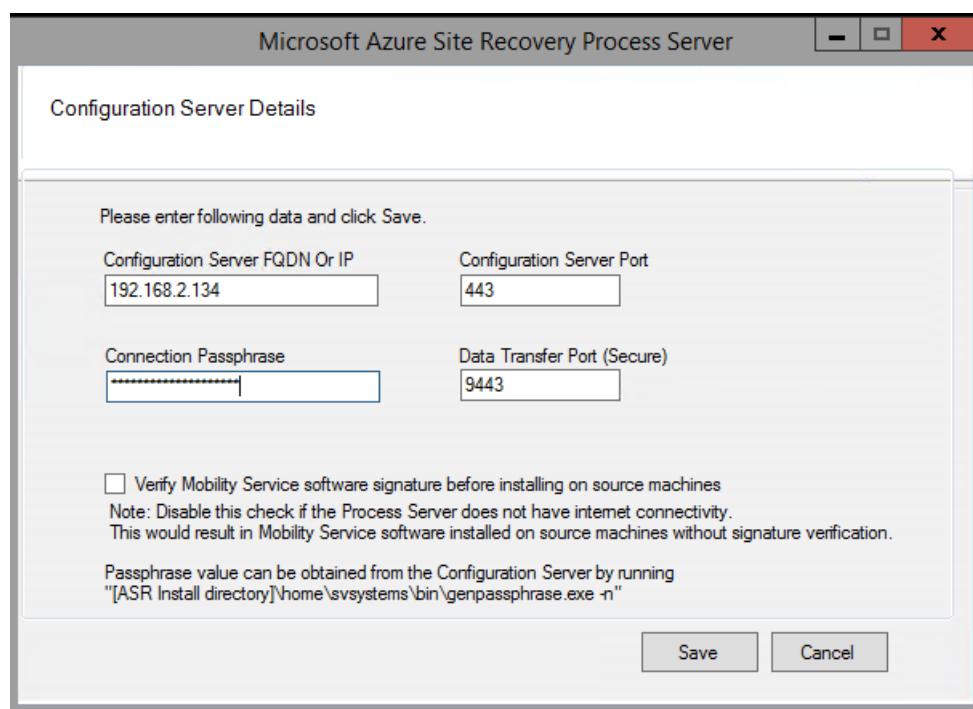
- On the configuration server, navigate to the Site Recovery installation folder **\home\svssystems\bin**:

```
cd %ProgramData%\ASR\home\svssystems\bin
```

- Run the below command to print out the current passphrase:

```
genpassphrase.exe -n
```

6. In **Data Transfer Port**, leave the default value unless you've specified a custom port.
7. Click **Save** save the settings, and register the process server.



Install a Linux master target server for failback

11/12/2019 • 10 minutes to read • [Edit Online](#)

After you fail over your virtual machines to Azure, you can fail back the virtual machines to the on-premises site. To fail back, you need to reprotect the virtual machine from Azure to the on-premises site. For this process, you need an on-premises master target server to receive the traffic.

If your protected virtual machine is a Windows virtual machine, then you need a Windows master target. For a Linux virtual machine, you need a Linux master target. Read the following steps to learn how to create and install a Linux master target.

IMPORTANT

Starting with release of the 9.10.0 master target server, the latest master target server can be only installed on an Ubuntu 16.04 server. New installations aren't allowed on CentOS6.6 servers. However, you can continue to upgrade your old master target servers by using the 9.10.0 version. Master target server on LVM is not supported.

Overview

This article provides instructions for how to install a Linux master target.

Post comments or questions at the end of this article or on the [Azure Recovery Services Forum](#).

Prerequisites

- To choose the host on which to deploy the master target, determine if the failback is going to be to an existing on-premises virtual machine or to a new virtual machine.
 - For an existing virtual machine, the host of the master target should have access to the data stores of the virtual machine.
 - If the on-premises virtual machine does not exist (in case of Alternate Location Recovery), the failback virtual machine is created on the same host as the master target. You can choose any ESXi host to install the master target.
- The master target should be on a network that can communicate with the process server and the configuration server.
- The version of the master target must be equal to or earlier than the versions of the process server and the configuration server. For example, if the version of the configuration server is 9.4, the version of the master target can be 9.4 or 9.3 but not 9.5.
- The master target can only be a VMware virtual machine and not a physical server.

Sizing guidelines for creating master target server

Create the master target in accordance with the following sizing guidelines:

- **RAM:** 6 GB or more
- **OS disk size:** 100 GB or more (to install OS)
- **Additional disk size for retention drive:** 1 TB
- **CPU cores:** 4 cores or more

The following Ubuntu kernels are supported.

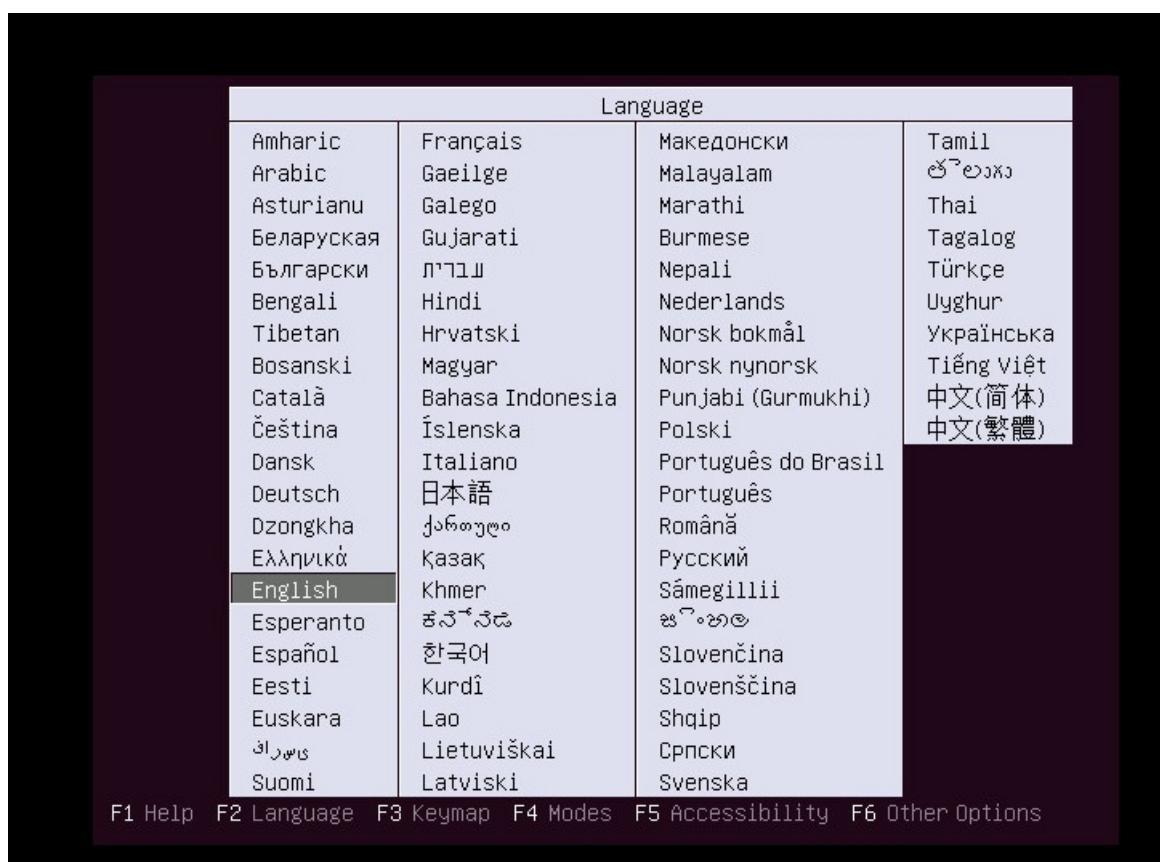
KERNEL SERIES	SUPPORT UP TO
4.4	4.4.0-81-generic
4.8	4.8.0-56-generic
4.10	4.10.0-24-generic

Deploy the master target server

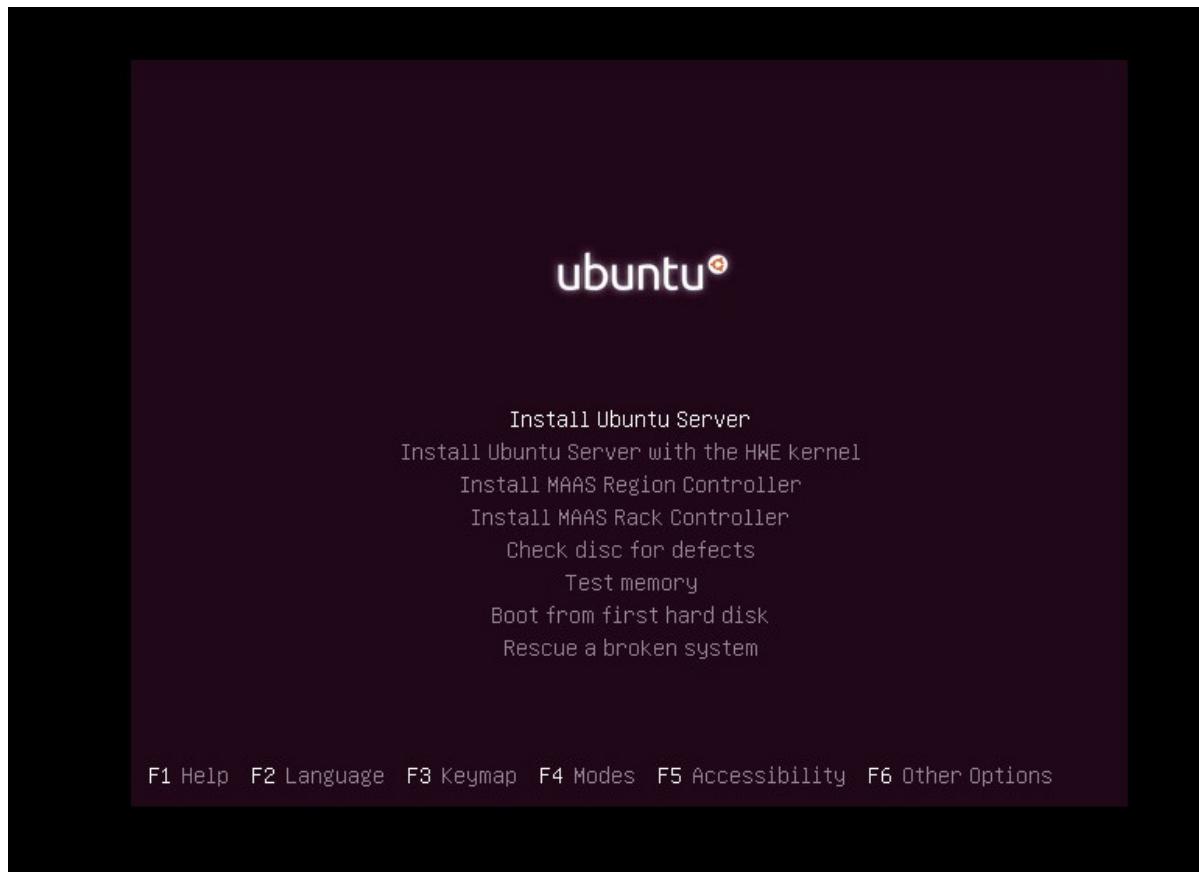
Install Ubuntu 16.04.2 Minimal

Take the following the steps to install the Ubuntu 16.04.2 64-bit operating system.

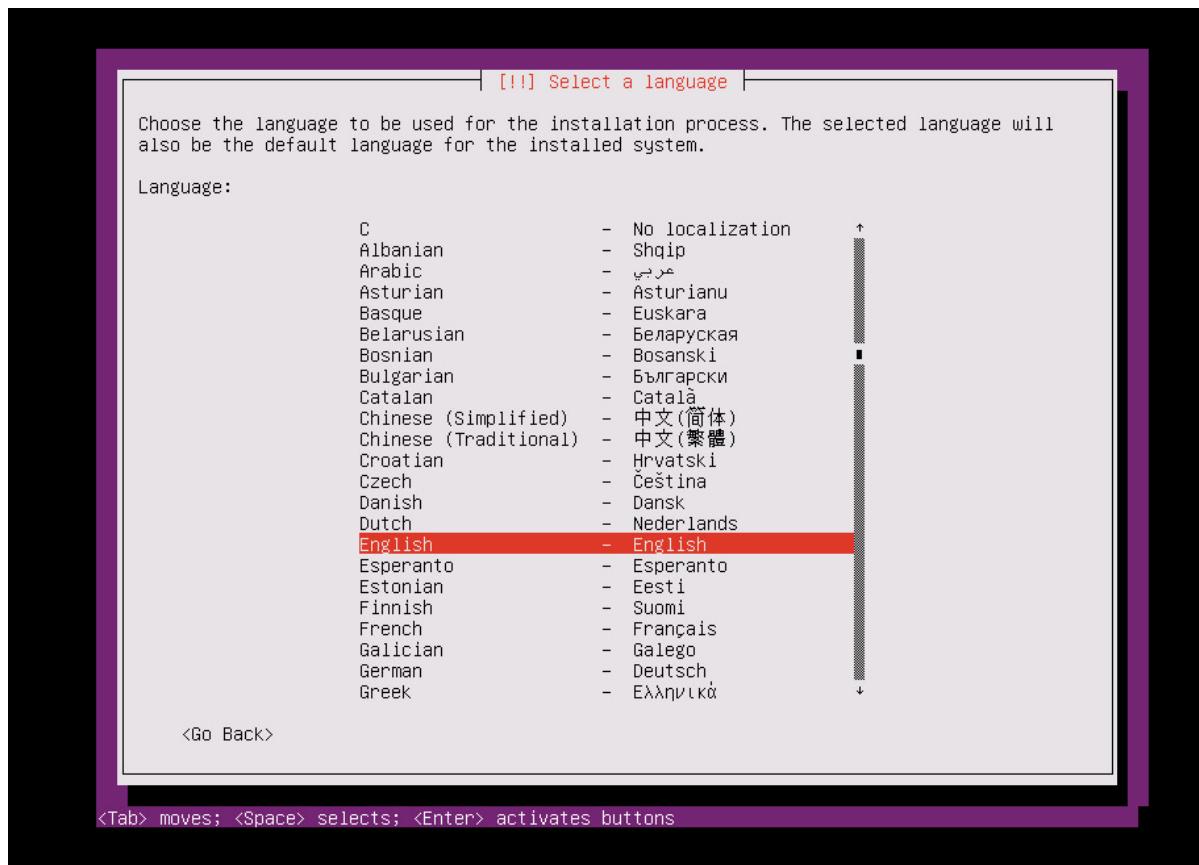
1. Go to the [download link](#), choose the closest mirror and download an Ubuntu 16.04.2 minimal 64-bit ISO.
Keep an Ubuntu 16.04.2 minimal 64-bit ISO in the DVD drive and start the system.
2. Select **English** as your preferred language, and then select **Enter**.



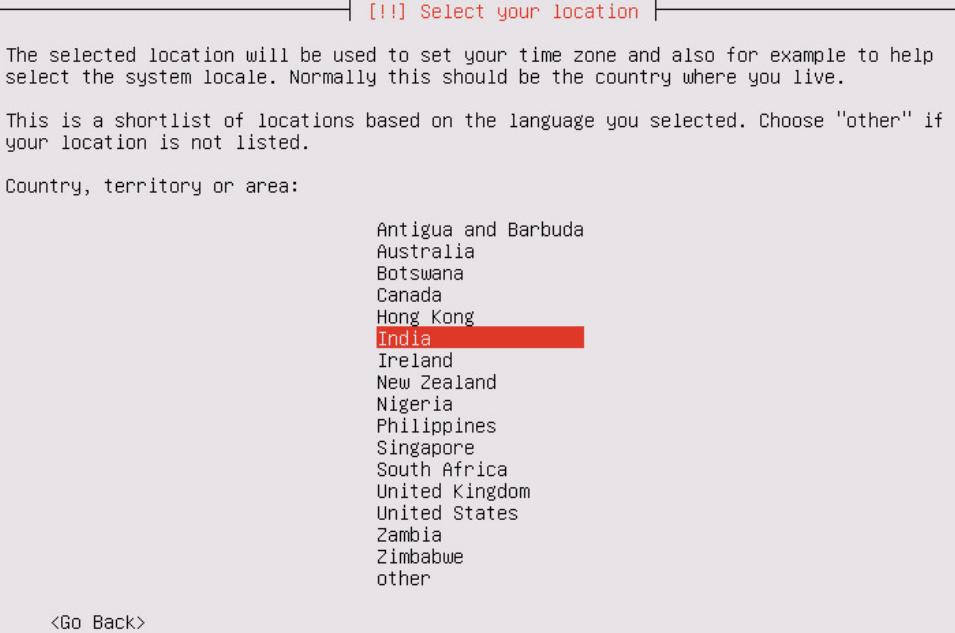
3. Select **Install Ubuntu Server**, and then select **Enter**.



4. Select **English** as your preferred language, and then select **Enter**.

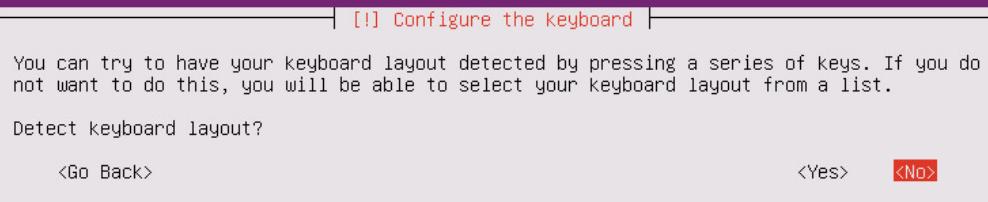


5. Select the appropriate option from the **Time Zone** options list, and then select **Enter**.



<Tab> moves; <Space> selects; <Enter> activates buttons

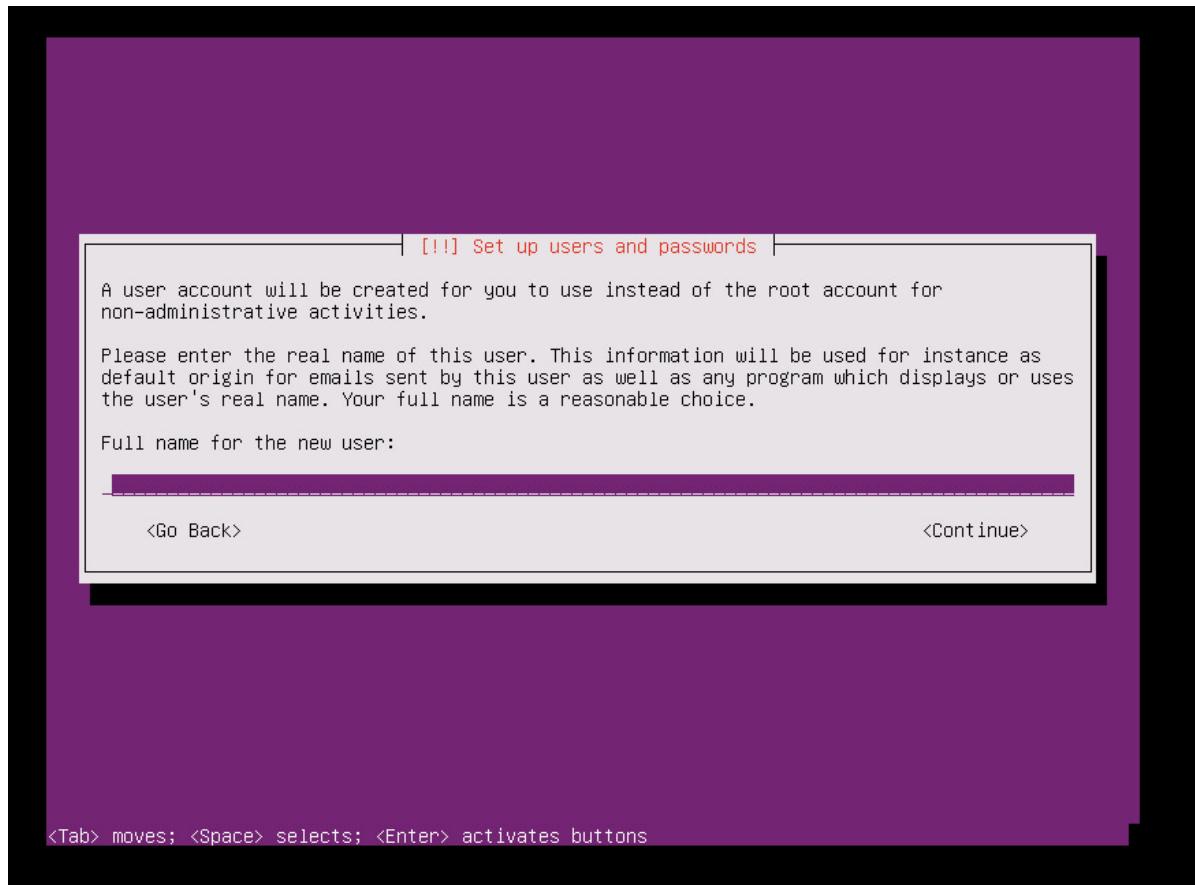
6. Select **No** (the default option), and then select **Enter**.



<Tab> moves; <Space> selects; <Enter> activates buttons

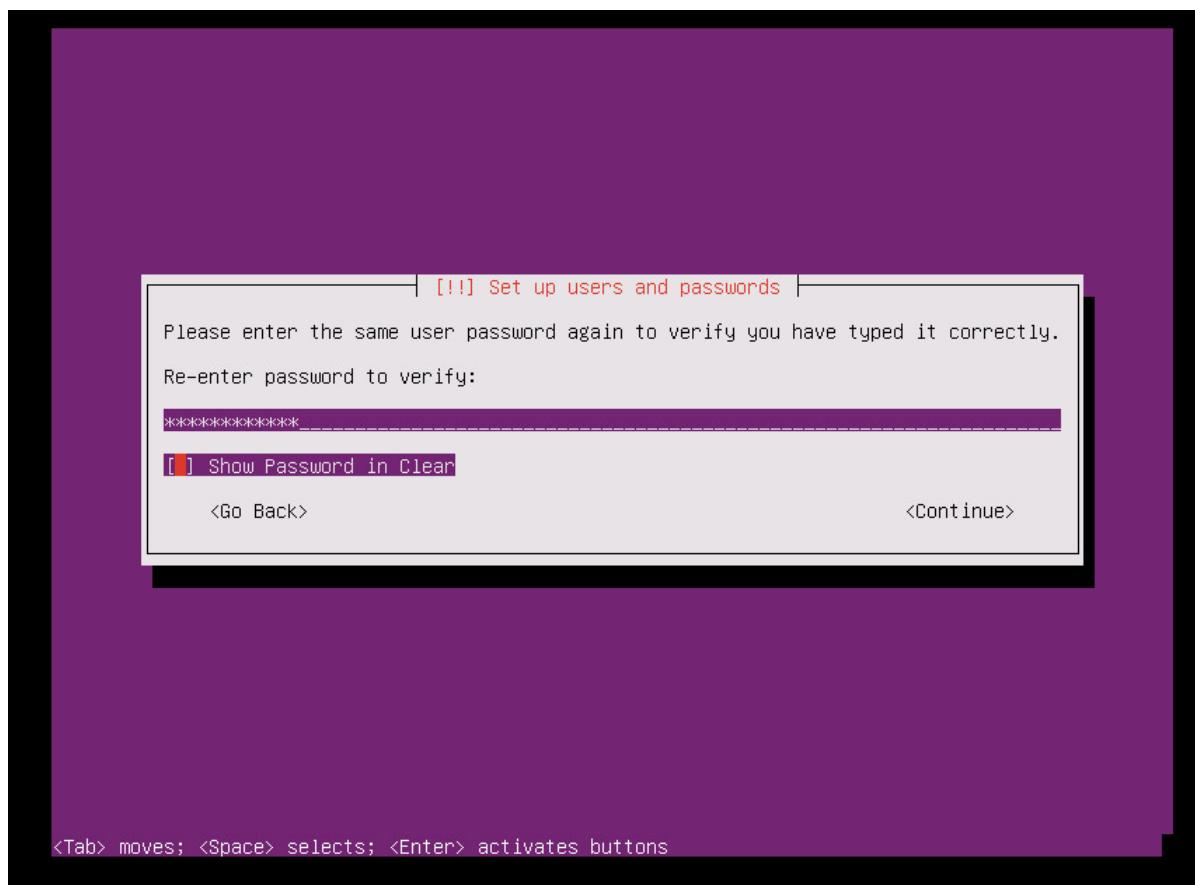
7. Select **English (US)** as the country/region of origin for the keyboard, and then select **Enter**.
8. Select **English (US)** as the keyboard layout, and then select **Enter**.
9. Enter the hostname for your server in the **Hostname** box, and then select **Continue**.

10. To create a user account, enter the user name, and then select **Continue**.



11. Enter the password for the new user account, and then select **Continue**.

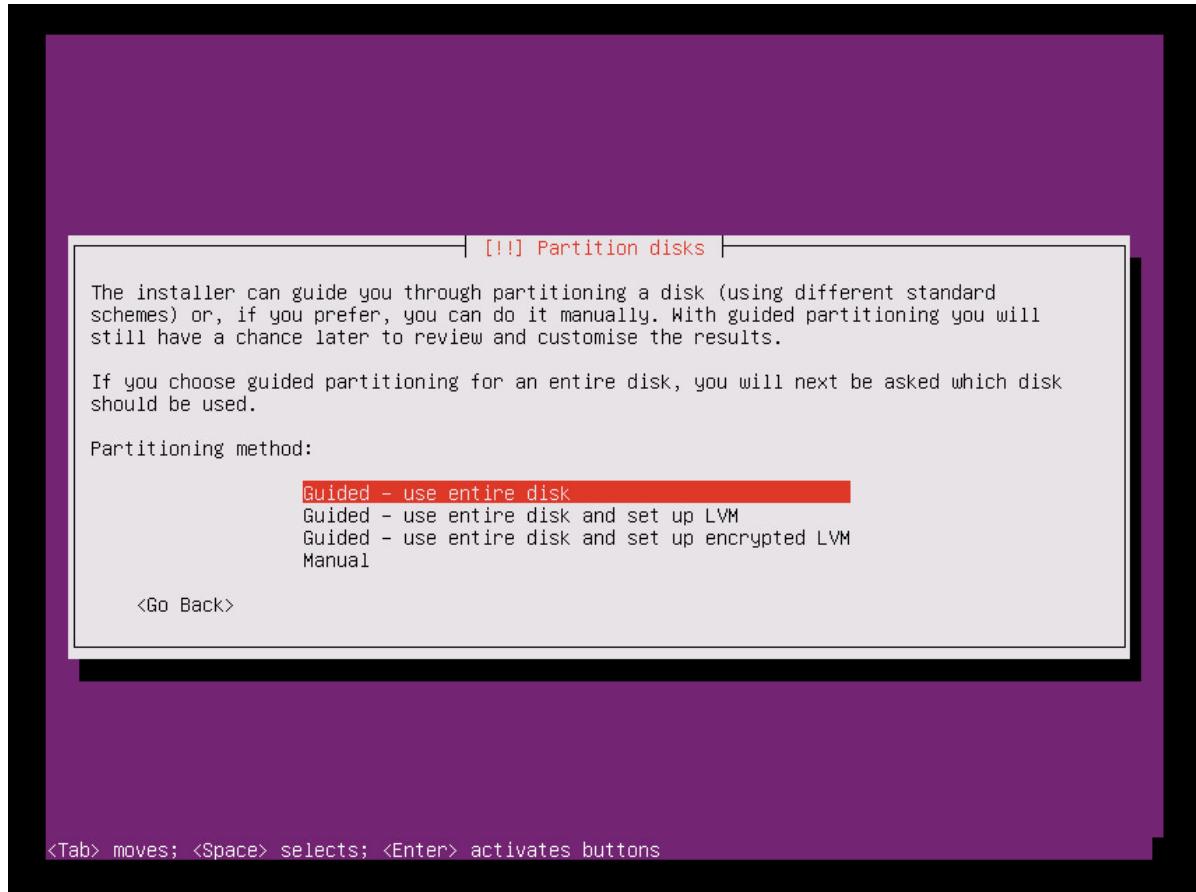
12. Confirm the password for the new user, and then select **Continue**.



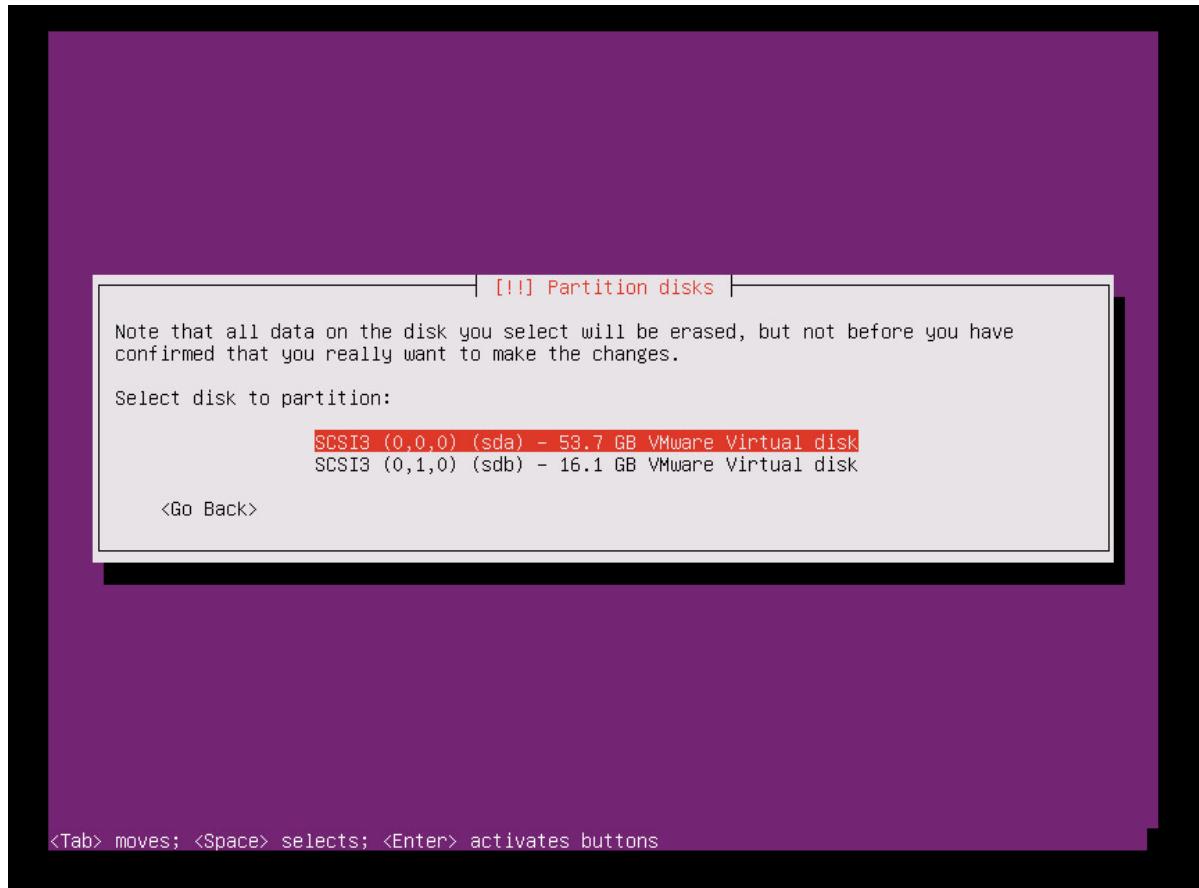
13. In the next selection for encrypting your home directory, select **No** (the default option), and then select

Enter.

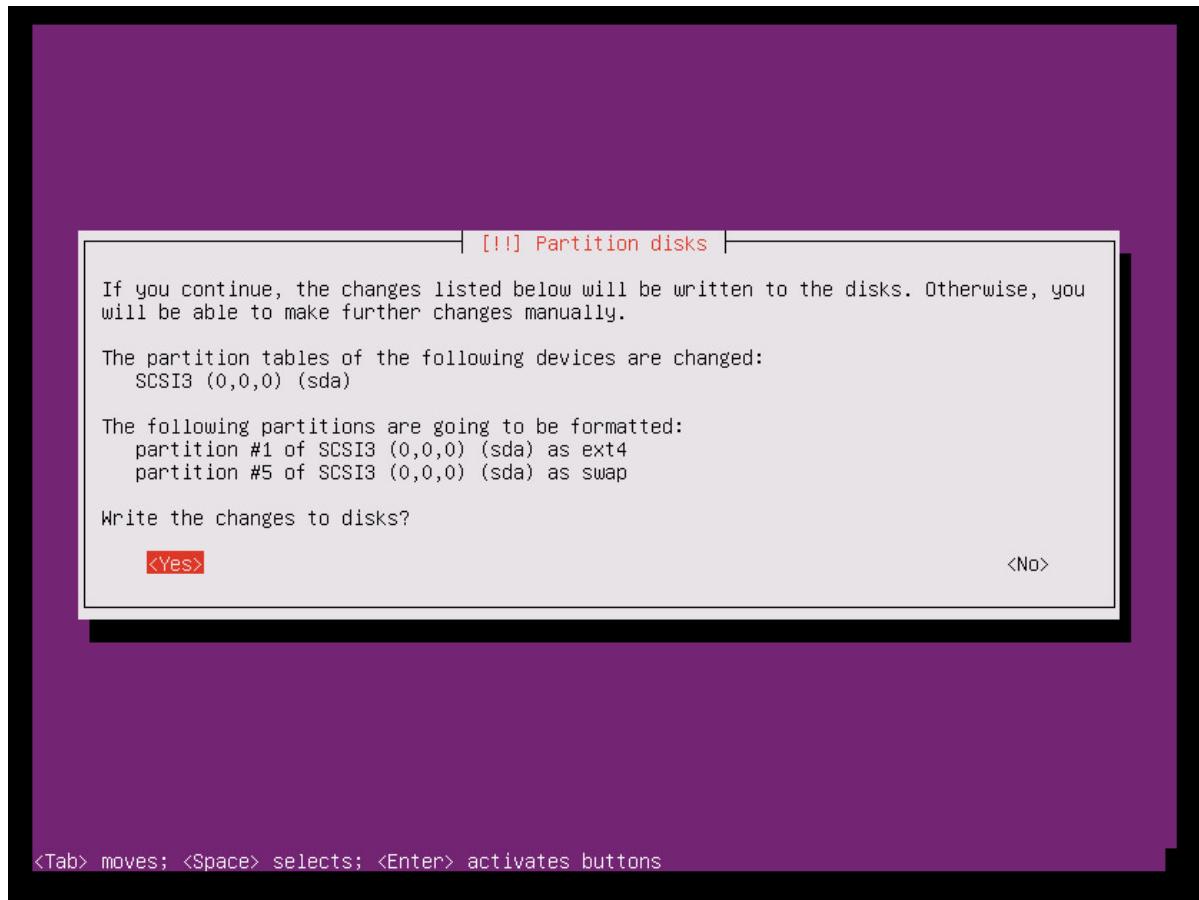
14. If the time zone that's displayed is correct, select **Yes** (the default option), and then select **Enter**. To reconfigure your time zone, select **No**.
15. From the partitioning method options, select **Guided - use entire disk**, and then select **Enter**.



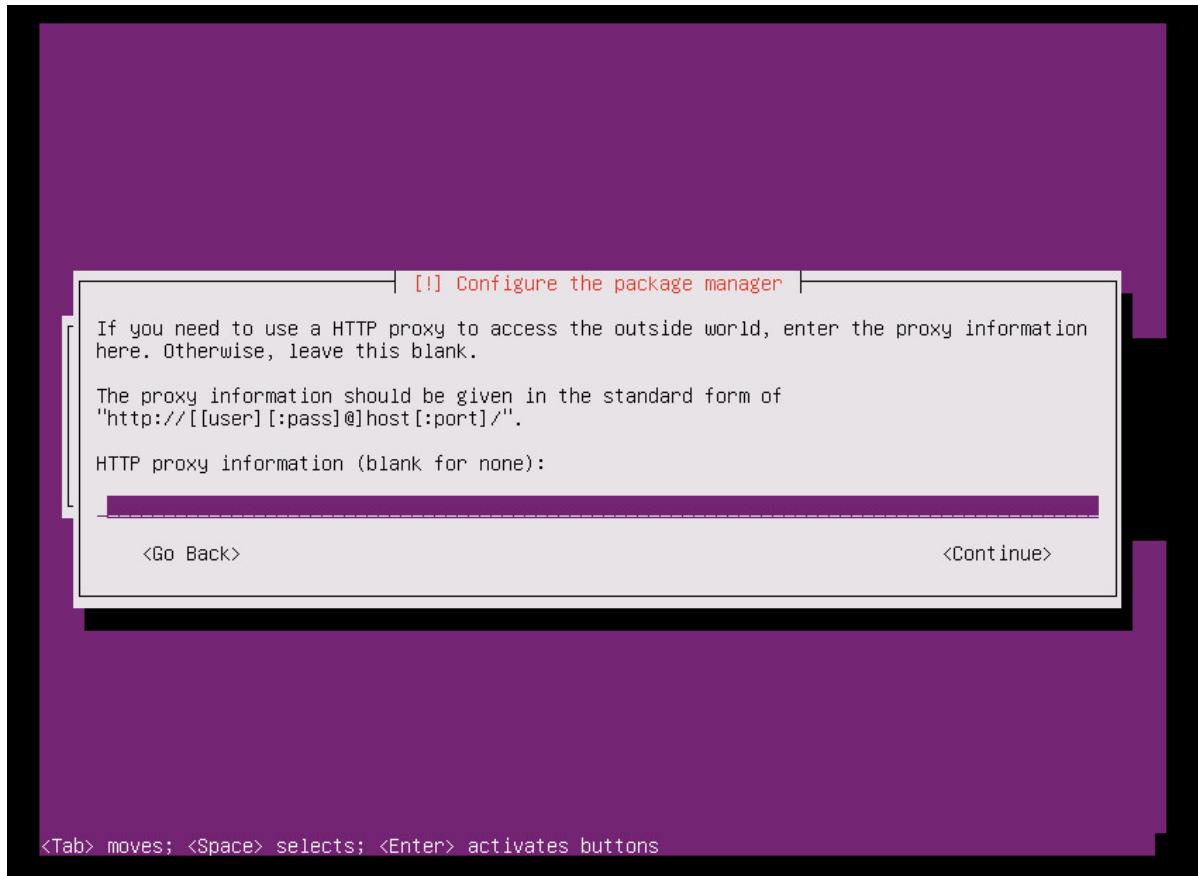
16. Select the appropriate disk from the **Select disk to partition** options, and then select **Enter**.



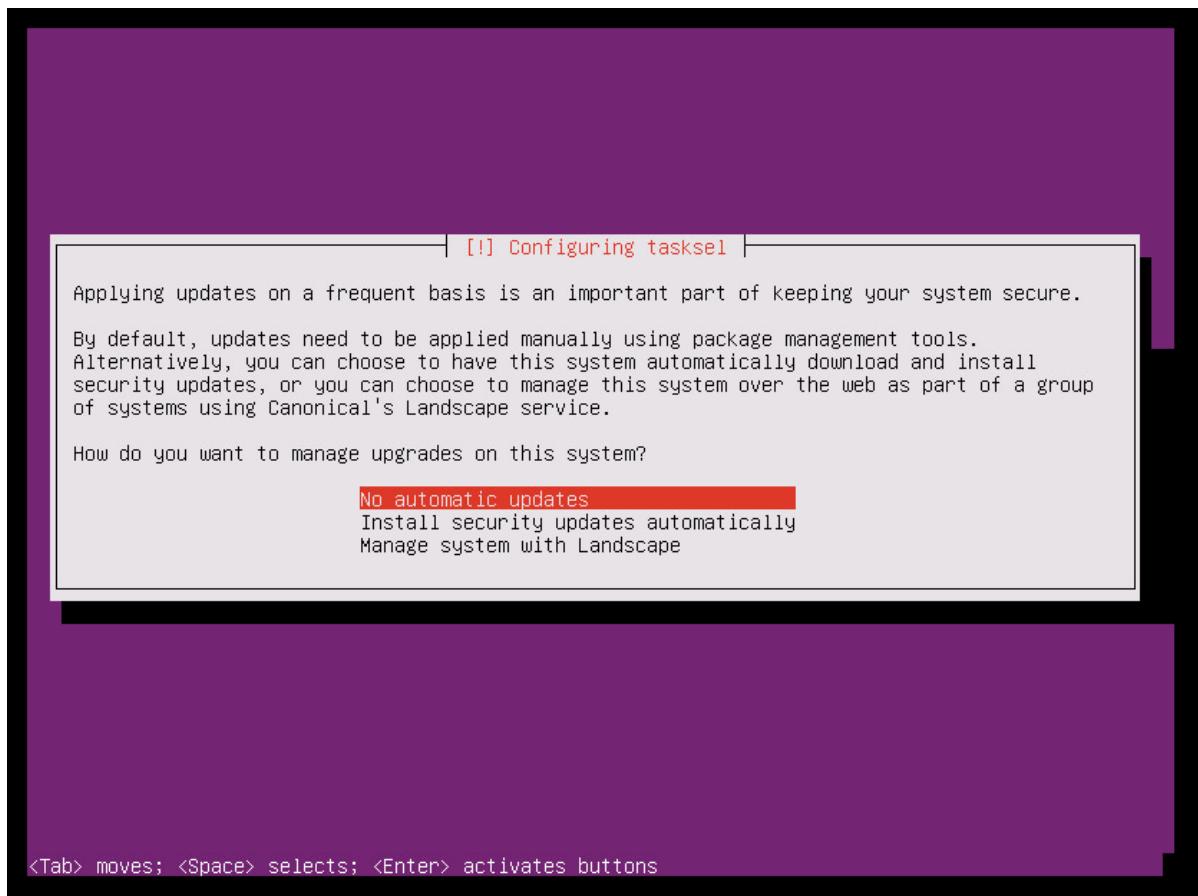
17. Select **Yes** to write the changes to disk, and then select **Enter**.



18. In the configure proxy selection, select the default option, select **Continue**, and then select **Enter**.



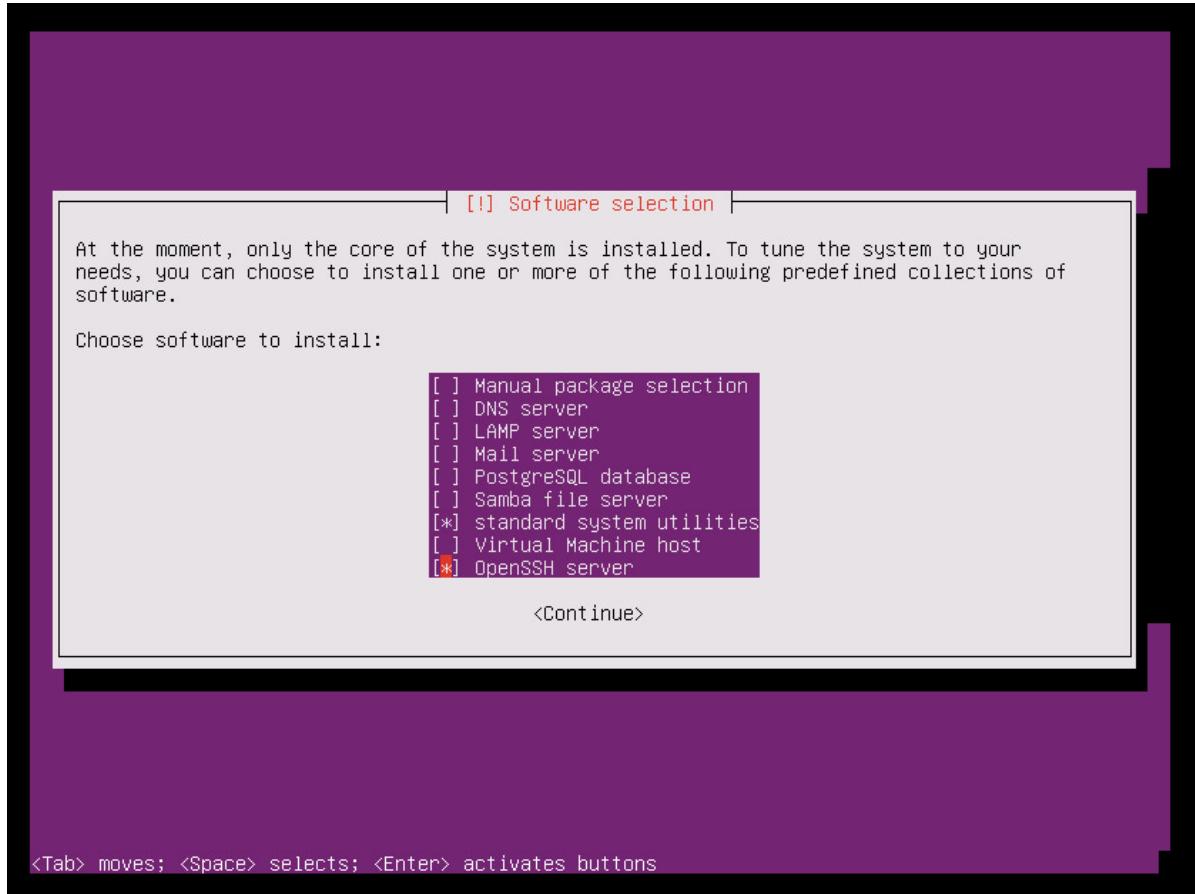
19. Select **No automatic updates** option in the selection for managing upgrades on your system, and then select **Enter**.



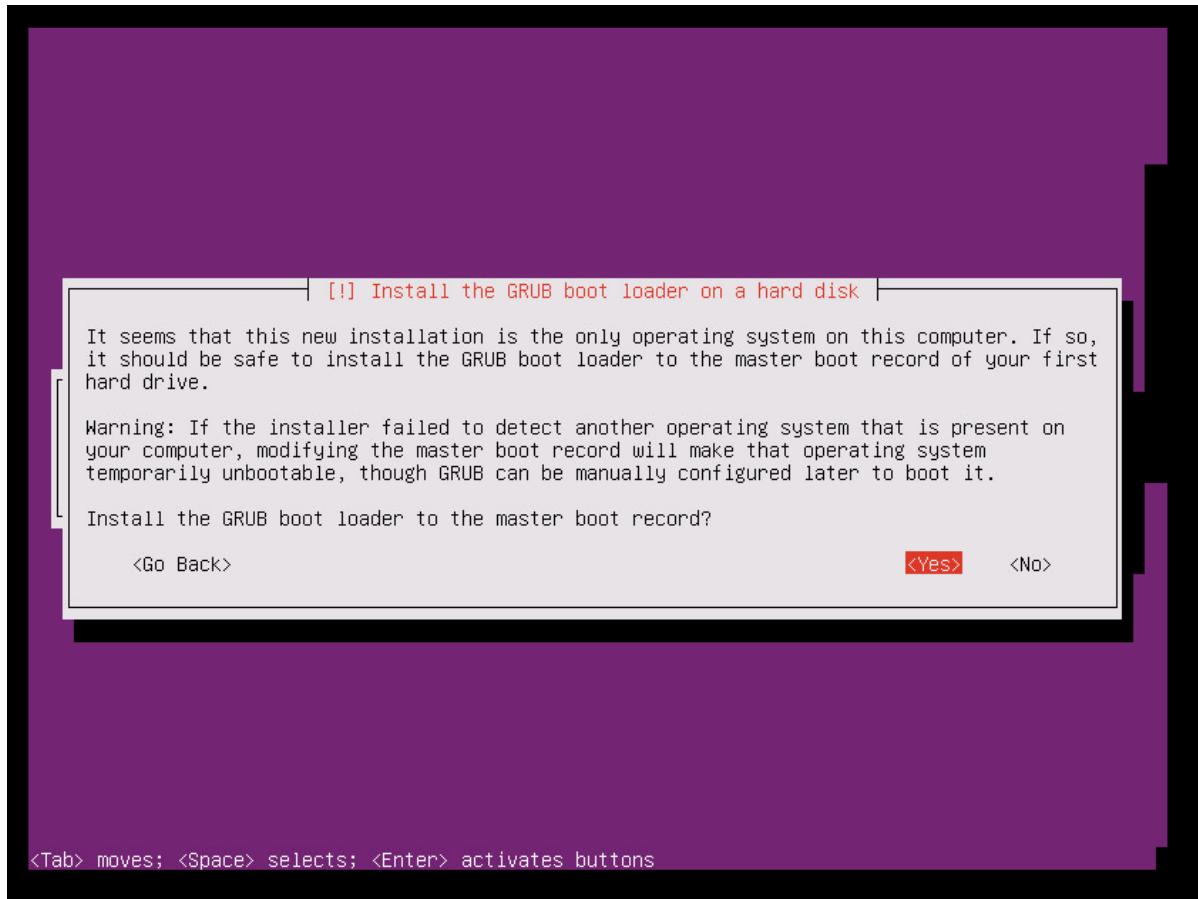
WARNING

Because the Azure Site Recovery master target server requires a very specific version of the Ubuntu, you need to ensure that the kernel upgrades are disabled for the virtual machine. If they are enabled, then any regular upgrades cause the master target server to malfunction. Make sure you select the **No automatic updates** option.

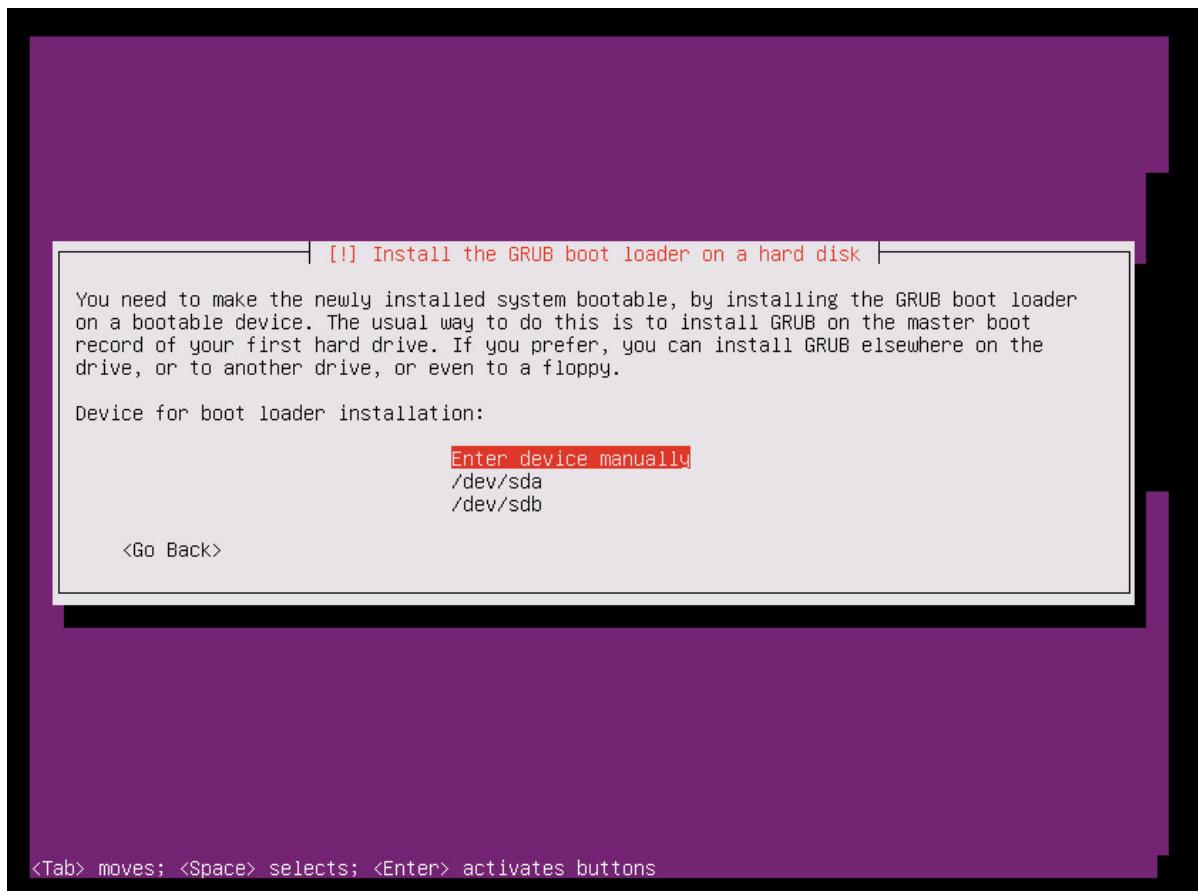
20. Select default options. If you want openSSH for SSH connect, select the **OpenSSH server** option, and then select **Continue**.



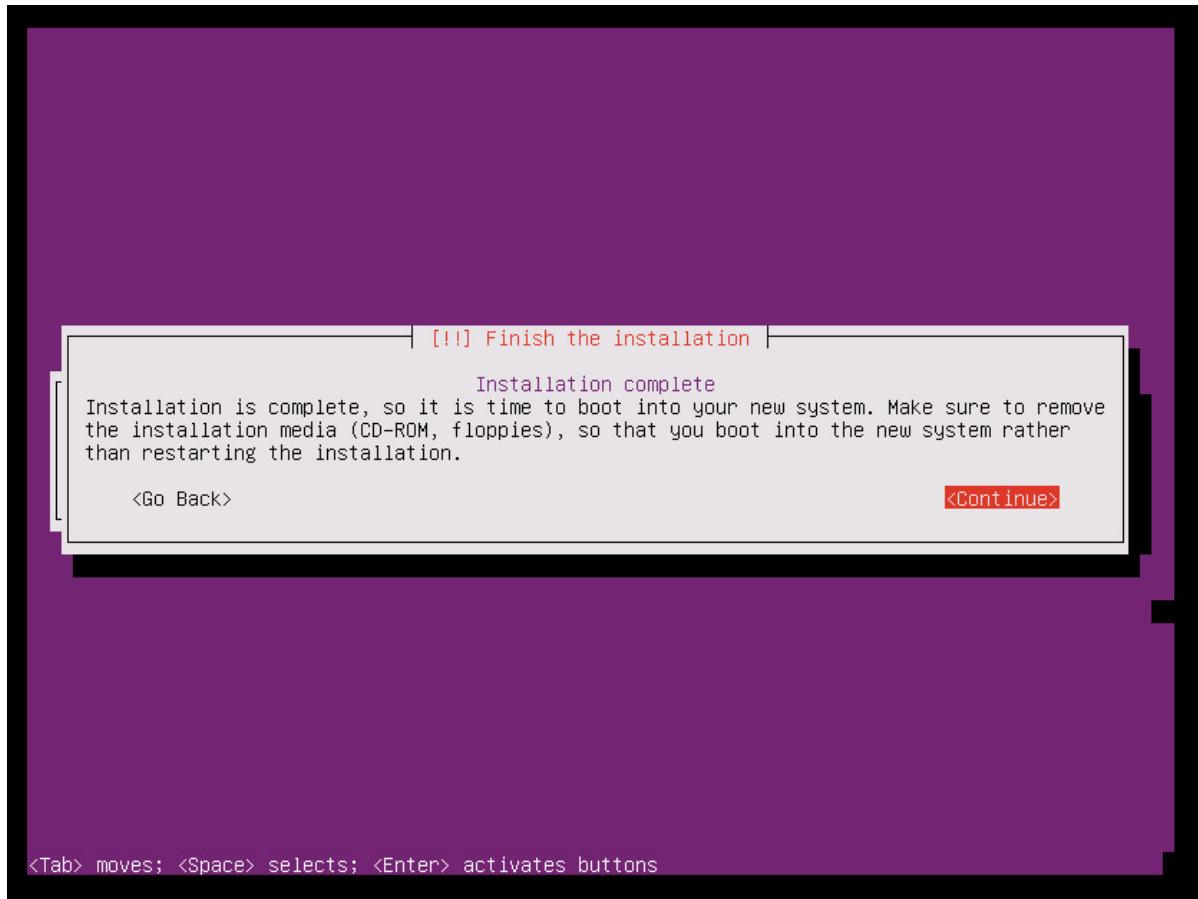
21. In the selection for installing the GRUB boot loader, Select **Yes**, and then select **Enter**.



22. Select the appropriate device for the boot loader installation (preferably **/dev/sda**), and then select **Enter**.



23. Select **Continue**, and then select **Enter** to finish the installation.



24. After the installation has finished, sign in to the VM with the new user credentials. (Refer to **Step 10** for more information.)
25. Use the steps that are described in the following screenshot to set the ROOT user password. Then sign in as ROOT user.

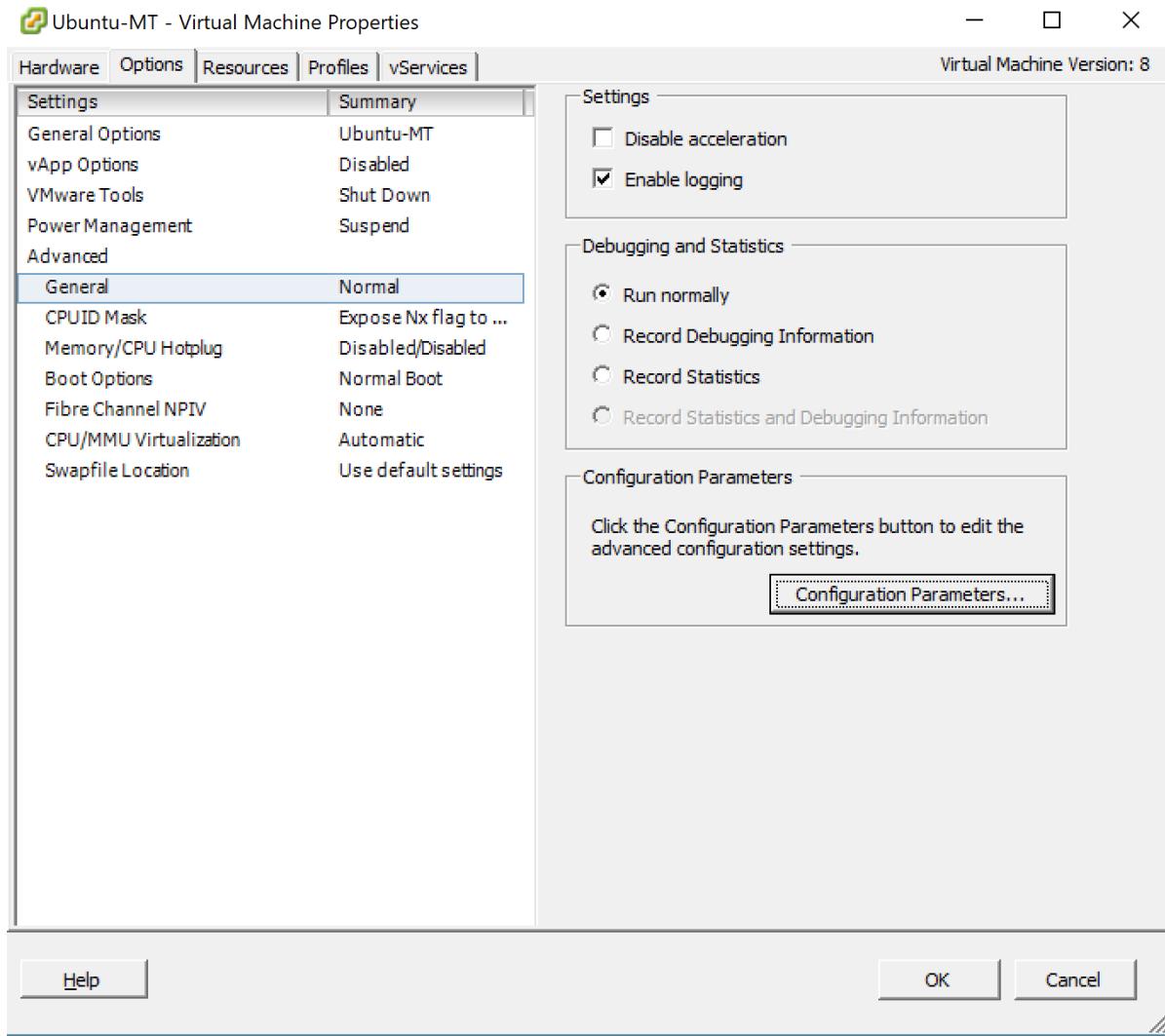
```
mtuser@UbuntuMT:~#  
mtuser@UbuntuMT:~# sudo passwd root  
[sudo] password for mtuser:  
Enter new UNIX password:  
Retype new UNIX password:  
passwd: password updated successfully  
mtuser@UbuntuMT:~#  
mtuser@UbuntuMT:~#  
mtuser@UbuntuMT:~# su  
Password:  
root@UbuntuMT:~#
```

A terminal window showing the command 'sudo passwd root' being run. It prompts for the password of the current user ('mtuser') and then asks for a new password for the root user. After entering the new password twice and confirming its success, the user then runs 'su' to switch to the root account.

Configure the machine as a master target server

To get the ID for each SCSI hard disk in a Linux virtual machine, the **disk.EnableUUID = TRUE** parameter needs to be enabled. To enable this parameter, take the following steps:

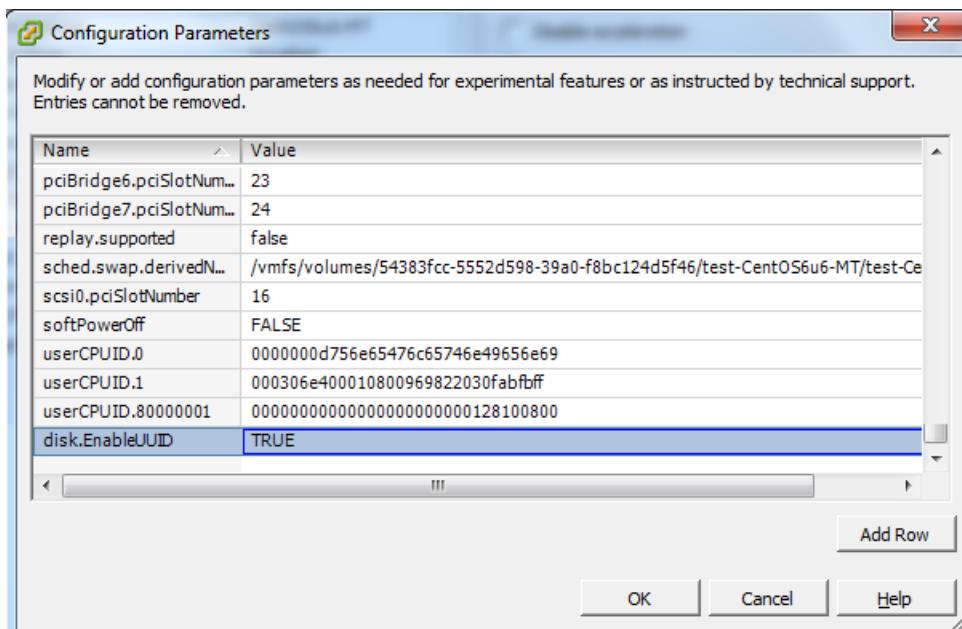
1. Shut down your virtual machine.
2. Right-click the entry for the virtual machine in the left pane, and then select **Edit Settings**.
3. Select the **Options** tab.
4. In the left pane, select **Advanced > General**, and then select the **Configuration Parameters** button on the lower-right part of the screen.



The **Configuration Parameters** option is not available when the machine is running. To make this tab active, shut down the virtual machine.

5. See whether a row with **disk.EnableUUID** already exists.

- If the value exists and is set to **False**, change the value to **True**. (The values are not case-sensitive.)
- If the value exists and is set to **True**, select **Cancel**.
- If the value does not exist, select **Add Row**.
- In the name column, add **disk.EnableUUID**, and then set the value to **TRUE**.



Disable kernel upgrades

Azure Site Recovery master target server requires a specific version of the Ubuntu, ensure that the kernel upgrades are disabled for the virtual machine. If kernel upgrades are enabled, it can cause the master target server to malfunction.

Download and install additional packages

NOTE

Make sure that you have Internet connectivity to download and install additional packages. If you don't have Internet connectivity, you need to manually find these Deb packages and install them.

```
apt-get install -y multipath-tools lsscsi python-pyasn1 lvm2 kpartx
```

Get the installer for setup

If your master target has Internet connectivity, you can use the following steps to download the installer. Otherwise, you can copy the installer from the process server and then install it.

Download the master target installation packages

[Download the latest Linux master target installation bits.](#)

To download it using Linux, type:

```
wget https://aka.ms/latestlinuxmobsvc -O latestlinuxmobsvc.tar.gz
```

WARNING

Make sure that you download and unzip the installer in your home directory. If you unzip to **/usr/Local**, then the installation fails.

Access the installer from the process server

1. On the process server, go to **C:\Program Files (x86)\Microsoft Azure Site Recovery\home\svsystems\pushinstallsvc\repository**.
2. Copy the required installer file from the process server, and save it as **latestlinuxmobsvc.tar.gz** in your home directory.

Apply custom configuration changes

To apply custom configuration changes, use the following steps as a ROOT user:

1. Run the following command to untar the binary.

```
tar -xvf latestlinuxmobsvc.tar.gz
```

```
[csadmin@ContosoLinMT1 ~]$ [csadmin@ContosoLinMT1 ~]$ tar -xvzf Microsoft-ASR_UA_8.2.0.0_RHEL6-64_00000000000000000000000000000000.tar.gz
```

2. Run the following command to give permission.

```
chmod 755 ./ApplyCustomChanges.sh
```

3. Run the following command to run the script.

```
./ApplyCustomChanges.sh
```

NOTE

Run the script only once on the server. Then shut down the server. Restart the server after you add a disk, as described in the next section.

Add a retention disk to the Linux master target virtual machine

Use the following steps to create a retention disk:

1. Attach a new 1-TB disk to the Linux master target virtual machine, and then start the machine.
2. Use the **multipath -ll** command to learn the multipath ID of the retention disk: **multipath -ll**

```
[root@NAR-FBLINMT 31dec]# multipath -ll  
36000c2989daa2fe6dddcde67f2079afe dm-2 VMware,Virtual disk  
size=40G features='0' hwhandler='0' wp=rw  
`-- policy='round-robin 0' prio=1 status=active  
  `-- 2:0:1:0 sdb 8:16 active ready running  
[root@NAR-FBLINMT 31dec]#
```

3. Format the drive, and then create a file system on the new drive: **mkfs.ext4 /dev/mapper/<Retention disk's multipath id>**.

```
[root@NAR-FBLINMT 31dec]# mkfs.ext4 /dev/mapper/36000c2989daa2fe6dddcde67f2079afe  
mke2fs 1.41.12 (17-May-2010)  
Filesystem label=  
OS type: Linux  
Block size=4096 (log=2)  
Fragment size=4096 (log=2)  
Stride=0 blocks, Stripe width=0 blocks  
2621440 inodes, 10485760 blocks  
524288 blocks (5.00%) reserved for the super user  
First data block=0  
Maximum filesystem blocks=4294967296  
320 block groups  
32768 blocks per group, 32768 fragments per group  
8192 inodes per group  
Superblock backups stored on blocks:  
    32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,  
    4096000, 7962624  
  
Writing inode tables: done  
Creating journal (32768 blocks): done  
Writing superblocks and filesystem accounting information: done  
  
This filesystem will be automatically checked every 21 mounts or  
180 days, whichever comes first.  Use tune2fs -c or -i to override.  
[root@NAR-FBLINMT 31dec]#
```

4. After you create the file system, mount the retention disk.

```
mkdir /mnt/retention  
mount /dev/mapper/<Retention disk's multipath id> /mnt/retention
```

5. Create the **fstab** entry to mount the retention drive every time the system starts.

```
vi /etc/fstab
```

Select **Insert** to begin editing the file. Create a new line, and then insert the following text. Edit the disk multipath ID based on the highlighted multipath ID from the previous command.

/dev/mapper/<Retention disks multipath id> /mnt/retention ext4 rw 0 0

Select **Esc**, and then type **:wq** (write and quit) to close the editor window.

Install the master target

IMPORTANT

The version of the master target server must be equal to or earlier than the versions of the process server and the configuration server. If this condition is not met, reprotect succeeds, but replication fails.

NOTE

Before you install the master target server, check that the **/etc/hosts** file on the virtual machine contains entries that map the local hostname to the IP addresses that are associated with all network adapters.

1. Copy the passphrase from **C:\ProgramData\Microsoft Azure Site Recovery\private\connection.passphrase** on the configuration server. Then save it as **passphrase.txt** in the same local directory by running the following command:

```
echo <passphrase> >passphrase.txt
```

Example:

```
`echo iTUx70I47uxDuUVY >passphrase.txt`
```

2. Note down the configuration server's IP address. Run the following command to install the master target server and register the server with the configuration server.

```
/usr/local/ASR/Vx/bin/UnifiedAgentConfigurator.sh -i <ConfigurationServer IP Address> -P passphrase.txt
```

Example:

```
/usr/local/ASR/Vx/bin/UnifiedAgentConfigurator.sh -i 104.40.75.37 -P passphrase.txt
```

Wait until the script finishes. If the master target registers successfully, the master target is listed on the **Site Recovery Infrastructure** page of the portal.

Install the master target by using interactive installation

1. Run the following command to install the master target. For the agent role, choose **master target**.

```
./install
```

2. Choose the default location for installation, and then select **Enter** to continue.

```
[csadmin@ContosoLinMT1 ~]$ sudo ./install

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

#1) Respect the privacy of others.
#2) Think before you type.
#3) With great power comes great responsibility.

[sudo] password for csadmin:

Where do you want to install the agent (default /usr/local/ASR) :

Generating the certificate.

The chosen configuration for this VX is host based configuration...
Checking OS compatibility before installation...

Checking whether RPM package is present...
RPM architecture found is x86_64.

What is the Primary Role of this Agent ?

1. Mobility Service

Select 'Mobility Service' for installation on servers that need to be protected, or
for servers that act as targets in a failover/failback situation.

2. Master Target

Select 'Master Target' for installation on a hypervisor virtual machine that acts
as the protection target for other protected physical or virtual servers.

Please make your choice ? (1/2) [Default: 1] 2
Configuring Master Target. It takes at least 15 minutes.

[
```

After the installation has finished, register the configuration server by using the command line.

1. Note the IP address of the configuration server. You need it in the next step.
2. Run the following command to install the master target server and register the server with the configuration server.

```
./install -q -d /usr/local/ASR -r MT -v VmWare
/usr/local/ASR/Vx/bin/UnifiedAgentConfigurator.sh -i <ConfigurationServer IP Address> -P
passphrase.txt
```

Example:

```
/usr/local/ASR/Vx/bin/UnifiedAgentConfigurator.sh -i 104.40.75.37 -P passphrase.txt
```

Wait until the script finishes. If the master target is registered successfully, the master target is listed on the **Site Recovery Infrastructure** page of the portal.

Install VMware tools / open-vm-tools on the master target server

You need to install VMware tools or open-vm-tools on the master target so that it can discover the data stores. If the tools are not installed, the reprotect screen isn't listed in the data stores. After installation of the VMware tools, you need to restart.

Upgrade the master target server

Run the installer. It automatically detects that the agent is installed on the master target. To upgrade, select **Y**. After the setup has been completed, check the version of the master target installed by using the following command:

```
cat /usr/local/.vx_version
```

You will see that the **Version** field gives the version number of the master target.

Common issues

- Make sure you do not turn on Storage vMotion on any management components such as a master target. If the master target moves after a successful reprotect, the virtual machine disks (VMDKs) cannot be detached. In this case, failback fails.
- The master target should not have any snapshots on the virtual machine. If there are snapshots, failback fails.
- Due to some custom NIC configurations, the network interface is disabled during startup, and the master target agent cannot initialize. Make sure that the following properties are correctly set. Check these properties in the Ethernet card file's /etc/sysconfig/network-scripts/ifcfg-eth*.
 - BOOTPROTO=dhcp
 - ONBOOT=yes

Next steps

After the installation and registration of the master target has finished, you can see the master target appear on the **master target** section in **Site Recovery Infrastructure**, under the configuration server overview.

You can now proceed with [reprotection](#), followed by failback.

Manage the Mobility agent

11/12/2019 • 2 minutes to read • [Edit Online](#)

You set up mobility agent on your server when you use Azure Site Recovery for disaster recovery of VMware VMs and physical servers to Azure. Mobility agent coordinates communications between your protected machine, configuration server/scale-out process server and manages data replication. This article summarizes common tasks for managing mobility agent after it's deployed.

NOTE

This article has been updated to use the new Azure PowerShell Az module. You can still use the AzureRM module, which will continue to receive bug fixes until at least December 2020. To learn more about the new Az module and AzureRM compatibility, see [Introducing the new Azure PowerShell Az module](#). For Az module installation instructions, see [Install Azure PowerShell](#).

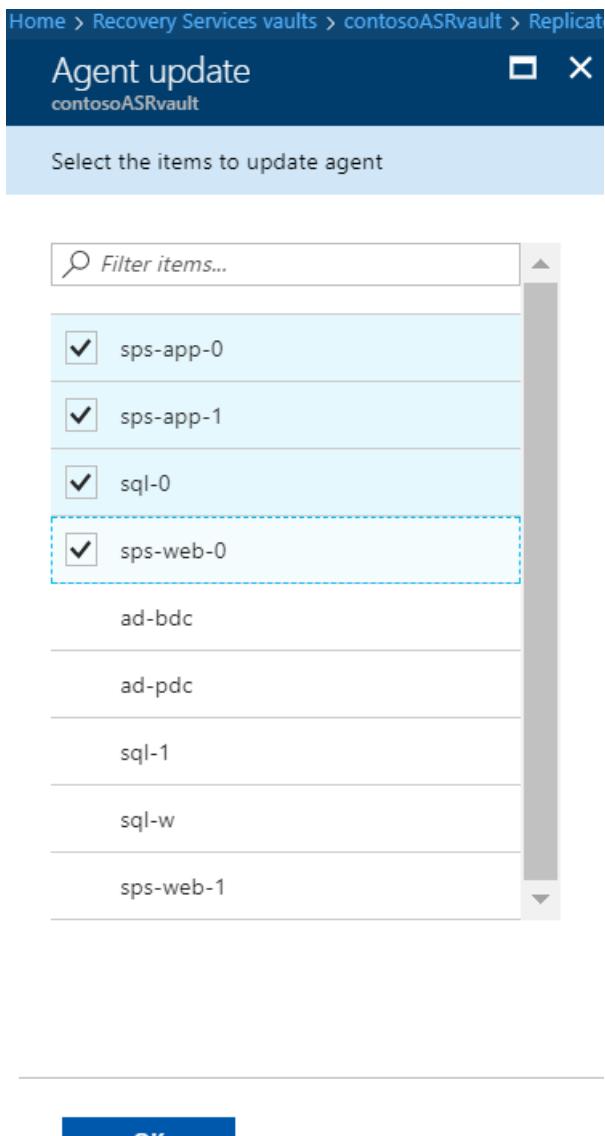
Update mobility service from Azure portal

1. Before you start ensure that the configuration server, scale-out process servers, and any master target servers that are a part of your deployment are updated before you update the Mobility Service on protected machines.
2. In the portal open the vault > **Replicated items**.
3. If the configuration server is the latest version, you see a notification that reads "New Site recovery replication agent update is available. Click to install."

The screenshot shows the Azure portal interface for managing replicated items. At the top, there are buttons for Refresh, Replicate, Columns, and Filter. A yellow banner displays a warning: "⚠️ New Mobility Service Update is available. Push install latest update on every physical and virtual machine →". Below the banner, a message says "Last refreshed at: 11/14/2019, 9:34:41 AM". A progress bar indicates "Finished loading data from service." The main table has columns: Name, Replication Health, Status, and Active location. One item is listed: Name is "VMware", Replication Health is "Healthy" (indicated by a green circle), Status is "Protected", and Active location is "Azure".

Name	Replication Health	Status	Active location
VMware	Healthy	Protected	Azure

4. Click the notification, and in **Agent update**, select the machines on which you want to upgrade the Mobility service. Then click **OK**.



5. The Update Mobility Service job starts for each of the selected machines.

Update Mobility service through powershell script on Windows server

Use following script to upgrade mobility service on a server through power shell cmdlet

```
Update-AzRecoveryServicesAsrMobilityService -ReplicationProtectedItem $rpi -Account  
$fabric.fabricSpecificDetails.RunAsAccounts[0]
```

Update account used for push installation of Mobility service

When you deployed Site Recovery, to enable push installation of the Mobility service, you specified an account that the Site Recovery process server uses to access the machines and install the service when replication is enabled for the machine. If you want to update the credentials for this account, follow [these instructions](#).

Uninstall Mobility service

On a Windows machine

Uninstall from the UI or from a command prompt.

- **From the UI:** In the Control Panel of the machine, select **Programs**. Select **Microsoft Azure Site Recovery Mobility Service/Master Target server** > **Uninstall**.

- **From a command prompt:** Open a command prompt window as an administrator on the machine. Run the following command:

```
MsiExec.exe /qn /x {275197FC-14FD-4560-A5EB-38217F80CBD1} /L+*V  
"C:\ProgramData\ASRSetupLogs\UnifiedAgentMSIUninstall.log"
```

On a Linux machine

1. On the Linux machine, sign in as a **root** user.
2. In a terminal, go to /usr/local/ASR.
3. Run the following command:

```
uninstall.sh -Y
```

Install Site Recovery VSS provider on source machine

Azure Site Recovery VSS provider is required on the source machine to generate application consistency points. If the installation of the provider didn't succeed through push installation, follow the below given guidelines to install it manually.

1. Open admin cmd window.
2. Navigate to the mobility service installation location. (Eg - C:\Program Files (x86)\Microsoft Azure Site Recovery\agent)
3. Run the script InMageVSSProvider_Uninstall.cmd . This will uninstall the service if it already exists.
4. Run the script InMageVSSProvider_Install.cmd to install the VSS provider manually.

Next steps

- [Set up disaster recovery for VMware VMs](#)
- [Set up disaster recovery for physical servers](#)

Manage the configuration server for VMware VM/physical server disaster recovery

11/12/2019 • 10 minutes to read • [Edit Online](#)

You set up an on-premises configuration server when you use [Azure Site Recovery](#) for disaster recovery of VMware VMs and physical servers to Azure. The configuration server coordinates communications between on-premises VMware and Azure and manages data replication. This article summarizes common tasks for managing the configuration server after it's deployed.

NOTE

This article has been updated to use the new Azure PowerShell Az module. You can still use the AzureRM module, which will continue to receive bug fixes until at least December 2020. To learn more about the new Az module and AzureRM compatibility, see [Introducing the new Azure PowerShell Az module](#). For Az module installation instructions, see [Install Azure PowerShell](#).

Update Windows license

The license provided with the OVF template is an evaluation license valid for 180 days. For uninterrupted usage, you must activate Windows with a procured license. License update can be done either through a standalone key or KMS standard key. Guidance is available at [DISM Windows command line for running OS](#). To obtain keys, refer to [KMS client set up](#).

Access configuration server

You can access the configuration server as follows:

- Sign in to the VM on which it's deployed, and Start **Azure Site Recovery Configuration Manager** from the desktop shortcut.
- Alternatively, you can access the configuration server remotely from <https://ConfigurationServerName:44315/>. Sign in with administrator credentials.

Modify VMware server settings

1. To associate a different VMware server with the configuration server, after [sign-in](#), select **Add vCenter Server/vSphere ESXi server**.
2. Enter the details, and then select **OK**.

Modify credentials for automatic discovery

1. To update the credentials used to connect to the VMware server for automatic discovery of VMware VMs, after [sign-in](#), choose the account and click **Edit**.
2. Enter the new credentials, and then select **OK**.

Modify VMware vCenter Server details and credentials

1. Log in to your Configuration server.
2. Launch the Azure Site Recovery Configuration Manager using the shortcut on your desktop.

Tip

The Configuration server can also be managed remotely using the <https://ConfigurationServerName/IP:44315>

3. Click on the **Manage vCenter Server/vSphere ESXi server**.

View/Edit configuration

 Manage connectivity
Establish communication to Microsoft Azure

 Recovery Services vault
Details of the vault to which the Configuration server is registered

 Manage vCenter Server/vSphere ESXi server credentials
To discover virtual machines managed by your vCenter Server/vSphere ESXi server

List of connected vCenter servers/vSphere ESXi hosts

Server name/IP	Server friendly name	Port	Account friendly name	Actions
vCenter01	MyVCenter	443	MyCredential	Edit Delete

Add vCenter Server/vSphere ESXi server

I do not have vCenter Server/vSphere ESXi server. I'll protect my servers by manually discovering them using IP addresses.

You can also modify the credentials through CSPSCfgtool.exe.

1. Login to the configuration server and launch CSPSCfgtool.exe
2. Choose the account you wish to modify and click **Edit**.
3. Enter the modified credentials and click **Ok**

Modify credentials for Mobility Service installation

Modify the credentials used to automatically install Mobility Service on the VMware VMs you enable for replication.

1. After [sign-in](#), select **Manage virtual machine credentials**
2. Choose the account you wish to modify and click **Edit**
3. Enter the new credentials, and then select **OK**.



Configure vCenter Server/vSphere ESXi server credentials

To discover virtual machines managed by your vCenter Server/vSphere ESXi server



Configure virtual machine credentials

To install Azure Site Recovery mobility service on virtual machines/physical servers that need to be protected

List of credentials

Operating system	Account friendly name	User name	
Windows	Windows	[REDACTED]	Edit Delete
Linux	Linux	[REDACTED]	Edit Delete

[Add virtual machine credentials](#)

I do not want to provide credentials here, I'll manually install mobility service on my servers before I enable protection.

Adding virtual machine credentials successful

[Continue](#)

You can also modify credentials through CSPSConfigtool.exe.

1. Log in to the configuration server and launch CSPSConfigtool.exe
2. Choose the account you wish to modify and click **Edit**
3. Enter the new credentials and click **Ok**.

Add credentials for Mobility service installation

If you missed adding credentials during OVF deployment of configuration server,

1. After [sign-in](#), select **Manage virtual machine credentials**.
2. Click on **Add virtual machine credentials**.

The screenshot shows a list of configuration tasks:

- Manage connectivity**: Establish communication to Microsoft Azure.
- Recovery Services vault**: Details of the vault to which the Configuration server is registered.
- Manage vCenter Server/vSphere ESXi server credentials**: To discover virtual machines managed by your vCenter Server/vSphere ESXi server.
- Manage virtual machine credentials**: To install Azure Site Recovery mobility service on virtual machines/physical servers that need to be protected.

List of credentials

Operating system	Account friendly name	User name	Actions
Windows	[redacted]	[redacted]	Edit Delete
Linux	[redacted]	[redacted]	Edit Delete

Add virtual machine credentials (button highlighted with a red box)

I do not want to provide credentials here, I'll manually install mobility service on my servers before I enable protection.

3. Enter the new credentials and click on **Add**.

You can also add credentials through CSPSConfigtool.exe.

1. Log in to the configuration server and launch CSPSConfigtool.exe
2. Click **Add**, enter the new credentials and click **Ok**.

Modify proxy settings

Modify the proxy settings used by the configuration server machine for internet access to Azure. If you have a process server machine in addition to the default process server running on the configuration server machine, modify the settings on both machines.

1. After [sign-in](#) to the configuration server, select **Manage connectivity**.
2. Update the proxy values. Then select **Save** to update the settings.

Add a network adapter

The Open Virtualization Format (OVF) template deploys the configuration server VM with a single network adapter.

- You can [add an additional adapter to the VM](#), but you must add it before you register the configuration server in the vault.
- To add an adapter after you register the configuration server in the vault, add the adapter in the VM properties. Then you need to [re-register](#) the server in the vault.

Reregister a configuration server in the same vault

You can reregister the configuration server in the same vault if you need to. If you have an additional process server machine, in addition to the default process server running on the configuration server machine, reregister

both machines.

1. In the vault, open **Manage > Site Recovery Infrastructure > Configuration Servers**.
2. In **Servers**, select **Download registration key** to download the vault credentials file.
3. Sign in to the configuration server machine.
4. In **%ProgramData%\ASR\home\svsystems\bin**, open **cspconfigtool.exe**.
5. On the **Vault Registration** tab, select **Browse**, and locate the vault credentials file that you downloaded.
6. If needed, provide proxy server details. Then select **Register**.
7. Open an admin PowerShell command window, and run the following command:

```
$pwd = ConvertTo-SecureString -String MyProxyUserPassword  
Set-OBMachineSetting -ProxyServer http://myproxyserver.domain.com -ProxyPort PortNumber -  
ProxyUserName domain\username -ProxyPassword $pwd
```

NOTE

In order to **pull latest certificates** from configuration server to scale-out process server execute the command "
<Installation Drive\Microsoft Azure Site Recovery\agent\cdpcli.exe>" --registermt

8. Finally, restart the obengine by executing the following command.

```
net stop obengine  
net start obengine
```

Register a configuration server with a different vault

WARNING

The following step disassociates the configuration server from the current vault, and the replication of all protected virtual machines under the configuration server is stopped.

1. Log in to the configuration server.
2. Open an admin PowerShell command window, and run the following command:

```
reg delete "HKLM\Software\Microsoft\Azure Site Recovery\Registration"  
net stop dra
```

3. Launch the configuration server appliance browser portal using the shortcut on your desktop.
4. Perform the registration steps similar to a new configuration server [registration](#).

Upgrade the configuration server

You run update rollups to update the configuration server. Updates can be applied for up to N-4 versions. For example:

- If you run 9.7, 9.8, 9.9, or 9.10, you can upgrade directly to 9.11.
- If you run 9.6 or earlier and you want to upgrade to 9.11, you must first upgrade to version 9.7 before 9.11.

For detailed guidance on Azure Site Recovery components support statement refer [here](#). Links to update rollups for upgrading to all versions of the configuration server are available [here](#).

IMPORTANT

With every new version 'N' of an Azure Site Recovery component that is released, all versions below 'N-4' is considered out of support. It is always advisable to upgrade to the latest versions available.

For detailed guidance on Azure Site Recovery components support statement refer [here](#).

Upgrade the server as follows:

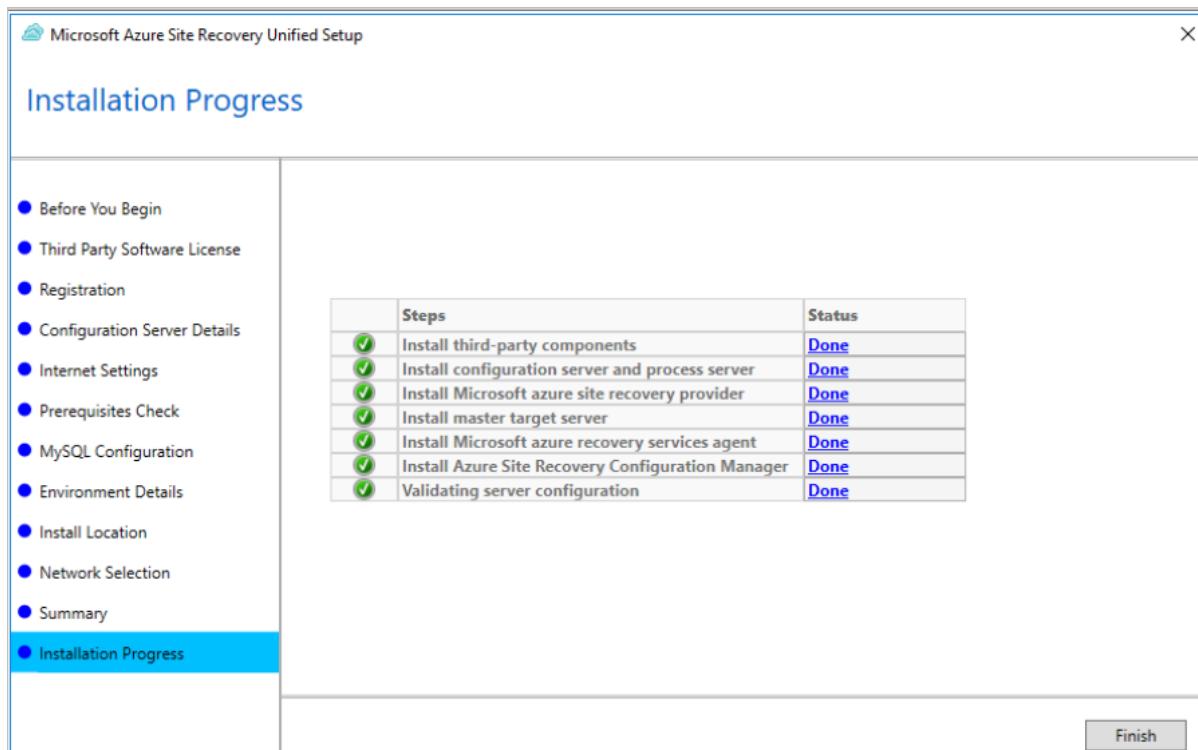
1. In the vault, go to **Manage > Site Recovery Infrastructure > Configuration Servers**.
2. If an update is available, a link appears in the **Agent Version** > column.

The screenshot shows the 'Servers' blade in the Azure Site Recovery Infrastructure section. On the left, there's a navigation menu with options like 'Backup', 'Site Recovery', 'Jobs', 'Alerts and Events', 'Backup Reports', 'Backup policies', 'Backup items', 'Replicated items', 'Site Recovery Infrastructure', 'Backup Infrastructure', and 'Recovery Plans (Site Recovery)'. The 'Site Recovery Infrastructure' option is selected. The main area displays a table of servers. One row for a 'Configuration Server' is highlighted, showing its connection status as 'Connected', its last heartbeat at '5/30/2018 11:27:31 AM', its agent version as '5.1.3300.0 (update availa...)', and its server type as 'Configuration Server'. A tooltip above the table states: 'One or more servers needs to be updated. Click on the 'Update available' link below to download the latest version of the software and install them on your server.' Below the table, there's a message: 'Finished loading data from service.'

3. Download the update installer file to the configuration server.

The screenshot shows two windows side-by-side. The left window is the 'Servers' blade, identical to the one in the previous screenshot. The right window is titled 'Update provider on Config...' and contains instructions for updating the configuration server. Step 1: 'Update Configuration Server On-premises activity' lists two steps: 1. Download the latest Microsoft Azure Site Recovery Unified Setup and 2. Install the provider on your Configuration Server. Below these steps is a table with columns 'SERVER NAME' and 'UPDATE STATUS'. A red box highlights the 'Click here to download...' link under the 'UPDATE STATUS' column for the configuration server listed in the table.

4. Double-click to run the installer.
5. The installer detects the current version running on the machine. Click **Yes** to start the upgrade.
6. When the upgrade completes the server configuration validates.



7. Click **Finish** to close the installer.
8. To upgrade rest of the Site Recovery components, refer to our [upgrade guidance](#).

Upgrade configuration server/process server from the command line

Run the installation file as follows:

```
UnifiedSetup.exe [/ServerMode <CS/PS>] [/InstallDrive <DriveLetter>] [/MySQLCredsFilePath <MySQL credentials file path>] [/VaultCredsFilePath <Vault credentials file path>] [/EnvType <VMWare/NonVMWare>] [/PSIP <IP address to be used for data transfer>] [/CSIP <IP address of CS to be registered with>] [/PassphraseFilePath <Passphrase file path>]
```

Sample usage

```
MicrosoftAzureSiteRecoveryUnifiedSetup.exe /q /x:C:\Temp\Extracted
cd C:\Temp\Extracted
UNIFIEDSETUP.EXE /AcceptThirdpartyEULA /servermode "CS" /InstallLocation "D:\" /MySQLCredsFilePath
"C:\Temp\MySQLCredentialsfile.txt" /VaultCredsFilePath "C:\Temp\MyVault.vaultcredentials" /EnvType "VMWare"
```

Parameters

PARAMETER NAME	TYPE	DESCRIPTION	VALUES
/ServerMode	Required	Specifies whether both the configuration and process servers should be installed, or the process server only	CS PS
/InstallLocation	Required	The folder in which the components are installed	Any folder on the computer
/MySQLCredsFilePath	Required	The file path in which the MySQL server credentials are stored	The file should be the format specified below

PARAMETER NAME	TYPE	DESCRIPTION	VALUES
/VaultCredsFilePath	Required	The path of the vault credentials file	Valid file path
/EnvType	Required	Type of environment that you want to protect	VMware NonVMware
/PSIP	Required	IP address of the NIC to be used for replication data transfer	Any valid IP Address
/CSIP	Required	The IP address of the NIC on which the configuration server is listening on	Any valid IP Address
/PassphraseFilePath	Required	The full path to location of the passphrase file	Valid file path
/BypassProxy	Optional	Specifies that the configuration server connects to Azure without a proxy	To do get this value from Venu
/ProxySettingsFilePath	Optional	Proxy settings (The default proxy requires authentication, or a custom proxy)	The file should be in the format specified below
DataTransferSecurePort	Optional	Port number on the PSIP to be used for replication data	Valid Port Number (default value is 9433)
/SkipSpaceCheck	Optional	Skip space check for cache disk	
/AcceptThirdpartyEULA	Required	Flag implies acceptance of third-party EULA	
/ShowThirdpartyEULA	Optional	Displays third-party EULA. If provided as input all other parameters are ignored	

Create file input for MySQLCredsFilePath

The MySQLCredsFilePath parameter takes a file as input. Create the file using the following format and pass it as input MySQLCredsFilePath parameter.

```
[MySQLCredentials]
MySQLRootPassword = "Password>
MySQLUserPassword = "Password"
```

Create file input for ProxySettingsFilePath

ProxySettingsFilePath parameter takes a file as input. Create the file using the following format and pass it as input ProxySettingsFilePath parameter.

```
[ProxySettings]
ProxyAuthentication = "Yes/No"
Proxy IP = "IP Address"
ProxyPort = "Port"
ProxyUserName="UserName"
ProxyPassword="Password"
```

Delete or unregister a configuration server

1. [Disable protection](#) for all VMs under the configuration server.
2. [Disassociate](#) and [delete](#) all replication policies from the configuration server.
3. [Delete](#) all vCenter servers/vSphere hosts that are associated with the configuration server.
4. In the vault, open **Site Recovery Infrastructure > Configuration Servers**.
5. Select the configuration server that you want to remove. Then, on the **Details** page, select **Delete**.

The screenshot shows the 'Configuration Server' interface for 'CONFIGSRV01'. At the top right, there is a 'More' button with three dots, which has a red box around it. A context menu is open over a configuration item, with the 'Delete' option highlighted by a red box. The configuration item details include: Recovery Services vault (ConsotoVault), IP address (10.10.20.66), Configuration Server version (9.3.0.0), Connected agents (4), Protected items (4), Connection status (Connected), Last heartbeat (2/14/2017), Provider version (5.1.1700.0), and Server ID (aeb54dc5-6e9d-4e16-89e7-49985f282072). Below this, there is a section for 'Associated servers' listing 'Process Ser...', 'vCenter Ser...', and 'Master Targ...'. The 'Configuration Server health' section lists various metrics with green checkmarks: Processor queue (0), CPU utilization (0 used), Memory usage (29.06% / 2.32 GB used of 8 GB), Free space (99.77% / 648.49 GB free of 650 GB), Process server services (Running), Web server (Running), and Database server (Running).

Delete with PowerShell

You can optionally delete the configuration server by using PowerShell.

1. [Install](#) the Azure PowerShell module.
2. Sign in to your Azure account by using this command:

```
Connect-AzAccount
```

3. Select the vault subscription.

```
Get-AzSubscription -SubscriptionName <your subscription name> | Select-AzSubscription
```

4. Set the vault context.

```
$vault = Get-AzRecoveryServicesVault -Name <name of your vault>
Set-AzSiteRecoveryVaultSettings -ARSVault $vault
```

5. Retrieve the configuration server.

```
$fabric = Get-AzSiteRecoveryFabric -FriendlyName <name of your configuration server>
```

6. Delete the configuration server.

```
Remove-AzSiteRecoveryFabric -Fabric $fabric [-Force]
```

NOTE

You can use the **-Force** option in Remove-AzSiteRecoveryFabric for forced deletion of the configuration server.

Generate configuration server Passphrase

1. Sign in to your configuration server, and then open a command prompt window as an administrator.
2. To change the directory to the bin folder, execute the command **cd %ProgramData%\ASR\home\svsystems\bin**
3. To generate the passphrase file, execute **genpassphrase.exe -v > MobSvc.passphrase**.
4. Your passphrase will be stored in the file located at **%ProgramData%\ASR\home\svsystems\bin\MobSvc.passphrase**.

Renew SSL certificates

The configuration server has an inbuilt web server, which orchestrates activities of the Mobility Service, process servers, and master target servers connected to it. The web server uses an SSL certificate to authenticate clients. The certificate expires after three years and can be renewed at any time.

Check expiry

For configuration server deployments before May 2016, certificate expiry was set to one year. If you have a certificate that is going to expire, the following occurs:

- When the expiry date is two months or less, the service starts sending notifications in the portal, and by email (if you subscribed to Site Recovery notifications).
- A notification banner appears on the vault resource page. For more information, select the banner.
- If you see an **Upgrade Now** button, it indicates that some components in your environment haven't been upgraded to 9.4.xxxx.x or higher versions. Upgrade the components before you renew the certificate. You can't renew on older versions.

Renew the certificate

1. In the vault, open **Site Recovery Infrastructure > Configuration Server**. Select the required configuration server.
2. The expiry date appears under **Configuration Server health**.
3. Select **Renew Certificates**.

Refresh Configuration server

1. In the Azure portal, navigate to **Recovery Services Vault > Manage > Site Recovery Infrastructure > For VMware & Physical machines > Configuration Servers**
2. Click on the configuration server you wish to refresh.

3. On the blade with details of chosen configuration server, click **More > Refresh Server**.
4. Monitor the progress of the job under **Recovery Services Vault > Monitoring > Site Recovery jobs**.

Fallback requirements

During reprotect and failback, the on-premises configuration server must be running and in a connected state. For successful failback, the virtual machine being failed back must exist in the configuration server database.

Ensure that you take regular scheduled backups of your configuration server. If a disaster occurs and the configuration server is lost, you must first restore the configuration server from a backup copy and ensure that the restored configuration server has the same IP address with which it was registered to the vault. Failback will not work if a different IP address is used for the restored configuration server.

Next steps

Review the tutorials for setting up disaster recovery of [VMware VMs](#) to Azure.

Manage process servers

11/12/2019 • 5 minutes to read • [Edit Online](#)

This article describes common tasks for managing the Site Recovery process server.

The process server is used to receive, optimize, and send replication data to Azure. It also performs a push installation of the Mobility service on VMware VMs and physical servers you want to replicate, and performs automatic discovery of on-premises machines. For replicating on-premises VMware VMs or physical servers to Azure, the process server is installed by default on the configuration server machine.

- For large deployments, you might need additional on-premises process servers to scale capacity.
- For failback from Azure to on-premises, you must set up a temporary process server in Azure. You can delete this VM when failback is done.

Learn more about the process server.

Upgrade a process server

When you deploy a process server on-premises, or as an Azure VM for failback, the latest version of the process server is installed. The Site Recovery teams release fixes and enhancements on a regular basis, and we recommend you keep process servers up-to-date. You can upgrade a process server as follows:

1. Sign in to the process server as an administrator.
2. Download the latest version of the [Unified Setup Installer](#).
3. Double-click the installer to launch the update process.
4. The installer detects the Site Recovery components that are installed, and upgrades them to the latest version.

Move VMs to balance the process server load

Balance the load by moving VMs between two process servers, as follows:

1. In the vault, under **Manage** click **Site Recovery Infrastructure**. Under **For VMware & Physical machines**, click **Configuration Servers**.
2. Click on the configuration server with which the process servers are registered.
3. Click on the process server for which you want to load balance traffic.

Win5

Process Server

[Load balance](#)[Switch](#)[Error Details](#)

Essentials ^

Recovery Services vault

Server ID

FQDN

IP address

Win5

Process Server version

Protected items

9.19.1.0

0

Last heartbeat at
11/16/2018 3:40:05 PM

Process Server health

Processor queue 0

CPU utilization 14% used

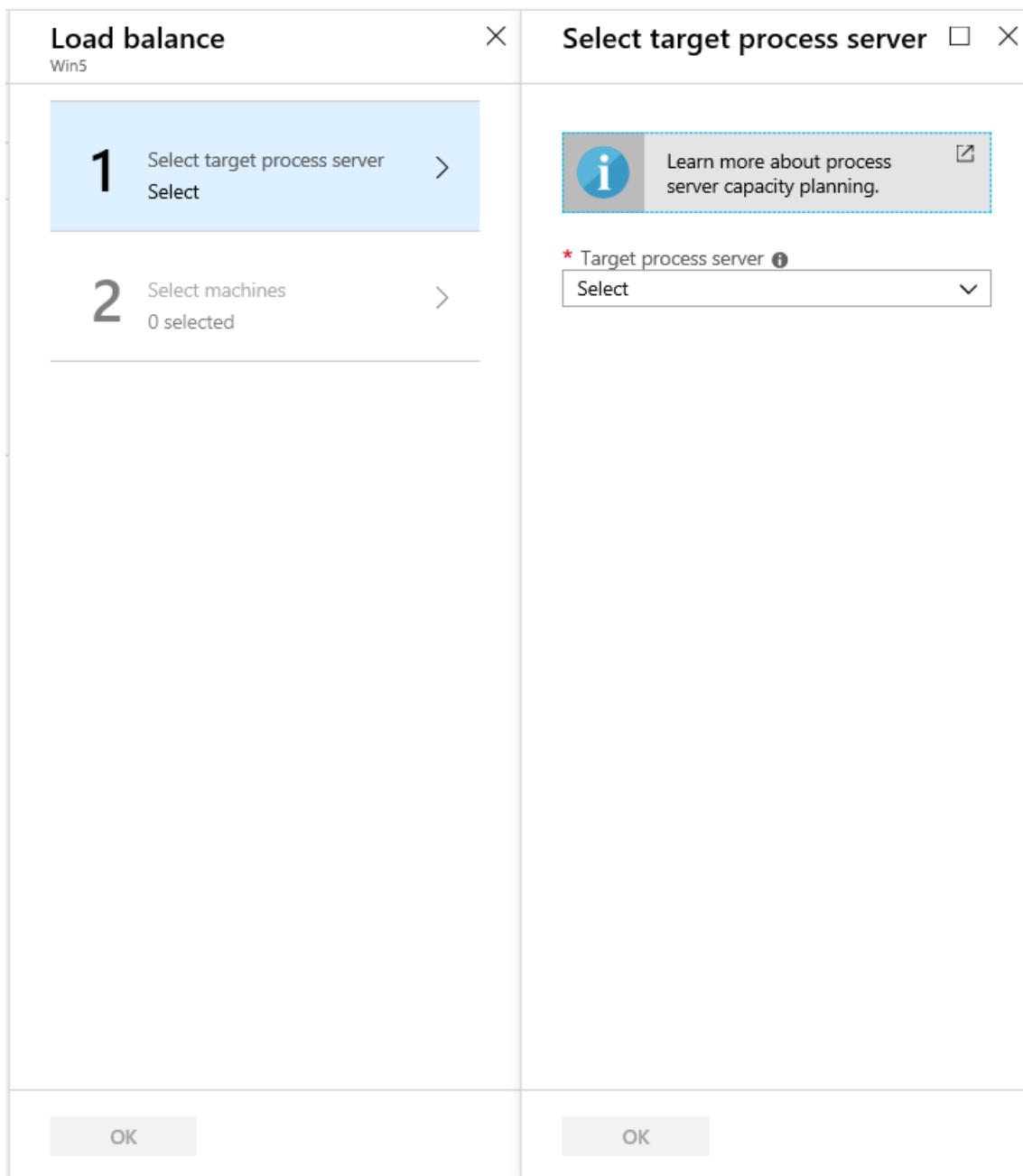
Memory usage UnKnown

Free space 79.77%

Process server services Running

Certificate Expires On 10/31/2021 6:33:02 AM

4. Click **Load balance**, select the target process server to which you want to move machines. Then click **OK**



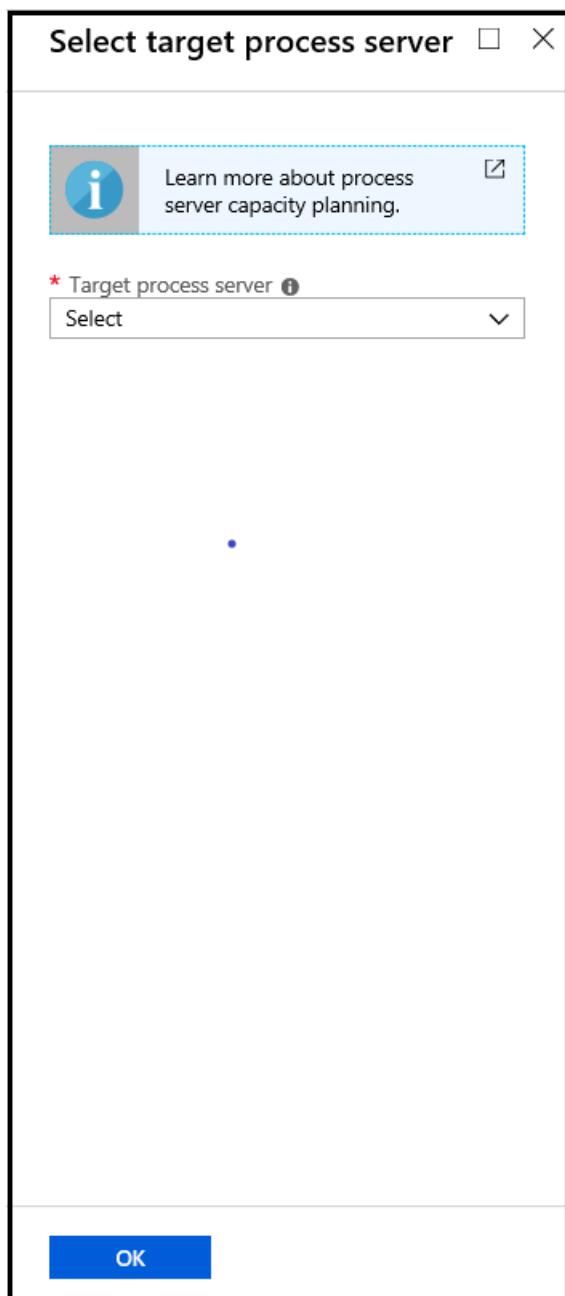
- Click **Select machines**, and choose the machines you want to move from the current to the target process server. Details of average data change are displayed against each virtual machine. Then click **OK**.
- In the vault, monitor the progress of the job under **Monitoring > Site Recovery jobs**.

It will take around 15 minutes for changes to be reflected in the portal. For a quicker effect, [refresh the configuration server](#).

Switch an entire workload to another process server

Move the entire workload handled by a process server to a different process server, as follows:

- In the vault, under **Manage** click **Site Recovery Infrastructure**. Under **For VMware & Physical machines**, click **Configuration Servers**.
- Click on the configuration server with which the process servers are registered.
- Click on the process server from which you want to switch the workload.
- Click on **Switch**, select the target process server to which you want to move the workload. Then click **OK**



5. In the vault, monitor the progress of the job under **Monitoring > Site Recovery jobs**.

It will take around 15 minutes for changes to be reflected in the portal. For a quicker effect, [refresh the configuration server](#).

Register a master target server

Master target server resides on configuration server and scale-out process servers. It must be registered with configuration server. In case there is a failure in this registration, it can impact the health of protected items. To register master target server with configuration server, login to the specific configuration server/scale-out process server on which the registration is required. Navigate to folder **%PROGRAMDATA%\ASR\Agent**, and run the following on administrator command prompt.

```
cmd  
cdpcli.exe --registermt  
  
net stop obengine  
  
net start obengine  
  
exit
```

Reregister a process server

Reregister a process server running on-premises or on an Azure VM with the configuration server as follows:

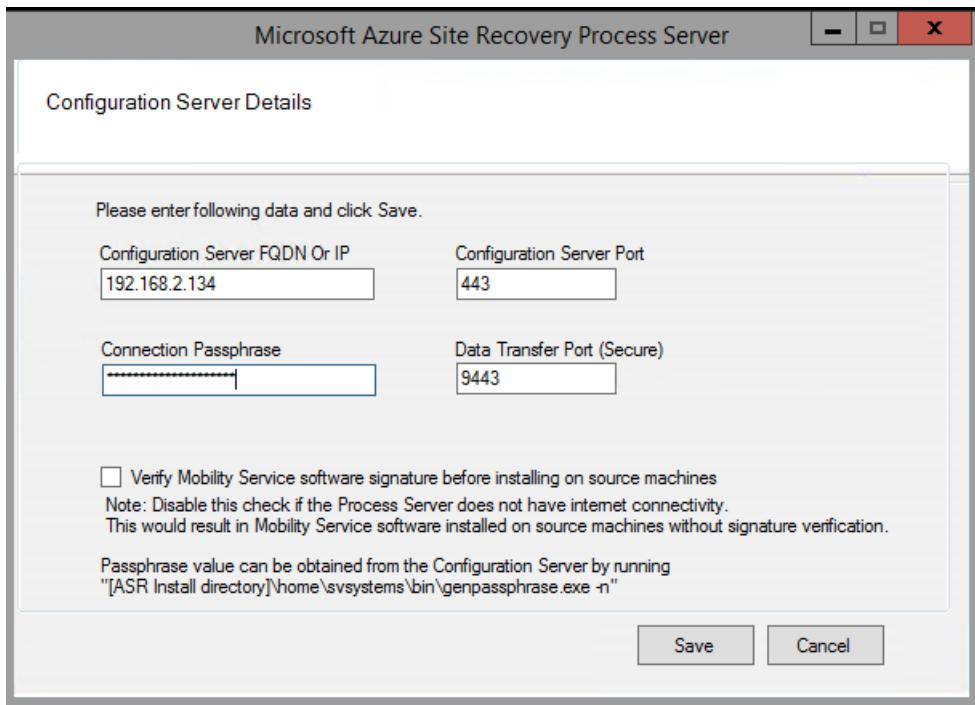
1. Establish a Remote Desktop Connection to the machine running the process server.
2. Run `cpsconfigtool.exe` to start the Azure Site Recovery Process Server configuration tool.
 - The tool is launched automatically the first time you sign into the process server.
 - If it doesn't open automatically, click its shortcut on the desktop.
3. In **Configuration server FQDN or IP**, specify the name or IP address of the configuration server with which to register the process server.
4. In **Configuration Server Port**, ensure that 443 is specified. This is the port on which the configuration server listens for requests.
5. In **Connection Passphrase**, specify the passphrase that you specified when you set up the configuration server. To find the passphrase:
 - On the configuration server, navigate to the Site Recovery installation folder `**\home\svssystems\bin**`:

```
cd %ProgramData%\ASR\home\svssystems\bin
```

- Run the below command to print out the current passphrase:

```
genpassphrase.exe -n
```

6. In **Data Transfer Port**, leave the default value unless you've specified a custom port.
7. Click **Save** save the settings, and register the process server.



After you've saved the settings, do the following:

1. On the process server, open an administrator command prompt.
2. Browse to folder **%PROGRAMDATA%\ASR\Agent**, and run the command:

```
cdpcli.exe --registermt  
net stop obengine  
net start obengine
```

Modify proxy settings for an on-premises process server

If an on-premises process server uses a proxy to connect to Azure, you can modify the proxy settings as follows:

1. Sign into the process server machine.
2. Open an Admin PowerShell command window, and run the following command:

```
$pwd = ConvertTo-SecureString -String MyProxyUserPassword  
Set-OBMachineSetting -ProxyServer http://myproxyserver.domain.com -ProxyPort PortNumber -ProxyUserName  
domain\username -ProxyPassword $pwd  
net stop obengine  
net start obengine
```

3. Browse to folder **%PROGRAMDATA%\ASR\Agent**, and run this command:

```
cmd  
cdpcli.exe --registermt  
  
net stop obengine  
  
net start obengine  
  
exit
```

Remove a process server

Follow the steps for your specific circumstances.

Unregister a connected process server

1. Establish a remote connection to the process server as an Administrator.
2. In the **Control Panel**, open **Programs > Uninstall a program**.
3. Uninstall the program **Microsoft Azure Site Recovery Mobility Service/Master Target Server**.
4. Uninstall the program **Microsoft Azure Site Recovery Configuration/Process Server**.
5. After the programs in steps 3 and 4 are uninstalled, uninstall **Microsoft Azure Site Recovery Configuration/Process Server Dependencies**.

Unregister a disconnected process server

Only use these steps if there's no way to revive the machine on which the process server is installed.

1. Sign in the configuration server as an Administrator.
2. Open an Administrative command prompt, and browse to `%ProgramData%\ASR\home\svsystems\bin`.
3. Run this command to get a list of one or more process servers.

```
perl Unregister-ASRComponent.pl -IPAddress <IP_of_Process_Server> -Component PS
```

- S.No: the process server serial number.
 - IP/Name: The IP address and name of the machine running the process server.
 - Heartbeat: Last heartbeat from the process server machine.
- ```
=====
S.No IP Name Heartbeat
=====
1 [REDACTED] testVM 2018-08-02 11:54:38
=====
```
- Please choose one of the above servers to un-register

4. Specify the serial number of the process server you want to unregister.
5. Unregistering a process server remove all of its details from the system, and displays the message:  
**Successfully unregistered server-name> (server-IP-address)**

### Exclude folders from anti-virus software

If anti-virus software is running on a scale-out process server (or master target server), exclude the following folders from anti-virus operations:

- C:\Program Files\Microsoft Azure Recovery Services Agent
- C:\ProgramData\ASR
- C:\ProgramData\ASRLogs
- C:\ProgramData\ASRSetupLogs
- C:\ProgramData\LogUploadServiceLogs
- C:\ProgramData\Microsoft Azure Site Recovery
- Process server installation directory. For example: C:\Program Files (x86)\Microsoft Azure Site Recovery

# Manage VMware vCenter Server

2/25/2020 • 5 minutes to read • [Edit Online](#)

This article summarizes management actions on a VMware vCenter Server in Azure Site Recovery.

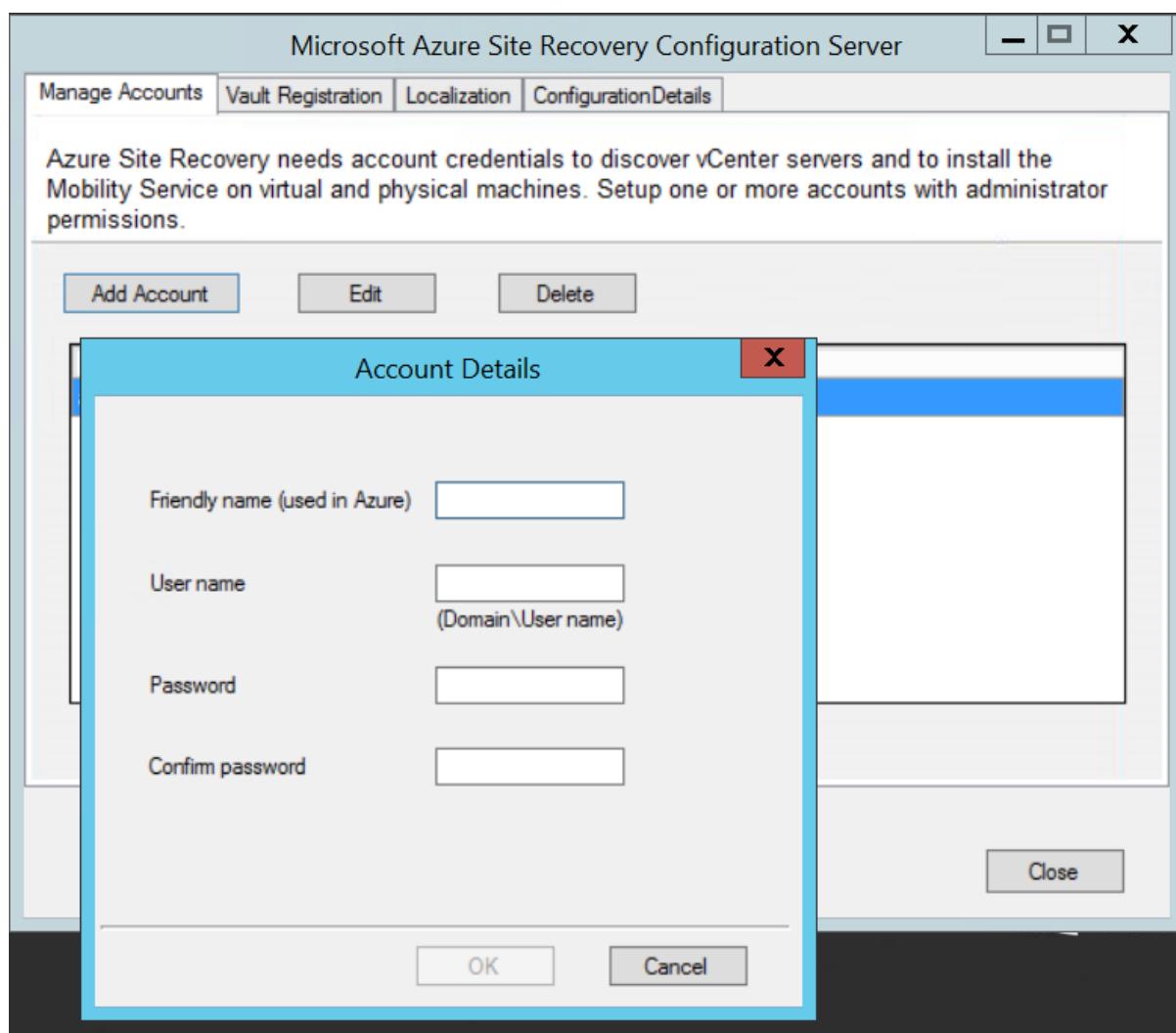
## Verify prerequisites for vCenter Server

The prerequisites for vCenter Servers and VMs during disaster recovery of VMware VMs to Azure are listed in the [support matrix](#).

## Set up an account for automatic discovery

When you set up disaster recovery for on-premises VMware VMs, Site Recovery needs access to the vCenter Server/vSphere host. The Site Recovery process server can then automatically discover VMs, and fail them over as needed. By default, the process server runs on the Site Recovery configuration server. Add an account for the configuration server to connect to the vCenter Server/vSphere host as follows:

1. Sign in to the configuration server.
2. Open the configuration server tool (`cspconfigtool.exe`) using the Desktop shortcut.
3. On the **Manage Account** tab, click **Add Account**.



4. Provide the account details, and click **OK** to add it. The account should have the privileges summarized in the account permissions table.

**NOTE**

It takes about 15 minutes to synchronize account information with Site Recovery.

### Account permissions

| TASK                                             | ACCOUNT                            | PERMISSIONS                                                     | DETAILS                                                                                                                                                                                                                                                                                                                                                             |
|--------------------------------------------------|------------------------------------|-----------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>VM discovery/migration (without failback)</b> | At least a read-only user account. | Data Center object -> Propagate to Child Object, role=Read-only | User assigned at datacenter level, and has access to all the objects in the datacenter.<br><br>To restrict access, assign the <b>No access</b> role with the <b>Propagate to child</b> object, to the child objects (vSphere hosts, datastores, virtual machines, and networks).                                                                                    |
| <b>Replication/failover</b>                      | At least a read-only user account. | Data Center object -> Propagate to Child Object, role=Read-only | User assigned at datacenter level, and has access to all the objects in the datacenter.<br><br>To restrict access, assign the <b>No access</b> role with the <b>Propagate to child</b> object to the child objects (vSphere hosts, datastores, virtual machines, and networks).<br><br>Useful for migration purposes, but not full replication, failover, failback. |

| Task                                 | Account                                                                                                                                 | Permissions                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Details                                                                                                                                                                                                                                                                          |
|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Replication/failover/failback</b> | We suggest you create a role (AzureSiteRecoveryRole) with the required permissions, and then assign the role to a VMware user or group. | Data Center object -> Propagate to Child Object, role=AzureSiteRecoveryRole<br>Datastore -> Allocate space, browse datastore, low-level file operations, remove file, update virtual machine files<br>Network -> Network assign<br>Resource -> Assign VM to resource pool, migrate powered off VM, migrate powered on VM<br>Tasks -> Create task, update task<br>Virtual machine -> Configuration<br>Virtual machine -> Interact -> answer question, device connection, configure CD media, configure floppy media, power off, power on, VMware tools install<br>Virtual machine -> Inventory -> Create, register, unregister<br>Virtual machine -> Provisioning -> Allow virtual machine download, allow virtual machine files upload<br>Virtual machine -> Snapshots -> Remove snapshots | User assigned at datacenter level, and has access to all the objects in the datacenter.<br><br>To restrict access, assign the <b>No access</b> role with the <b>Propagate to child</b> object, to the child objects (vSphere hosts, datastores, virtual machines, and networks). |

## Add VMware server to the vault

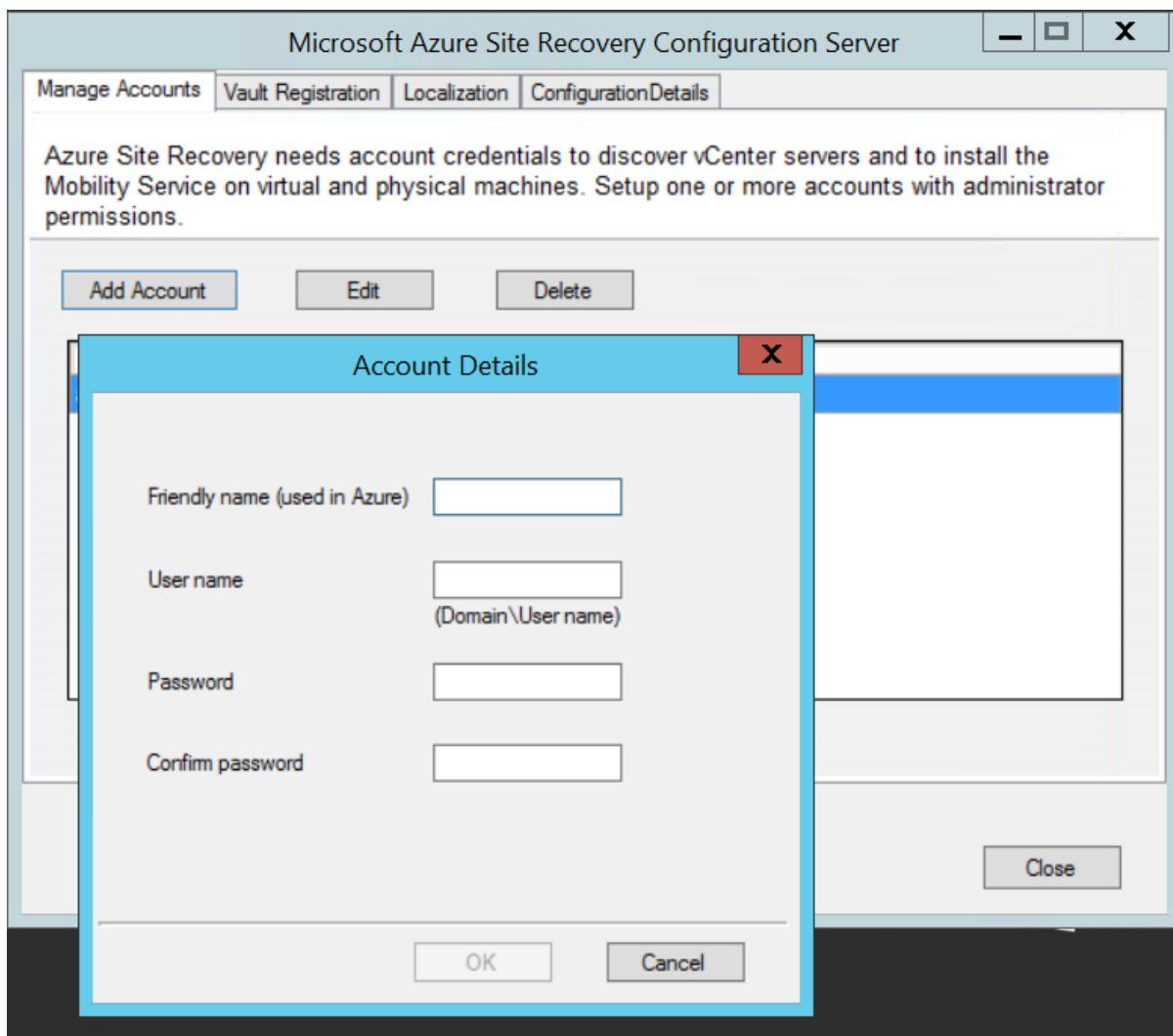
When you set up disaster recovery for on-premises VMware VMs, you add the vCenter Server/vSphere host on which you're discovering VMs to the Site Recovery vault, as follows:

1. In vault > **Site Recovery Infrastructure > Configuration Servers**, open the configuration server.
2. In **Details** page, click **vCenter**.
3. In **Add vCenter**, specify a friendly name for the vSphere host or vCenter server.
4. Specify the IP address or FQDN of the server.
5. Leave the port as 443 unless your VMware servers are configured to listen for requests on a different port.
6. Select the account used to connect to the VMware vCenter or vSphere ESXi server. Then click **OK**.

## Modify credentials

If necessary, you can modify the credentials used to connect to the vCenter Server/vSphere host as follows:

1. Sign in to the configuration server.
2. Open the configuration server tool (`cspconfigtool.exe`) using the Desktop shortcut.
3. Click **Add Account** on the **Manage Account** tab.



4. Provide the new account details, and click **OK**. The account needs the permissions listed in the [account permissions](#) table.
5. In the vault > **Site Recovery Infrastructure** > **Configuration Servers**, open the configuration server.
6. In **Details**, click **Refresh Server**.
7. After the Refresh Server job finishes, select the vCenter Server.
8. In **Summary**, select the newly added account in **vCenter server/vSphere host account**, and click **Save**.

The screenshot shows two windows side-by-side. On the left is the 'Configuration Server' details page, and on the right is the 'vCenter Summary' configuration dialog.

**Configuration Server Details Page:**

- Essentials:**
  - Recovery Services vault: [REDACTED]
  - IP address: [REDACTED]
  - Configuration Server version: 9.7.0.0
  - Connected agents: 26
  - Protected items: 16
- Associated servers:**

| NAME           | STATUS     | SERVER ROLE    | VERSION    | LAST HEART BEAT   |
|----------------|------------|----------------|------------|-------------------|
| Process Ser... | [REDACTED] | [REDACTED]     | [REDACTED] | [REDACTED]        |
| vcenter        | Connected  | vCenter Server | 5.1.2100.0 | 2/17/2017 8:16... |
| Master Targ... | [REDACTED] | [REDACTED]     | [REDACTED] | [REDACTED]        |
- Configuration Server health:**
  - Processor queue: 5
  - CPU utilization: 30% used
  - Memory usage: 59.21% (3.55 GB used of 6 GB)
  - Free space: 96.24% (571.31 GB free of 593.66 GB)
  - Process server services: Running
  - Web server: Running
  - Database server: Running
  - Certificate Expires On: 12/19/2019 7:44:09 AM

**vCenter Summary Configuration Dialog:**

- Save, Discard, More buttons.
- Configuration Server: futurajd-CSPSMT
- \* vCenter server/vSphere host friendly name: vcenter
- \* vCenter server/vSphere host name or IP address: BCDR-vcenter.fareast.corp.microsoft.com
- \* Port: 443
- \* vCenter server/vSphere host account: machine

## Delete a vCenter Server

1. In the vault > **Site Recovery Infrastructure** > **Configuration Servers**, open the configuration server.
2. On the **Details** page, select the vCenter server.
3. Click on the **Delete** button.

The screenshot shows the Configuration Server interface with the 'vCenter Summary' tab selected. On the left, there's a sidebar with 'Configuration Server' navigation and a 'vCenter' summary card. The main area displays 'Associated servers' and 'Configuration Server health' sections. On the right, a modal window titled 'vCenter Summary' is open, showing configuration fields for a vCenter server. The 'vCenter server/vSphere host friendly name' field contains 'vcenter'. The 'Port' field is set to '443'. The 'vCenter server/vSphere host account' dropdown is set to 'vcenter'. A tooltip 'Error Details' is visible above the configuration fields.

## Modify the IP address and port

You can modify the IP address of the vCenter Server, or the ports used for communication between the server and Site Recovery. By default, Site Recovery accesses vCenter Server/vSphere host information through port 443.

1. In the vault > **Site Recovery Infrastructure** > **Configuration Servers**, click on the configurations server to which the vCenter Server is added.
2. In **vCenter servers**, click on the vCenter Server you want to modify.
3. In **Summary**, update the IP address and port, and save the changes.

The screenshot shows the 'vCenter Summary' configuration dialog box. At the top, there are 'Save' and 'Discard' buttons, and a 'More' link. Below these are several configuration fields:

- Configuration Server**: A dropdown menu currently showing 'vCenter'.
- \* vCenter server/vSphere host friendly name**: An input field containing 'vCenter'.
- \* vCenter server/vSphere host name or IP address**: An input field containing '192.168.1.100'.
- \* Port**: An input field containing '443'.
- \* vCenter server/vSphere host account**: A dropdown menu currently showing 'vCenter\_creds'.

4. For changes to become effective, wait for 15 minutes or [refresh the configuration server](#).

## Migrate all VMs to a new server

If you want to migrate all VMs to use a new vCenter Server, you just need to update the IP address assigned to the vCenter Server. Don't add another VMware account, since that might lead to duplicate entries. Update the address as follows:

1. In the vault > **Site Recovery Infrastructure** > **Configuration Servers**, click on the configurations server to which the vCenter Server is added.
2. In the **vCenter servers** section, click on the vCenter Server that you want to migrate from.
3. In **Summary**, update the IP address to that of the new vCenter Server, and save the changes.
4. As soon as the IP address is updated, Site Recovery starts receiving VM discovery information from the new vCenter Server. This doesn't impact ongoing replication activities.

## Migrate a few VMs to a new server

If you only want to migrate a few of your replicating VMs to a new vCenter Server, do the following:

1. [Add](#) the new vCenter Server to the configuration server.
2. [Disable replication](#) for VMs that will move to the new server.
3. In VMware, migrate the VMs to the new vCenter Server.
4. [Enable replication](#) for the migrated VMs again, selecting the new vCenter Server.

## Migrate most VMs to a new server

If the number of VMs that you want to migrate to a new vCenter Server is higher than the number of VMs that will remain on the original vCenter Server, do the following:

1. [Update the IP address](#) assigned to the vCenter Server in the configuration server settings, to the address of the new vCenter Server.
2. [Disable replication](#) for the few VMs that remain on the old server.
3. [Add the old vCenter Server](#) and its IP address to the configuration server.
4. [Re-enable replication](#) for the VMs that remain on the old server.

## Next steps

If you have any issues, see [Troubleshoot vCenter Server discovery failures](#).

# Service updates in Site Recovery

9/11/2019 • 4 minutes to read • [Edit Online](#)

This article provides an overview of [Azure Site Recovery](#) updates, and describes how to upgrade Site Recovery components.

Site Recovery publishes service updates on a regular basis. Updates include new features, support improvements, component updates, and bug fixes. In order to take advantage of the latest features and fixes, we recommend running the latest versions of Site Recovery components.

## Updates support

### Support statement for Azure Site Recovery

We recommend always upgrading to the latest component versions:

**With every new version 'N' of an Azure Site Recovery component that's released, all versions below 'N-4' are considered to be out of support.**

#### IMPORTANT

Official support is for upgrading from > N-4 version to N version. For example, if you're running you are on N-6, you need to first upgrade to N-4, and then upgrade to N.

### Links to currently supported update rollups

Review the latest update rollup (version N) in [this article](#). Remember that Site Recovery provides support for N-4 versions.

## Component expiry

Site Recovery notifies you of expired components (or nearing expiry) by email (if you subscribed to email notifications), or on the vault dashboard in the portal.

- In addition, when updates are available, in the infrastructure view for your scenario in the portal, an **Update available** button appears next to the component. This button redirects you to a link for downloading the latest component version.
- Vaults dashboard notifications aren't available if you're replicating Hyper-V VMs.

Emails notifications are sent as follows.

| TIME                            | FREQUENCY      |
|---------------------------------|----------------|
| 60 days before component expiry | Once bi-weekly |
| Next 53 days                    | Once a week    |
| Last 7 days                     | Once a day     |
| After expiry                    | Once bi-weekly |

### Upgrading outside official support

If the difference between your component version and the latest release version is greater than four, this is considered out of support. In this case, upgrade as follows:

1. Upgrade the currently installed component to your current version plus four. For example, if your version is 9.16, then upgrade to 9.20.
2. Then, upgrade to the next compatible version. So in our example, after upgrading 9.16 to 9.20, upgrade to 9.24.

Follow the same process for all relevant components.

## Support for latest operating systems/kernels

### NOTE

If you have a maintenance window scheduled, and a reboot is included in it, we recommend that you first upgrade Site Recovery components, and then proceed with the rest of the scheduled activities in the maintenance window.

1. Before upgrading operating system/kernel versions, verify if the target version is supported Site Recovery.
  - Azure VM support.
  - VMware/physical server support
  - Hyper-V support.
2. Review [available updates](#) to find out what you want to upgrade.
3. Upgrade to the latest Site Recovery version.
4. Upgrade the operating system/kernel to the required versions.
5. Reboot.

This process ensures that the machine operating system/kernel is upgraded to the latest version, and that the latest Site Recovery changes needed to support the new version are loaded on to the machine.

## Azure VM disaster recovery to Azure

In this scenario, we strongly recommend that you [enable automatic updates](#). You can allow Site Recovery to manage updates as follows:

- During the enable replication process.
- By setting the extension update settings inside the vault.

If you want to manually manage updates, do the following:

1. In the vault > **Replicated Items**, click this notification at the top of the screen:  
**New Site Recovery replication agent update is available. Click to install ->**
2. Select the VMs for which you want to apply the update, and then click **OK**.

## VMware VM/physical server disaster recovery to Azure

1. Based on your current version and the [support statement](#), install the update first on the on-premises configuration server, using [these instructions](#).
2. If you have scale-out process servers, update them next, using [these instructions](#).
3. To update the Mobility agent on each protected machine, refer to [this article](#).

### Reboot after Mobility service upgrade

A reboot is recommended after every upgrade of the Mobility service, to ensure that all the latest changes are

loaded on the source machine.

A reboot isn't mandatory, unless the difference between the agent version during last reboot, and the current version, is greater than four.

The example in the table shows how this works.

| AGENT VERSION (LAST REBOOT) | UPGRADE TO | MANDATORY REBOOT?                                                        |
|-----------------------------|------------|--------------------------------------------------------------------------|
| 9.16                        | 9.18       | Not mandatory                                                            |
| 9.16                        | 9.19       | Not mandatory                                                            |
| 9.16                        | 9.20       | Not mandatory                                                            |
| 9.16                        | 9.21       | Mandatory.<br><br>Upgrade to 9.20, then reboot before upgrading to 9.21. |

## Hyper-V VM disaster recovery to Azure

### Between a Hyper-V site and Azure

1. Download the update for the Microsoft Azure Site Recovery Provider.
2. Install the Provider on each Hyper-V server registered in Site Recovery. If you're running a cluster, upgrade on all cluster nodes.

### Between an on-premises VMM site and Azure

1. Download the update for the Microsoft Azure Site Recovery Provider.
2. Install the Provider on the VMM server. If VMM is deployed in a cluster, install the Provider on all cluster nodes.
3. Install the latest Microsoft Azure Recovery Services agent on all Hyper-V hosts or cluster nodes.

### Between two on-premises VMM sites

1. Download the latest update for the Microsoft Azure Site Recovery Provider.
2. Install the latest Provider on the VMM server managing the secondary recovery site. If VMM is deployed in a cluster, install the Provider on all cluster nodes.
3. After the recovery site is updated, install the Provider on the VMM server that's managing the primary site.

## Next steps

Follow our [Azure Updates](#) page to track new updates and releases.

# Remove servers and disable protection

7/14/2019 • 8 minutes to read • [Edit Online](#)

This article describes how to unregister servers from a Recovery Services vault, and how to disable protection for machines protected by Site Recovery.

## Unregister a configuration server

If you replicate VMware VMs or Windows/Linux physical servers to Azure, you can unregister an unconnected configuration server from a vault as follows:

1. [Disable protection of virtual machines](#).
2. [Disassociate or delete replication policies](#).
3. [Delete the configuration server](#)

## Unregister a VMM server

1. Stop replicating virtual machines in clouds on the VMM server you want to remove.
2. Delete any network mappings used by clouds on the VMM server that you want to delete. In **Site Recovery Infrastructure > For System Center VMM > Network Mapping**, right-click the network mapping > **Delete**.
3. Note the ID of the VMM server.
4. Disassociate replication policies from clouds on the VMM server you want to remove. In **Site Recovery Infrastructure > For System Center VMM > Replication Policies**, double-click the associated policy. Right-click the cloud > **Disassociate**.
5. Delete the VMM server or active node. In **Site Recovery Infrastructure > For System Center VMM > VMM Servers**, right-click the server > **Delete**.
6. If your VMM server was in a Disconnected state, then download and run the [cleanup script](#) on the VMM server. Open PowerShell with the **Run as Administrator** option, to change the execution policy for the default (LocalMachine) scope. In the script, specify the ID of the VMM server you want to remove. The script removes registration and cloud pairing information from the server.
7. Run the cleanup script on any secondary VMM server.
8. Run the cleanup script on any other passive VMM cluster nodes that have the Provider installed.
9. Uninstall the Provider manually on the VMM server. If you have a cluster, remove from all nodes.
10. If your virtual machines were replicating to Azure, you need to uninstall the Microsoft Recovery Services agent from Hyper-V hosts in the deleted clouds.

## Unregister a Hyper-V host in a Hyper-V Site

Hyper-V hosts that aren't managed by VMM are gathered into a Hyper-V site. Remove a host in a Hyper-V site as follows:

1. Disable replication for Hyper-V VMs located on the host.
2. Disassociate policies for the Hyper-V site. In **Site Recovery Infrastructure > For Hyper-V Sites > Replication Policies**, double-click the associated policy. Right-click the site > **Disassociate**.
3. Delete Hyper-V hosts. In **Site Recovery Infrastructure > For Hyper-V Sites > Hyper-V Hosts**, right-click the server > **Delete**.
4. Delete the Hyper-V site after all hosts have been removed from it. In **Site Recovery Infrastructure > For Hyper-V Sites > Hyper-V Sites**, right-click the site > **Delete**.

5. If your Hyper-V host was in a **Disconnected** state, then run the following script on each Hyper-V host that you removed. The script cleans up settings on the server, and unregisters it from the vault.

```

pushd .
try
{
 $windowsIdentity=[System.Security.Principal.WindowsIdentity]::GetCurrent()
 $principal=new-object System.Security.Principal.WindowsPrincipal($windowsIdentity)
 $administrators=[System.Security.Principal.WindowsBuiltInRole]::Administrator
 $isAdmin=$principal.IsInRole($administrators)
 if (!$isAdmin)
 {
 "Please run the script as an administrator in elevated mode."
 $choice = Read-Host
 return;
 }

 $error.Clear()
 "This script will remove the old Azure Site Recovery Provider related properties. Do you want to
continue (Y/N) ?"
 $choice = Read-Host

 if (!($choice -eq 'Y' -or $choice -eq 'y'))
 {
 "Stopping cleanup."
 return;
 }

 $serviceName = "dra"
 $service = Get-Service -Name $serviceName
 if ($service.Status -eq "Running")
 {
 "Stopping the Azure Site Recovery service..."
 net stop $serviceName
 }

 $asrHivePath = "HKLM:\SOFTWARE\Microsoft\Azure Site Recovery"
 $registrationPath = $asrHivePath + '\Registration'
 $proxySettingsPath = $asrHivePath + '\ProxySettings'
 $draIdvalue = 'DraID'
 $idMgmtCloudContainerId='IdMgmtCloudContainerId'

 if (Test-Path $asrHivePath)
 {
 if (Test-Path $registrationPath)
 {
 "Removing registration related registry keys."
 Remove-Item -Recurse -Path $registrationPath
 }

 if (Test-Path $proxySettingsPath)
 {
 "Removing proxy settings"
 Remove-Item -Recurse -Path $proxySettingsPath
 }

 $regNode = Get-ItemProperty -Path $asrHivePath
 if($regNode.DraID -ne $null)
 {
 "Removing DraId"
 Remove-ItemProperty -Path $asrHivePath -Name $draIdValue
 }
 if($regNode.IdMgmtCloudContainerId -ne $null)
 {
 "Removing IdMgmtCloudContainerId"
 Remove-ItemProperty -Path $asrHivePath -Name $idMgmtCloudContainerId
 }
 }
}

```

```

 }
 "Registry keys removed."
 }

 # First retrieve all the certificates to be deleted
 $ASRcerts = Get-ChildItem -Path cert:\localmachine\my | where-object
 {$_.friendlyname.startswith('ASR_SRSAUTH_CERT_KEY_CONTAINER') -or
 $_.friendlyname.startswith('ASR_HYPER_V_HOST_CERT_KEY_CONTAINER')}
 # Open a cert store object
 $store = New-Object System.Security.Cryptography.X509Certificates.X509Store("My", "LocalMachine")
 $store.Open('ReadWrite')
 # Delete the certs
 "Removing all related certificates"
 foreach ($cert in $ASRcerts)
 {
 $store.Remove($cert)
 }
}catch
{
 [system.exception]
 Write-Host "Error occurred" -ForegroundColor "Red"
 $error[0]
 Write-Host "FAILED" -ForegroundColor "Red"
}
popd

```

## Disable protection for a VMware VM or physical server (VMware to Azure)

1. In **Protected Items > Replicated Items**, right-click the machine > **Disable replication**.
2. In **Disable replication** page, select one of these options:
  - **Disable replication and remove (recommended)** - This option removes the replicated item from Azure Site Recovery and the replication for the machine is stopped. Replication configuration on Configuration Server is cleaned up and Site Recovery billing for this protected server is stopped. Note that this option can only be used when Configuration Server is in connected state.
  - **Remove** - This option is supposed to be used only if the source environment is deleted or not accessible (not connected). This removes the replicated item from Azure Site Recovery (billing is stopped). Replication configuration on the Configuration Server **will not** be cleaned up.

### NOTE

In both the options mobility service will not be uninstalled from the protected servers, you need to uninstall it manually. If you plan to protect the server again using the same Configuration server, you can skip uninstalling the mobility service.

### NOTE

If you have already failed over a VM and it is running in Azure, note that disable protection doesn't remove / affect the failed over VM.

## Disable protection for a Azure VM (Azure to Azure)

- In **Protected Items > Replicated Items**, right-click the machine > **Disable replication**.

**NOTE**

mobility service will not be uninstalled from the protected servers, you need to uninstall it manually. If you plan to protect the server again, you can skip uninstalling the mobility service.

## Disable protection for a Hyper-V virtual machine (Hyper-V to Azure)

**NOTE**

Use this procedure if you're replicating Hyper-V VMs to Azure without a VMM server. If you are replicating your virtual machines using the **System Center VMM to Azure** scenario, then follow the instructions Disable protection for a Hyper-V virtual machine replicating using the System Center VMM to Azure scenario

1. In **Protected Items > Replicated Items**, right-click the machine > **Disable replication**.

2. In **Disable replication**, you can select the following options:

- **Disable replication and remove (recommended)** - This option removes the replicated item from Azure Site Recovery and the replication for the machine is stopped. Replication configuration on the on-premises virtual machine will be cleaned up and Site Recovery billing for this protected server is stopped.
- **Remove** - This option is supposed to be used only if the source environment is deleted or not accessible (not connected). This removes the replicated item from Azure Site Recovery (billing is stopped). Replication configuration on the on-premises virtual machine **will not** be cleaned up.

**NOTE**

> If you chose the \*\*Remove\*\* option then run the following set of scripts to clean up the replication settings on-premises Hyper-V Server.

**NOTE**

If you have already failed over a VM and it is running in Azure, note that disable protection doesn't remove / affect the failed over VM.

1. On the source Hyper-V host server, to remove replication for the virtual machine. Replace SQLVM1 with the name of your virtual machine and run the script from an administrative PowerShell

```
$vmName = "SQLVM1"
$vm = Get-WmiObject -Namespace "root\virtualization\v2" -Query "Select * From MsVm_ComputerSystem Where ElementName = '$vmName'"
$replicationService = Get-WmiObject -Namespace "root\virtualization\v2" -Query "Select * From MsVm_ReplicationService"
$replicationService.RemoveReplicationRelationship($vm.__PATH)
```

## Disable protection for a Hyper-V virtual machine replicating to Azure using the System Center VMM to Azure scenario

1. In **Protected Items > Replicated Items**, right-click the machine > **Disable replication**.

2. In **Disable replication**, select one of these options:

- **Disable replication and remove (recommended)** - This option remove the replicated item from Azure Site Recovery and the replication for the machine is stopped. Replication configuration on the on-premises virtual machine is cleaned up and Site Recovery billing for this protected server is stopped.
- **Remove** - This option is supposed to be used only if the source environment is deleted or not accessible (not connected). This removes the replicated item from Azure Site Recovery (billing is stopped). Replication configuration on the on-premises virtual machine **will not** be cleaned up.

**NOTE**

If you chose the **Remove** option, then run the following scripts to clean up the replication settings on-premises VMM Server.

3. Run this script on the source VMM server, using PowerShell (administrator privileges required) from the VMM console. Replace the placeholder **SQLVM1** with the name of your virtual machine.

```
$vm = get-scvirtualmachine -Name "SQLVM1"
Set-SCVirtualMachine -VM $vm -ClearDRProtection
```

4. The above steps clear the replication settings on the VMM server. To stop replication for the virtual machine running on the Hyper-V host server, run this script. Replace SQLVM1 with the name of your virtual machine, and host01.contoso.com with the name of the Hyper-V host server.

```
$vmName = "SQLVM1"
$hostName = "host01.contoso.com"
$vm = Get-WmiObject -Namespace "root\virtualization\v2" -Query "Select * From MsVm_ComputerSystem Where ElementName = '$vmName'" -computername $hostName
$replicationService = Get-WmiObject -Namespace "root\virtualization\v2" -Query "Select * From MsVm_ReplicationService" -computername $hostName
$replicationService.RemoveReplicationRelationship($vm.__PATH)
```

## Disable protection for a Hyper-V virtual machine replicating to secondary VMM Server using the System Center VMM to VMM scenario

1. In **Protected Items > Replicated Items**, right-click the machine > **Disable replication**.
2. In **Disable replication**, select one of these options:
  - **Disable replication and remove (recommended)** - This option remove the replicated item from Azure Site Recovery and the replication for the machine is stopped. Replication configuration on the on-premises virtual machine is cleaned up and Site Recovery billing for this protected server is stopped.
  - **Remove** - This option is supposed to be used only if the source environment is deleted or not accessible (not connected). This removes the replicated item from Azure Site Recovery (billing is stopped). Replication configuration on the on-premises virtual machine **will not** be cleaned up. Run the following set of scripts to clean up the replication settings on-premises virtual machines.

**NOTE**

If you chose the **Remove** option, then run the following scripts to clean up the replication settings on-premises VMM Server.

3. Run this script on the source VMM server, using PowerShell (administrator privileges required) from the VMM console. Replace the placeholder **SQLVM1** with the name of your virtual machine.

```
$vm = get-scvirtualmachine -Name "SQLVM1"
Set-SCVirtualMachine -VM $vm -ClearDRProtection
```

4. On the secondary VMM server, run this script to clean up the settings for the secondary virtual machine:

```
$vm = get-scvirtualmachine -Name "SQLVM1"
Remove-SCVirtualMachine -VM $vm -Force
```

5. On the secondary VMM server, refresh the virtual machines on the Hyper-V host server, so that the secondary VM gets detected again in the VMM console.
6. The above steps clear up the replication settings on the VMM server. If you want to stop replication for the virtual machine, run the following script on the primary and secondary VMs. Replace SQLVM1 with the name of your virtual machine.

```
Remove-VMReplication -VMName "SQLVM1"
```

# Delete a Site Recovery Services vault

1/10/2020 • 2 minutes to read • [Edit Online](#)

This article describes how to delete a Recovery Services vault for Site Recovery. To delete a vault used in Azure Backup, see [Delete a Backup vault in Azure](#).

## NOTE

This article has been updated to use the new Azure PowerShell Az module. You can still use the AzureRM module, which will continue to receive bug fixes until at least December 2020. To learn more about the new Az module and AzureRM compatibility, see [Introducing the new Azure PowerShell Az module](#). For Az module installation instructions, see [Install Azure PowerShell](#).

## Before you start

Before you can delete a vault you must remove registered servers, and items in the vault. What you need to remove depends on the replication scenarios you've deployed.

## Delete a vault-Azure VM to Azure

1. Follow [these instructions](#) to delete all protected VMs.
2. Then, delete the vault.

## Delete a vault-VMware VM to Azure

1. Follow [these instructions](#) to delete all protected VMs.
2. Follow [these steps](#) to delete all replication policies.
3. Delete references to vCenter using [these steps](#).
4. Follow [these instructions](#) to decommission a configuration server.
5. Then, delete the vault.

## Delete a vault-Hyper-V VM (with VMM) to Azure

1. Follow [these steps](#) to delete Hyper-V VMs managed by System Center VMM.
2. Disassociate and delete all replication policies. Do this in your vault > **Site Recovery Infrastructure > For System Center VMM > Replication Policies**.
3. Follow [these steps](#) to unregister a connected VMM server.
4. Then, delete the vault.

## Delete a vault-Hyper-V VM to Azure

1. Follow [these steps](#) to delete all protected VMs.
2. Disassociate and delete all replication policies. Do this in your vault > **Site Recovery Infrastructure > For Hyper-V Sites > Replication Policies**.
3. Follow [these instructions](#) to unregister a Hyper-V host.
4. Delete the Hyper-V site.
5. Then, delete the vault.

## Use PowerShell to force delete the vault

### IMPORTANT

If you're testing the product and aren't concerned about data loss, use the force delete method to rapidly remove the vault and all its dependencies. The PowerShell command deletes all the contents of the vault and is **not reversible**.

To delete the Site Recovery vault even if there are protected items, use these commands:

```
Connect-AzAccount

Select-AzSubscription -SubscriptionName "XXXXX"

$vault = Get-AzRecoveryServicesVault -Name "vaultname"

Remove-AzRecoveryServicesVault -Vault $vault
```

Learn more about [Get-AzRecoveryServicesVault](#), and [Remove-AzRecoveryServicesVault](#).

# Set up disaster recovery at scale for VMware VMs/physical servers

1/10/2020 • 10 minutes to read • [Edit Online](#)

This article describes how to set up disaster recovery to Azure for large numbers (> 1000) of on-premises VMware VMs or physical servers in your production environment, using the [Azure Site Recovery](#) service.

## Define your BCDR strategy

As part of your business continuity and disaster recovery (BCDR) strategy, you define recovery point objectives (RPOs) and recovery time objectives (RTOs) for your business apps and workloads. RTO measures the duration of time and service level within which a business app or process must be restored and available, in order to avoid continuity issues.

- Site Recovery provides continuous replication for VMware VMs and physical servers, and an [SLA](#) for RTO.
- As you plan for large-scale disaster recovery for VMware VMs and figure out the Azure resources you need, you can specify an RTO value that will be used for capacity calculations.

## Best practices

Some general best practices for large-scale disaster recovery. These best practices are discussed in more detail in the next sections of the document.

- **Identify target requirements:** Estimate out capacity and resource needs in Azure before you set up disaster recovery.
- **Plan for Site Recovery components:** Figure out what Site Recovery components (configuration server, process servers) you need to meet your estimated capacity.
- **Set up one or more scale-out process servers:** Don't use the process server that's running by default on the configuration server.
- **Run the latest updates:** The Site Recovery team releases new versions of Site Recovery components on a regular basis, and you should make sure you're running the latest versions. To help with that, track [what's new](#) for updates, and [enable and install updates](#) as they release.
- **Monitor proactively:** As you get disaster recovery up and running, you should proactively monitor the status and health of replicated machines, and infrastructure resources.
- **Disaster recovery drills:** You should run disaster recovery drills on a regular basis. These don't impact on your production environment, but do help ensure that failover to Azure will work as expected when needed.

## Gather capacity planning information

Gather information about your on-premises environment, to help assess and estimate your target (Azure) capacity needs.

- For VMware, run the Deployment Planner for VMware VMs to do this.
- For physical servers, gather the information manually.

### Run the Deployment Planner for VMware VMs

The Deployment Planner helps you to gather information about your VMware on-premises environment.

- Run the Deployment Planner during a period that represents typical churn for your VMs. This will generate

more accurate estimates and recommendations.

- We recommend that you run the Deployment Planner on the configuration server machine, since the Planner calculates throughput from the server on which it's running. [Learn more](#) about measuring throughput.
- If you don't yet have a configuration server set up:
  - [Get an overview](#) of Site Recovery components.
  - [Set up a configuration server](#), in order to run the Deployment Planner on it.

Then run the Planner as follows:

1. [Learn about](#) the Deployment Planner. You can download the latest version from the portal, or [download it directly](#).
2. Review the [prerequisites](#) and [latest updates](#) for the Deployment Planner, and [download and extract](#) the tool.
3. [Run the Deployment Planner](#) on the configuration server.
4. [Generate a report](#) to summarize estimations and recommendations.
5. Analyze the [report recommendations](#) and [cost estimations](#).

#### NOTE

By default, the tool is configured to profile and generates report for up to 1000 VMs. You can change this limit by increasing the MaxVMsSupported key value in the ASRDeploymentPlanner.exe.config file.

## Plan target (Azure) requirements and capacity

Using your gathered estimations and recommendations, you can plan for target resources and capacity. If you ran the Deployment Planner for VMware VMs, you can use a number of the [report recommendations](#) to help you.

- **Compatible VMs:** Use this number to identify the number of VMs that are ready for disaster recovery to Azure. Recommendations about network bandwidth and Azure cores are based on this number.
- **Required network bandwidth:** Note the bandwidth you need for delta replication of compatible VMs.
  - When you run the Planner you specify the desired RPO in minutes. The recommendations show you the bandwidth needed to meet that RPO 100% and 90% of the time.
  - The network bandwidth recommendations take into account the bandwidth needed for total number of configuration servers and process servers recommended in the Planner.
- **Required Azure cores:** Note the number of cores you need in the target Azure region, based on the number of compatible VMs. If you don't have enough cores, at failover Site Recovery won't be able to create the required Azure VMs.
- **Recommended VM batch size:** The recommended batch size is based on the ability to finish initial replication for the batch within 72 hours by default, while meeting an RPO of 100%. The hour value can be modified.

You can use these recommendations to plan for Azure resources, network bandwidth, and VM batching.

## Plan Azure subscriptions and quotas

We want to make sure that available quotas in the target subscription are sufficient to handle failover.

| Task | Details | Action |
|------|---------|--------|
|      |         |        |

| Task                         | Details                                                                                                                    | Action                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Check cores</b>           | If cores in the available quota don't equal or exceed the total target count at the time of failover, failovers will fail. | <p>For VMware VMs, check you have enough cores in the target subscription to meet the Deployment Planner core recommendation.</p> <p>For physical servers, check that Azure cores meet your manual estimations.</p> <p>To check quotas, in the Azure portal &gt; <b>Subscription</b>, click <b>Usage + quotas</b>.</p> <p><a href="#">Learn more</a> about increasing quotas.</p> |
| <b>Check failover limits</b> | The number of failovers mustn't exceed Site Recovery failover limits.                                                      | If failovers exceed the limits, you can add subscriptions, and fail over to multiple subscriptions, or increase quota for a subscription.                                                                                                                                                                                                                                         |

## Failover limits

The limits indicate the number of failovers that are supported by Site Recovery within one hour, assuming three disks per machine.

What does comply mean? To start an Azure VM, Azure requires some drivers to be in boot start state, and services like DHCP to be set to start automatically.

- Machines that comply will already have these settings in place.
- For machines running Windows, you can proactively check compliance, and make them compliant if needed. [Learn more](#).
- Linux machines are only brought into compliance at the time of failover.

| MACHINE COMPLIES WITH AZURE? | AZURE VM LIMITS (MANAGED DISK FAILOVER) |
|------------------------------|-----------------------------------------|
| Yes                          | 2000                                    |
| No                           | 1000                                    |

- Limits assume that minimal other jobs are in progress in the target region for the subscription.
- Some Azure regions are smaller, and might have slightly lower limits.

## Plan infrastructure and VM connectivity

After failover to Azure you need your workloads to operate as they did on-premises, and to enable users to access workloads running on the Azure VMs.

- [Learn more](#) about failing over your Active Directory or DNS on-premises infrastructure to Azure.
- [Learn more](#) about preparing to connect to Azure VMs after failover.

## Plan for source capacity and requirements

It's important that you have sufficient configuration servers and scale-out process servers to meet capacity requirements. As you begin your large-scale deployment, start off with a single configuration server, and a single scale-out process server. As you reach the prescribed limits, add additional servers.

## NOTE

For VMware VMs, the Deployment Planner makes some recommendations about the configuration and process servers you need. We recommend that you use the tables included in the following procedures, instead of following the Deployment Planner recommendation.

## Set up a configuration server

Configuration server capacity is affected by the number of machines replicating, and not by data churn rate. To figure out whether you need additional configuration servers, use these defined VM limits.

| CPU                                      | MEMORY | CACHE DISK | REPLICATED MACHINE LIMIT                                                        |
|------------------------------------------|--------|------------|---------------------------------------------------------------------------------|
| 8 vCPUs<br>2 sockets * 4 cores @ 2.5 Ghz | 16 GB  | 600 GB     | Up to 550 machines<br>Assumes that each machine has three disks of 100 GB each. |

- These limits are based on a configuration server set up using an OVF template.
- The limits assume that you're not using the process server that's running by default on the configuration server.

If you need to add a new configuration server, follow these instructions:

- [Set up a configuration server](#) for VMware VM disaster recovery, using an OVF template.
- [Set up a configuration server](#) manually for physical servers, or for VMware deployments that can't use an OVF template.

As you set up a configuration server, note that:

- When you set up a configuration server, it's important to consider the subscription and vault within which it resides, since these shouldn't be changed after setup. If you do need to change the vault, you have to disassociate the configuration server from the vault, and reregister it. This stops replication of VMs in the vault.
- If you want to set up a configuration server with multiple network adapters, you should do this during set up. You can't do this after registering the configuration server in the vault.

## Set up a process server

Process server capacity is affected by data churn rates, and not by the number of machines enabled for replication.

- For large deployments you should always have at least one scale-out process server.
- To figure out whether you need additional servers, use the following table.
- We recommend that you add a server with the highest spec.

| CPU                                     | MEMORY | CACHE DISK | CHURN RATE       |
|-----------------------------------------|--------|------------|------------------|
| 12 vCPUs<br>2 sockets*6 cores @ 2.5 Ghz | 24 GB  | 1 GB       | Up to 2 TB a day |

Set up the process server as follows:

1. Review the [prerequisites](#).
2. Install the server in the [portal](#), or from the [command line](#).
3. Configure replicated machines to use the new server. If you already have machines replicating:
  - You can [move](#) an entire process server workload to the new process server.

- Alternatively, you can [move](#) specific VMs to the new process server.

## Enable large-scale replication

After planning capacity and deploying the required components and infrastructure, enable replication for large numbers of VMs.

1. Sort machines into batches. You enable replication for VMs within a batch, and then move on to the next batch.
  - For VMware VMs, you can use the [recommended VM batch size](#) in the Deployment Planner report.
  - For physical machines, we recommend you identify batches based on machines that have a similar size and amount of data, and on available network throughput. The aim is to batch machines that are likely to finish their initial replication in around the same amount of time.
2. If disk churn for a machine is high, or exceeds limits in Deployment thePlanner, you can move non-critical files you don't need to replicate (such as log dumps or temp files) off the machine. For VMware VMs, you can move these files to a separate disk, and then [exclude that disk](#) from replication.
3. Before you enable replication, check that machines meet [replication requirements](#).
4. Configure a replication policy for [VMware VMs](#) or [physical servers](#).
5. Enable replication for [VMware VMs](#) or [physical servers](#). This kicks off the initial replication for the selected machines.

## Monitor your deployment

After you kick off replication for the first batch of VMs, start monitoring your deployment as follows:

1. Assign a disaster recovery administrator to monitor the health status of replicated machines.
2. [Monitor events](#) for replicated items and the infrastructure.
3. [Monitor the health](#) of your scale-out process servers.
4. Sign up to get [email notifications](#) for events, for easier monitoring.
5. Conduct regular [disaster recovery drills](#), to ensure that everything's working as expected.

## Plan for large-scale failovers

In an event of disaster, you might need to fail over a large number of machines/workloads to Azure. Prepare for this type of event as follows.

You can prepare in advance for failover as follows:

- [Prepare your infrastructure and VMs](#) so that your workloads will be available after failover, and so that users can access the Azure VMs.
- Note the [failover limits](#) earlier in this document. Make sure your failovers will fall within these limits.
- Run regular [disaster recovery drills](#). Drills help to:
  - Find gaps in your deployment before failover.
  - Estimate end-to-end RTO for your apps.
  - Estimate end-to-end RPO for your workloads.
  - Identify IP address range conflicts.
  - As you run drills, we recommend that you don't use production networks for drills, avoid using the same subnet names in production and test networks, and clean up test failovers after every drill.

To run a large-scale failover, we recommend the following:

1. Create recovery plans for workload failover.
  - Each recovery plan can trigger failover of up to 50 machines.
  - [Learn more](#) about recovery plans.
2. Add Azure Automation runbook scripts to recovery plans, to automate any manual tasks on Azure. Typical tasks include configuring load balancers, updating DNS etc. [Learn more](#)
3. Before failover, prepare Windows machines so that they comply with the Azure environment. [Failover limits](#) are higher for machines that comply. [Learn more](#) about runbooks.
4. Trigger failover with the [Start-AzRecoveryServicesAsrPlannedFailoverJob](#) PowerShell cmdlet, together with a recovery plan.

## Next steps

[Monitor Site Recovery](#)

# Manage VM network interfaces for on-premises disaster recovery to Azure

11/12/2019 • 2 minutes to read • [Edit Online](#)

A virtual machine (VM) in Azure must have at least one network interface attached to it. It can have as many network interfaces attached to it as the VM size supports.

By default, the first network interface attached to an Azure virtual machine is defined as the primary network interface. All other network interfaces in the virtual machine are secondary network interfaces. Also by default, all outbound traffic from the virtual machine is sent out the IP address that's assigned to the primary IP configuration of the primary network interface.

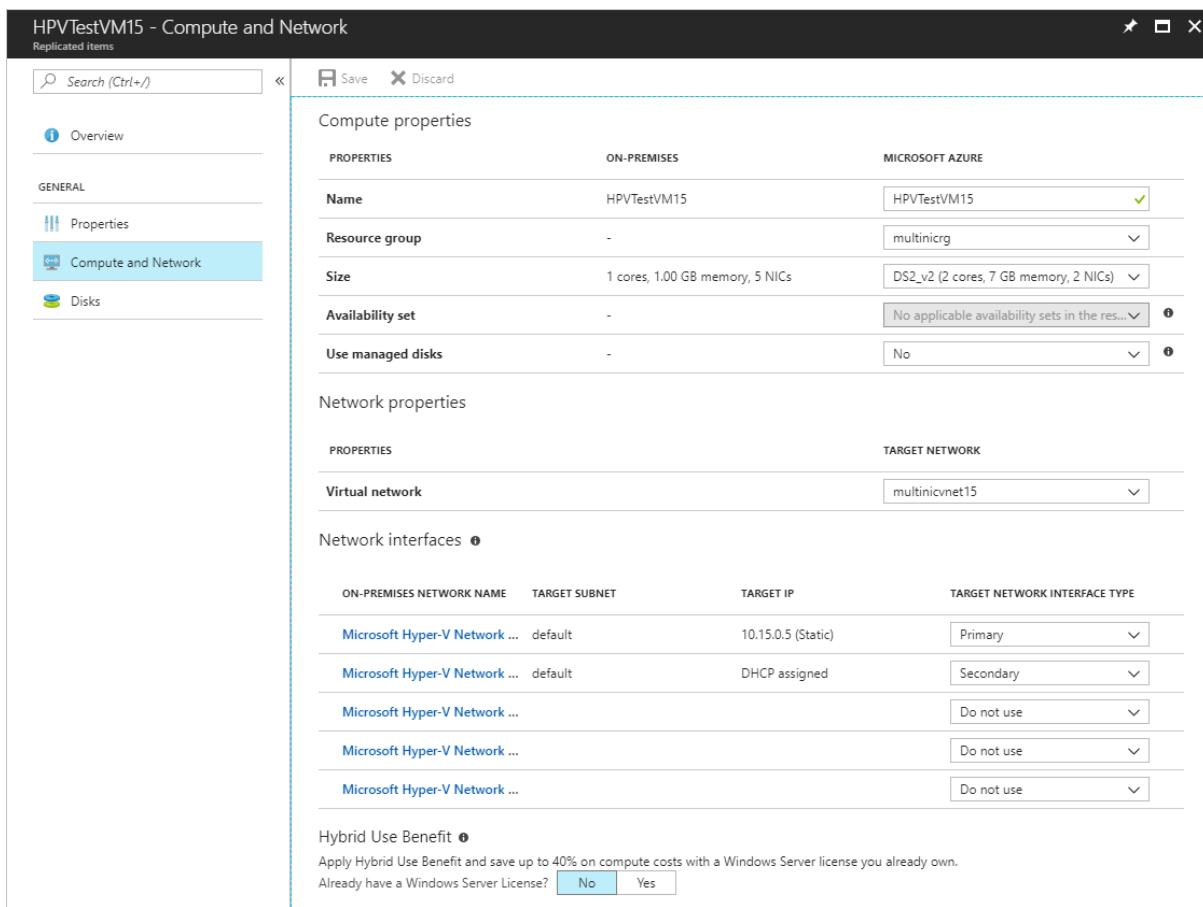
In an on-premises environment, virtual machines or servers can have multiple network interfaces for different networks within the environment. Different networks are typically used for performing specific operations such as upgrades, maintenance, and internet access. When you're migrating or failover to Azure from an on-premises environment, keep in mind that network interfaces in the same virtual machine must all be connected to the same virtual network.

By default, Azure Site Recovery creates as many network interfaces on an Azure virtual machine as are connected to the on-premises server. You can avoid creating redundant network interfaces during migration or failover by editing the network interface settings under the settings for the replicated virtual machine.

## Select the target network

For VMware and physical machines, and for Hyper-V (without System Center Virtual Machine Manager) virtual machines, you can specify the target virtual network for individual virtual machines. For Hyper-V virtual machines managed with Virtual Machine Manager, use [network mapping](#) to map VM networks on a source Virtual Machine Manager server and target Azure networks.

1. Under **Replicated items** in a Recovery Services vault, select any replicated item to access the settings for that replicated item.
2. Select the **Compute and Network** tab to access the network settings for the replicated item.
3. Under **Network properties**, choose a virtual network from the list of available network interfaces.



Modifying the target network affects all network interfaces for that specific virtual machine.

For Virtual Machine Manager clouds, modifying network mapping affects all virtual machines and their network interfaces.

## Select the target interface type

Under the **Network interfaces** section of the **Compute and Network** pane, you can view and edit network interface settings. You can also specify the target network interface type.

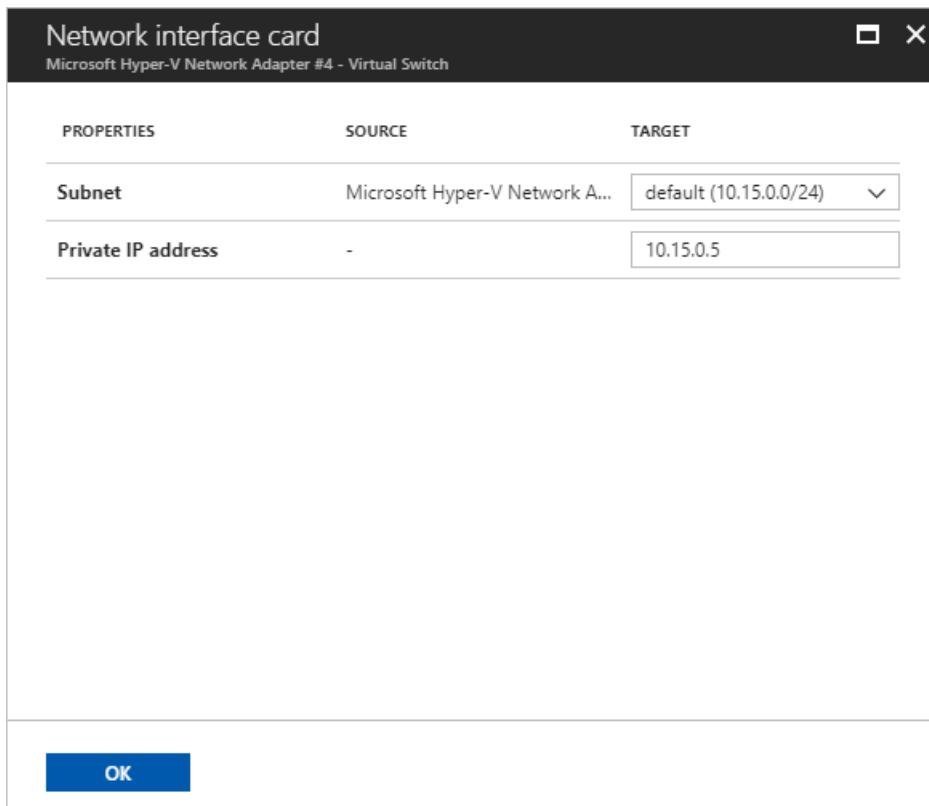
- A **Primary** network interface is required for failover.
- All other selected network interfaces, if any, are **Secondary** network interfaces.
- Select **Do not use** to exclude a network interface from creation at failover.

By default, when you're enabling replication, Site Recovery selects all detected network interfaces on the on-premises server. It marks one as **Primary** and all others as **Secondary**. Any subsequent interfaces added on the on-premises server are marked **Do not use** by default. When you're adding more network interfaces, ensure that the correct Azure virtual machine target size is selected to accommodate all required network interfaces.

## Modify network interface settings

You can modify the subnet and IP address for a replicated item's network interfaces. If an IP address is not specified, Site Recovery will assign the next available IP address from the subnet to the network interface at failover.

1. Select any available network interface to open the network interface settings.
2. Choose the desired subnet from the list of available subnets.
3. Enter the desired IP address (as required).



4. Select **OK** to finish editing and return to the **Compute and Network** pane.
5. Repeat steps 1-4 for other network interfaces.
6. Select **Save** to save all changes.

## Next steps

[Learn more](#) about network interfaces for Azure virtual machines.

# Connect to Azure VMs after failover from on-premises

11/14/2019 • 6 minutes to read • [Edit Online](#)

This article describes how to set up connectivity so that you can successfully connect to Azure VMs after failover.

When you set up disaster recovery of on-premises virtual machines (VMs) and physical servers to Azure, [Azure Site Recovery](#) starts replicating machines to Azure. Then, when outages occur, you can fail over to Azure from your on-premises site. When failover occurs, Site Recovery creates Azure VMs, using replicated on-premises data. As part of disaster recovery planning, you need to figure out how to connect to apps running on these Azure VMs after failover.

In this article you learn how to:

- Prepare on-premises machines before failover.
- Prepare Azure VMs after failover.
- Retain IP addresses on Azure VMs after failover.
- Assign new IP addresses to Azure VMs after failover.

## Prepare on-premises machines

To ensure connectivity to Azure VMs, prepare your on-premises machines before failover.

### Prepare Windows machines

On on-premises Windows machines, do the following:

1. Configure Windows settings. These include removing any static persistent routes or WinHTTP proxy, and setting the disk SAN policy to **OnlineAll**. [Follow](#) these instructions.
2. Make sure [these services](#) are running.
3. Enable remote desktop (RDP) to allow remote connections to the on-premises machine. [Learn how](#) to enable RDP with PowerShell.
4. To access an Azure VM over the internet after failover, in Windows Firewall on the on-premises machine, allow TCP and UDP in the Public profile, and set RDP as an allowed app for all profiles.
5. If you want to access an Azure VM over a site-to-site VPN after failover, in Windows Firewall on the on-premises machine, allow RDP for the Domain and Private profiles. [Learn](#) how to allow RDP traffic.
6. Make sure that there are no Windows updates pending on the on-premises VM when you trigger a failover. If there are, updates might start installing on the Azure VM after failover, and you won't be able to sign into the VM until updates finish.

### Prepare Linux machines

On on-premises Linux machines, do the following:

1. Check that the Secure Shell service is set to start automatically on system boot.
2. Check that firewall rules allow an SSH connection.

## Configure Azure VMs after failover

After failover, do the following on the Azure VMs that are created.

1. To connect to the VM over the internet, assign a public IP address to the VM. You can't use the same public IP address for the Azure VM that you used for your on-premises machine. [Learn more](#)
2. Check that network security group (NSG) rules on the VM allow incoming connections to the RDP or SSH port.
3. Check [Boot diagnostics](#) to view the VM.

#### NOTE

The Azure Bastion service offers private RDP and SSH access to Azure VMs. [Learn more](#) about this service.

## Set a public IP address

As an alternative to assigning a public IP address manually to an Azure VM, you can assign the address during failover using a script or Azure automation runbook in a Site Recovery [recovery plan](#), or you can set up DNS-level routing using Azure Traffic Manager. [Learn more](#) about setting up a public address.

## Assign an internal address

To set the internal IP address of an Azure VM after failover, you have a couple of options:

- **Retain same IP address:** You can use the same IP address on the Azure VM as the one allocated to the on-premises machine.
- **Use different IP address:** You can use a different IP address for the Azure VM.

## Retain IP addresses

Site Recovery lets you retain the same IP addresses when failing over to Azure. Retaining the same IP address avoids potential network issues after failover, but does introduce some complexity.

- If the target Azure VM uses the same IP address/subnet as your on-premises site, you can't connect between them using a site-to-site VPN connection or ExpressRoute, because of the address overlap. Subnets must be unique.
- You need a connection from on-premises to Azure after failover, so that apps are available on Azure VMs. Azure doesn't support stretched VLANs, so if you want to retain IP addresses you need to take the IP space over to Azure by failing over the entire subnet, in addition to the on-premises machine.
- Subnet failover ensures that a specific subnet isn't available simultaneously on-premises and in Azure.

Retaining IP addresses requires the following steps:

- In the Compute & Network properties of the replicated item, set network and IP addressing for the target Azure VM to mirror the on-premises setting.
- Subnets must be managed as part of the disaster recovery process. You need an Azure VNet to match the on-premises network, and after failover network routes must be modified to reflect that the subnet has moved to Azure, and new IP address locations.

## Failover example

Let's look at an example.

- The fictitious company Woodgrove Bank hosts their business apps on-premises. They host their mobile apps in Azure.
- They connect from on-premises to Azure over site-to-site VPN.
- Woodgrove is using Site Recovery to replicate on-premises machines to Azure.
- Their on-premises apps use hard-coded IP addresses, so they want to retain the same IP addresses in Azure.

- On-premises the machines running the apps are running in three subnets:
  - 192.168.1.0/24.
  - 192.168.2.0/24
  - 192.168.3.0/24
- Their apps running in Azure are located in the Azure VNet **Azure Network** in two subnets:
  - 172.16.1.0/24
  - 172.16.2.0/24.

In order to retain the addresses, here's what they do.

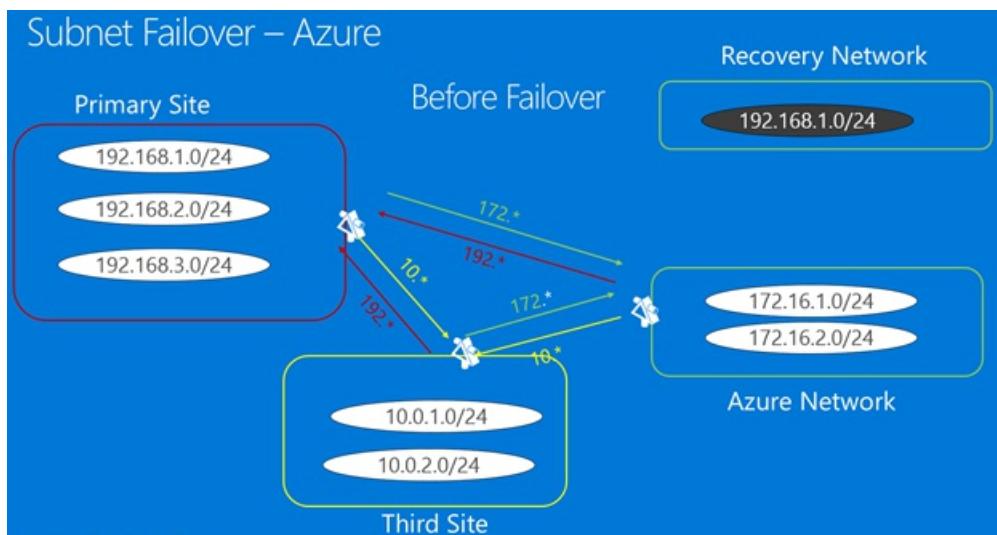
- When they enable replication, they specify that machines should replicate to the **Azure Network**.
- They create **Recovery Network** in Azure. This VNet mirrors the 192.168.1.0/24 subnet in their on-premises network.
- Woodgrove sets up a [VNet-to-VNet connection](#) between the two networks.

#### NOTE

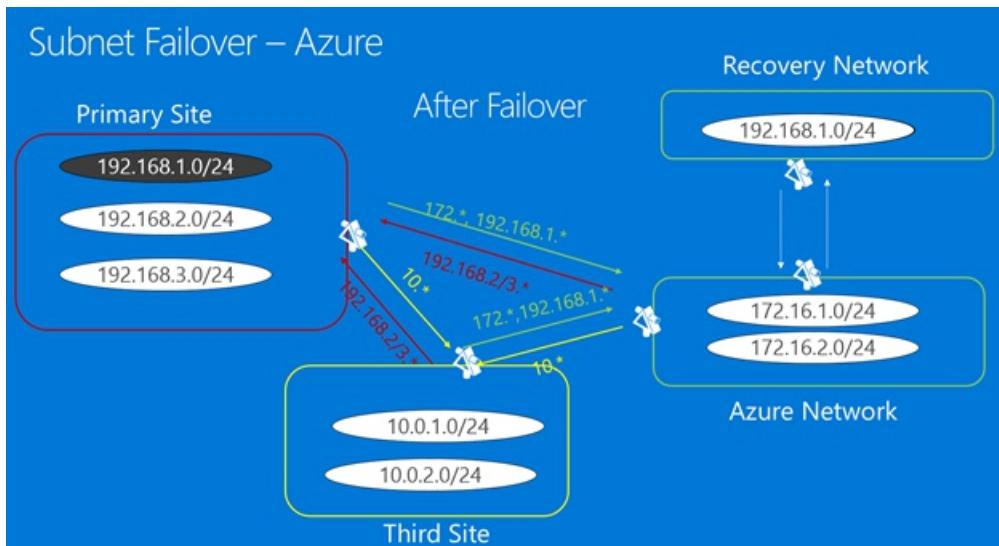
Depending on application requirements, a VNet-to-VNet connection could be set up before failover, as a manual step/scripted step/Azure automation runbook in a Site Recovery [recovery plan](#), or after failover is complete.

- Before failover, on the machine properties in Site Recovery, they set the target IP address to the address of the on-premises machine, as described in the next procedure.
- After failover, the Azure VMs are created with the same IP address. Woodgrove connects from **Azure Network** to **Recovery Network** VNet using VNet peering (with transit connectivity enabled).
- On-premises, Woodgrove needs to make network changes, including modifying routes to reflect that 192.168.1.0/24 has moved to Azure.

#### Infrastructure before failover



#### Infrastructure after failover



## Set target network settings

Before failover, specify the network settings and IP address for the target Azure VM.

1. In the Recovery Services vault -> **Replicated items**, select the on-premises machine.
2. In the **Compute and Network** page for the machine, click **Edit**, to configure network and adapter settings for the target Azure VM.
3. In **Network properties**, select the target network in which the Azure VM will be located when it's created after failover.
4. In **Network interfaces**, configure the network adapters in the target network. By default Site Recovery shows all detected NICs on the on-premises machine.
  - In **Target network interface type** you can set each NIC as **Primary**, **Secondary**, or **Do not create** if you don't need that specific NIC in the target network. One network adapter must be set as primary for failover. Note that modifying the target network affects all NICs for the Azure VM.
  - Click the NIC name to specify the subnet in which the Azure VM will be deployed.
  - Overwrite **Dynamic** with the private IP address you want to assign to target Azure VM. If an IP address isn't specified Site Recovery will assign the next available IP address in the subnet to the NIC at failover.
  - [Learn more](#) about managing NICs for on-premises failover to Azure.

## Get new IP addresses

In this scenario, the Azure VM gets a new IP address after failover. A DNS update to update records for failed over machines to point to the IP address of the Azure VM.

## Next steps

[Learn about](#) replicating on-premises Active Directory and DNS to Azure.

# Set up disaster recovery to Azure for on-premises physical servers

1/14/2020 • 9 minutes to read • [Edit Online](#)

The [Azure Site Recovery](#) service contributes to your disaster recovery strategy by managing and orchestrating replication, failover, and failback of on-premises machines, and Azure virtual machines (VMs).

This tutorial shows you how to set up disaster recovery of on-premises physical Windows and Linux servers to Azure. In this tutorial, you learn how to:

- Set up Azure and on-premises prerequisites
- Create a Recovery Services vault for Site Recovery
- Set up the source and target replication environments
- Create a replication policy
- Enable replication for a server

## Prerequisites

To complete this tutorial:

- Make sure that you understand the [architecture and components](#) for this scenario.
- Review the [support requirements](#) for all components.
- Make sure that the servers you want to replicate comply with [Azure VM requirements](#).
- Prepare Azure. You need an Azure subscription, an Azure virtual network, and a storage account.
- Prepare an account for automatic installation of the Mobility service on each server you want to replicate.

Before you begin, note that:

- After failover to Azure, physical servers can't be failed back to on-premises physical machines. You can only fail back to VMware VMs.
- This tutorial sets up physical server disaster recovery to Azure with the simplest settings. If you want to learn about other options, read through our How To guides:
  - Set up the [replication source](#), including the Site Recovery configuration server.
  - Set up the [replication target](#).
  - Configure a [replication policy](#), and [enable replication](#).

### Set up an Azure account

Get a Microsoft [Azure account](#).

- You can start with a [free trial](#).
- Learn about [Site Recovery pricing](#), and get [pricing details](#).
- Find out which [regions are supported](#) for Site Recovery.

### Verify Azure account permissions

Make sure your Azure account has permissions for replication of VMs to Azure.

- Review the [permissions](#) you need to replicate machines to Azure.
- Verify and modify [role-based access](#) permissions.

### Set up an Azure network

Set up an [Azure network](#).

- Azure VMs are placed in this network when they're created after failover.
- The network should be in the same region as the Recovery Services vault

## Set up an Azure storage account

Set up an [Azure storage account](#).

- Site Recovery replicates on-premises machines to Azure storage. Azure VMs are created from the storage after failover occurs.
- The storage account must be in the same region as the Recovery Services vault.

### Prepare an account for Mobility service installation

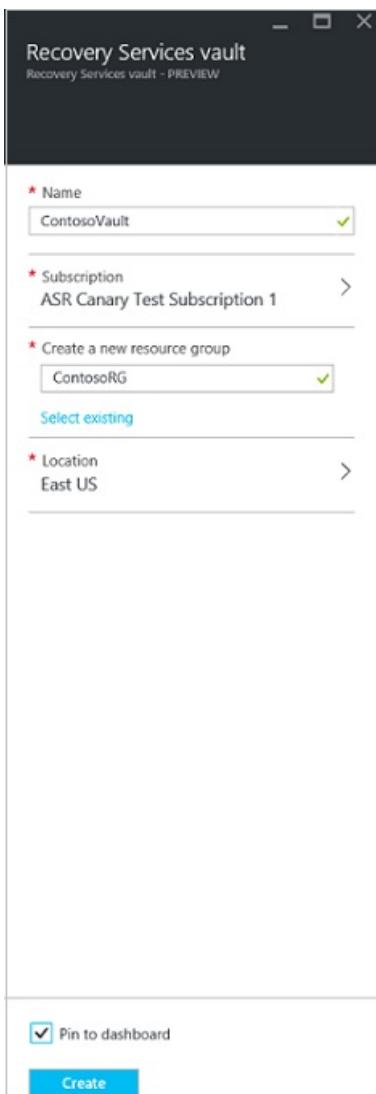
The Mobility service must be installed on each server you want to replicate. Site Recovery installs this service automatically when you enable replication for the server. To install automatically, you need to prepare an account that Site Recovery will use to access the server.

- You can use a domain or local account
- For Windows VMs, if you're not using a domain account, disable Remote User Access control on the local machine. To do this, in the register under **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System**, add the DWORD entry **LocalAccountTokenFilterPolicy**, with a value of 1.
- To add the registry entry to disable the setting from a CLI, type:  

```
REG ADD HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v LocalAccountTokenFilterPolicy /t REG_DWORD /d 1.
```
- For Linux, the account should be root on the source Linux server.

## Create a vault

1. Sign in to the [Azure portal](#) > **Recovery Services**.
2. Click **Create a resource** > **Monitoring + Management** > **Backup and Site Recovery**.
3. In **Name**, specify a friendly name to identify the vault. If you have more than one subscription, select the appropriate one.
4. [Create a resource group](#), or select an existing one. Specify an Azure region.
5. To quickly access the vault from the dashboard, click **Pin to dashboard** > **Create**.



The new vault will appear on the **Dashboard > All resources**, and on the main **Recovery Services vaults** page.

## Select a protection goal

Select what to replicate, and to replicate it to.

1. Click **Recovery Services vaults** > vault.
2. In the Resource Menu, click **Site Recovery** > **Prepare Infrastructure** > **Protection goal**.
3. In **Protection goal**, select **To Azure** > **Not virtualized/Other**.

## Set up the source environment

Set up the configuration server, register it in the vault, and discover VMs.

1. Click **Site Recovery** > **Prepare Infrastructure** > **Source**.
2. If you don't have a configuration server, click **+Configuration server**.
3. In **Add Server**, check that **Configuration Server** appears in **Server type**.
4. Download the Site Recovery Unified Setup installation file.
5. Download the vault registration key. You need this when you run Unified Setup. The key is valid for five days after you generate it.

**Add Server**  
ContosoDR - PREVIEW

Server type  
Configuration Server

**i** Adding Configuration Server may take 15 minutes to 30 minutes

Register your Configuration Server  
On-premises

1. Make sure server on which you plan to set up the Configuration Server is running Windows Server 2012 R2 virtual machine
2. Configure Proxy so that server can access the [Service URLs](#)
3. [Download](#) the Microsoft Azure Site Recovery Unified Setup
4. Download the vault registration key  
[Download](#)
5. Run the installer to set up the Configuration Server and Process Server and use the vault registration key to register it with the vault. [Learn more](#).
6. Run `cpsconfigtool.exe` to create one or more management accounts on the configuration server.
7. If you're protecting VMware VMs make sure the management accounts have administrator permissions on the vCenter server/vSphere host: Server/ESXi host from which you'll replicate virtual machines. [Learn more](#).
8. If you're protecting physical servers make sure the management accounts have administrator permissions on the physical host.

## Register the configuration server in the vault

Do the following before you start:

### Verify time accuracy

On the configuration server machine, make sure that the system clock is synchronized with a [Time Server](#). It should match. If it's 15 minutes in front or behind, setup might fail.

### Verify connectivity

Make sure the machine can access these URLs based on your environment:

| NAME                   | COMMERCIAL URL                            | GOVERNMENT URL                            | DESCRIPTION                                                                      |
|------------------------|-------------------------------------------|-------------------------------------------|----------------------------------------------------------------------------------|
| Azure Active Directory | <code>login.microsoftonline.com</code>    | <code>login.microsoftonline.us</code>     | Used for access control and identity management by using Azure Active Directory. |
| Backup                 | <code>*.backup.windowsazure.com</code>    | <code>*.backup.windowsazure.us</code>     | Used for replication data transfer and coordination.                             |
| Replication            | <code>*.hypervrecoverymanager.wind</code> | <code>*.hypervrecoverymanager.wind</code> | Used for application management operations and coordination.                     |

| Name                 | Commercial URL               | Government URL                | Description                                                                           |
|----------------------|------------------------------|-------------------------------|---------------------------------------------------------------------------------------|
| Storage              | *.blob.core.windows.net      | *.blob.core.usgovcloudapi.net | Used for access to the storage account that stores replicated data.                   |
| Telemetry (optional) | dc.services.visualstudio.com | dc.services.visualstudio.com  | Used for telemetry.                                                                   |
| Time synchronization | time.windows.com             | time.nist.gov                 | Used to check time synchronization between system and global time in all deployments. |

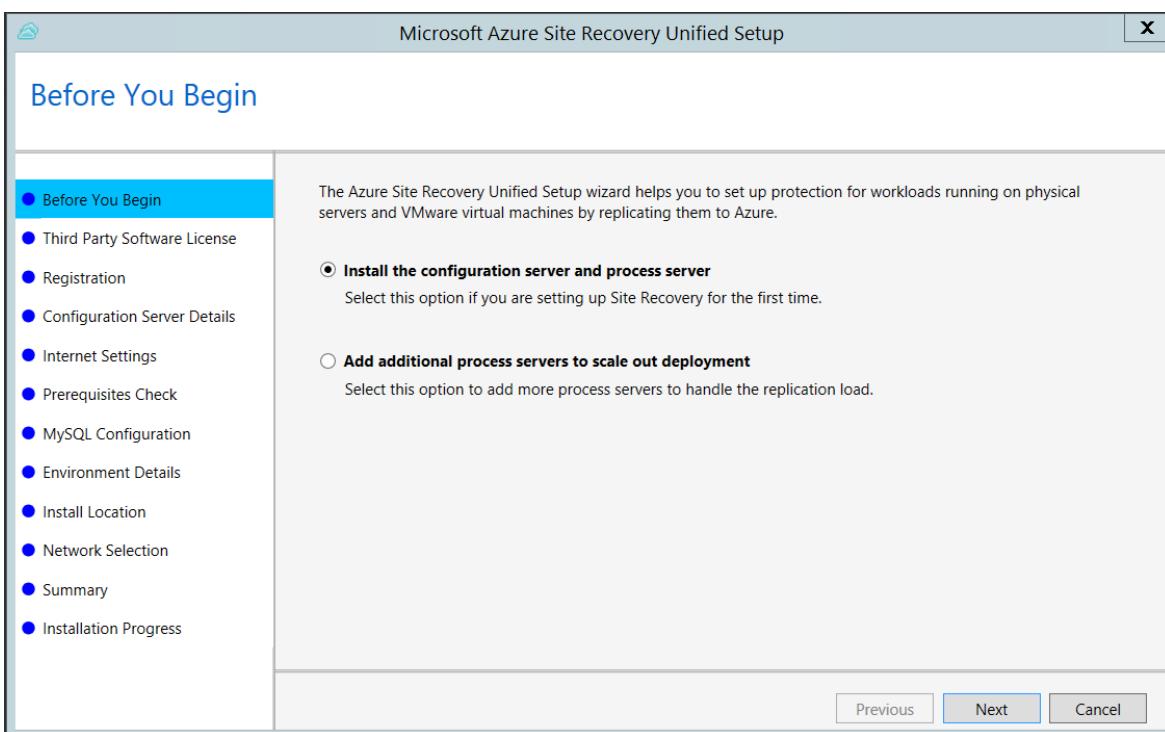
IP address-based firewall rules should allow communication to all of the Azure URLs that are listed above over HTTPS (443) port. To simplify and limit the IP Ranges, it is recommended that URL filtering be done.

- **Commercial IPs** - Allow the [Azure Datacenter IP Ranges](#), and the HTTPS (443) port. Allow IP address ranges for the Azure region of your subscription to support the AAD, Backup, Replication, and Storage URLs.
- **Government IPs** - Allow the [Azure Government Datacenter IP Ranges](#), and the HTTPS (443) port for all USGov Regions (Virginia, Texas, Arizona, and Iowa) to support AAD, Backup, Replication, and Storage URLs.

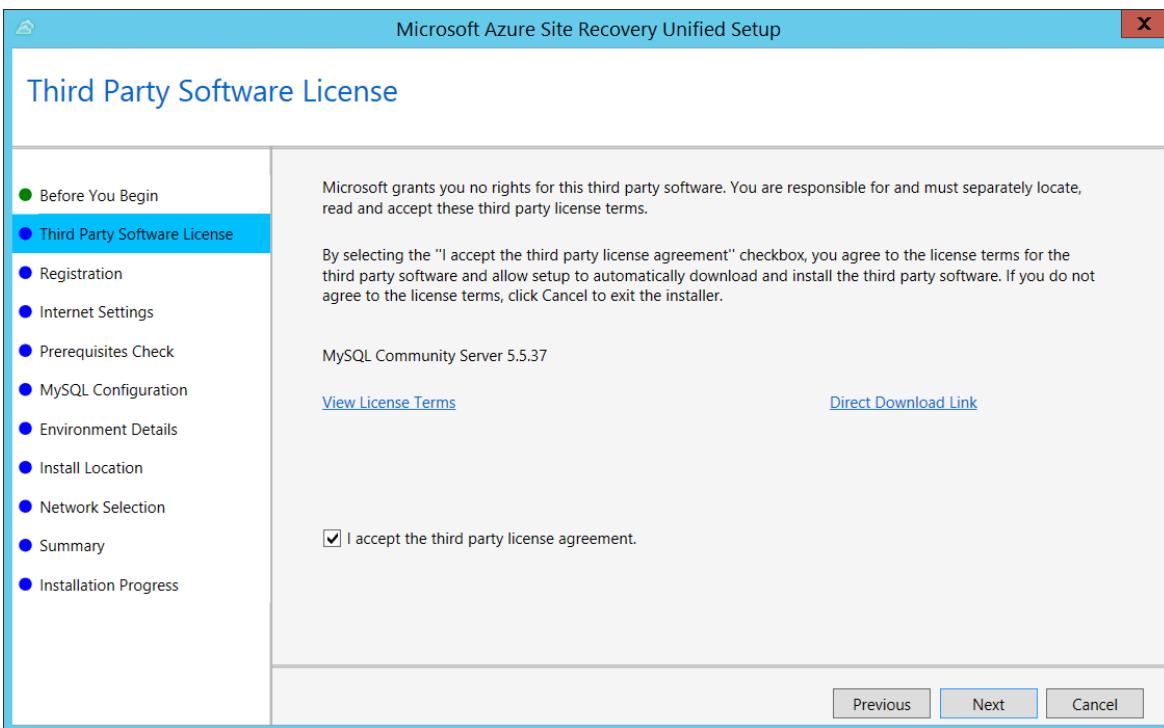
#### Run setup

Run Unified Setup as a Local Administrator, to install the configuration server. The process server and the master target server are also installed by default on the configuration server.

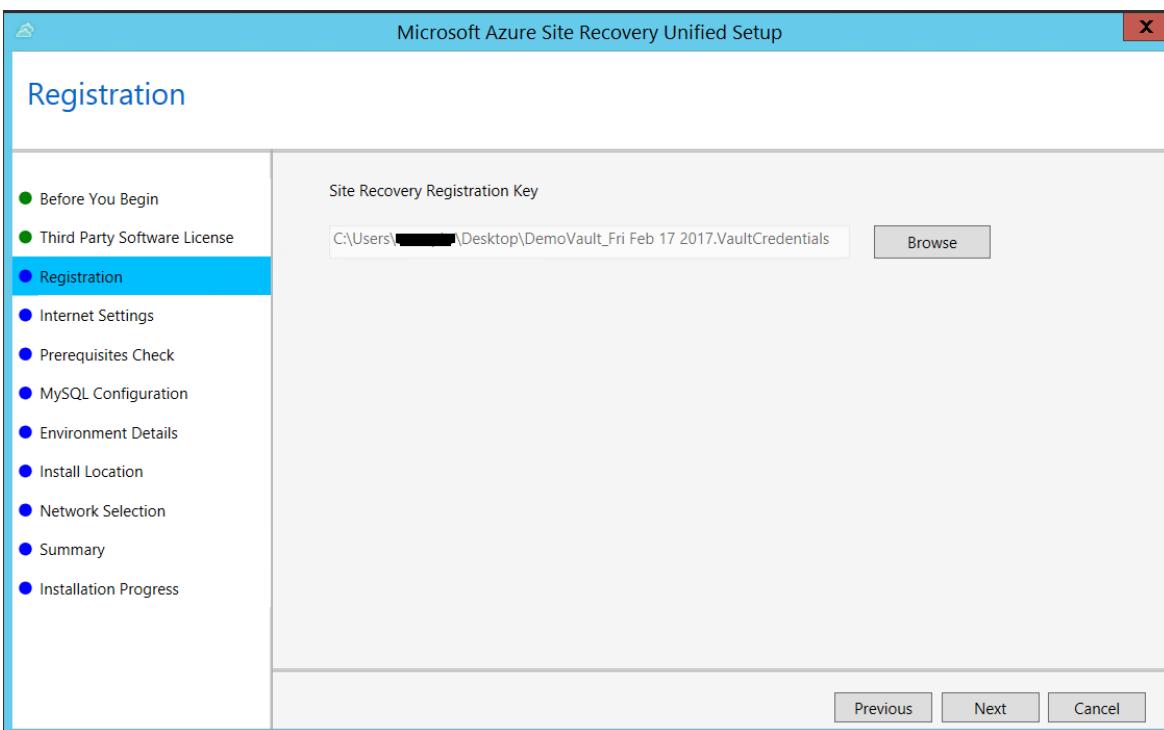
1. Run the Unified Setup installation file.
2. In **Before You Begin**, select **Install the configuration server and process server**.



3. In **Third Party Software License**, click **I Accept** to download and install MySQL.

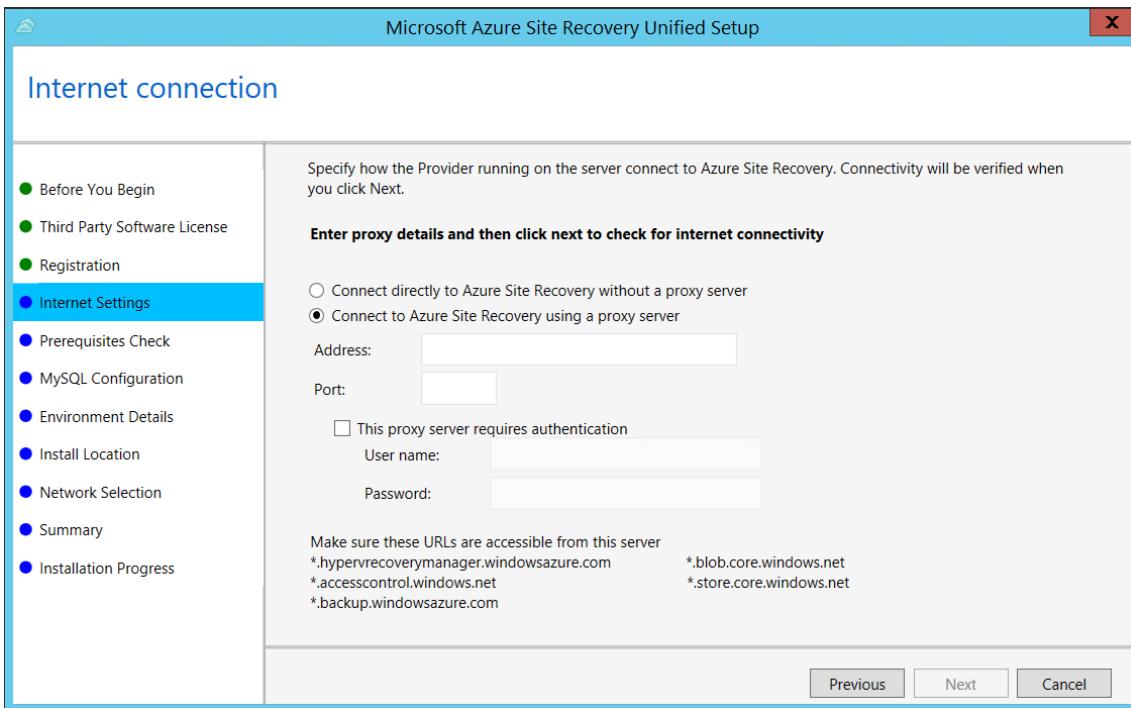


4. In **Registration**, select the registration key you downloaded from the vault.

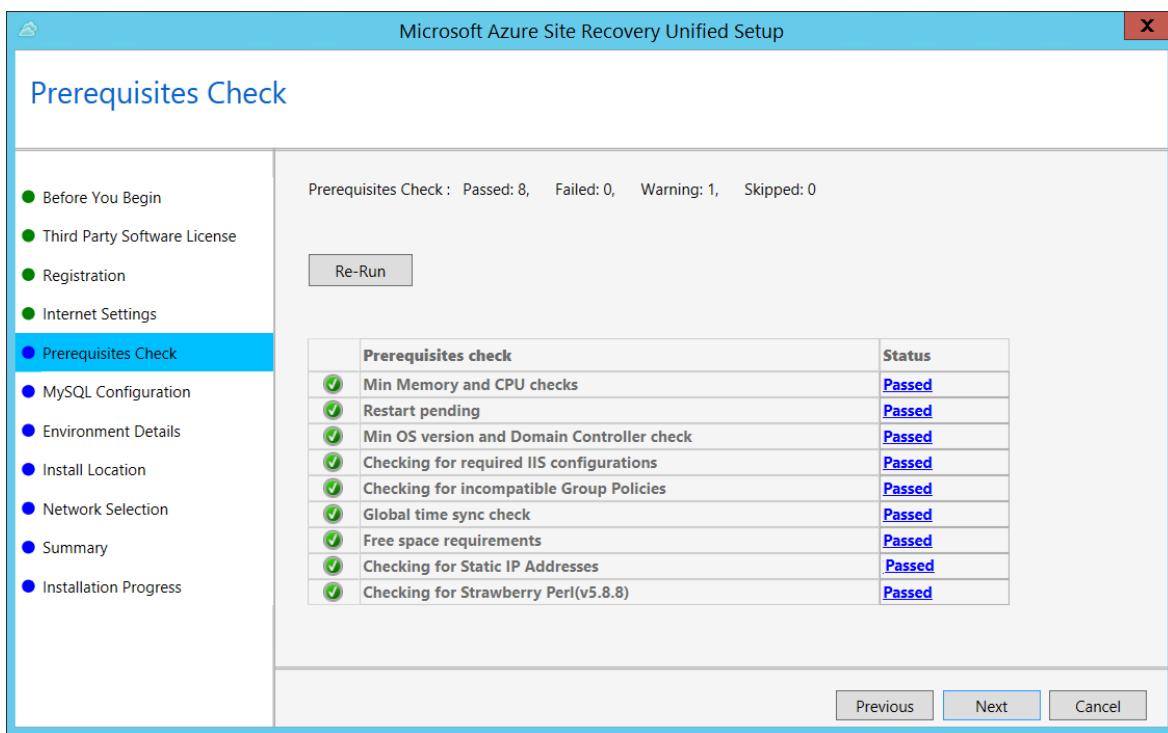


5. In **Internet Settings**, specify how the Provider running on the configuration server connects to Azure Site Recovery over the Internet. Make sure you've allowed the required URLs.

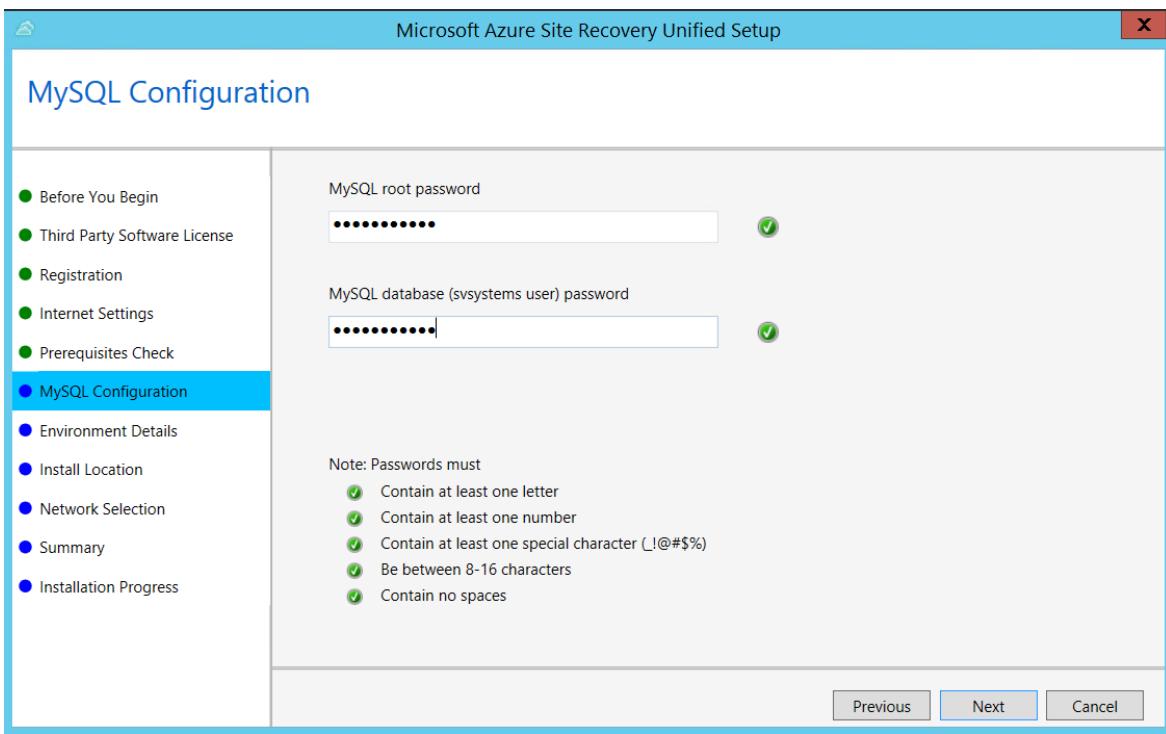
- If you want to connect with the proxy that's currently set up on the machine, select **Connect to Azure Site Recovery using a proxy server**.
- If you want the Provider to connect directly, select **Connect directly to Azure Site Recovery without a proxy server**.
- If the existing proxy requires authentication, or if you want to use a custom proxy for the Provider connection, select **Connect with custom proxy settings**, and specify the address, port, and credentials.



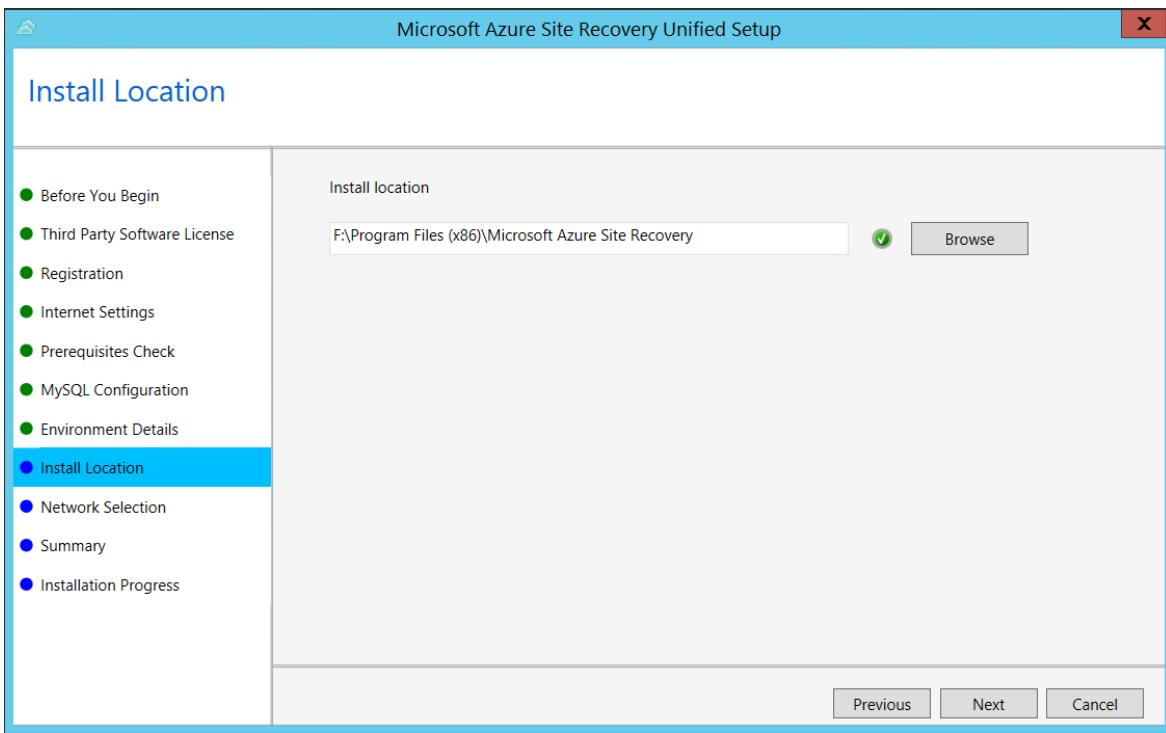
6. In **Prerequisites Check**, Setup runs a check to make sure that installation can run. If a warning appears about the **Global time sync check**, verify that the time on the system clock (**Date and Time** settings) is the same as the time zone.



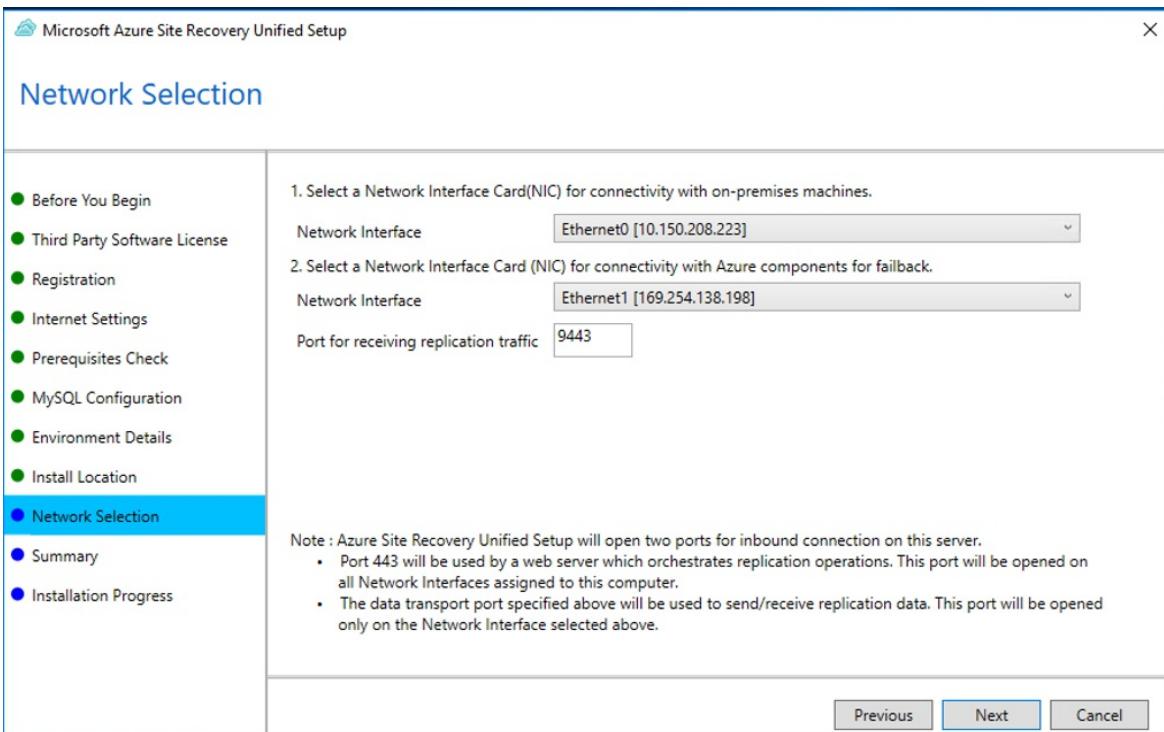
7. In **MySQL Configuration**, create credentials for logging on to the MySQL server instance that is installed.



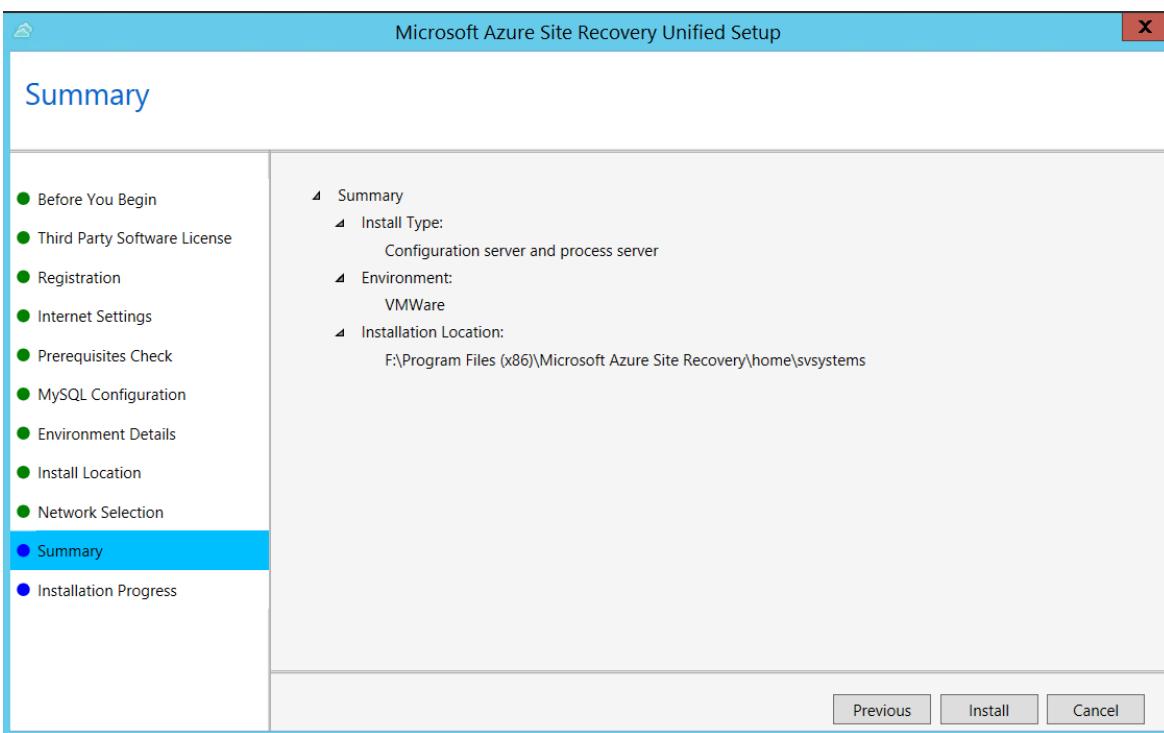
8. In **Environment Details**, select No if you're replicating Azure Stack VMs or physical servers.
9. In **Install Location**, select where you want to install the binaries and store the cache. The drive you select must have at least 5 GB of disk space available, but we recommend a cache drive with at least 600 GB of free space.



10. In **Network Selection**, first select the NIC that the in-built process server uses for discovery and push installation of mobility service on source machines, and then select the NIC that Configuration Server uses for connectivity with Azure. Port 9443 is the default port used for sending and receiving replication traffic, but you can modify this port number to suit your environment's requirements. In addition to the port 9443, we also open port 443, which is used by a web server to orchestrate replication operations. Do not use port 443 for sending or receiving replication traffic.



11. In **Summary**, review the information and click **Install**. When installation finishes, a passphrase is generated. You will need this when you enable replication, so copy it and keep it in a secure location.



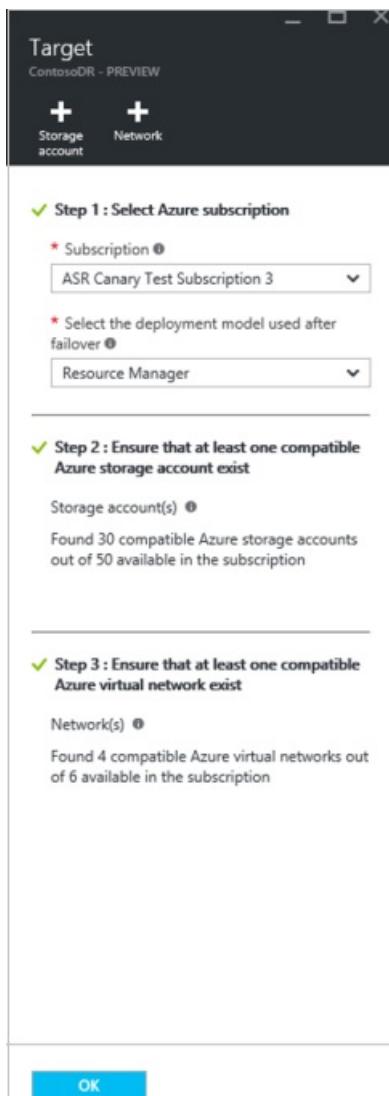
After registration finishes, the server is displayed on the **Settings > Servers** blade in the vault.

After registration finishes, the configuration server is displayed on the **Settings > Servers** page in the vault.

## Set up the target environment

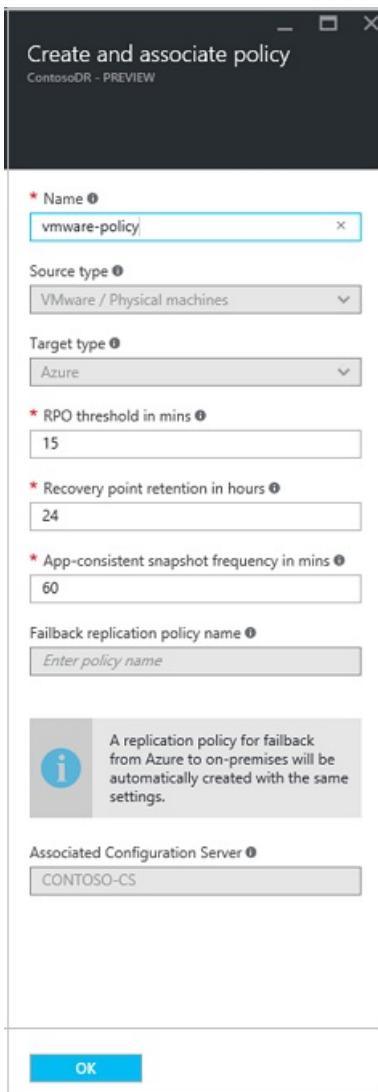
Select and verify target resources.

1. Click **Prepare infrastructure > Target**, and select the Azure subscription you want to use.
2. Specify the target deployment model.
3. Site Recovery checks that you have one or more compatible Azure storage accounts and networks.



## Create a replication policy

1. To create a new replication policy, click **Site Recovery infrastructure > Replication Policies > +Replication Policy**.
2. In **Create replication policy**, specify a policy name.
3. In **RPO threshold**, specify the recovery point objective (RPO) limit. This value specifies how often data recovery points are created. An alert is generated if continuous replication exceeds this limit.
4. In **Recovery point retention**, specify how long (in hours) the retention window is for each recovery point. Replicated VMs can be recovered to any point in a window. Up to 24 hours retention is supported for machines replicated to premium storage, and 72 hours for standard storage.
5. In **App-consistent snapshot frequency**, specify how often (in minutes) recovery points containing application-consistent snapshots will be created. Click **OK** to create the policy.



The policy is automatically associated with the configuration server. By default, a matching policy is automatically created for failback. For example, if the replication policy is **rep-policy** then a failback policy **rep-policy-failback** is created. This policy isn't used until you initiate a failback from Azure.

## Enable replication

Enable replication for each server.

- Site Recovery will install the Mobility service when replication is enabled.
  - When you enable replication for a server, it can take 15 minutes or longer for changes to take effect, and appear in the portal.
1. Click **Replicate application > Source**.
  2. In **Source**, select the configuration server.
  3. In **Machine type**, select **Physical machines**.
  4. Select the process server (the configuration server). Then click **OK**.
  5. In **Target**, select the subscription and the resource group in which you want to create the Azure VMs after failover. Choose the deployment model that you want to use in Azure (classic or resource management).
  6. Select the Azure storage account you want to use for replicating data.
  7. Select the Azure network and subnet to which Azure VMs will connect, when they're created after failover.
  8. Select **Configure now for selected machines**, to apply the network setting to all machines you select for protection. Select **Configure later** to select the Azure network per machine.
  9. In **Physical Machines**, and click **+Physical machine**. Specify the name and IP address. Select the operating system of the machine you want to replicate. It takes a few minutes for the servers to be discovered and

listed.

10. In **Properties > Configure properties**, select the account that will be used by the process server to automatically install the Mobility service on the machine.
11. In **Replication settings > Configure replication settings**, verify that the correct replication policy is selected.
12. Click **Enable Replication**. You can track progress of the **Enable Protection** job in **Settings > Jobs > Site Recovery Jobs**. After the **Finalize Protection** job runs the machine is ready for failover.

To monitor servers you add, you can check the last discovered time for them in **Configuration Servers > Last Contact At**. To add machines without waiting for a scheduled discovery time, highlight the configuration server (don't click it), and click **Refresh**.

## Next steps

[Run a disaster recovery drill.](#)

# Set up the configuration server for disaster recovery of physical servers to Azure

7/5/2019 • 6 minutes to read • [Edit Online](#)

This article describes how to set up your on-premises environment to start replicating physical servers running Windows or Linux into Azure.

## Prerequisites

The article assumes that you already have:

- A Recovery Services vault in the [Azure portal](#).
- A physical computer on which to install the configuration server.
- If you've disabled TLS 1.0 on the machine on which you're installing the configuration server, make sure that TLS 1.2 is enabled, and that the .NET Framework version 4.6 or later is installed on the machine (with strong cryptography enabled). [Learn more](#).

### Configuration server minimum requirements

The following table lists the minimum hardware, software, and network requirements for a configuration server.

### Configuration and process server requirements

## Hardware requirements

| COMPONENT                              | REQUIREMENT                                                                           |
|----------------------------------------|---------------------------------------------------------------------------------------|
| CPU cores                              | 8                                                                                     |
| RAM                                    | 16 GB                                                                                 |
| Number of disks                        | 3, including the OS disk, process server cache disk, and retention drive for failback |
| Free disk space (process server cache) | 600 GB                                                                                |
| Free disk space (retention disk)       | 600 GB                                                                                |

## Software requirements

| COMPONENT               | REQUIREMENT                                   |
|-------------------------|-----------------------------------------------|
| Operating system        | Windows Server 2012 R2<br>Windows Server 2016 |
| Operating system locale | English (en-us)                               |

| COMPONENT                                       | REQUIREMENT                                                                                                                                                                                                                                                                                                  |
|-------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Windows Server roles                            | <p>Don't enable these roles:</p> <ul style="list-style-type: none"> <li>- Active Directory Domain Services</li> <li>- Internet Information Services</li> <li>- Hyper-V</li> </ul>                                                                                                                            |
| Group policies                                  | <p>Don't enable these group policies:</p> <ul style="list-style-type: none"> <li>- Prevent access to the command prompt.</li> <li>- Prevent access to registry editing tools.</li> <li>- Trust logic for file attachments.</li> <li>- Turn on Script Execution.</li> </ul> <p><a href="#">Learn more</a></p> |
| IIS                                             | <ul style="list-style-type: none"> <li>- No pre-existing default website</li> <li>- No pre-existing website/application listening on port 443</li> <li>- Enable <a href="#">anonymous authentication</a></li> <li>- Enable <a href="#">FastCGI</a> setting</li> </ul>                                        |
| FIPS (Federal Information Processing Standards) | Do not enable FIPS mode                                                                                                                                                                                                                                                                                      |
|                                                 |                                                                                                                                                                                                                                                                                                              |

## Network requirements

| COMPONENT                                                                                      | REQUIREMENT                                                       |
|------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|
| IP address type                                                                                | Static                                                            |
| Ports                                                                                          | 443 (Control channel orchestration)<br>9443 (Data transport)      |
| NIC type                                                                                       | VMXNET3 (if the configuration server is a VMware VM)              |
|                                                                                                |                                                                   |
| <b>Internet access</b> (the server needs access to the following URLs, directly or via proxy): |                                                                   |
| *.backup.windowsazure.com                                                                      | Used for replicated data transfer and coordination                |
| *.store.core.windows.net                                                                       | Used for replicated data transfer and coordination                |
| *.blob.core.windows.net                                                                        | Used to access storage account that stores replicated data        |
| *.hypervrecoverymanager.windowsazure.com                                                       | Used for replication management operations and coordination       |
| https://management.azure.com                                                                   | Used for replication management operations and coordination       |
| *.services.visualstudio.com                                                                    | Used for telemetry purposes (optional)                            |
| time.nist.gov                                                                                  | Used to check time synchronization between system and global time |

| COMPONENT                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | REQUIREMENT                                                                                                                                                  |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| time.windows.com                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Used to check time synchronization between system and global time                                                                                            |
| <ul style="list-style-type: none"> <li>• <a href="https://login.microsoftonline.com">https://login.microsoftonline.com</a></li> <li>• <a href="https://secure.aadcdn.microsoftonline-p.com">https://secure.aadcdn.microsoftonline-p.com</a></li> <li>• <a href="https://login.live.com">https://login.live.com</a></li> <li>• <a href="https://graph.windows.net">https://graph.windows.net</a></li> <li>• <a href="https://login.windows.net">https://login.windows.net</a></li> <li>• <a href="https://www.live.com">https://www.live.com</a></li> <li>• <a href="https://www.microsoft.com">https://www.microsoft.com</a></li> </ul> | OVF setup needs access to these URLs. They're used for access control and identity management by Azure Active Directory.                                     |
| <a href="https://dev.mysql.com/get/Downloads/MySQLInstaller/mysql-installer-community-5.7.20.0.msi">https://dev.mysql.com/get/Downloads/MySQLInstaller/mysql-installer-community-5.7.20.0.msi</a>                                                                                                                                                                                                                                                                                                                                                                                                                                       | To complete MySQL download.<br>In a few regions, the download might be redirected to the CDN URL. Ensure that the CDN URL is also whitelisted, if necessary. |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                                                                                                                                              |

## Required software

| COMPONENT               | REQUIREMENT                                                                                                                                              |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| VMware vSphere PowerCLI | <a href="#">PowerCLI version 6.0</a> should be installed if the Configuration Server is running on a VMware VM.                                          |
| MYSQL                   | MySQL should be installed. You can install manually, or Site Recovery can install it. (Refer to <a href="#">configure settings</a> for more information) |
|                         |                                                                                                                                                          |

## Sizing and capacity requirements

The following table summarizes capacity requirements for the configuration server. If you're replicating multiple VMware VMs, review the [capacity planning considerations](#) and run the [Azure Site Recovery Deployment Planner tool](#).

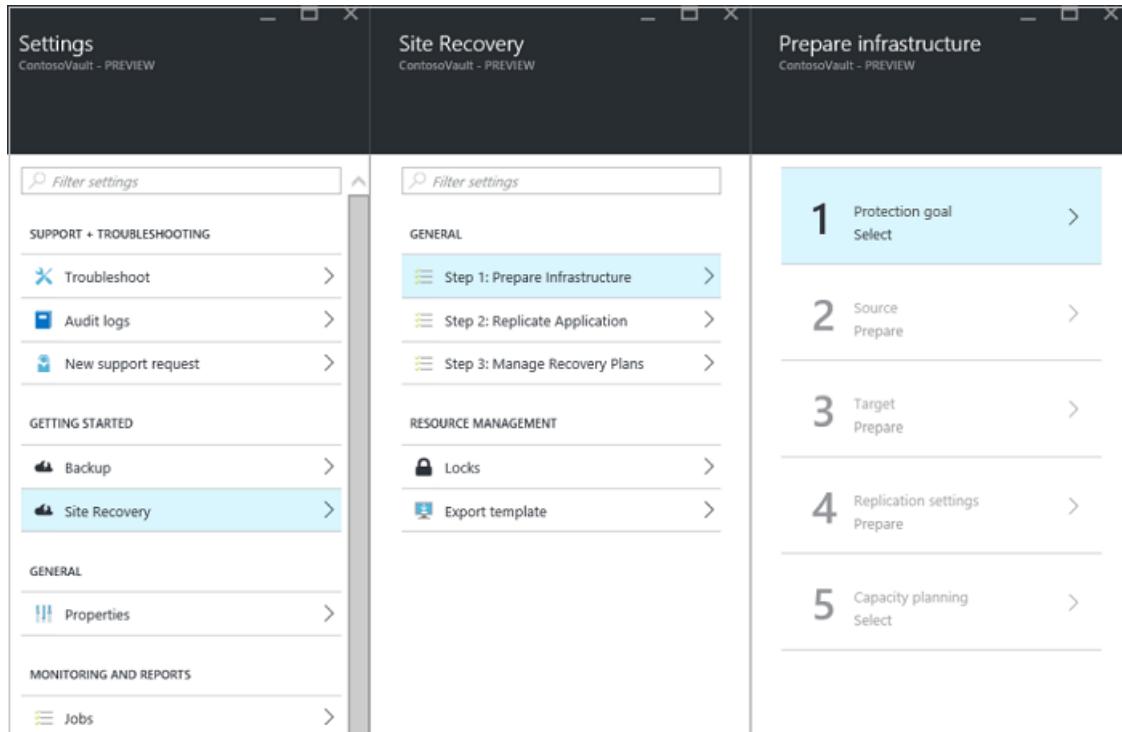
| CPU                                          | MEMORY | CACHE DISK | DATA CHANGE RATE | REPLICATED MACHINES |
|----------------------------------------------|--------|------------|------------------|---------------------|
| 8 vCPUs<br><br>2 sockets * 4 cores @ 2.5 GHz | 16 GB  | 300 GB     | 500 GB or less   | < 100 machines      |
| 12 vCPUs<br><br>2 socks * 6 cores @ 2.5 GHz  | 18 GB  | 600 GB     | 500 GB-1 TB      | 100 to 150 machines |
| 16 vCPUs<br><br>2 socks * 8 cores @ 2.5 GHz  | 32 GB  | 1 TB       | 1-2 TB           | 150 -200 machines   |
|                                              |        |            |                  |                     |

**NOTE**

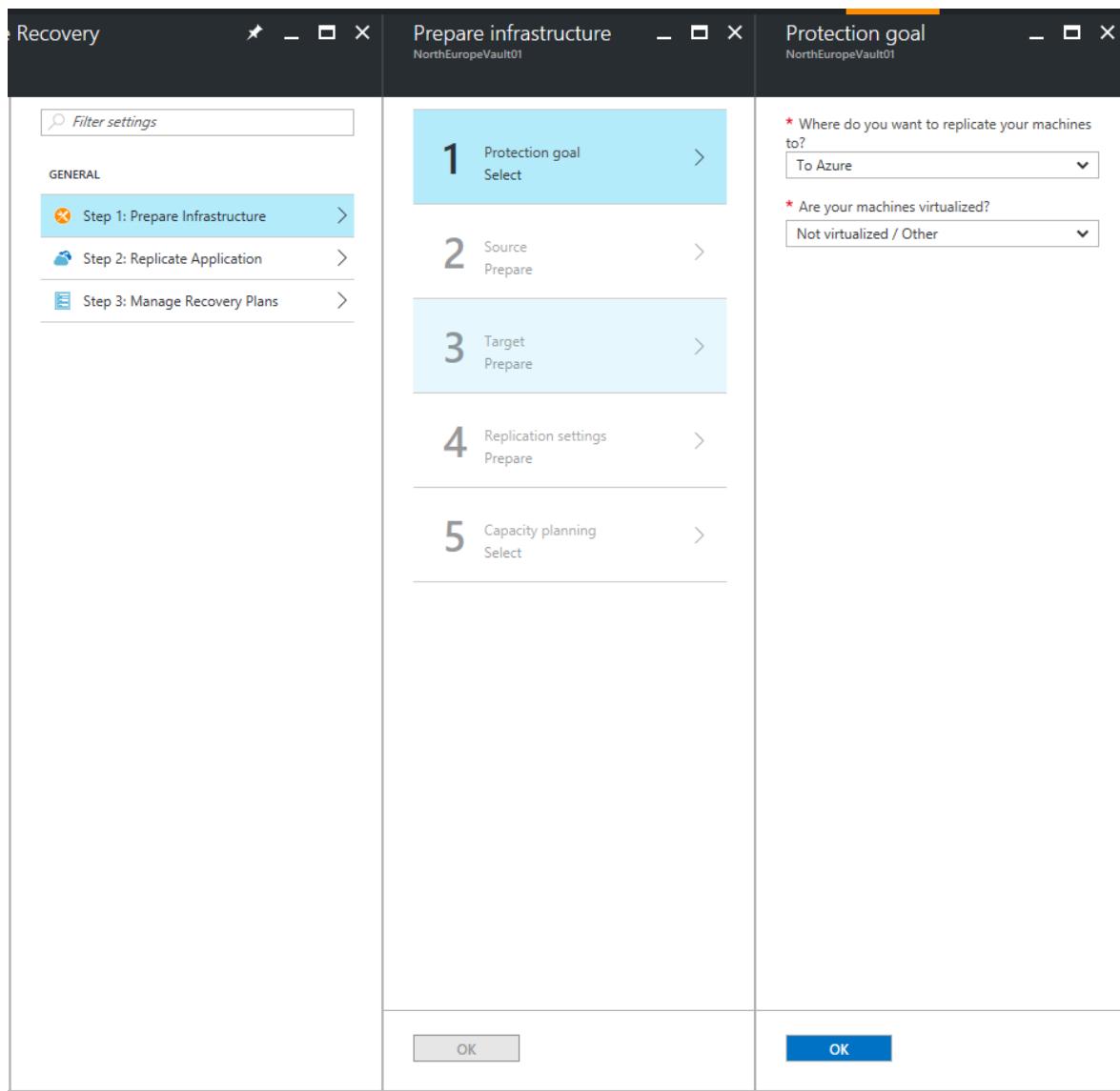
HTTPS-based proxy servers are not supported by the configuration server.

## Choose your protection goals

1. In the Azure portal, go to the **Recovery Services** vaults blade and select your vault.
2. In the **Resource** menu of the vault, click **Getting Started > Site Recovery > Step 1: Prepare Infrastructure > Protection goal**.

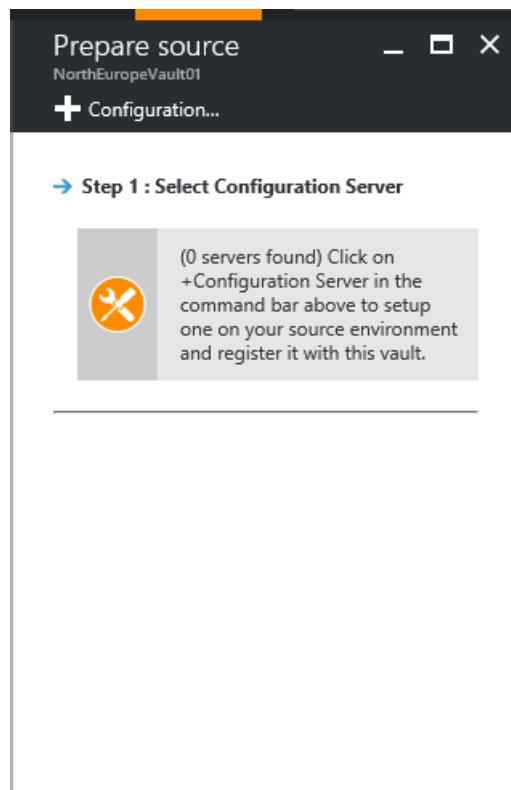


3. In **Protection goal**, select **To Azure** and **Not virtualized/Other**, and then click **OK**.

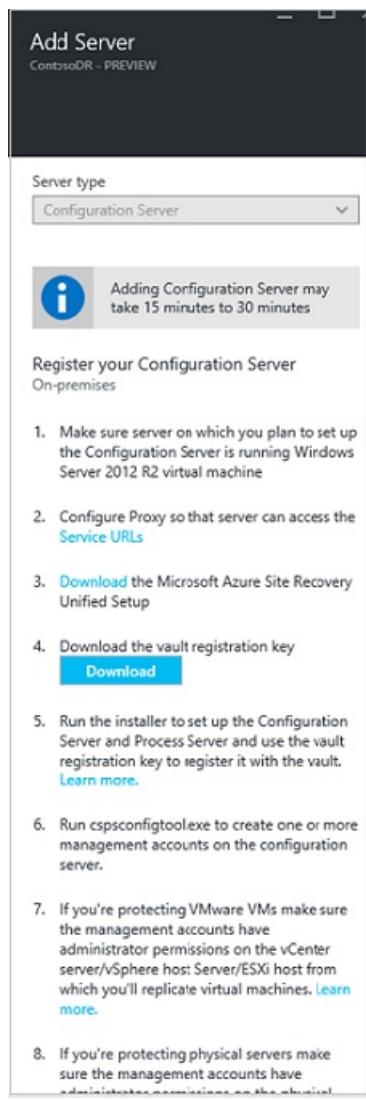


## Set up the source environment

1. In **Prepare source**, if you don't have a configuration server, click **+Configuration server** to add one.



2. In the **Add Server** blade, check that **Configuration Server** appears in **Server type**.
3. Download the Site Recovery Unified Setup installation file.
4. Download the vault registration key. You need the registration key when you run Unified Setup. The key is valid for five days after you generate it.



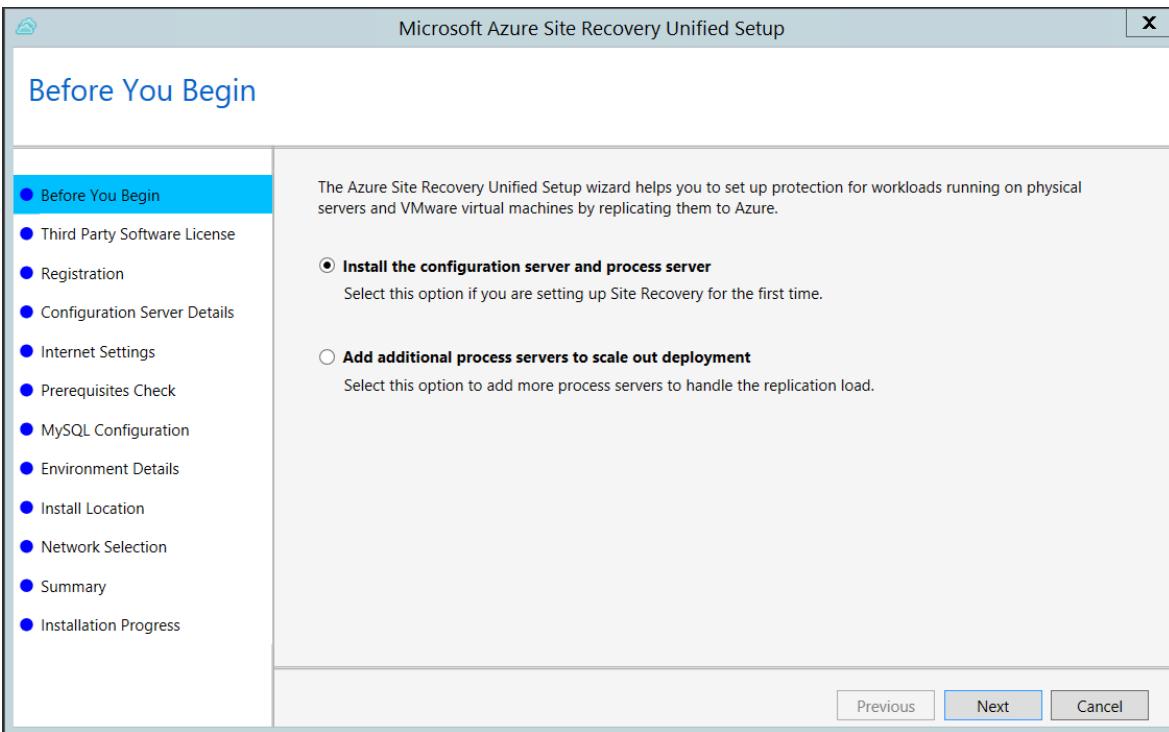
5. On the machine you're using as the configuration server, run **Azure Site Recovery Unified Setup** to install the configuration server, the process server, and the master target server.

#### Run Azure Site Recovery Unified Setup

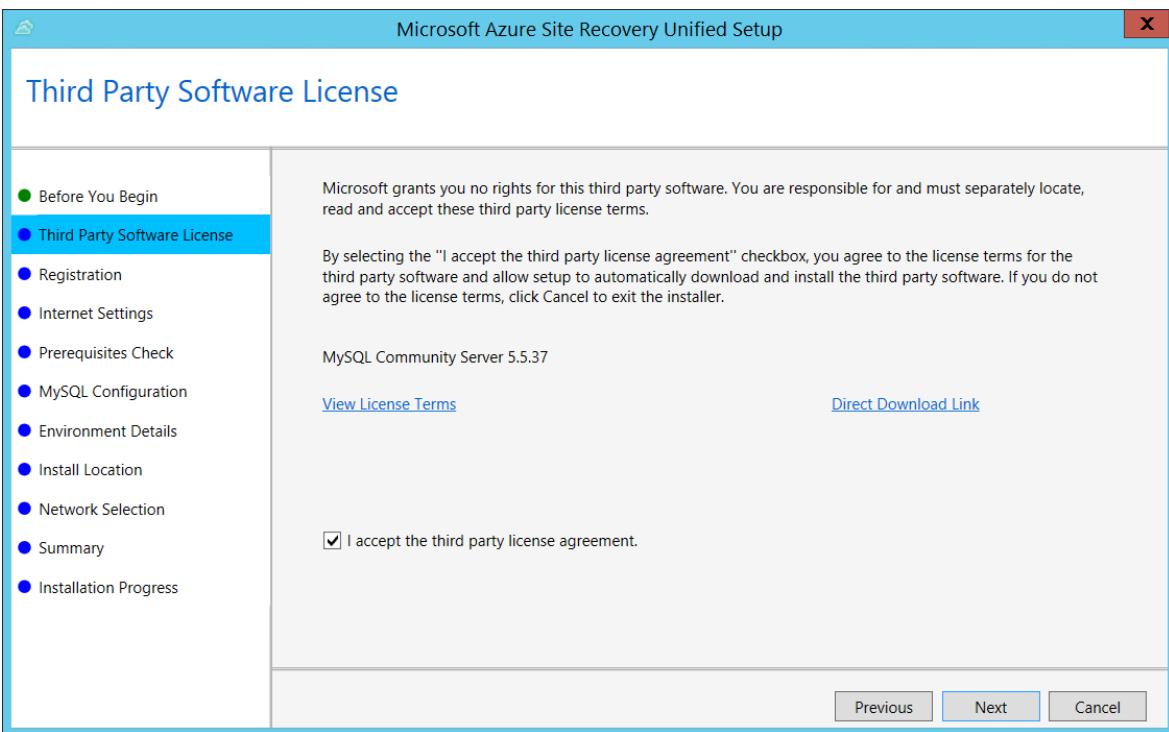
##### TIP

Configuration server registration fails if the time on your computer's system clock is more than five minutes off of local time. Synchronize your system clock with a [time server](#) before starting the installation.

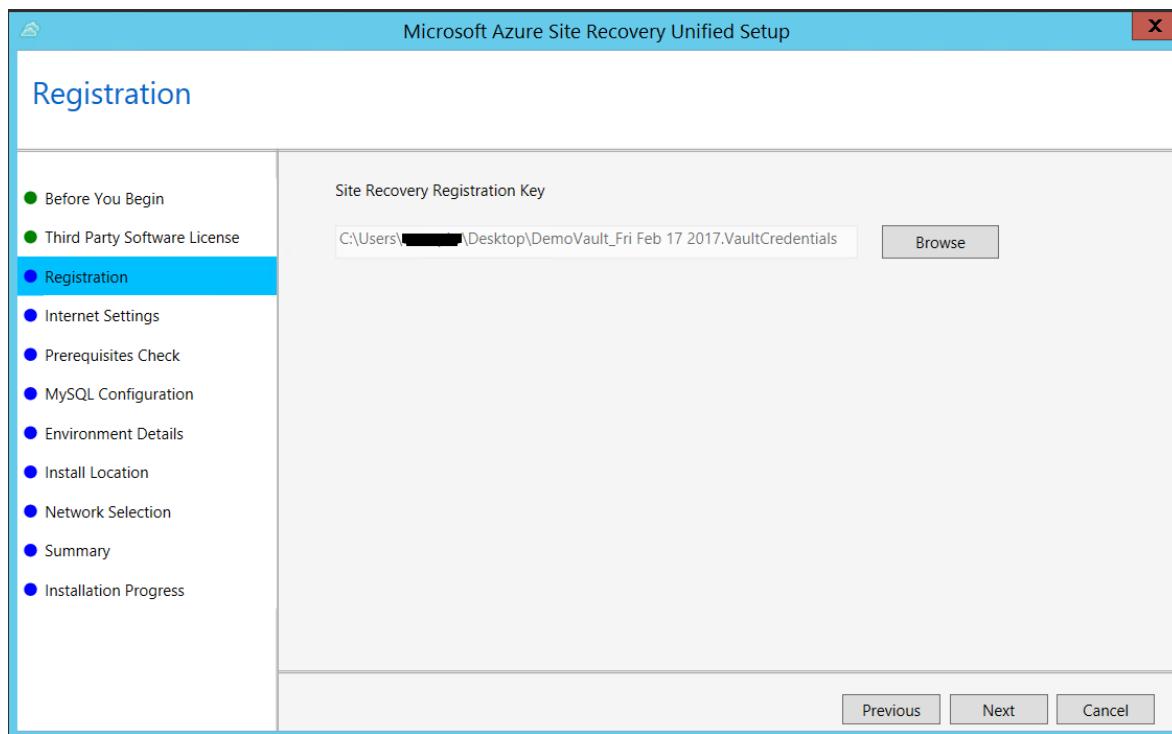
1. Run the Unified Setup installation file.
2. In **Before You Begin**, select **Install the configuration server and process server**.



3. In **Third Party Software License**, click **I Accept** to download and install MySQL.

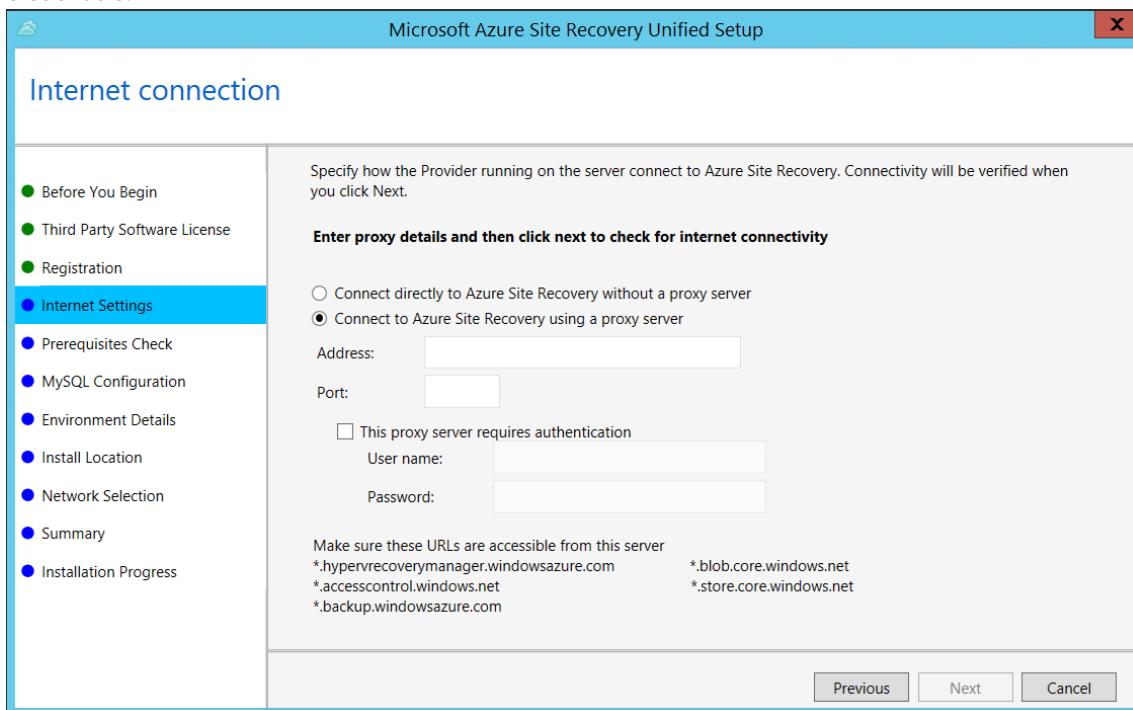


4. In **Registration**, select the registration key you downloaded from the vault.

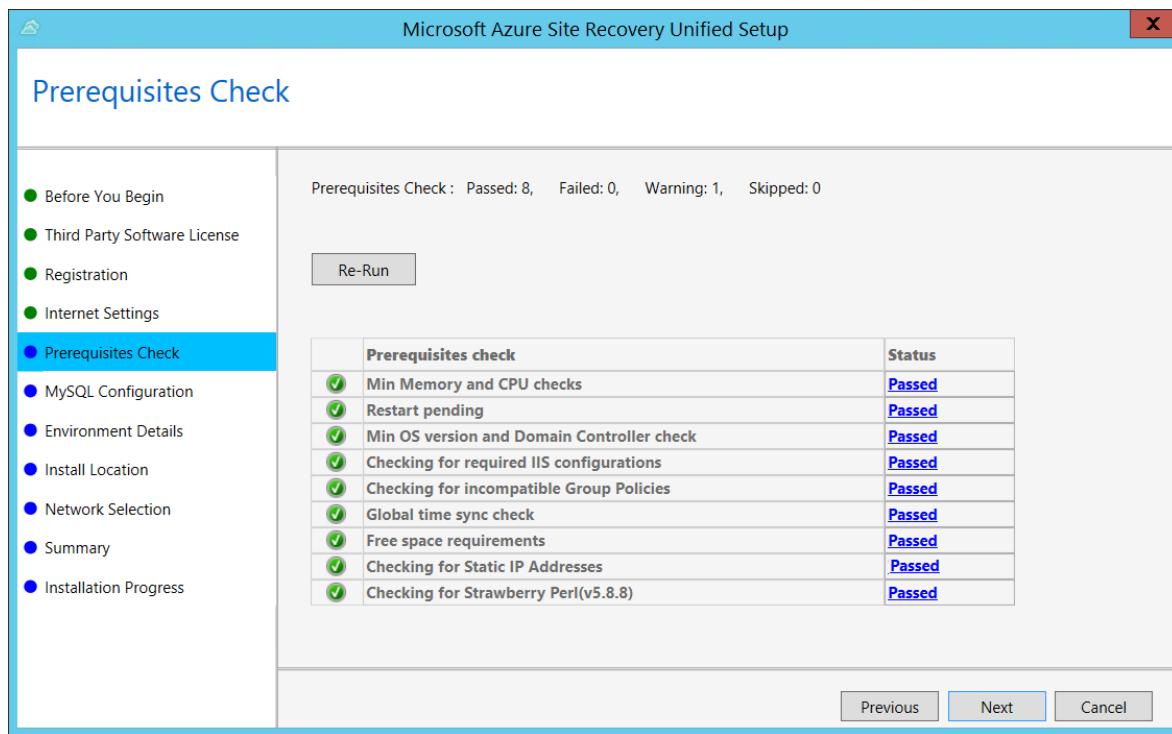


5. In **Internet Settings**, specify how the Provider running on the configuration server connects to Azure Site Recovery over the Internet. Make sure you've allowed the required URLs.

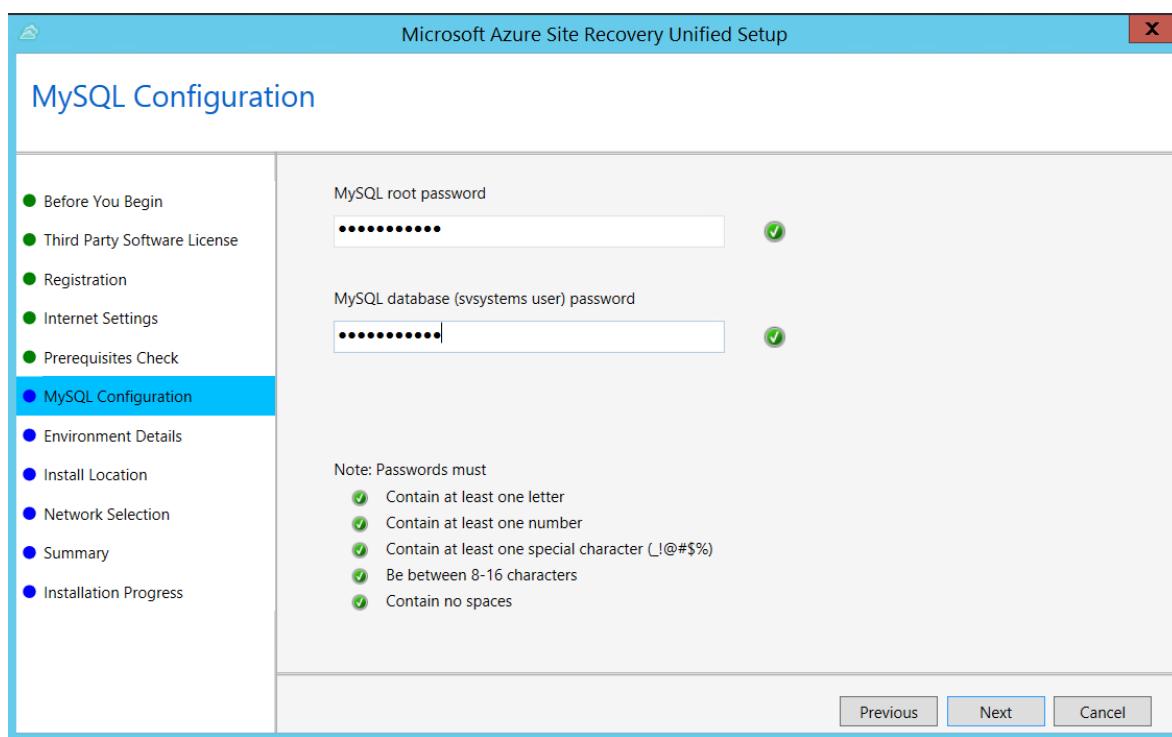
- If you want to connect with the proxy that's currently set up on the machine, select **Connect to Azure Site Recovery using a proxy server**.
- If you want the Provider to connect directly, select **Connect directly to Azure Site Recovery without a proxy server**.
- If the existing proxy requires authentication, or if you want to use a custom proxy for the Provider connection, select **Connect with custom proxy settings**, and specify the address, port, and credentials.



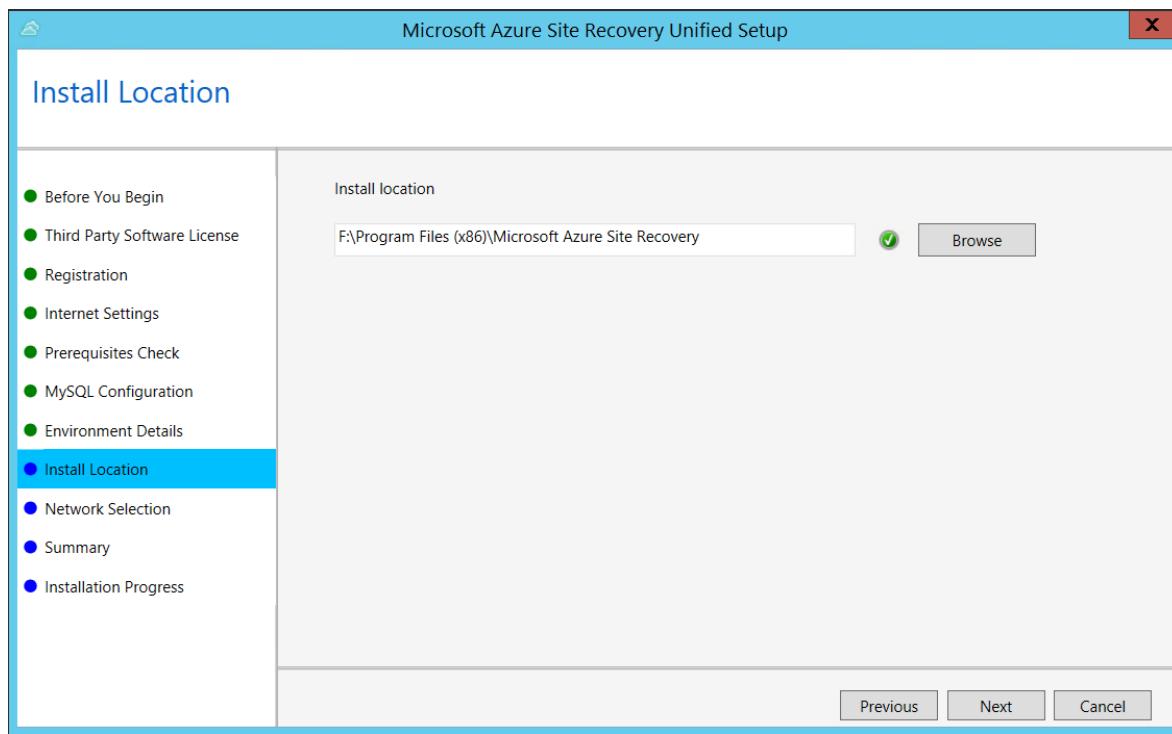
6. In **Prerequisites Check**, Setup runs a check to make sure that installation can run. If a warning appears about the **Global time sync check**, verify that the time on the system clock (**Date and Time** settings) is the same as the time zone.



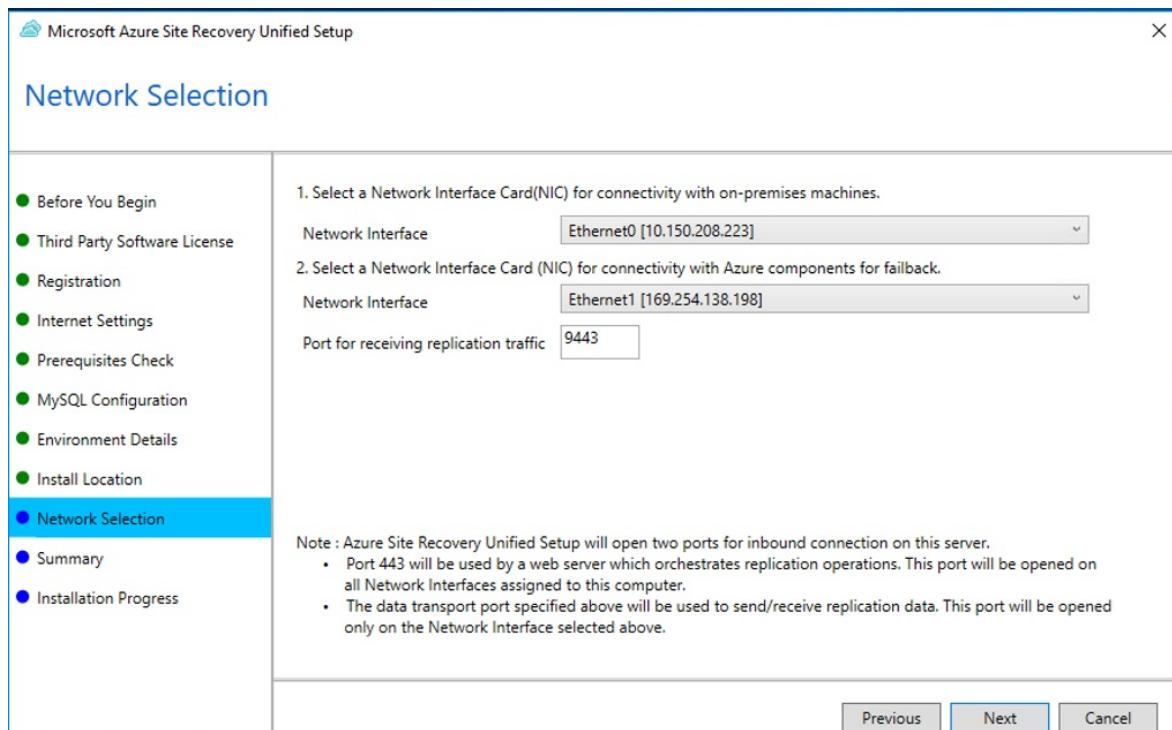
7. In **MySQL Configuration**, create credentials for logging on to the MySQL server instance that is installed.



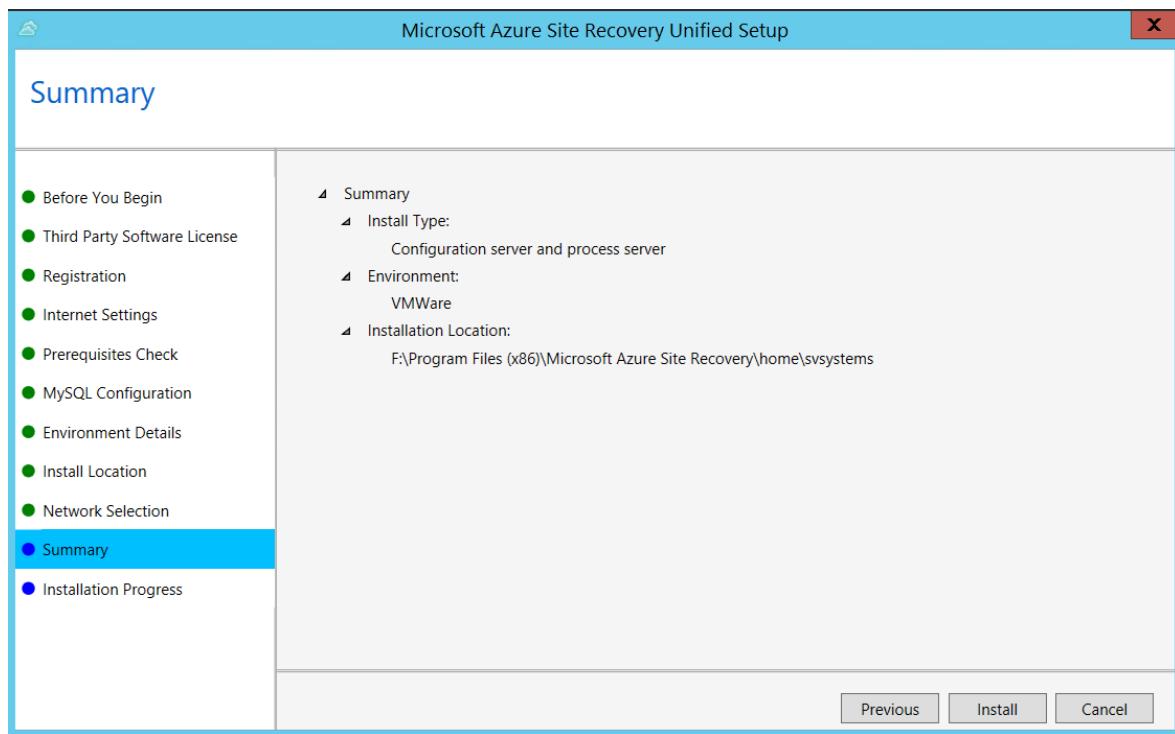
8. In **Environment Details**, select No if you're replicating Azure Stack VMs or physical servers.
9. In **Install Location**, select where you want to install the binaries and store the cache. The drive you select must have at least 5 GB of disk space available, but we recommend a cache drive with at least 600 GB of free space.



10. In **Network Selection**, first select the NIC that the in-built process server uses for discovery and push installation of mobility service on source machines, and then select the NIC that Configuration Server uses for connectivity with Azure. Port 9443 is the default port used for sending and receiving replication traffic, but you can modify this port number to suit your environment's requirements. In addition to the port 9443, we also open port 443, which is used by a web server to orchestrate replication operations. Do not use port 443 for sending or receiving replication traffic.



11. In **Summary**, review the information and click **Install**. When installation finishes, a passphrase is generated. You will need this when you enable replication, so copy it and keep it in a secure location.



After registration finishes, the server is displayed on the **Settings > Servers** blade in the vault.

#### NOTE

The configuration server can be installed via a command line. [Learn more](#).

## Common issues

### Installation failures

| SAMPLE ERROR MESSAGE                                                                                                                                                | RECOMMENDED ACTION                              |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------|
| ERROR Failed to load Accounts. Error: System.IO.IOException:<br>Unable to read data from the transport connection when<br>installing and registering the CS server. | Ensure that TLS 1.0 is enabled on the computer. |

### Registration failures

Registration failures can be debugged by reviewing the logs in the **%ProgramData%\ASRLogs** folder.

| SAMPLE ERROR MESSAGE                                                                                                                                                                                                                                                                        | RECOMMENDED ACTION                                                                                                                          |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| <b>09:20:06:</b> InnerException.Type:<br>SrsRestApiClientLib.AcsException,InnerException.<br>Message: ACS50008: SAML token is invalid.<br>Trace ID: 1921ea5b-4723-4be7-8087-a75d3f9e1072<br>Correlation ID: 62fea7e6-2197-4be4-a2c0-71ceb7aa2d97><br>Timestamp: <b>2016-12-12 14:50:08Z</b> | Ensure that the time on your system clock is not more than 15 minutes off the local time. Rerun the installer to complete the registration. |

| SAMPLE ERROR MESSAGE                                                                                                                                                                                                                                                                                                                                                                                                                  | RECOMMENDED ACTION                                                                                                                          |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>09:35:27</b> :DRRegistrationException while trying to get all disaster recovery vault for the selected certificate: : Threw Exception.Type:Microsoft.DisasterRecovery.Registration.DRRegistrationException, Exception.Message: ACS50008: SAML token is invalid.</p> <p>Trace ID: e5ad1af1-2d39-4970-8eef-096e325c9950<br/> Correlation ID: abe9deb8-3e64-464d-8375-36db9816427a<br/> Timestamp: <b>2016-05-19 01:35:39Z</b></p> | Ensure that the time on your system clock is not more than 15 minutes off the local time. Rerun the installer to complete the registration. |
| <p>06:28:45:Failed to create certificate<br/> 06:28:45:Setup cannot proceed. A certificate required to authenticate to Site Recovery cannot be created. Rerun Setup</p>                                                                                                                                                                                                                                                               | Ensure that you're running setup as a local administrator.                                                                                  |

## Next steps

Next step involves [setting up your target environment](#) in Azure.

# Prepare the target environment for disaster recovery of VMware VMs or physical servers to Azure

11/6/2019 • 2 minutes to read • [Edit Online](#)

This article describes how to prepare your target Azure environment to start replicating VMware virtual machines or physical servers to Azure.

## Prerequisites

The article assumes:

- You have created a Recovery Services Vault on [Azure portal](#) to protect your source machines
- You have setup your on-premises environment to replicate the source [VMware virtual machines](#) or [physical servers](#) to Azure.

## Prepare target

After completing the **Step 1: Select Protection goal** and **Step 2: Prepare Source**, you are taken to **Step 3: Target**

The screenshot shows two windows side-by-side:

- Prepare infrastructure (Left Window):**
  - Step 1:** Protection goal (VMware VMs/physical servers) - Status: ✓
  - Step 2:** Source (CONTOSO-CS2/Contoso-vCent...) - Status: ✓
  - Step 3:** Target Prepare - Status: > (highlighted in blue)
  - Step 4:** Replication settings Prepare - Status: >
  - Step 5:** Capacity planning Select - Status: >
- Target (Right Window):**
  - Step 1: Select Azure subscription**
  - Subscription:** ASR GQLs in PROD
  - Select the deployment model used after failover:** Resource Manager
  - Step 2: Ensure that at least one compatible Azure virtual network exist**
  - Network(s):** Found 4 compatible Azure virtual networks out of 19 available in the subscription

Both windows have an 'OK' button at the bottom.

- Subscription:** From the drop-down menu, select the Subscription that you want to replicate your virtual machines or physical servers to.
- Deployment Model:** Select the deployment model (Classic or Resource Manager)

Based on the chosen deployment model, a validation is run to ensure that you have at least one virtual network in the target subscription to replicate and failover your virtual machine or physical server to.

Once the validations complete successfully, click OK to go to the next step.

If you don't have a virtual network, you can create one by clicking the + Network button at the top of the page.

## Next steps

[Configure replication settings.](#)

# About the Mobility service for VMware VMs and physical servers

2/21/2020 • 6 minutes to read • [Edit Online](#)

When you set up disaster recovery for VMware VMs and physical servers using [Azure Site Recovery](#), you install the Site Recovery Mobility service on each on-premises VMware VM and physical server. The Mobility service captures data writes on the machine, and forwards them to the Site Recovery process server. You can deploy the Mobility Service using the following methods:

- **Push installation:** Site Recovery installs mobility agent on the server when protection is enabled via Azure portal.
- **Install manually:** You can install the Mobility service manually on each machine through [UI](#) or [command prompt](#).
- **Automated deployment:** You can automate installation with software deployment tools such as Configuration Manager.

#### NOTE

The Mobility agent uses approximately 6%-10% of memory on source machines for VMware VMs or physical machines.

## Anti-virus on replicated machines

If machines you want to replicate have active anti-virus software running, make sure you exclude the Mobility service installation folder from anti-virus operations (`C:\ProgramData\ASR\agent`). This ensures that replication works as expected.

## Push installation

Push installation is an integral part of "[Enable Replication](#)" job triggered in the portal. After choosing the set of virtual machines you wish to protect and trigger "Enable Replication", configuration server pushes mobility agent on to the servers, installs the agent and complete registration of agent with configuration server. For successful completion of this operation,

- Ensure that all push installation [prerequisites](#) are met.
- Ensure that all configurations of servers fall under [support matrix of VMware to Azure DR scenario](#).

Details of push installation workflow has been described in the following sections.

#### From 9.23 version onwards

During push installation of mobility agent, following steps are performed

1. Pushes agent on to the source machine. Copying the agent on to source machine can fail due to multiple environmental errors. Visit [our guidance](#) to troubleshoot push installation failures.
2. After agent is successfully copied on to the server prerequisite checks are performed on the server. Installation fails if one or more of the [prerequisites](#) are not met. If all prerequisites are met, installation is triggered.
3. Azure Site Recovery VSS provider is installed on the server as part of Mobility agent installation. This provider is used to generate Application consistent points. If installation of VSS provider fails, this step will

be skipped and agent installation will continue.

4. If agent installation succeeds but VSS provider installation fails, then job status is marked as "Warning". This does not impact crash consistency points generation.
  - a. To generate application consistent points, refer to [our guidance](#) to complete installation of Site Recovery VSS provider manually.
  - b. If you do not wish application consistent points to be generated, [modify the replication policy](#) to turn off application consistent points.

## Before 9.22 versions

1. Pushes agent on to the source machine. Copying the agent on to source machine can fail due to multiple environmental errors. Visit [our guidance](#) to troubleshoot push installation failures.
2. After agent is successfully copied on to the server prerequisite checks are performed on the server. Installation fails if one or more of the [prerequisites](#) are not met. If all prerequisites are met, installation is triggered.
3. Azure Site Recovery VSS provider is installed on the server as part of Mobility agent installation. This provider is used to generate Application consistent points. If installation of VSS provider fails, then agent installation will fail. To avoid failure of mobility agent installation, use [9.23 version](#) or higher to generate crash consistent points and install VSS provider manually.

## Install mobility agent through UI

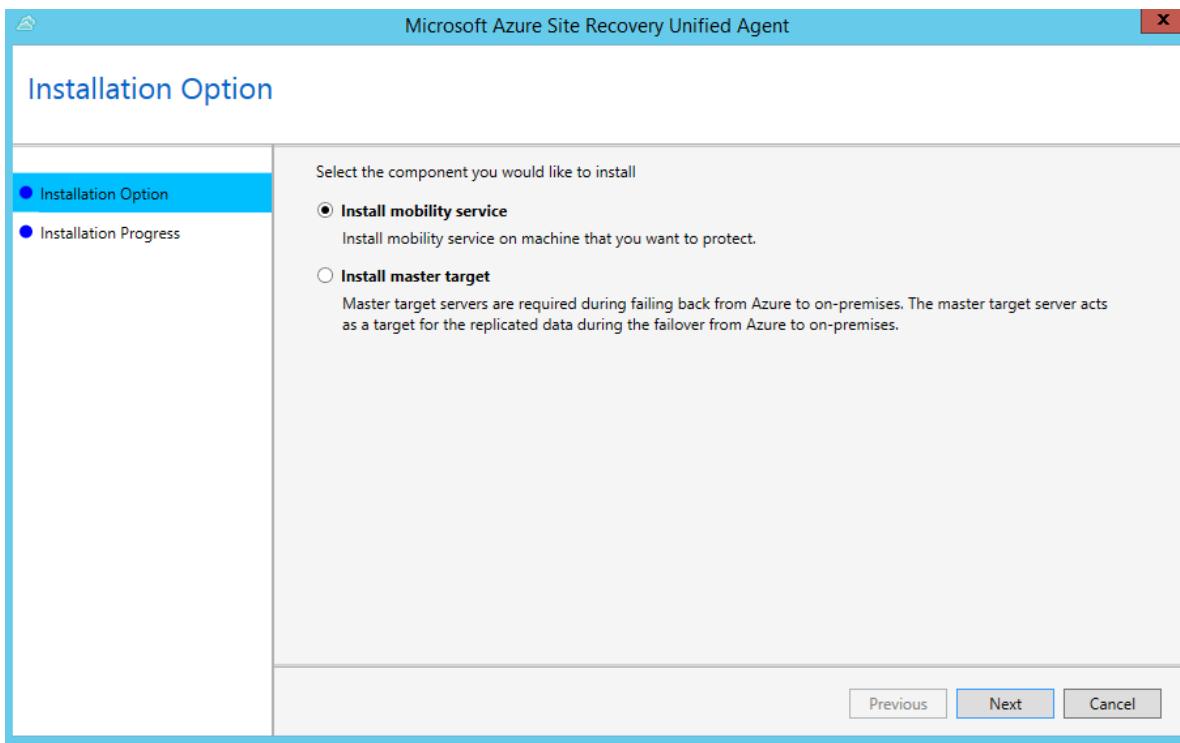
### Prerequisite

- Ensure that all configurations of servers fall under [support matrix of VMware to Azure DR scenario](#).
- [Locate the installer](#) based on the operating system of the server.

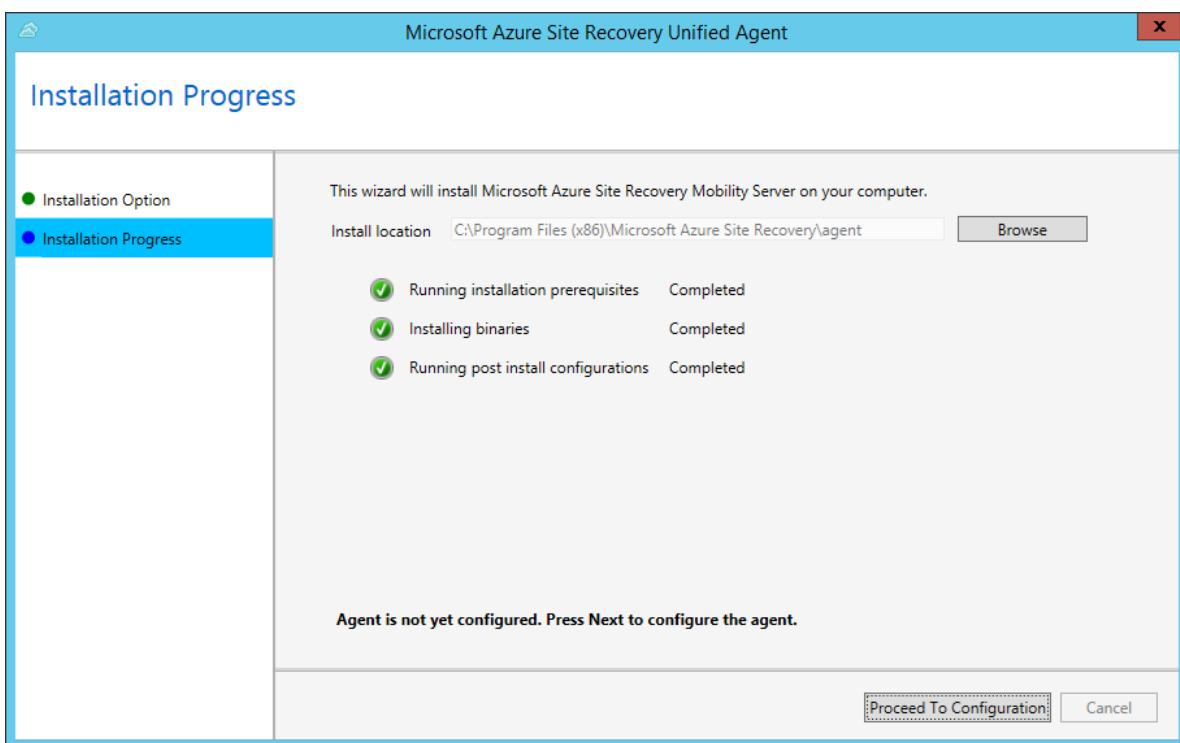
#### IMPORTANT

If you are replicating Azure IaaS VM from one Azure region to another, don't use this method. Use the command-line-based installation method instead.

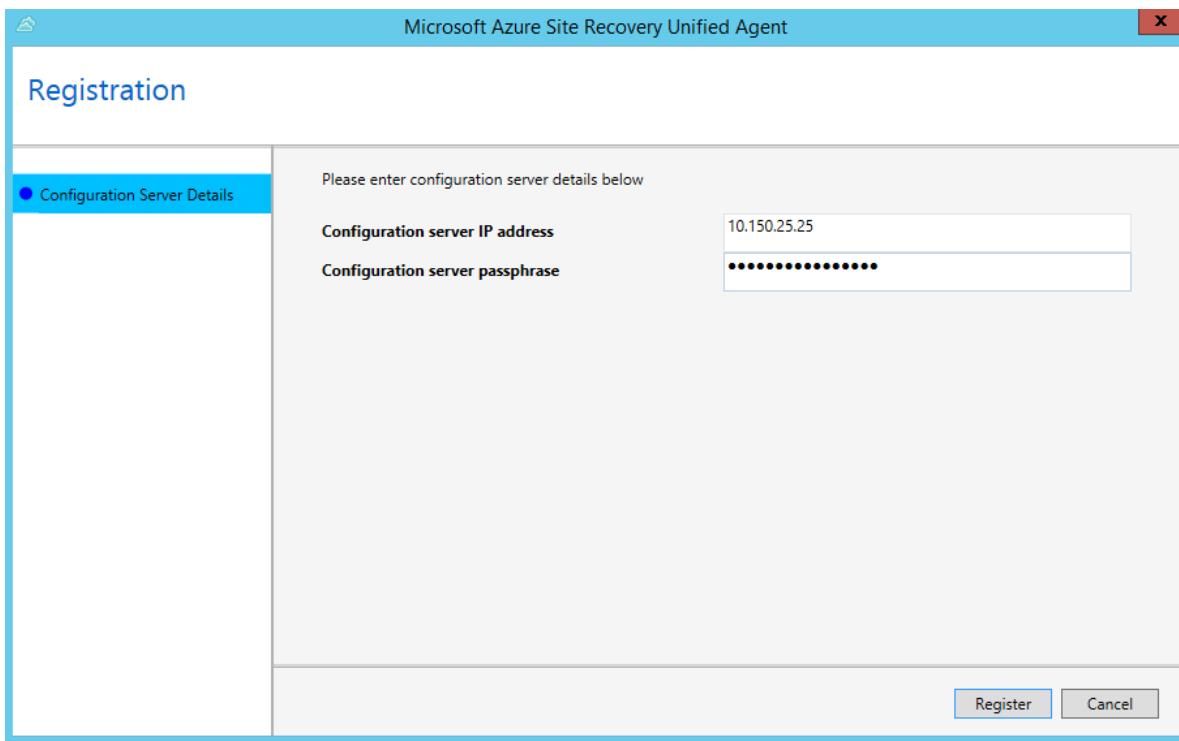
1. Copy the installation file to the machine, and run it.
2. In **Installation Option**, select **Install mobility service**.
3. Select the installation location > **Install**.



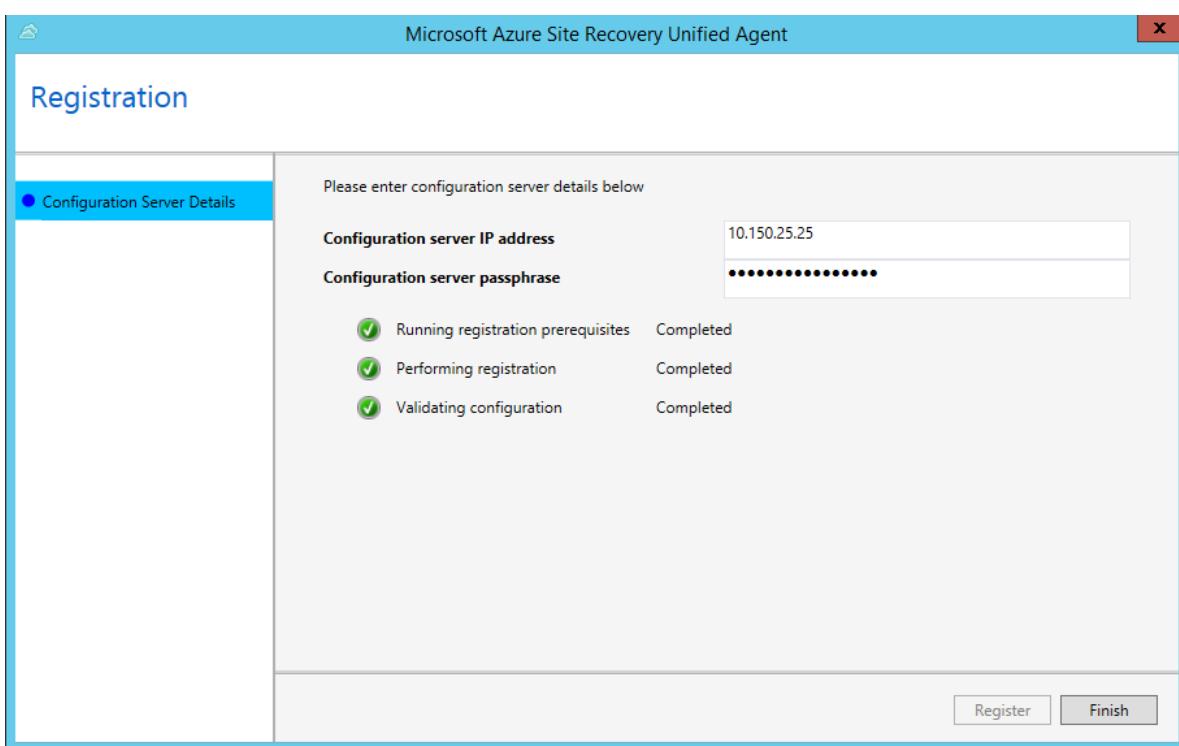
4. Monitor the installation in **Installation Progress**. After the installation is finished, select **Proceed to Configuration** to register the service with the configuration server.



5. In **Configuration Server Details**, specify the IP address and passphrase you configured.



6. Select **Register** to finish the registration.



## Install mobility agent through command prompt

### Prerequisite

- Ensure that all configurations of servers fall under [support matrix of VMware to Azure DR scenario](#).
- [Locate the installer](#) based on the operating system of the server.

### On a Windows machine

- Copy the installer to a local folder (for example, C:\Temp) on the server that you want to protect.

```

cd C:\Temp
ren Microsoft-ASR_UA*Windows*release.exe MobilityServiceInstaller.exe
MobilityServiceInstaller.exe /q /x:C:\Temp\Extracted
cd C:\Temp\Extracted

```

- Install as follows:

```

UnifiedAgent.exe /Role "MS" /InstallLocation "C:\Program Files (x86)\Microsoft Azure Site Recovery"
/Platform "VmWare" /Silent

```

- Register the agent with the configuration server.

```

cd C:\Program Files (x86)\Microsoft Azure Site Recovery\agent
UnifiedAgentConfigurator.exe /CSEndPoint <CSIP> /PassphraseFilePath <PassphraseFilePath>

```

#### Installation settings

| SETTING          | DETAILS                                                                                                                                                                                                                                |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Usage            | UnifiedAgent.exe /Role <MS/MT> /InstallLocation <Install Location> /Platform "VmWare" /Silent                                                                                                                                          |
| Setup logs       | Under<br>%ProgramData%\ASRSetupLogs\ASRUnifiedAgentInstaller.log<br>.                                                                                                                                                                  |
| /Role            | Mandatory installation parameter. Specifies whether the Mobility service (MS) or master target (MT) should be installed.                                                                                                               |
| /InstallLocation | Optional parameter. Specifies the Mobility service installation location (any folder).                                                                                                                                                 |
| /Platform        | Mandatory. Specifies the platform on which Mobility Service is installed. <b>VMware</b> for VMware VMs/physical servers; <b>Azure</b> for Azure VMs.<br><br>If you're treating Azure VMs as physical machines, specify <b>VMware</b> . |
| /Silent          | Optional. Specifies whether to run the installer in silent mode.                                                                                                                                                                       |

#### Registration settings

| SETTING                  | DETAILS                                                                                              |
|--------------------------|------------------------------------------------------------------------------------------------------|
| Usage                    | UnifiedAgentConfigurator.exe /CSEndPoint <CSIP><br>/PassphraseFilePath <PassphraseFilePath>          |
| Agent configuration logs | Under<br>%ProgramData%\ASRSetupLogs\ASRUnifiedAgentConfigurat or.log.                                |
| /CSEndPoint              | Mandatory parameter. Specifies the IP address of the configuration server. Use any valid IP address. |

| SETTING             | DETAILS                                                                      |
|---------------------|------------------------------------------------------------------------------|
| /PassphraseFilePath | Mandatory. Location of the passphrase. Use any valid UNC or local file path. |

### On a Linux machine

1. Copy the installer to a local folder (for example, /tmp) on the server that you want to protect. In a terminal, run the following commands:

```
cd /tmp ;
tar -xvf Microsoft-ASR_UA*release.tar.gz
```

2. Install as follows:

```
sudo ./install -d <Install Location> -r MS -v VmWare -q
```

3. After installation is finished, Mobility Service must be registered to the configuration server. Run the following command to register Mobility Service with the configuration server:

```
/usr/local/ASR/Vx/bin/UnifiedAgentConfigurator.sh -i <CSIP> -P /var/passphrase.txt
```

### Installation settings

| SETTING | DETAILS                                                                                                                                              |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| Usage   | <code>./install -d &lt;Install Location&gt; -r &lt;MS/MT&gt; -v VmWare -q</code>                                                                     |
| -r      | Mandatory installation parameter. Specifies whether the Mobility service (MS) or master target (MT) should be installed.                             |
| -d      | Optional parameter. Specifies the Mobility service installation location: /usr/local/ASR.                                                            |
| -v      | Mandatory. Specifies the platform on which Mobility Service is installed. <b>VMware</b> for VMware VMs/physical servers; <b>Azure</b> for Azure VMs. |
| -q      | Optional. Specifies whether to run the installer in silent mode.                                                                                     |

### Registration settings

| SETTING | DETAILS                                                                                                                         |
|---------|---------------------------------------------------------------------------------------------------------------------------------|
| Usage   | <code>cd /usr/local/ASR/Vx/bin</code><br><code>UnifiedAgentConfigurator.sh -i &lt;CSIP&gt; -P &lt;PassphraseFilePath&gt;</code> |
| -i      | Mandatory parameter. Specifies the IP address of the configuration server. Use any valid IP address.                            |
| -P      | Mandatory. Full file path of the file in which the passphrase is saved. Use any valid folder.                                   |

| SETTING | DETAILS |
|---------|---------|
|---------|---------|

## Azure Virtual Machine agent

- **Windows VMs:** From version 9.7.0.0 of the Mobility service, the [Azure VM agent](#) is installed by the Mobility service installer. This ensures that when the machine fails over to Azure, the Azure VM meets the agent installation prerequisite for using any Vm extension.
- **Linux VMs:** The [WALinuxAgent](#) must be installed manually on the Azure VM after failover.

## Locate installer files

Go to %ProgramData%\ASR\home\svsystems\pushinstallsvc\repository folder on configuration server. Check which installer you need based on operating system. The following table summarizes the installer files for each VMware VM and physical server operating system. You can review [supported operating systems](#) before you start.

| INSTALLER FILE                                  | OPERATING SYSTEM (64-BIT ONLY)                                                               |
|-------------------------------------------------|----------------------------------------------------------------------------------------------|
| Microsoft-ASR_UA*Windows*release.exe            | Windows Server 2016; Windows Server 2012 R2; Windows Server 2012; Windows Server 2008 R2 SP1 |
| Microsoft-ASR_UA*RHEL6-64*release.tar.gz        | Red Hat Enterprise Linux (RHEL) 6.*<br>CentOS 6.*                                            |
| Microsoft-ASR_UA*RHEL7-64*release.tar.gz        | Red Hat Enterprise Linux (RHEL) 7.*<br>CentOS 7.*                                            |
| Microsoft-ASR_UA*SLES12-64*release.tar.gz       | SUSE Linux Enterprise Server 12 SP1,SP2,SP3                                                  |
| Microsoft-ASR_UA*SLES11-SP3-64*release.tar.gz   | SUSE Linux Enterprise Server 11 SP3                                                          |
| Microsoft-ASR_UA*SLES11-SP4-64*release.tar.gz   | SUSE Linux Enterprise Server 11 SP4                                                          |
| Microsoft-ASR_UA*OL6-64*release.tar.gz          | Oracle Enterprise Linux 6.4, 6.5                                                             |
| Microsoft-ASR_UA*UBUNTU-14.04-64*release.tar.gz | Ubuntu Linux 14.04                                                                           |
| Microsoft-ASR_UA*UBUNTU-16.04-64*release.tar.gz | Ubuntu Linux 16.04 LTS server                                                                |
| Microsoft-ASR_UA*DEBIAN7-64*release.tar.gz      | Debian 7                                                                                     |
| Microsoft-ASR_UA*DEBIAN8-64*release.tar.gz      | Debian 8                                                                                     |

## Next steps

[Set up push installation for the Mobility service.](#)

# Prepare source machine for push installation of mobility agent

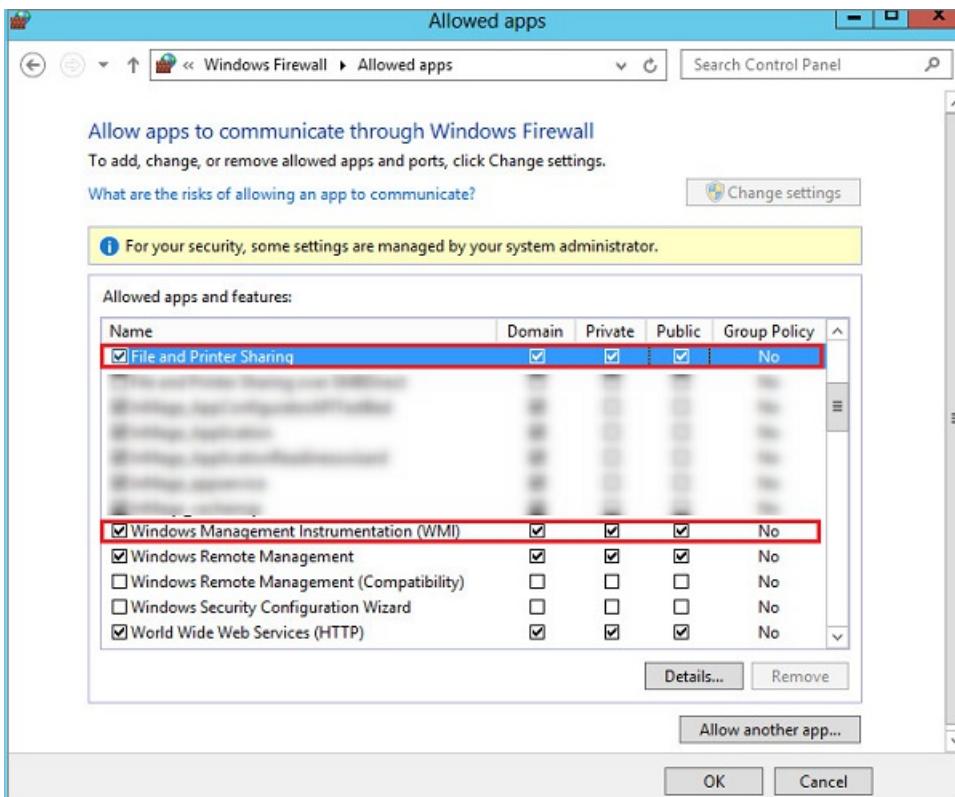
11/19/2019 • 2 minutes to read • [Edit Online](#)

When you set up disaster recovery for VMware VMs and physical servers using [Azure Site Recovery](#), you install the [Site Recovery Mobility service](#) on each on-premises VMware VM and physical server. The Mobility service captures data writes on the machine, and forwards them to the Site Recovery process server.

## Install on Windows machine

On each Windows machine you want to protect, do the following:

1. Ensure that there's network connectivity between the machine and the process server. If you haven't set up a separate process server, then by default it's running on the configuration server.
2. Create an account that the process server can use to access the computer. The account should have administrator rights, either local or domain. Use this account only for the push installation and for agent updates.
3. If you don't use a domain account, disable Remote User Access control on the local computer as follows:
  - Under HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System registry key, add a new DWORD: **LocalAccountTokenFilterPolicy**. Set the value to **1**.
  - To do this at a command prompt, run the following command:  
`REG ADD  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v  
LocalAccountTokenFilterPolicy /t REG\_DWORD /d
4. In Windows Firewall on the machine you want to protect, select **Allow an app or feature through Firewall**. Enable **File and Printer Sharing** and **Windows Management Instrumentation (WMI)**. For computers that belong to a domain, you can configure the firewall settings by using a Group Policy object (GPO).



5. Add the account that you created in CSPSCfgtool. To do this, sign in to your configuration server.
6. Open **cspscfgtool.exe**. It's available as a shortcut on the desktop and in the %ProgramData%\ASR\home\svsystems\bin folder.
7. On the **Manage Accounts** tab, select **Add Account**.
8. Add the account you created.
9. Enter the credentials you use when you enable replication for a computer.

## Install on Linux machine

On each Linux machine that you want to protect, do the following:

1. Ensure that there's network connectivity between the Linux machine and the process server.
2. Create an account that the process server can use to access the computer. The account should be a **root** user on the source Linux server. Use this account only for the push installation and for updates.
3. Check that the /etc/hosts file on the source Linux server has entries that map the local hostname to IP addresses associated with all network adapters.
4. Install the latest openssh, openssh-server, and openssl packages on the computer that you want to replicate.
5. Ensure that Secure Shell (SSH) is enabled and running on port 22.
6. Enable SFTP subsystem and password authentication in the sshd\_config file. To do this, sign in as **root**.
7. In the **/etc/ssh/sshd\_config** file, find the line that begins with **PasswordAuthentication**.
8. Uncomment the line, and change the value to **yes**.
9. Find the line that begins with **Subsystem**, and uncomment the line.

```
override default of no subsystems
Subsystem sftp /usr/libexec.openssh.sftp-server
```

10. Restart the **sshd** service.
11. Add the account that you created in CSPSConfigtool. To do this, sign in to your configuration server.
12. Open **cspscfgitool.exe**. It's available as a shortcut on the desktop and in the %ProgramData%\home\svsystems\bin folder.
13. On the **Manage Accounts** tab, select **Add Account**.
14. Add the account you created.
15. Enter the credentials you use when you enable replication for a computer.

## Anti-virus on replicated machines

If machines you want to replicate have active anti-virus software running, make sure you exclude the Mobility service installation folder from anti-virus operations (*C:\ProgramData\ASR\agent*). This ensures that replication works as expected.

## Next steps

After the Mobility Service is installed, in the Azure portal, select + **Replicate** to start protecting these VMs. Learn more about enabling replication for [VMware VMs](#) and [physical servers](#).

# Automate Mobility Service installation

2/14/2020 • 10 minutes to read • [Edit Online](#)

This article describes how to automate installation and updates for the Mobility Service agent in [Azure Site Recovery](#).

When you deploy Site Recovery for disaster recovery of on-premises VMware VMs and physical servers to Azure, you install the Mobility Service agent on each machine you want to replicate. The Mobility Service captures data writes on the machine, and forwards them to the Site Recovery process server for replication. You can deploy the Mobility Service in a few ways:

- **Push installation:** Let Site Recovery install the Mobility service agent when you enable replication for a machine in the Azure portal.
- **Manual installation:** Install the Mobility service manually on each machine. [Learn more](#) about push and manual installation.
- **Automated deployment:** Automate installation with software deployment tools such as Microsoft Endpoint Configuration Manager, or third-party tools such as JetPatch.

Automated installation and updating provides a solution if:

- Your organization doesn't allow for push installation on protected servers.
- Your company policy requires passwords to be changed periodically. You have to specify a password for the push installation.
- Your security policy doesn't permit adding firewall exceptions for specific machines.
- You're acting as a hosting service provider and don't want to provide customer machine credentials that are needed for push installation with Site Recovery.
- You need to scale agent installations to lots of servers simultaneously.
- You want to schedule installations and upgrades during planned maintenance windows.

## Prerequisites

To automate the installation, you need the following items:

- A deployed software installation solution such as [Configuration Manager](#) or [JetPatch](#).
- Deployment prerequisites in place in [Azure](#) and [on-premises](#) for VMware disaster recovery, or for [physical server](#) disaster recovery. Review the [support requirements](#) for disaster recovery.

## Prepare for automated deployment

The following table summarizes tools and processes for automating Mobility Service deployment.

| TOOL | DETAILS | INSTRUCTIONS |
|------|---------|--------------|
|------|---------|--------------|

| TOOL                         | DETAILS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | INSTRUCTIONS                                                                                                            |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| <b>Configuration Manager</b> | <p>1. Verify that you have the <a href="#">prerequisites</a> listed above in place.</p> <p>2. Deploy disaster recovery by setting up the source environment, including downloading an OVA file to deploy the Site Recovery configuration server as a VMware VM using an OVF template.</p> <p>3. You register the configuration server with the Site Recovery service, set up the target Azure environment, and configure a replication policy.</p> <p>4. For automated Mobility Service deployment, you create a network share containing the configuration server passphrase and Mobility Service installation files.</p> <p>5. You create a Configuration Manager package containing the installation or updates, and prepare for Mobility Service deployment.</p> <p>6. You can then enable replication to Azure for the machines that have the Mobility Service installed.</p> | <a href="#">Automate with Configuration Manager</a>                                                                     |
| <b>JetPatch</b>              | <p>1. Verify that you have the <a href="#">prerequisites</a> listed above in place.</p> <p>2. Deploy disaster recovery by setting up the source environment, including downloading and deploying JetPatch Agent Manager for Azure Site Recovery in your Site Recovery environment, using an OVF template.</p> <p>3. You register the configuration server with Site Recovery, set up the target Azure environment, and configure a replication policy.</p> <p>4. For automated deployment, initialize and complete the JetPatch Agent Manager configuration.</p> <p>5. In JetPatch you can create a Site Recovery policy to automate deployment and upgrade of the Mobility Service agent.</p> <p>6. You can then enable replication to Azure for the machines that have the Mobility Service installed.</p>                                                                       | <a href="#">Automate with JetPatch Agent Manager</a><br><br><a href="#">Troubleshoot agent installation in JetPatch</a> |

## Automate with Configuration Manager

### Prepare the installation files

1. Make sure you have the prerequisites in place.
2. Create a secure network file share (SMB share) that can be accessed by the machine running the configuration server.
3. In Configuration Manager, [categorize the servers](#) on which you want to install or update the Mobility Service. One collection should contain all Windows servers, the other all Linux servers.
4. On the network share, create a folder:
  - For installation on Windows machines, create a folder named *MobSvcWindows*.
  - For installation on Linux machines, create a folder named *MobSvcLinux*.
5. Sign in to the configuration server machine.
6. On the configuration server machine, open an administrative command prompt.
7. To generate the passphrase file, run this command:

```
cd %ProgramData%\ASR\home\svsystems\bin
genpassphrase.exe -v > MobSvc.passphrase
```

8. Copy the *MobSvc.passphrase* file to the Windows folder and the Linux folder.
9. To browse to the folder that contains the installation files, run this command:

```
cd %ProgramData%\ASR\home\svsystems\pushinstallsvc\repository
```

10. Copy these installation files to the network share:
  - For Windows, copy *Microsoft-ASR\_UA\_version\_Windows\_GA\_date\_Release.exe* to *MobSvcWindows*.
  - For Linux, copy the following files to *MobSvcLinux*:
    - *Microsoft-ASR\_UARHEL6-64release.tar.gz*
    - *Microsoft-ASR\_UARHEL7-64release.tar.gz*
    - *Microsoft-ASR\_UASLES11-SP3-64release.tar.gz*
    - *Microsoft-ASR\_UASLES11-SP4-64release.tar.gz*
    - *Microsoft-ASR\_UAOL6-64release.tar.gz*
    - *Microsoft-ASR\_UAUBUNTU-14.04-64release.tar.gz*
11. As described in the following procedures, copy the code to the Windows or Linux folders. We're assuming that:
  - The configuration server's IP address is `192.168.3.121`.
  - The secure network file share is `\ContosoSecureFS\MobilityServiceInstallers`.

### **Copy code to the Windows folder**

Copy the following code:

- Save the code in the *MobSvcWindows* folder as *install.bat*.
- Replace the `[CSIP]` placeholders in this script with the actual values of the IP address of your configuration server.
- The script supports new installations of the Mobility Service agent, and updates to agents that are already installed.

```
Time /t >> C:\Temp\logfile.log
REM ======
REM === Clean up the folders =====
```

```

RMDIR /S /q %temp%\MobSvc
MKDIR %Temp%\MobSvc
mkdir C:\Temp
REM =====

REM === Copy new files =====
COPY M*.* %Temp%\MobSvc
CD %Temp%\MobSvc
REN Micro*.exe MobSvcInstaller.exe
REM =====

REM === Extract the installer =====
MobSvcInstaller.exe /q /x:%Temp%\MobSvc\Extracted
REM === Wait 10s for extraction to complete =====
TIMEOUT /t 10
REM =====

REM === Perform installation =====
REM =====

CD %Temp%\MobSvc\Extracted
whoami >> C:\Temp\logfile.log
SET PRODKEY=HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall
REG QUERY %PRODKEY%\{275197FC-14FD-4560-A5EB-38217F80CBD1}
IF NOT %ERRORLEVEL% EQU 0 (
 echo "Product is not installed. Goto INSTALL." >> C:\Temp\logfile.log
 GOTO :INSTALL
) ELSE (
 echo "Product is installed." >> C:\Temp\logfile.log

 echo "Checking for Post-install action status." >> C:\Temp\logfile.log
 GOTO :POSTINSTALLCHECK
)

:POSTINSTALLCHECK
REG QUERY "HKLM\SOFTWARE\Wow6432Node\InMage Systems\Installed Products\5" /v "PostInstallActions" | Find
"Succeeded"
If %ERRORLEVEL% EQU 0 (
 echo "Post-install actions succeeded. Checking for Configuration status." >> C:\Temp\logfile.log
 GOTO :CONFIGURATIONCHECK
) ELSE (
 echo "Post-install actions didn't succeed. Goto INSTALL." >> C:\Temp\logfile.log
 GOTO :INSTALL
)

:CONFIGURATIONCHECK
REG QUERY "HKLM\SOFTWARE\Wow6432Node\InMage Systems\Installed Products\5" /v "AgentConfigurationStatus" |
Find "Succeeded"
If %ERRORLEVEL% EQU 0 (
 echo "Configuration has succeeded. Goto UPGRADE." >> C:\Temp\logfile.log
 GOTO :UPGRADE
) ELSE (
 echo "Configuration didn't succeed. Goto CONFIGURE." >> C:\Temp\logfile.log
 GOTO :CONFIGURE
)

:INSTALL
echo "Perform installation." >> C:\Temp\logfile.log
UnifiedAgent.exe /Role MS /InstallLocation "C:\Program Files (x86)\Microsoft Azure Site Recovery" /Platform
"VmWare" /Silent
IF %ERRORLEVEL% EQU 0 (
 echo "Installation has succeeded." >> C:\Temp\logfile.log
 (GOTO :CONFIGURE)
) ELSE (
 echo "Installation has failed." >> C:\Temp\logfile.log
 GOTO :ENDSCRIPT
)

```

```

:CONFIGURE
echo "Perform configuration." >> C:\Temp\logfile.log
cd "C:\Program Files (x86)\Microsoft Azure Site Recovery\agent"
UnifiedAgentConfigurator.exe /CSEndPoint "[CSIP]" /PassphraseFilePath %Temp%\MobSvc\MobSvc.passphrase
IF %ERRORLEVEL% EQU 0 (
 echo "Configuration has succeeded." >> C:\Temp\logfile.log
) ELSE (
 echo "Configuration has failed." >> C:\Temp\logfile.log
)
GOTO :ENDSCRIPT

:UPGRADE
echo "Perform upgrade." >> C:\Temp\logfile.log
UnifiedAgent.exe /Platform "VmWare" /Silent
IF %ERRORLEVEL% EQU 0 (
 echo "Upgrade has succeeded." >> C:\Temp\logfile.log
) ELSE (
 echo "Upgrade has failed." >> C:\Temp\logfile.log
)
GOTO :ENDSCRIPT

:ENDSCRIPT
echo "End of script." >> C:\Temp\logfile.log

```

## Copy code to the Linux folder

Copy the following code:

- Save the code in the *MobSvcLinux* folder as *install\_linux.sh*.
- Replace the **[CSIP]** placeholders in this script with the actual values of the IP address of your configuration server.
- The script supports new installations of the Mobility Service agent, and updates to agents that are already installed.

```

#!/usr/bin/env bash

rm -rf /tmp/MobSvc
mkdir -p /tmp/MobSvc
INSTALL_DIR='/usr/local/ASR'
VX_VERSION_FILE='/usr/local/.vx_version'

echo "======" >> /tmp/MobSvc/sccm.log
echo `date` >> /tmp/MobSvc/sccm.log
echo "======" >> /tmp/MobSvc/sccm.log

if [-f /etc/oracle-release] && [-f /etc/redhat-release]; then
 if grep -q 'Oracle Linux Server release 6.*' /etc/oracle-release; then
 if uname -a | grep -q x86_64; then
 OS="OL6-64"
 echo $OS >> /tmp/MobSvc/sccm.log
 cp *OL6*.tar.gz /tmp/MobSvc
 fi
 fi
elif [-f /etc/redhat-release]; then
 if grep -q 'Red Hat Enterprise Linux Server release 6.* (Santiago)' /etc/redhat-release || \
 grep -q 'CentOS Linux release 6.* (Final)' /etc/redhat-release || \
 grep -q 'CentOS release 6.* (Final)' /etc/redhat-release; then
 if uname -a | grep -q x86_64; then
 OS="RHEL6-64"
 echo $OS >> /tmp/MobSvc/sccm.log
 cp *RHEL6*.tar.gz /tmp/MobSvc
 fi
 elif grep -q 'Red Hat Enterprise Linux Server release 7.* (Maipo)' /etc/redhat-release || \
 grep -q 'CentOS Linux release 7.* (Core)' /etc/redhat-release; then
 if uname -a | grep -q x86_64; then
 OS="RHEL7-64"
 echo $OS >> /tmp/MobSvc/sccm.log
 cp *RHEL7*.tar.gz /tmp/MobSvc
 fi
 fi
fi

```

```

OS="RHEL7-64"
echo $OS >> /tmp/MobSvc/sccm.log
cp *RHEL7*.tar.gz /tmp/MobSvc
fi
fi
elif [-f /etc/SuSE-release] && grep -q 'VERSION = 11' /etc/SuSE-release; then
 if grep -q "SUSE Linux Enterprise Server 11" /etc/SuSE-release && grep -q 'PATCHLEVEL = 3' /etc/SuSE-
release; then
 if uname -a | grep -q x86_64; then
 OS="SLES11-SP3-64"
 echo $OS >> /tmp/MobSvc/sccm.log
 cp *SLES11-SP3*.tar.gz /tmp/MobSvc
 fi
 elif grep -q "SUSE Linux Enterprise Server 11" /etc/SuSE-release && grep -q 'PATCHLEVEL = 4' /etc/SuSE-
release; then
 if uname -a | grep -q x86_64; then
 OS="SLES11-SP4-64"
 echo $OS >> /tmp/MobSvc/sccm.log
 cp *SLES11-SP4*.tar.gz /tmp/MobSvc
 fi
 fi
else
 exit 1
fi

if [-z "$OS"]; then
 exit 1
fi

Install()
{
 echo "Perform Installation." >> /tmp/MobSvc/sccm.log
 ./install -q -d ${INSTALL_DIR} -r MS -v VmWare
 RET_VAL=$?
 echo "Installation Returncode: $RET_VAL" >> /tmp/MobSvc/sccm.log
 if [$RET_VAL -eq 0]; then
 echo "Installation has succeeded. Proceed to configuration." >> /tmp/MobSvc/sccm.log
 Configure
 else
 echo "Installation has failed." >> /tmp/MobSvc/sccm.log
 exit $RET_VAL
 fi
}

Configure()
{
 echo "Perform configuration." >> /tmp/MobSvc/sccm.log
 ${INSTALL_DIR}/Vx/bin/UnifiedAgentConfigurator.sh -i [CSIP] -P MobSvc.passphrase
 RET_VAL=$?
 echo "Configuration Returncode: $RET_VAL" >> /tmp/MobSvc/sccm.log
 if [$RET_VAL -eq 0]; then
 echo "Configuration has succeeded." >> /tmp/MobSvc/sccm.log
 else
 echo "Configuration has failed." >> /tmp/MobSvc/sccm.log
 exit $RET_VAL
 fi
}

Upgrade()
{
 echo "Perform Upgrade." >> /tmp/MobSvc/sccm.log

```

```

./install -q -v VmWare
RET_VAL=$?
echo "Upgrade Returncode: $RET_VAL" >> /tmp/MobSvc/sccm.log
if [$RET_VAL -eq 0]; then
 echo "Upgrade has succeeded." >> /tmp/MobSvc/sccm.log
else
 echo "Upgrade has failed." >> /tmp/MobSvc/sccm.log
 exit $RET_VAL
fi
}

cp MobSvc.passphrase /tmp/MobSvc
cd /tmp/MobSvc

tar -zxf *.tar.gz

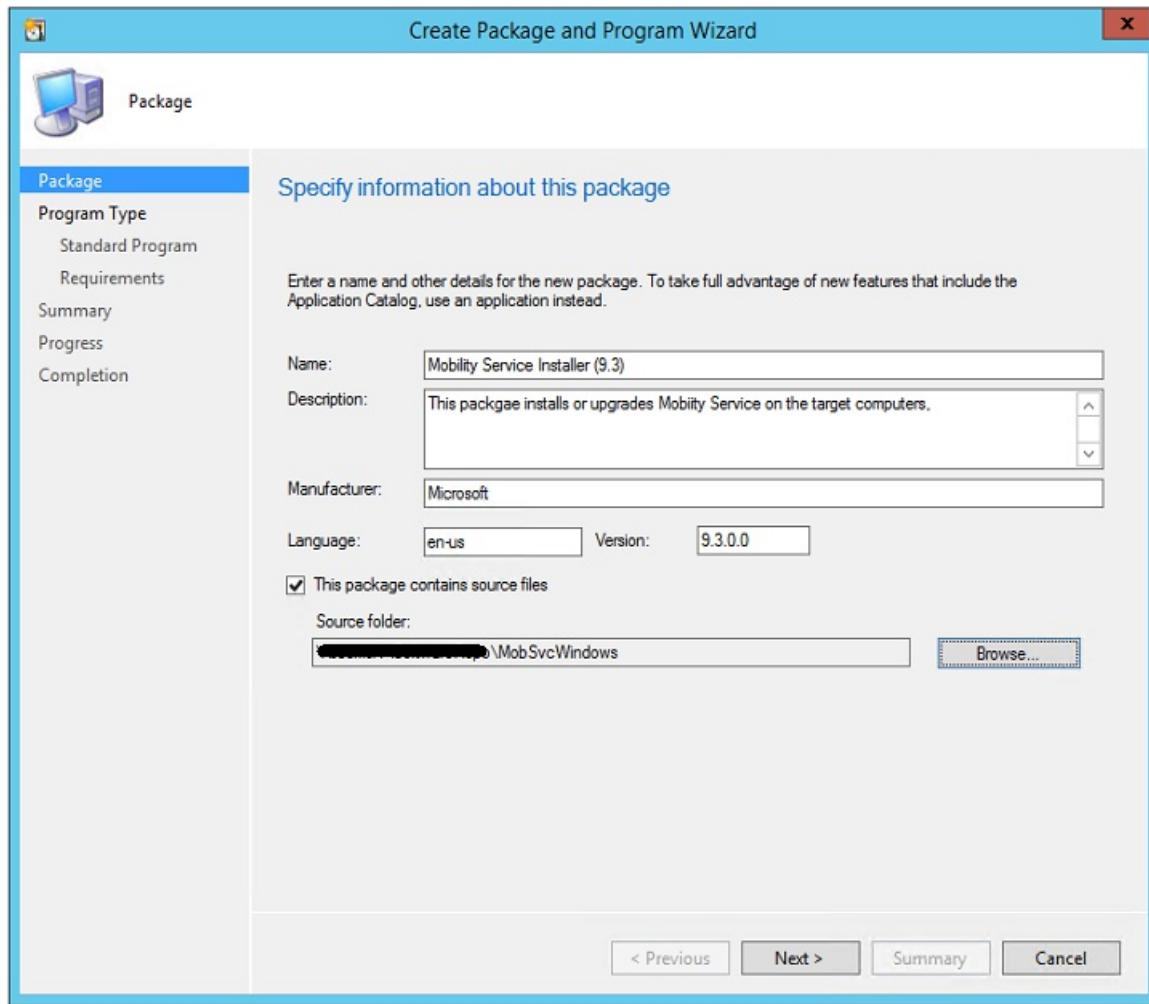
if [-e ${VX_VERSION_FILE}]; then
 echo "${VX_VERSION_FILE} exists. Checking for configuration status." >> /tmp/MobSvc/sccm.log
 agent_configuration=$(grep ^AGENT_CONFIGURATION_STATUS "${VX_VERSION_FILE}" | cut -d "=" -f2 | tr -d " ")
 echo "agent_configuration=$agent_configuration" >> /tmp/MobSvc/sccm.log
 if ["$agent_configuration" == "Succeeded"]; then
 echo "Agent is already configured. Proceed to Upgrade." >> /tmp/MobSvc/sccm.log
 Upgrade
 else
 echo "Agent is not configured. Proceed to Configure." >> /tmp/MobSvc/sccm.log
 Configure
 fi
else
 Install
fi

cd /tmp

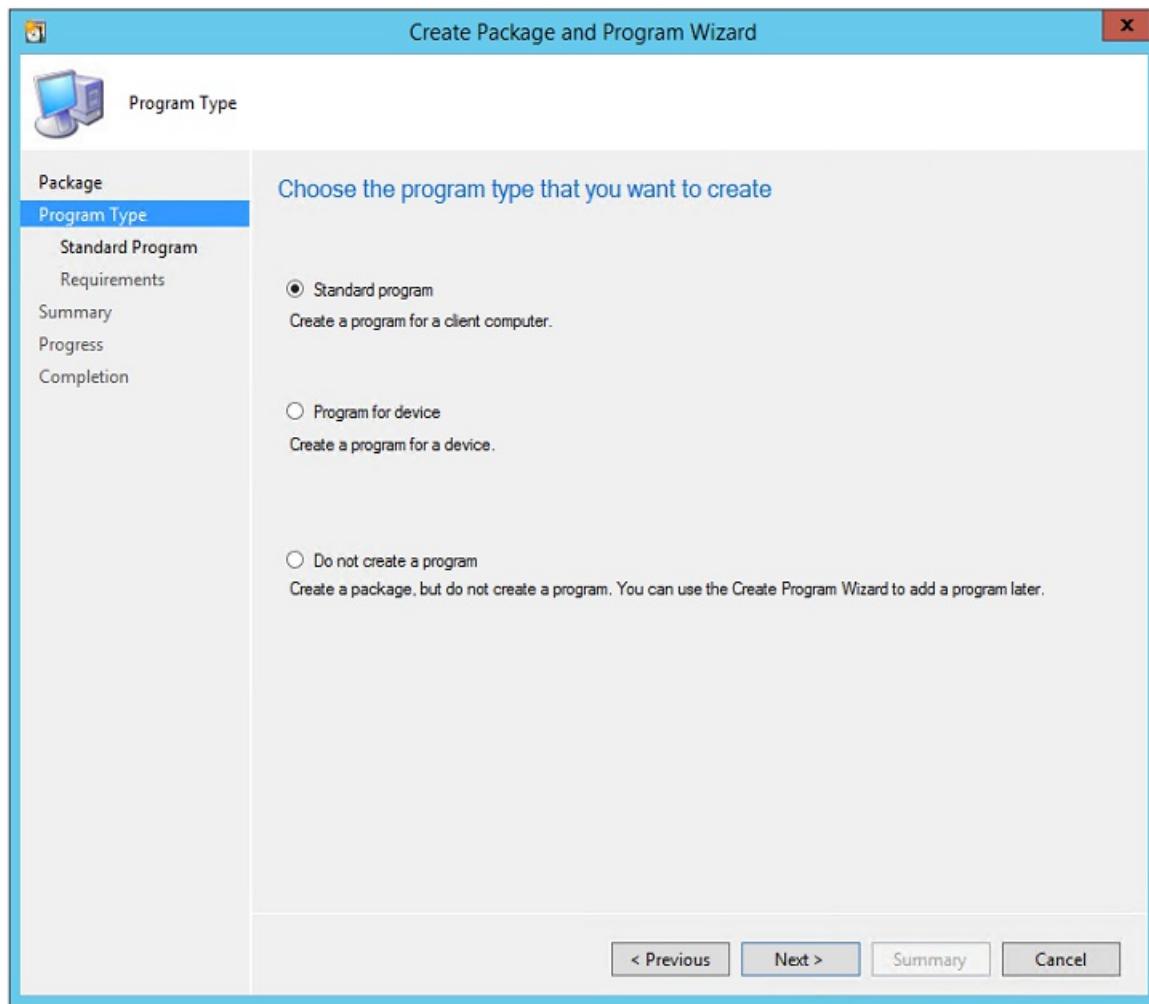
```

## Create a package

1. Sign in to the Configuration Manager console and go to **Software Library > Application Management > Packages**.
2. Right-click **Packages > Create Package**.
3. Provide package details including a name, description, manufacturer, language, and version.
4. Select **This package contains source files**.
5. Click **Browse**, and select the network share and folder that contains the relevant installer (*MobSvcWindows* or *MobSvcLinux*). Then, select **Next**.

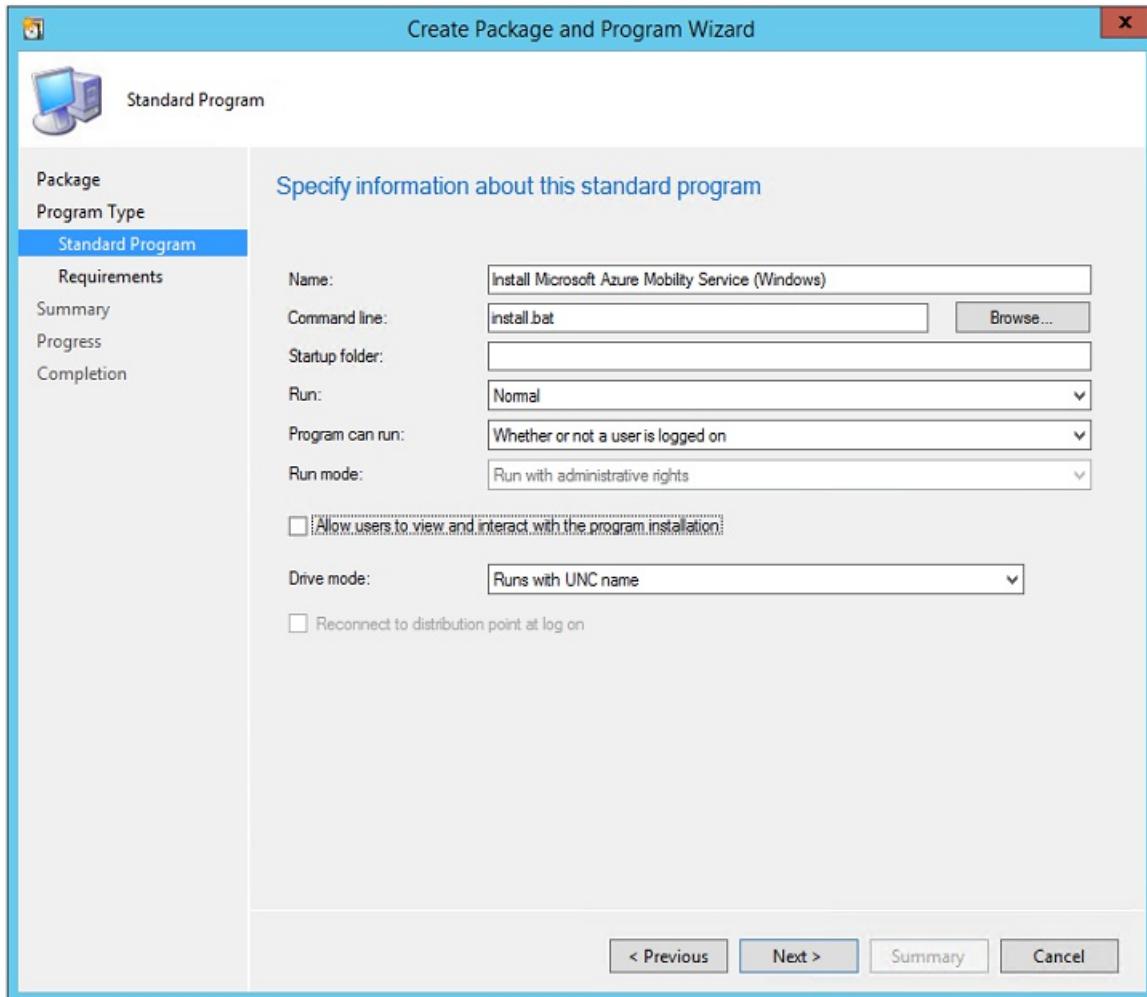


6. In **Choose the program type that you want to create** page, select **Standard Program > Next**.



7. In **Specify information about this standard program** page, specify the following values:

| PARAMETER               | WINDOWS VALUE                                      | LINUX VALUE                                       |
|-------------------------|----------------------------------------------------|---------------------------------------------------|
| <b>Name</b>             | Install Microsoft Azure Mobility Service (Windows) | Install Microsoft Azure Mobility Service (Linux). |
| <b>Command line</b>     | install.bat                                        | ./install_linux.sh                                |
| <b>Program can run</b>  | Whether or not a user is logged on                 | Whether or not a user is logged on                |
| <b>Other parameters</b> | Use default setting                                | Use default setting                               |



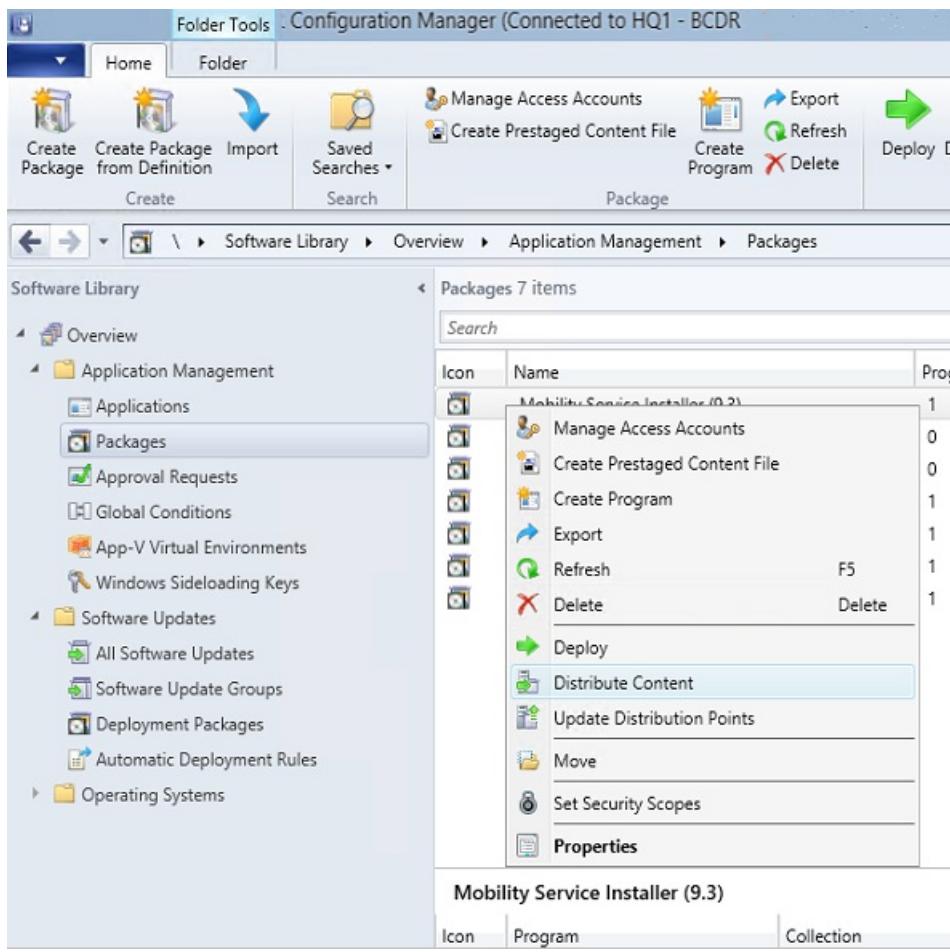
8. In **Specify the requirements for this standard program**, do the following tasks:

- For Windows machines, select **This program can run only on specified platforms**. Then, select the [supported Windows operating systems](#) and select **Next**.
- For Linux machines, select **This program can run on any platform**. Then select **Next**.

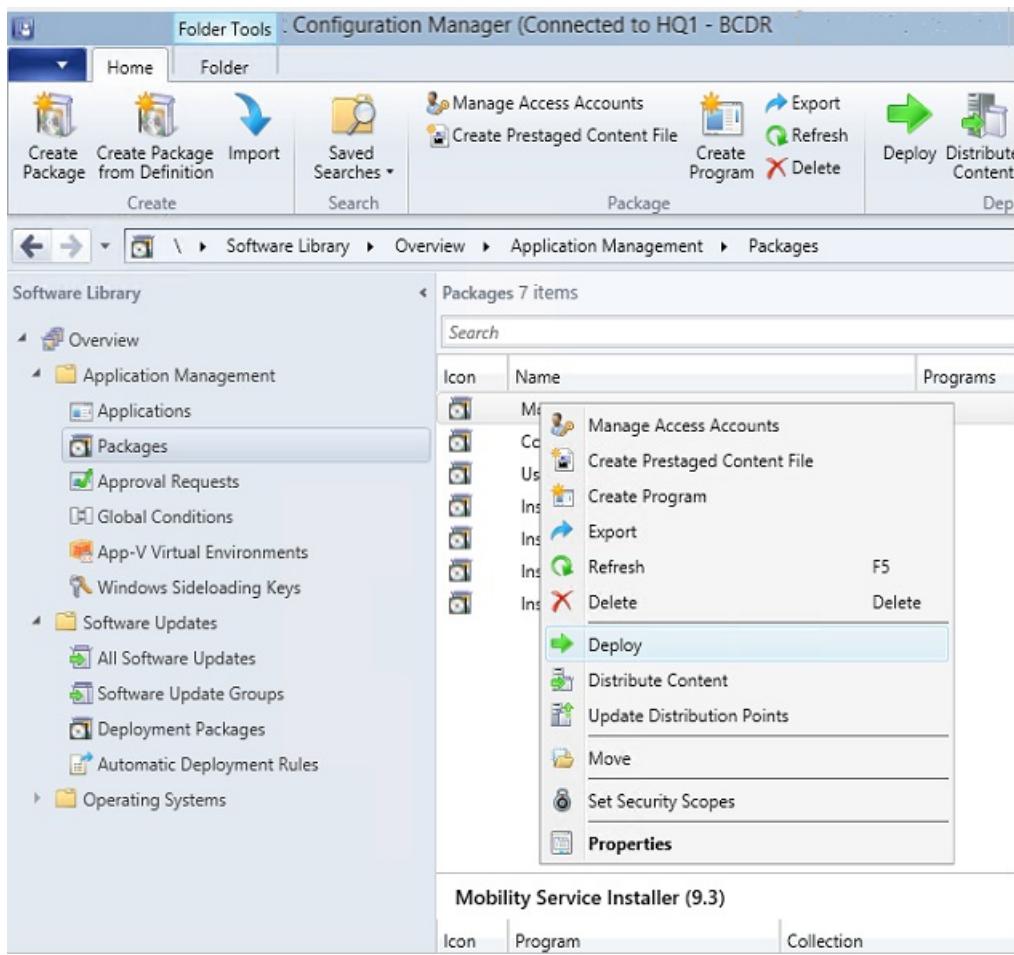
9. Finish the wizard.

### Deploy the package

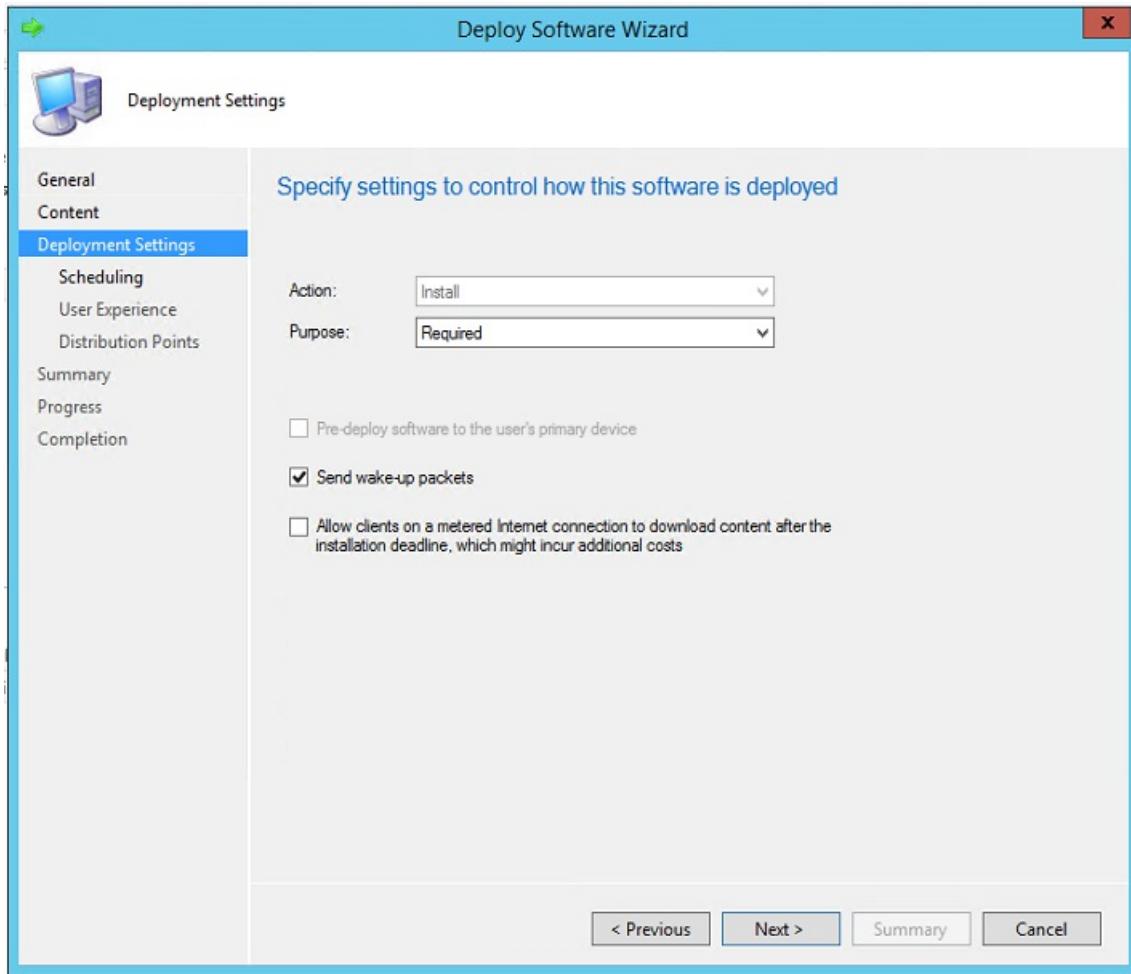
1. In the Configuration Manager console, right-click the package and select **Distribute Content**.



2. Select the distribution points on to which the packages should be copied. [Learn more](#).
3. Complete the wizard. The package then starts replicating to the specified distribution points.
4. After the package distribution finishes, right-click the package > **Deploy**.



5. Select the Windows or Linux device collection you created previously.
6. On the **Specify the content destination** page, select **Distribution Points**.
7. In **Specify settings to control how this software is deployed** page, set **Purpose** to **Required**.



8. In **Specify the schedule for this deployment**, set up a schedule. [Learn more](#).
  - The Mobility Service is installed in accordance with the schedule you specify.
  - To avoid unnecessary reboots, schedule the package installation during your monthly maintenance window or software updates window.
9. On the **Distribution Points** page, configure settings and finish the wizard.
10. Monitor deployment progress in the Configuration Manager console. Go to **Monitoring > Deployments** > *<your package name>*.

#### Uninstall the Mobility Service

You can create Configuration Manager packages to uninstall the Mobility Service. For example, the following script uninstalls the Mobility Service:

```
Time /t >> C:\logfile.log
REM =====
REM === Check if Mob Svc is already installed =====
REM === If not installed no operation required =====
REM === Else run uninstall command =====
REM === {275197FC-14FD-4560-A5EB-38217F80CBD1} is ===
REM === guid for Mob Svc Installer =====
whoami >> C:\logfile.log
NET START | FIND "InMage Scout Application Service"
IF %ERRORLEVEL% EQU 1 (GOTO :INSTALL) ELSE GOTO :UNINSTALL
:NOOPERATION
 echo "No Operation Required." >> c:\logfile.log
 GOTO :ENDSCRIPT
:UNINSTALL
 echo "Uninstall" >> C:\logfile.log
 MsiExec.exe /qn /x {275197FC-14FD-4560-A5EB-38217F80CBD1} /L+*V
"C:\ProgramData\ASRSetupLogs\UnifiedAgentMSIUninstall.log"
:ENDSCRIPT
```

## Next steps

[Enable replication for VMs.](#)

# Fail over and fail back physical servers replicated to Azure

12/26/2019 • 7 minutes to read • [Edit Online](#)

This tutorial describes how to fail over on-premises physical servers that are replicating to Azure with [Azure Site Recovery](#). After you've failed over, you fail back from Azure to your on-premises site when it's available.

## Before you start

- [Learn](#) about the failover process in disaster recovery.
- If you want to fail over multiple machines, [learn](#) how to gather machines together in a recovery plan.
- Before you do a full failover, run a [disaster recovery drill](#) to ensure that everything is working as expected.
- Follow [these instructions](#) to prepare to connect to Azure VMs after failover.

## Run a failover

### Verify server properties

Verify the server properties, and make sure that it complies with [Azure requirements](#) for Azure VMs.

1. In **Protected Items**, click **Replicated Items**, and select the machine.
2. In the **Replicated item** pane, there's a summary of machine information, health status, and the latest available recovery points. Click **Properties** to view more details.
3. In **Compute and Network**, you can modify the Azure name, resource group, target size, [availability set](#), and managed disk settings
4. You can view and modify network settings, including the network/subnet in which the Azure VM will be located after failover, and the IP address that will be assigned to it.
5. In **Disks**, you can see information about the machine operating system and data disks.

### Fail over to Azure

1. In **Settings > Replicated items** click the machine > **Failover**.
2. In **Failover** select a **Recovery Point** to fail over to. You can use one of the following options:
  - **Latest:** This option first processes all the data sent to Site Recovery. It provides the lowest RPO (Recovery Point Objective) because the Azure VM created after failover has all the data that was replicated to Site Recovery when the failover was triggered.
  - **Latest processed:** This option fails over the machine to the latest recovery point processed by Site Recovery. This option provides a low RTO (Recovery Time Objective), because no time is spent processing unprocessed data.
  - **Latest app-consistent:** This option fails over the machine to the latest app-consistent recovery point processed by Site Recovery.
  - **Custom:** Specify a recovery point.
3. Select **Shut down machine before beginning failover** if you want Site Recovery to try to shut down source machine before triggering the failover. Failover continues even if shutdown fails. You can follow the failover progress on the **Jobs** page.
4. If you prepared to connect to the Azure VM, connect to validate it after the failover.
5. After you verify, **Commit** the failover. This deletes all the available recovery points.

## WARNING

Don't cancel a failover in progress. Before failover begins, machine replication stops. If you cancel the failover, it stops, but the machine won't replicate again. For physical servers, additional failover processing can take around eight to ten minutes to complete.

## Automate actions during failover

You might want to automate actions during failover. To do this, you can use scripts or Azure automation runbooks in recovery plans.

- [Learn](#) about creating and customizing recovery plans, including adding scripts.
- [Learn](#) about adding Azure Automation runbooks to recovery plans.

## Configure settings after failover

After failover you need to [configure Azure settings](#) to connect to the replicated Azure VMs. In addition, set up [internal and public](#) IP addressing.

## Prepare for reprotection and failback

After failing over to Azure, you reprotect Azure VMs by replicating them to the on-premises site. Then after they're replicating, you can fail them back to on-premises, by running a failover from Azure to your on-premises site.

1. Physical servers replicated to Azure using Site Recovery can only fail back as VMware VMs. You need a VMware infrastructure in order to fail back. Follow the steps in [this article](#) to prepare for reprottection and failback, including setting up a process server in Azure, and an on-premises master target server, and configuring a site-to-site VPN, or ExpressRoute private peering, for failback.
2. Make sure that the on-premises configuration server is running and connected to Azure. During failover to Azure, the on-premises site might not be accessible, and the configuration server might be unavailable or shut down. During failback, the VM must exist in the configuration server database. Otherwise, failback is unsuccessful.
3. Delete any snapshots on the on-premises master target server. Reprotection won't work if there are snapshots. The snapshots on the VM are automatically merged during a reprotect job.
4. If you're reprotecting VMs gathered into a replication group for multi-VM consistency, make sure they all have the same operating system (Windows or Linux) and make sure that the master target server you deploy has the same type of operating system. All VMs in a replication group must use the same master target server.
5. Open [the required ports](#) for failback.
6. Ensure that the vCenter Server is connected before failback. Otherwise, disconnecting disks and attaching them back to the virtual machine fails.
7. If a vCenter server manages the VMs to which you'll fail back, make sure that you have the required permissions. If you perform a read-only user vCenter discovery and protect virtual machines, protection succeeds, and failover works. However, during reprottection, failover fails because the datastores can't be discovered, and aren't listed during reprottection. To resolve this problem, you can update the vCenter credentials with an [appropriate account/permissions](#), and then retry the job.
8. If you used a template to create your virtual machines, ensure that each VM has its own UUID for the disks. If the on-premises VM UUID clashes with the UUID of the master target server because both were created from the same template, reprottection fails. Deploy from a different template.
9. If you're failing back to an alternate vCenter Server, make sure that the new vCenter Server and the master target server are discovered. Typically if they're not the datastores aren't accessible, or aren't visible in **Reprotect**.

10. Verify the following scenarios in which you can't fail back:

- If you're using either the ESXi 5.5 free edition or the vSphere 6 Hypervisor free edition. Upgrade to a different version.
- If you have a Windows Server 2008 R2 SP1 physical server.
- VMs that have [been migrated](#).
- A VM that's been moved to another resource group.
- A replica Azure VM that's been deleted.
- A replica Azure VM that isn't protected (replicating to the on-premises site).

11. [Review the types of fallback](#) you can use - original location recovery and alternate location recovery.

## Reprotect Azure VMs to an alternate location

This procedure presumes that the on-premises VM isn't available.

1. In the vault > **Settings** > **Replicated items**, right-click the machine that was failed over > **Re-Protect**.
2. In **Re-protect**, verify that **Azure to On-premises**, is selected.
3. Specify the on-premises master target server, and the process server.
4. In **Datastore**, select the master target datastore to which you want to recover the disks on-premises. - Use this option if the on-premises VM has been deleted or doesn't exist, and you need to create new disks. - This setting is ignored if the disks already exists, but you do need to specify a value.
5. Select the master target retention drive. The fallback policy is automatically selected.
6. Click **OK** to begin reprottection. A job begins to replicate the Azure VM to the on-premises site. You can track the progress on the **Jobs** tab.

### NOTE

If you want to recover the Azure VM to an existing on-premises VM, mount the on-premises virtual machine's datastore with read/write access, on the master target server's ESXi host.

## Fail back from Azure

Run the failover as follows:

1. On the **Replicated Items** page, right-click the machine > **Unplanned Failover**.
2. In **Confirm Failover**, verify that the failover direction is from Azure. 3. Select the recovery point that you want to use for the failover.
  - We recommend that you use the **Latest** recovery point. The app-consistent point is behind the latest point in time, and causes some data loss.
  - **Latest** is a crash-consistent recovery point.
  - When failover runs, Site Recovery shuts down the Azure VMs, and boots up the on-premises VM. There will be some downtime, so choose an appropriate time.
3. Right-click the machine, and click **Commit**. This triggers a job that removes the Azure VMs.
4. Verify that Azure VMs have been shut down as expected.

## Reprotect on-premises machines to Azure

Data should now be back on your on-premises site, but it isn't replicating to Azure. You can start replicating to Azure again as follows:

1. In the vault > **Settings** > **Replicated Items**, select the failed back VMs that have failed back, and click **Re-Protect**.

2. Select the process server that is used to send the replicated data to Azure, and click **OK**.

## Next steps

After the reprotect job finishes, the on-premises VM is replicating to Azure. As needed, you can [run another failover](#) to Azure.

# Manage the Mobility agent

11/12/2019 • 2 minutes to read • [Edit Online](#)

You set up mobility agent on your server when you use Azure Site Recovery for disaster recovery of VMware VMs and physical servers to Azure. Mobility agent coordinates communications between your protected machine, configuration server/scale-out process server and manages data replication. This article summarizes common tasks for managing mobility agent after it's deployed.

## NOTE

This article has been updated to use the new Azure PowerShell Az module. You can still use the AzureRM module, which will continue to receive bug fixes until at least December 2020. To learn more about the new Az module and AzureRM compatibility, see [Introducing the new Azure PowerShell Az module](#). For Az module installation instructions, see [Install Azure PowerShell](#).

## Update mobility service from Azure portal

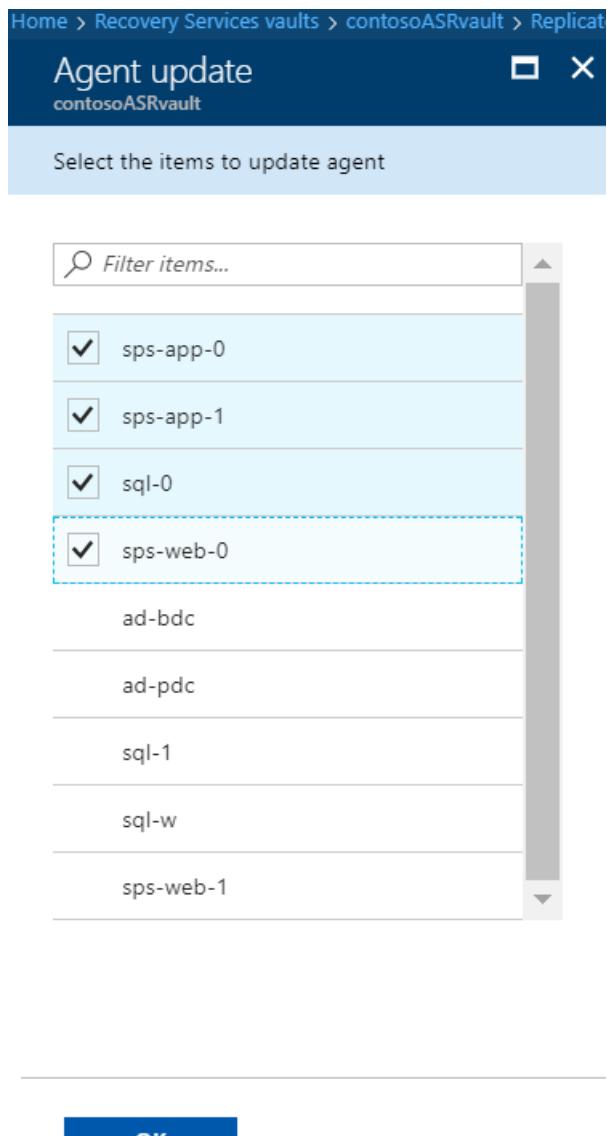
1. Before you start ensure that the configuration server, scale-out process servers, and any master target servers that are a part of your deployment are updated before you update the Mobility Service on protected machines.
2. In the portal open the vault > **Replicated items**.
3. If the configuration server is the latest version, you see a notification that reads "New Site recovery replication agent update is available. Click to install."

The screenshot shows the 'Replicated items' page in the Azure portal. At the top, there are buttons for Refresh, Replicate, Columns, and Filter. A yellow banner displays a warning: '⚠️ New Mobility Service Update is available. Push install latest update on every physical and virtual machine →'. Below the banner, a message says 'Last refreshed at: 11/14/2019, 9:34:41 AM'. The main area contains a table with the following data:

| Name | Replication Health | Status    | Active location | ... |
|------|--------------------|-----------|-----------------|-----|
| test | Healthy            | Protected | westus          | ... |

A search bar at the bottom left says 'Filter items...'. The entire screenshot is framed by a light gray border.

4. Click the notification, and in **Agent update**, select the machines on which you want to upgrade the Mobility service. Then click **OK**.



5. The Update Mobility Service job starts for each of the selected machines.

## Update Mobility service through powershell script on Windows server

Use following script to upgrade mobility service on a server through power shell cmdlet

```
Update-AzRecoveryServicesAsrMobilityService -ReplicationProtectedItem $rpi -Account
$fabric.fabricSpecificDetails.RunAsAccounts[0]
```

## Update account used for push installation of Mobility service

When you deployed Site Recovery, to enable push installation of the Mobility service, you specified an account that the Site Recovery process server uses to access the machines and install the service when replication is enabled for the machine. If you want to update the credentials for this account, follow [these instructions](#).

## Uninstall Mobility service

### On a Windows machine

Uninstall from the UI or from a command prompt.

- **From the UI:** In the Control Panel of the machine, select **Programs**. Select **Microsoft Azure Site Recovery Mobility Service/Master Target server** > **Uninstall**.

- **From a command prompt:** Open a command prompt window as an administrator on the machine. Run the following command:

```
MsiExec.exe /qn /x {275197FC-14FD-4560-A5EB-38217F80CBD1} /L+*V
"C:\ProgramData\ASRSetupLogs\UnifiedAgentMSIUninstall.log"
```

#### On a Linux machine

1. On the Linux machine, sign in as a **root** user.
2. In a terminal, go to /usr/local/ASR.
3. Run the following command:

```
uninstall.sh -Y
```

## Install Site Recovery VSS provider on source machine

Azure Site Recovery VSS provider is required on the source machine to generate application consistency points. If the installation of the provider didn't succeed through push installation, follow the below given guidelines to install it manually.

1. Open admin cmd window.
2. Navigate to the mobility service installation location. (Eg - C:\Program Files (x86)\Microsoft Azure Site Recovery\agent)
3. Run the script InMageVSSProvider\_Uninstall.cmd . This will uninstall the service if it already exists.
4. Run the script InMageVSSProvider\_Install.cmd to install the VSS provider manually.

## Next steps

- [Set up disaster recovery for VMware VMs](#)
- [Set up disaster recovery for physical servers](#)

# Manage the configuration server for physical server disaster recovery

11/14/2019 • 11 minutes to read • [Edit Online](#)

You set up an on-premises configuration server when you use the [Azure Site Recovery](#) service for disaster recovery of physical servers to Azure. The configuration server coordinates communications between on-premises machines and Azure, and manages data replication. This article summarizes common tasks for managing the configuration server after it's been deployed.

## NOTE

This article has been updated to use the new Azure PowerShell Az module. You can still use the AzureRM module, which will continue to receive bug fixes until at least December 2020. To learn more about the new Az module and AzureRM compatibility, see [Introducing the new Azure PowerShell Az module](#). For Az module installation instructions, see [Install Azure PowerShell](#).

## Prerequisites

The table summarizes the prerequisites for deploying the on-premises configuration server machine.

| COMPONENT                              | REQUIREMENT                                                                                                     |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| CPU cores                              | 8                                                                                                               |
| RAM                                    | 16 GB                                                                                                           |
| Number of disks                        | 3, including the OS disk, process server cache disk, and retention drive for failback                           |
| Disk free space (process server cache) | 600 GB                                                                                                          |
| Disk free space (retention disk)       | 600 GB                                                                                                          |
| Operating system                       | Windows Server 2012 R2<br>Windows Server 2016                                                                   |
| Operating system locale                | English (US)                                                                                                    |
| VMware vSphere PowerCLI version        | Not required                                                                                                    |
| Windows Server roles                   | Don't enable these roles:<br>- Active Directory Domain Services<br>- Internet Information Services<br>- Hyper-V |

| COMPONENT       | REQUIREMENT                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Group policies  | <p>Don't enable these group policies:</p> <ul style="list-style-type: none"> <li>- Prevent access to the command prompt</li> <li>- Prevent access to registry editing tools</li> <li>- Trust logic for file attachments</li> <li>- Turn on Script Execution</li> </ul> <p><a href="#">Learn more</a></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| IIS             | <ul style="list-style-type: none"> <li>- No pre-existing default website</li> <li>- Enable <a href="#">Anonymous Authentication</a></li> <li>- Enable <a href="#">FastCGI</a> setting</li> <li>- No pre-existing website/application listening on port 443</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| NIC type        | VMXNET3 (when deployed as a VMware VM)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| IP address type | Static                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Internet access | <p>The server needs access to these URLs:</p> <ul style="list-style-type: none"> <li>- *.accesscontrol.windows.net</li> <li>- *.backup.windowsazure.com</li> <li>- *.store.core.windows.net</li> <li>- *.blob.core.windows.net</li> <li>- *.hypervrecoverymanager.windowsazure.com</li> <li>- <a href="https://management.azure.com">https://management.azure.com</a></li> <li>- *.services.visualstudio.com</li> <li>-</li> </ul> <p><a href="https://dev.mysql.com/get/Downloads/MySQLInstaller/mysql-installer-community-5.7.20.0.msi">https://dev.mysql.com/get/Downloads/MySQLInstaller/mysql-installer-community-5.7.20.0.msi</a> (not required for Scale-out Process Servers)</p> <ul style="list-style-type: none"> <li>- time.nist.gov</li> <li>- time.windows.com</li> </ul> |
| Ports           | 443 (Control channel orchestration)<br>9443 (Data transport)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

## Download the latest installation file

The latest version of the configuration server installation file is available in the Site Recovery portal. Additionally, it can be downloaded directly from the [Microsoft Download Center](#).

1. Log on to the Azure portal and browse to your Recovery Services Vault.
2. Browse to **Site Recovery Infrastructure > Configuration Servers** (under For VMware & Physical Machines).
3. Click the **+Servers** button.
4. On the **Add Server** page, click the Download button to download the Registration key. You need this key during the Configuration Server installation to register it with Azure Site Recovery service.
5. Click the **Download the Microsoft Azure Site Recovery Unified Setup** link to download the latest version of the Configuration Server.

Server type  
Configuration Server

Adding Configuration Server may take 15 minutes to 30 minutes

Register your Configuration Server  
On-premises

1. Make sure server on which you plan to set up the Configuration Server is running Windows Server 2012 R2 virtual machine
2. Configure Proxy so that server can access the Service URLs
3. Download the Microsoft Azure Site Recovery Unified Setup
4. Download the vault registration key  
[Download](#)
5. Run the installer to set up the Configuration Server and Process Server and use the vault registration key to register it with the vault.  
[Learn more](#).
6. Run cpsconfigtool.exe to create one or more management accounts on the configuration server.
7. If you're protecting VMware VMs make sure the management accounts have administrator permissions on the vCenter server/Sphere host Server/ESXi host from which you'll replicate virtual machines. [Learn more](#).
8. If you're protecting physical servers make sure the management accounts have administrator permissions on the physical server.

## Install and register the server

1. Run the Unified Setup installation file.
2. In **Before You Begin**, select **Install the configuration server and process server**.

**Before You Begin**

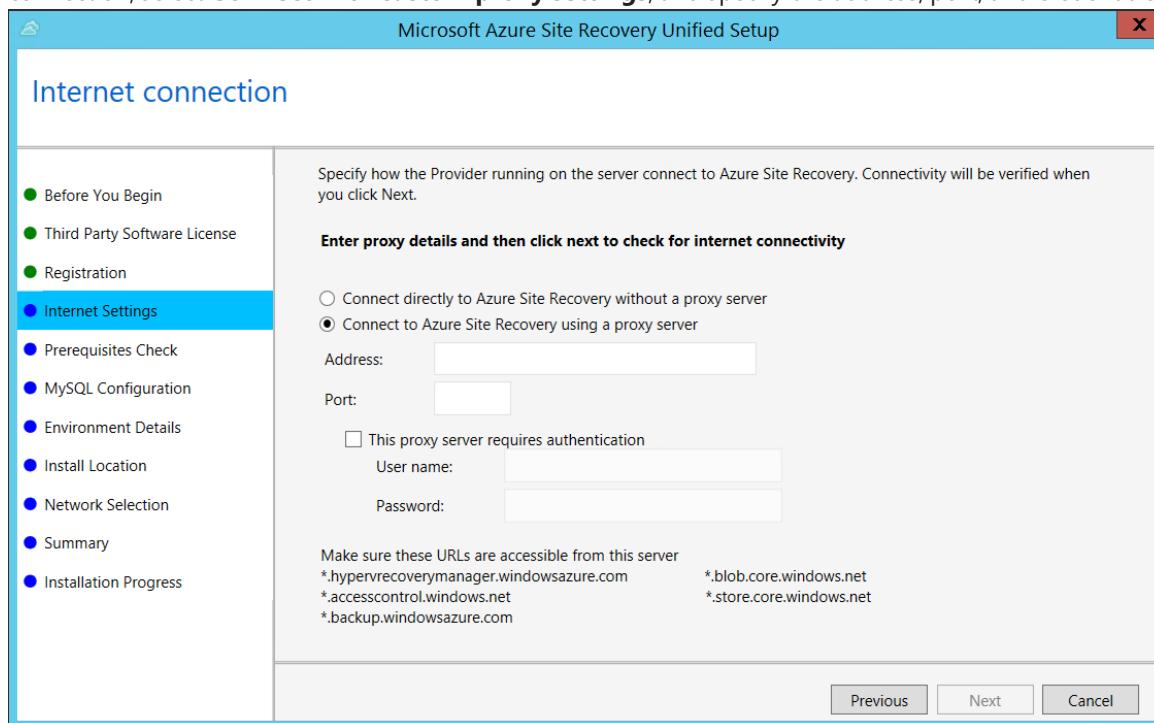
The Azure Site Recovery Unified Setup wizard helps you to set up protection for workloads running on physical servers and VMware virtual machines by replicating them to Azure.

**Install the configuration server and process server**  
Select this option if you are setting up Site Recovery for the first time.

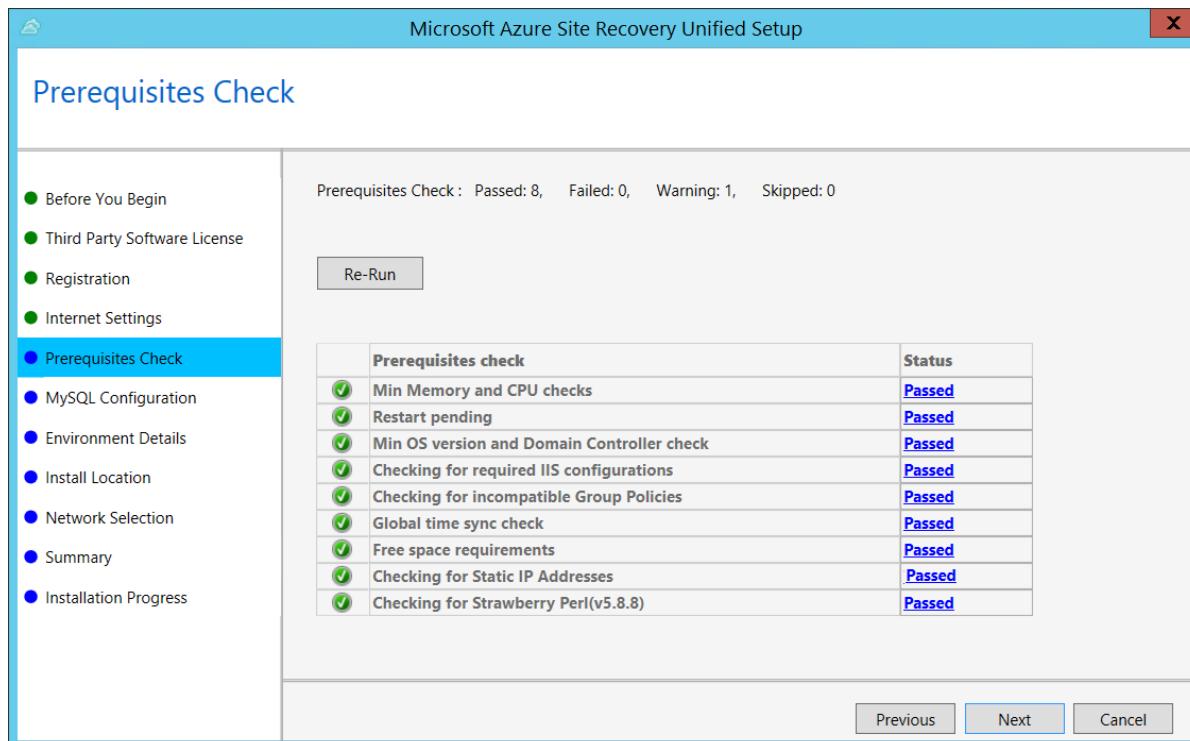
**Add additional process servers to scale out deployment**  
Select this option to add more process servers to handle the replication load.

3. In **Third Party Software License**, click **I Accept** to download and install MySQL.
4. In **Internet Settings**, specify how the Provider running on the configuration server connects to Azure Site Recovery over the Internet. Make sure you've allowed the required URLs.
  - If you want to connect with the proxy that's currently set up on the machine, select **Connect to Azure Site Recovery using a proxy server**.

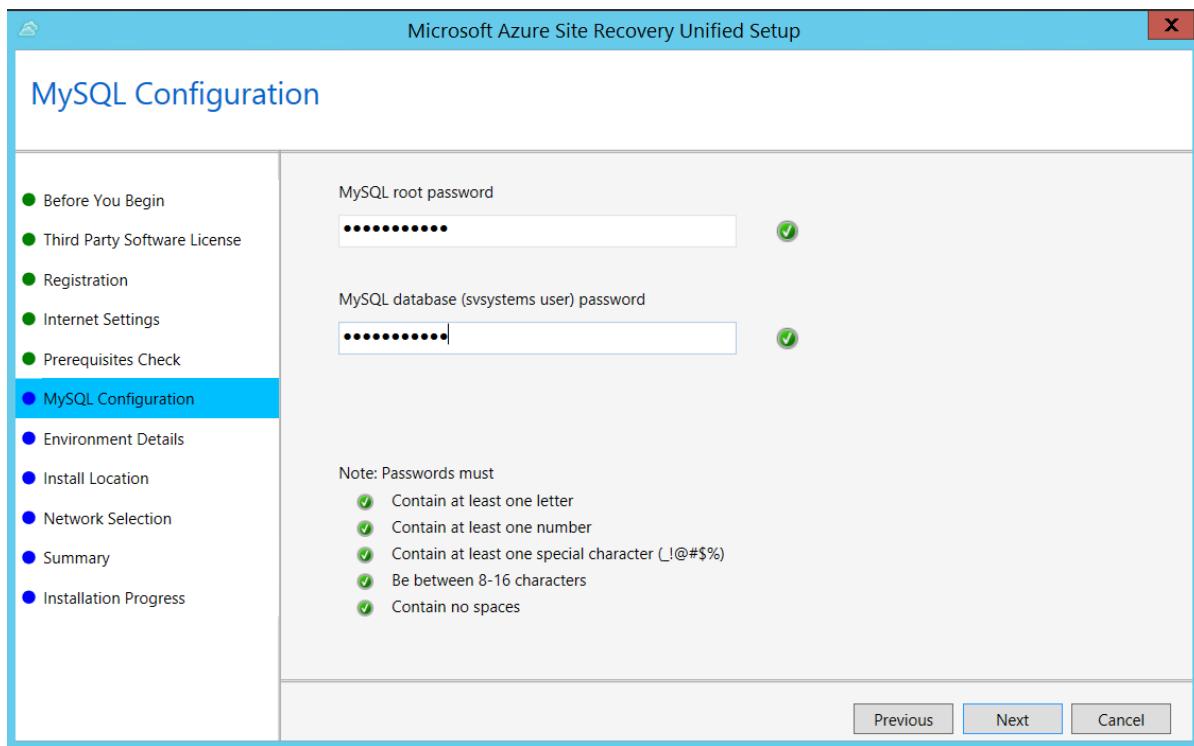
- If you want the Provider to connect directly, select **Connect directly to Azure Site Recovery without a proxy server**.
- If the existing proxy requires authentication, or if you want to use a custom proxy for the Provider connection, select **Connect with custom proxy settings**, and specify the address, port, and credentials.



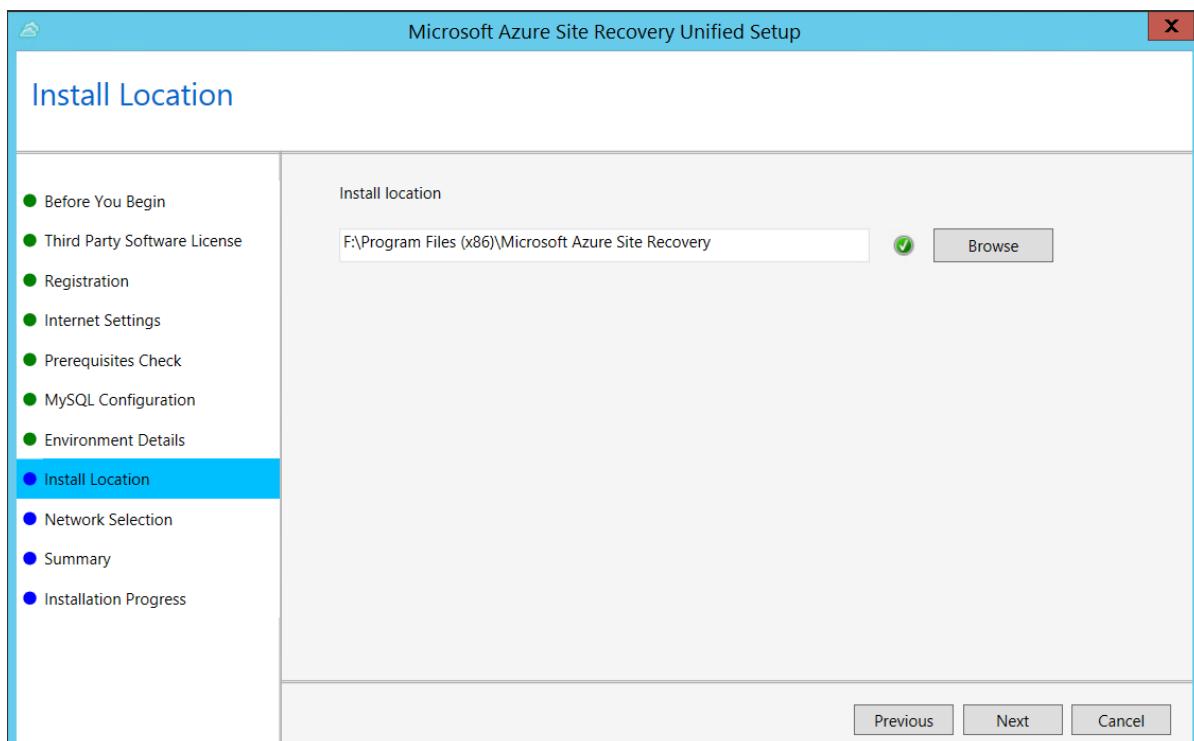
5. In **Prerequisites Check**, Setup runs a check to make sure that installation can run. If a warning appears about the **Global time sync check**, verify that the time on the system clock (**Date and Time** settings) is the same as the time zone.



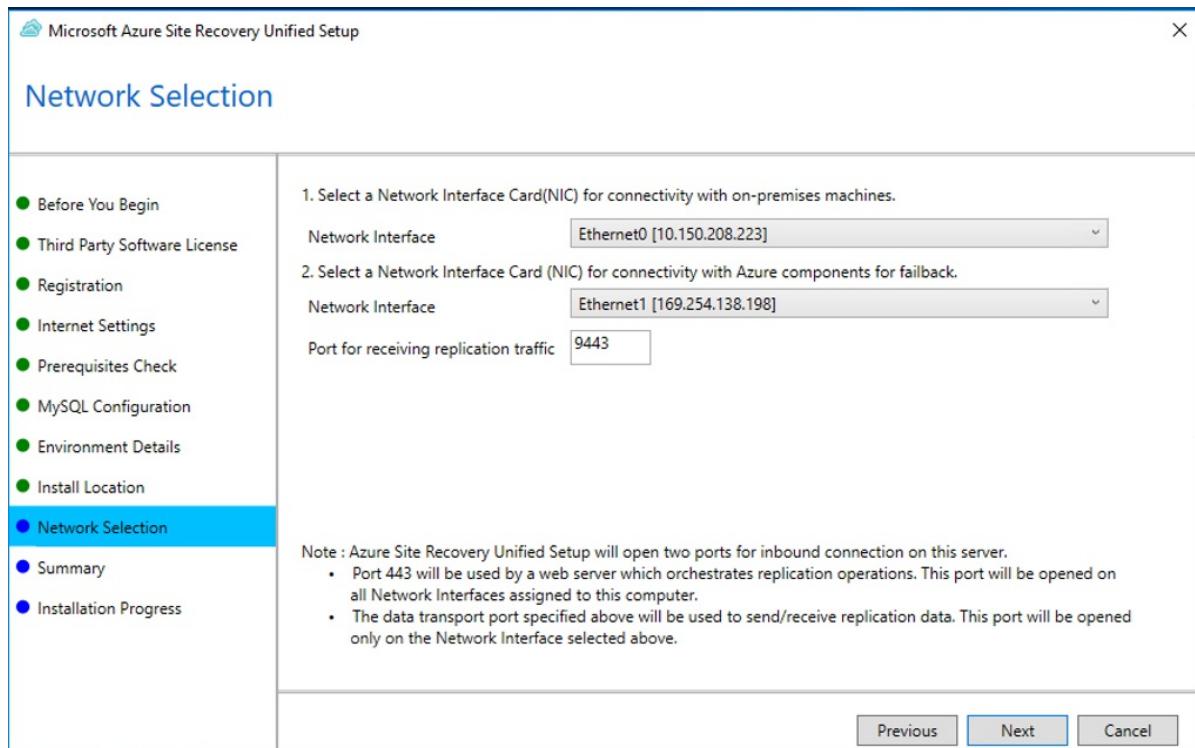
6. In **MySQL Configuration**, create credentials for logging on to the MySQL server instance that is installed.



7. In **Environment Details**, select whether you're going to replicate VMware VMs. If you are, then Setup checks that PowerCLI 6.0 is installed.
8. In **Install Location**, select where you want to install the binaries and store the cache. The drive you select must have at least 5 GB of disk space available, but we recommend a cache drive with at least 600 GB of free space.



9. In **Network Selection**, first select the NIC that the in-built process server uses for discovery and push installation of mobility service on source machines, and then select the NIC that Configuration Server uses for connectivity with Azure. Port 9443 is the default port used for sending and receiving replication traffic, but you can modify this port number to suit your environment's requirements. In addition to the port 9443, we also open port 443, which is used by a web server to orchestrate replication operations. Do not use port 443 for sending or receiving replication traffic.



10. In **Summary**, review the information and click **Install**. When installation finishes, a passphrase is generated. You will need this when you enable replication, so copy it and keep it in a secure location.

After registration finishes, the server is displayed on the **Settings > Servers** blade in the vault.

## Install from the command line

Run the installation file as follows:

```
UnifiedSetup.exe [/ServerMode <CS/PS>] [/InstallDrive <DriveLetter>] [/MySQLCredsFilePath <MySQL credentials file path>] [/VaultCredsFilePath <Vault credentials file path>] [/EnvType <VMWare/NonVMWare>] [/PSIP <IP address to be used for data transfer>] [/CSIP <IP address of CS to be registered with>] [/PassphraseFilePath <Passphrase file path>]
```

### Sample usage

```
MicrosoftAzureSiteRecoveryUnifiedSetup.exe /q /x:C:\Temp\Extracted
cd C:\Temp\Extracted
UNIFIEDSETUP.EXE /AcceptThirdpartyEULA /servermode "CS" /InstallLocation "D:\" /MySQLCredsFilePath "C:\Temp\MySQLCredentialsfile.txt" /VaultCredsFilePath "C:\Temp\MyVault.vaultcredentials" /EnvType "VMWare"
```

### Parameters

| PARAMETER NAME   | TYPE     | DESCRIPTION                                                                                                  | VALUES                     |
|------------------|----------|--------------------------------------------------------------------------------------------------------------|----------------------------|
| /ServerMode      | Required | Specifies whether both the configuration and process servers should be installed, or the process server only | CS<br>PS                   |
| /InstallLocation | Required | The folder in which the components are installed                                                             | Any folder on the computer |

| PARAMETER NAME         | TYPE     | DESCRIPTION                                                                      | VALUES                                           |
|------------------------|----------|----------------------------------------------------------------------------------|--------------------------------------------------|
| /MySQLCredsFilePath    | Required | The file path in which the MySQL server credentials are stored                   | The file should be the format specified below    |
| /VaultCredsFilePath    | Required | The path of the vault credentials file                                           | Valid file path                                  |
| /EnvType               | Required | Type of environment that you want to protect                                     | VMware<br>NonVMware                              |
| /PSIP                  | Required | IP address of the NIC to be used for replication data transfer                   | Any valid IP Address                             |
| /CSIP                  | Required | The IP address of the NIC on which the configuration server is listening on      | Any valid IP Address                             |
| /PassphraseFilePath    | Required | The full path to location of the passphrase file                                 | Valid file path                                  |
| /BypassProxy           | Optional | Specifies that the configuration server connects to Azure without a proxy        | To do get this value from Venu                   |
| /ProxySettingsFilePath | Optional | Proxy settings (The default proxy requires authentication, or a custom proxy)    | The file should be in the format specified below |
| DataTransferSecurePort | Optional | Port number on the PSIP to be used for replication data                          | Valid Port Number (default value is 9433)        |
| /SkipSpaceCheck        | Optional | Skip space check for cache disk                                                  |                                                  |
| /AcceptThirdpartyEULA  | Required | Flag implies acceptance of third-party EULA                                      |                                                  |
| /ShowThirdpartyEULA    | Optional | Displays third-party EULA. If provided as input all other parameters are ignored |                                                  |

### Create file input for MySQLCredsFilePath

The MySQLCredsFilePath parameter takes a file as input. Create the file using the following format and pass it as input MySQLCredsFilePath parameter.

```
[MySQLCredentials]
MySQLRootPassword = "Password"
MySQLUserPassword = "Password"
```

### Create file input for ProxySettingsFilePath

ProxySettingsFilePath parameter takes a file as input. Create the file using the following format and pass it as

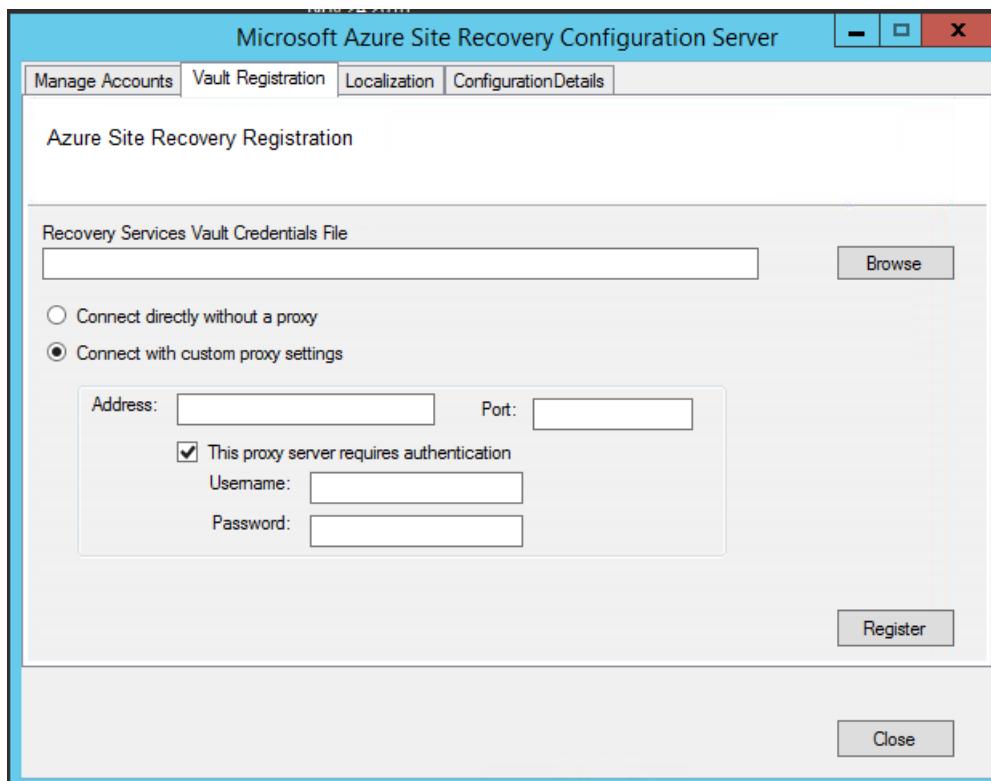
input ProxySettingsFilePath parameter.

```
[ProxySettings]
ProxyAuthentication = "Yes/No"
Proxy IP = "IP Address"
ProxyPort = "Port"
ProxyUserName="UserName"
ProxyPassword="Password"
```

## Modify proxy settings

You can modify proxy settings for the configuration server machine as follows:

1. Log on to the configuration server.
2. Launch the cspconfigtool.exe using the shortcut on your desktop.
3. Click the **Vault Registration** tab.
4. Download a new vault registration file from the portal, and provide it as input to the tool.



5. Provide the new proxy details and click the **Register** button.
6. Open an Admin PowerShell command window.
7. Run the following command:

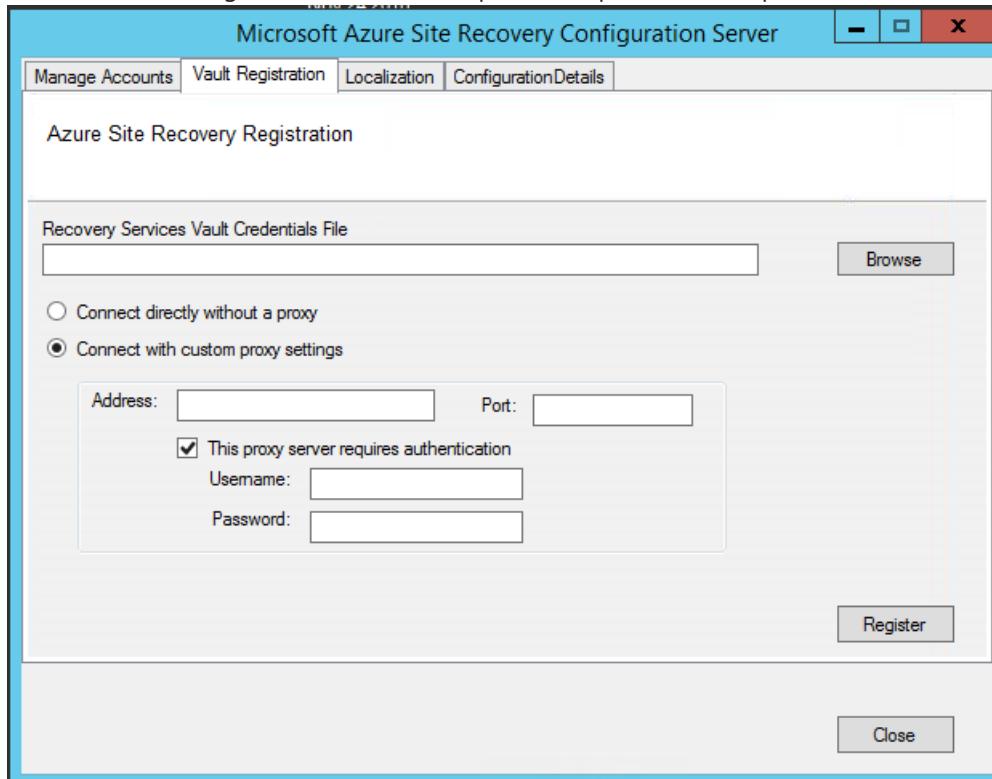
```
$Pwd = ConvertTo-SecureString -String MyProxyUserPassword
Set-OBMachineSetting -ProxyServer http://myproxyserver.domain.com -ProxyPort PortNumber -ProxyUserName
domain\username -ProxyPassword $Pwd
net stop obengine
net start obengine
```

**WARNING**

If you have additional process servers attached to the configuration server, you need to [fix the proxy settings on all the scale-out process servers](#) in your deployment.

## Reregister a configuration server with the same vault

1. Log in to your Configuration Server.
2. Launch the cspconfigtool.exe using the shortcut on your desktop.
3. Click the **Vault Registration** tab.
4. Download a new registration file from the portal and provide it as input to the tool.



5. Provide the Proxy Server details and click the **Register** button.

6. Open an Admin PowerShell command window.

7. Run the following command

```
$Pwd = ConvertTo-SecureString -String MyProxyUserPassword
Set-OBMachineSetting -ProxyServer http://myproxyserver.domain.com -ProxyPort PortNumber -ProxyUserName
domain\username -ProxyPassword $Pwd
net stop obengine
net start obengine
```

**WARNING**

If you have multiple process server, you need to [reregister them](#).

## Register a configuration server with a different vault

### **WARNING**

The following step disassociates the configuration server from the current vault, and the replication of all protected virtual machines under the configuration server is stopped.

1. Log onto the configuration server
2. from an admin command prompt, run the command:

```
reg delete HKLM\Software\Microsoft\Azure Site Recovery\Registration
net stop dra
```

3. Launch the cspconfigtool.exe using the shortcut on your desktop.
4. Click the **Vault Registration** tab.
5. Download a new registration file from the portal and provide it as input to the tool.
6. Provide the Proxy Server details and click the **Register** button.
7. Open an Admin PowerShell command window.
8. Run the following command

```
$pwd = ConvertTo-SecureString -String MyProxyUserPassword
Set-OBMachineSetting -ProxyServer http://myproxyserver.domain.com -ProxyPort PortNumber -ProxyUserName
domain\username -ProxyPassword $pwd
net stop obengine
net start obengine
```

## Upgrade a configuration server

You run update rollups to update the configuration server. Updates can be applied for up to N-4 versions. For example:

- If you're running 9.7, 9.8, 9.9, or 9.10 - you can upgrade directly to 9.11.
- If you're running 9.6 or earlier, and you want to upgrade to 9.11, you must first upgrade to version 9.7 before 9.11.

Links to update rollups for upgrading to all versions of the configuration server are available in the [wiki updates page](#).

Upgrade the server as follows:

1. Download the update installer file to the configuration server.
2. Double-click to run the installer.
3. The installer detects the current version running on the machine.
4. Click **OK** to confirm, and run the upgrade.

## Delete or unregister a configuration server

### WARNING

Ensure the following before you start decommissioning your Configuration Server.

1. [Disable protection](#) for all virtual machines under this Configuration Server.
2. [Disassociate and Delete](#) all Replication policies from the Configuration Server.
3. [Delete](#) all vCenters servers/vSphere hosts that are associated to the Configuration Server.

## Delete the Configuration Server from Azure portal

1. In Azure portal, browse to **Site Recovery Infrastructure > Configuration Servers** from the Vault menu.
2. Click the configuration server that you want to decommission.
3. On the Configuration Server's details page, click the **Delete** button.
4. Click **Yes** to confirm the deletion of the server.

## Uninstall the configuration server and its dependencies

### TIP

If you plan to reuse the Configuration Server with Azure Site Recovery again, then you can skip to step 4 directly

1. Log on to the Configuration Server as an Administrator.
2. Open up Control Panel > Program > Uninstall Programs
3. Uninstall the programs in the following sequence:
  - Microsoft Azure Recovery Services Agent
  - Microsoft Azure Site Recovery Mobility Service/Master Target server
  - Microsoft Azure Site Recovery Provider
  - Microsoft Azure Site Recovery Configuration Server/Process Server
  - Microsoft Azure Site Recovery Configuration Server Dependencies
  - MySQL Server 5.5
4. Run the following command from and admin command prompt.

```
reg delete HKLM\Software\Microsoft\Azure Site Recovery\Registration
```

## Delete or unregister a configuration server (PowerShell)

1. [Install](#) Azure PowerShell module
2. Login into to your Azure account using the command

```
Connect-AzAccount
```

3. Select the subscription under which the vault is present

```
Get-AzSubscription -SubscriptionName <your subscription name> | Select-AzSubscription
```

4. Now set up your vault context

```
$Vault = Get-AzRecoveryServicesVault -Name <name of your vault>
Set-AzSiteRecoveryVaultSettings -ARSVault $Vault
```

5. Get select your configuration server

```
$Fabric = Get-AzSiteRecoveryFabric -FriendlyName <name of your configuration server>
```

## 6. Delete the Configuration Server

```
Remove-AzSiteRecoveryFabric -Fabric $Fabric [-Force]
```

### NOTE

The **-Force** option in the Remove-AzSiteRecoveryFabric can be used to force the removal/deletion of the Configuration server.

## Renew SSL certificates

The configuration server has an inbuilt web server, which orchestrates activities of the Mobility service, process servers, and master target servers connected to it. The web server uses an SSL certificate to authenticate clients. The certificate expires after three years, and can be renewed at any time.

### Check expiry

For configuration server deployments before May 2016, certificate expiry was set to one year. If you have a certificate is going to expire, the following occurs:

- When the expiry date is two months or less, the service starts sending notifications in the portal, and by email (if you subscribed to Azure Site Recovery notifications).
- A notification banner appears on the vault resource page. Click the banner for more details.
- If you see an **Upgrade Now** button, this indicates that there are some components in your environment that haven't been upgraded to 9.4.xxxx.x or higher versions. Upgrade components before you renew the certificate. You can't renew on older versions.

### Renew the certificate

1. In the vault, open **Site Recovery Infrastructure > Configuration Server**, and click the required configuration server.
2. The expiry date appears under **Configuration Server health**
3. Click **Renew Certificates**.

## Common issues

### Installation failures

| SAMPLE ERROR MESSAGE                                                                                                                                                | RECOMMENDED ACTION                              |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------|
| ERROR Failed to load Accounts. Error: System.IO.IOException:<br>Unable to read data from the transport connection when<br>installing and registering the CS server. | Ensure that TLS 1.0 is enabled on the computer. |

### Registration failures

Registration failures can be debugged by reviewing the logs in the **%ProgramData%\ASRLogs** folder.

| SAMPLE ERROR MESSAGE                                                                                                                                                                                                                                                                        | RECOMMENDED ACTION                                                                                                                          |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| <b>09:20:06:</b> InnerException.Type:<br>SrsRestApiClientLib.AcsException,InnerException.<br>Message: ACS50008: SAML token is invalid.<br>Trace ID: 1921ea5b-4723-4be7-8087-a75d3f9e1072<br>Correlation ID: 62fea7e6-2197-4be4-a2c0-71ceb7aa2d97><br>Timestamp: <b>2016-12-12 14:50:08Z</b> | Ensure that the time on your system clock is not more than 15 minutes off the local time. Rerun the installer to complete the registration. |

| SAMPLE ERROR MESSAGE                                                                                                                                                                                                                                                                                                                                                                                                                  | RECOMMENDED ACTION                                                                                                                          |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>09:35:27</b> :DRRegistrationException while trying to get all disaster recovery vault for the selected certificate: : Threw Exception.Type:Microsoft.DisasterRecovery.Registration.DRRegistrationException, Exception.Message: ACS50008: SAML token is invalid.</p> <p>Trace ID: e5ad1af1-2d39-4970-8eef-096e325c9950<br/> Correlation ID: abe9deb8-3e64-464d-8375-36db9816427a<br/> Timestamp: <b>2016-05-19 01:35:39Z</b></p> | Ensure that the time on your system clock is not more than 15 minutes off the local time. Rerun the installer to complete the registration. |
| <p>06:28:45:Failed to create certificate<br/> 06:28:45:Setup cannot proceed. A certificate required to authenticate to Site Recovery cannot be created. Rerun Setup</p>                                                                                                                                                                                                                                                               | Ensure that you're running setup as a local administrator.                                                                                  |

## Next steps

Review the tutorials for setting up disaster recovery of [physical servers](#) to Azure.

# Manage process servers

11/12/2019 • 5 minutes to read • [Edit Online](#)

This article describes common tasks for managing the Site Recovery process server.

The process server is used to receive, optimize, and send replication data to Azure. It also performs a push installation of the Mobility service on VMware VMs and physical servers you want to replicate, and performs automatic discovery of on-premises machines. For replicating on-premises VMware VMs or physical servers to Azure, the process server is installed by default on the configuration server machine.

- For large deployments, you might need additional on-premises process servers to scale capacity.
- For failback from Azure to on-premises, you must set up a temporary process server in Azure. You can delete this VM when failback is done.

Learn more about the process server.

## Upgrade a process server

When you deploy a process server on-premises, or as an Azure VM for failback, the latest version of the process server is installed. The Site Recovery teams release fixes and enhancements on a regular basis, and we recommend you keep process servers up-to-date. You can upgrade a process server as follows:

1. Sign in to the process server as an administrator.
2. Download the latest version of the [Unified Setup Installer](#).
3. Double-click the installer to launch the update process.
4. The installer detects the Site Recovery components that are installed, and upgrades them to the latest version.

## Move VMs to balance the process server load

Balance the load by moving VMs between two process servers, as follows:

1. In the vault, under **Manage** click **Site Recovery Infrastructure**. Under **For VMware & Physical machines**, click **Configuration Servers**.
2. Click on the configuration server with which the process servers are registered.
3. Click on the process server for which you want to load balance traffic.

**Win5**  
Process Server

Load balance   Switch   Error Details

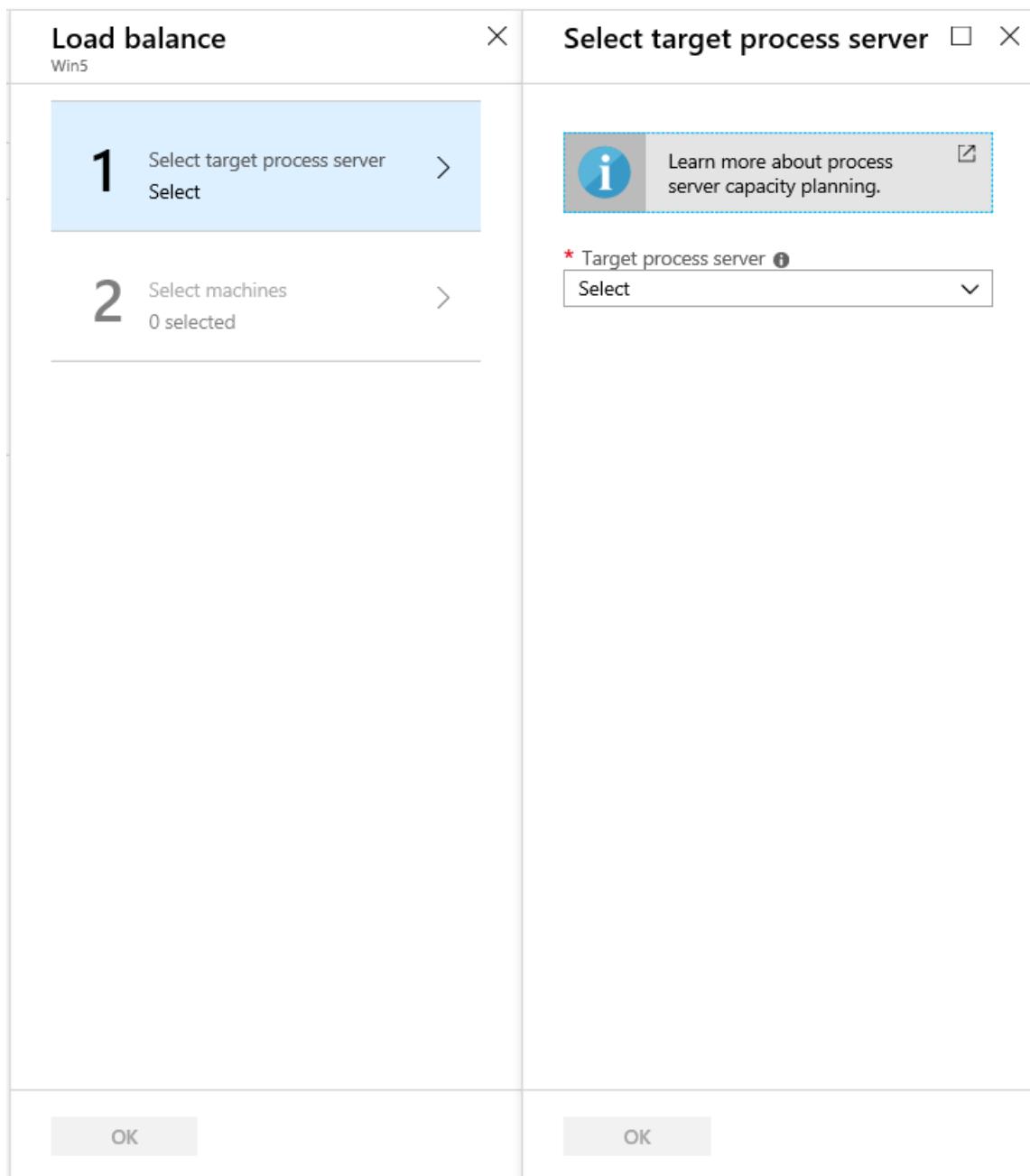
**Essentials ^**

|                         |                 |
|-------------------------|-----------------|
| Recovery Services vault | Server ID       |
|                         |                 |
| FQDN                    | IP address      |
| Win5                    |                 |
| Process Server version  | Protected items |
| 9.19.1.0                | 0               |
| Last heartbeat at       |                 |
| 11/16/2018 3:40:05 PM   |                 |

**Process Server health**

|                                |                       |
|--------------------------------|-----------------------|
| <b>Processor queue</b>         | 0                     |
| <b>CPU utilization</b>         | 14% used              |
| <b>Memory usage</b>            | UnKnown               |
| <b>Free space</b>              | 79.77%                |
| <b>Process server services</b> | Running               |
| <b>Certificate Expires On</b>  | 10/31/2021 6:33:02 AM |

4. Click **Load balance**, select the target process server to which you want to move machines. Then click **OK**



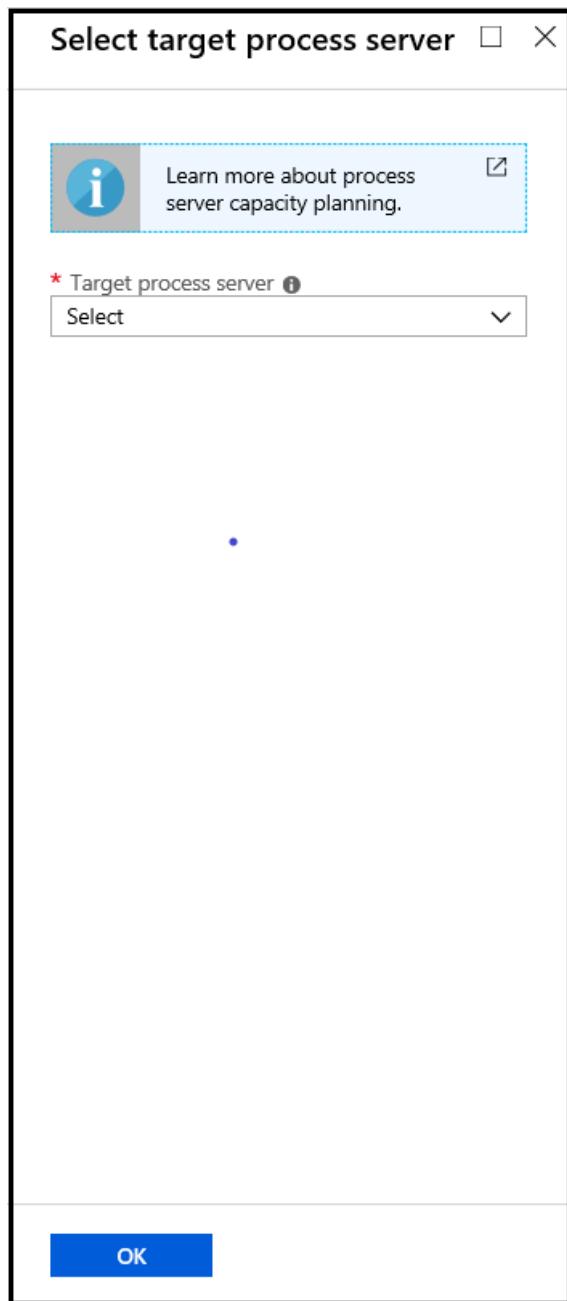
5. Click **Select machines**, and choose the machines you want to move from the current to the target process server. Details of average data change are displayed against each virtual machine. Then click **OK**.
6. In the vault, monitor the progress of the job under **Monitoring > Site Recovery jobs**.

It will take around 15 minutes for changes to be reflected in the portal. For a quicker effect, [refresh the configuration server](#).

## Switch an entire workload to another process server

Move the entire workload handled by a process server to a different process server, as follows:

1. In the vault, under **Manage** click **Site Recovery Infrastructure**. Under **For VMware & Physical machines**, click **Configuration Servers**.
2. Click on the configuration server with which the process servers are registered.
3. Click on the process server from which you want to switch the workload.
4. Click on **Switch**, select the target process server to which you want to move the workload. Then click **OK**



5. In the vault, monitor the progress of the job under **Monitoring > Site Recovery jobs**.

It will take around 15 minutes for changes to be reflected in the portal. For a quicker effect, [refresh the configuration server](#).

## Register a master target server

Master target server resides on configuration server and scale-out process servers. It must be registered with configuration server. In case there is a failure in this registration, it can impact the health of protected items. To register master target server with configuration server, login to the specific configuration server/scale-out process server on which the registration is required. Navigate to folder **%PROGRAMDATA%\ASR\Agent**, and run the following on administrator command prompt.

```
cmd
cdpcli.exe --registermt

net stop obengine

net start obengine

exit
```

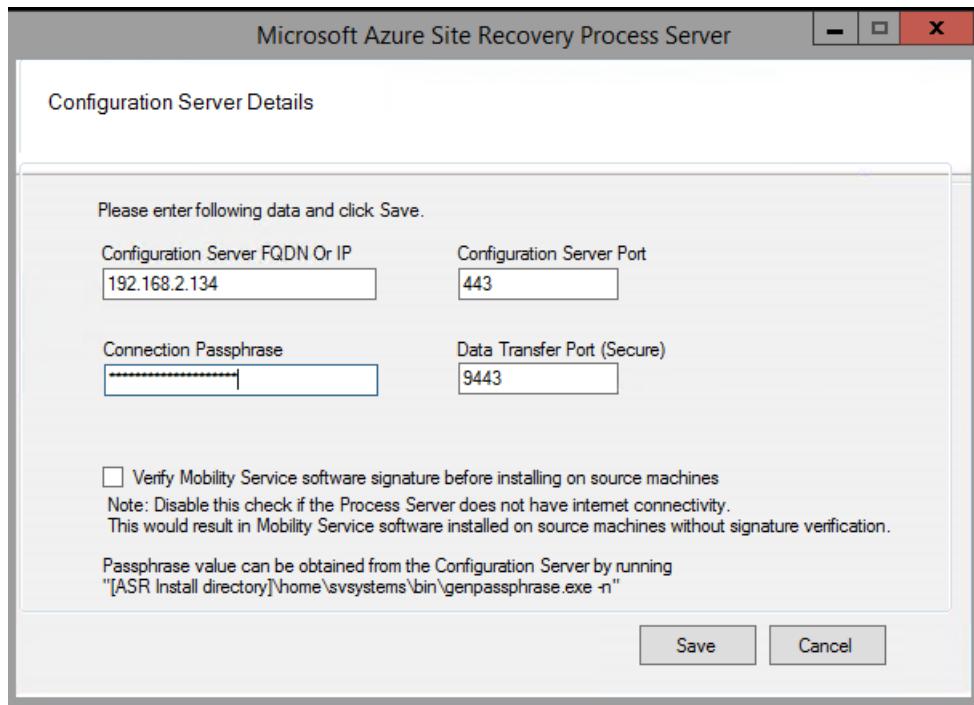
## Reregister a process server

Reregister a process server running on-premises or on an Azure VM with the configuration server as follows:

1. Establish a Remote Desktop Connection to the machine running the process server.
2. Run cspconfigtool.exe to start the Azure Site Recovery Process Server configuration tool.
  - The tool is launched automatically the first time you sign into the process server.
  - If it doesn't open automatically, click its shortcut on the desktop.
3. In **Configuration server FQDN or IP**, specify the name or IP address of the configuration server with which to register the process server.
4. In **Configuration Server Port**, ensure that 443 is specified. This is the port on which the configuration server listens for requests.
5. In **Connection Passphrase**, specify the passphrase that you specified when you set up the configuration server. To find the passphrase:
  - On the configuration server, navigate to the Site Recovery installation folder \*\*\home\svsystems\bin\*\*:

```
cd %ProgramData%\ASR\home\svsystems\bin
```
  - Run the below command to print out the current passphrase:

```
genpassphrase.exe -n
```
6. In **Data Transfer Port**, leave the default value unless you've specified a custom port.
7. Click **Save** save the settings, and register the process server.



After you've saved the settings, do the following:

1. On the process server, open an administrator command prompt.
2. Browse to folder **%PROGRAMDATA%\ASR\Agent**, and run the command:

```
cdpcli.exe --registermt
net stop obengine
net start obengine
```

## Modify proxy settings for an on-premises process server

If an on-premises process server uses a proxy to connect to Azure, you can modify the proxy settings as follows:

1. Sign into the process server machine.
2. Open an Admin PowerShell command window, and run the following command:

```
$pwd = ConvertTo-SecureString -String MyProxyUserPassword
Set-OBMachineSetting -ProxyServer http://myproxyserver.domain.com -ProxyPort PortNumber -ProxyUserName
domain\username -ProxyPassword $pwd
net stop obengine
net start obengine
```

3. Browse to folder **%PROGRAMDATA%\ASR\Agent**, and run this command:

```
cmd
cdpcli.exe --registermt

net stop obengine

net start obengine

exit
```

## Remove a process server

Follow the steps for your specific circumstances.

### Unregister a connected process server

1. Establish a remote connection to the process server as an Administrator.
2. In the **Control Panel**, open **Programs > Uninstall a program**.
3. Uninstall the program **Microsoft Azure Site Recovery Mobility Service/Master Target Server**.
4. Uninstall the program **Microsoft Azure Site Recovery Configuration/Process Server**.
5. After the programs in steps 3 and 4 are uninstalled, uninstall **Microsoft Azure Site Recovery Configuration/Process Server Dependencies**.

### Unregister a disconnected process server

Only use these steps if there's no way to revive the machine on which the process server is installed.

1. Sign in the configuration server as an Administrator.
2. Open an Administrative command prompt, and browse to `%ProgramData%\ASR\home\svsystems\bin`.
3. Run this command to get a list of one or more process servers.

```
perl Unregister-ASRComponent.pl -IPAddress <IP_of_Process_Server> -Component PS
```

- S. No: the process server serial number.
- IP/Name: The IP address and name of the machine running the process server.
- Heartbeat: Last heartbeat from the process server machine.

```
=====
S.No IP Name Heartbeat
=====
1 [REDACTED] testVM 2018-08-02 11:54:38
=====
```

Please choose one of the above servers to un-register

4. Specify the serial number of the process server you want to unregister.
5. Unregistering a process server remove all of its details from the system, and displays the message:  
**Successfully unregistered server-name> (server-IP-address)**

### Exclude folders from anti-virus software

If anti-virus software is running on a scale-out process server (or master target server), exclude the following folders from anti-virus operations:

- C:\Program Files\Microsoft Azure Recovery Services Agent
- C:\ProgramData\ASR
- C:\ProgramData\ASRLogs
- C:\ProgramData\ASRSetupLogs
- C:\ProgramData\LogUploadServiceLogs
- C:\ProgramData\Microsoft Azure Site Recovery
- Process server installation directory. For example: C:\Program Files (x86)\Microsoft Azure Site Recovery

# Remove servers and disable protection

7/14/2019 • 8 minutes to read • [Edit Online](#)

This article describes how to unregister servers from a Recovery Services vault, and how to disable protection for machines protected by Site Recovery.

## Unregister a configuration server

If you replicate VMware VMs or Windows/Linux physical servers to Azure, you can unregister an unconnected configuration server from a vault as follows:

1. [Disable protection of virtual machines](#).
2. [Disassociate or delete replication policies](#).
3. [Delete the configuration server](#)

## Unregister a VMM server

1. Stop replicating virtual machines in clouds on the VMM server you want to remove.
2. Delete any network mappings used by clouds on the VMM server that you want to delete. In **Site Recovery Infrastructure > For System Center VMM > Network Mapping**, right-click the network mapping > **Delete**.
3. Note the ID of the VMM server.
4. Disassociate replication policies from clouds on the VMM server you want to remove. In **Site Recovery Infrastructure > For System Center VMM > Replication Policies**, double-click the associated policy. Right-click the cloud > **Disassociate**.
5. Delete the VMM server or active node. In **Site Recovery Infrastructure > For System Center VMM > VMM Servers**, right-click the server > **Delete**.
6. If your VMM server was in a Disconnected state, then download and run the [cleanup script](#) on the VMM server. Open PowerShell with the **Run as Administrator** option, to change the execution policy for the default (LocalMachine) scope. In the script, specify the ID of the VMM server you want to remove. The script removes registration and cloud pairing information from the server.
7. Run the cleanup script on any secondary VMM server.
8. Run the cleanup script on any other passive VMM cluster nodes that have the Provider installed.
9. Uninstall the Provider manually on the VMM server. If you have a cluster, remove from all nodes.
10. If your virtual machines were replicating to Azure, you need to uninstall the Microsoft Recovery Services agent from Hyper-V hosts in the deleted clouds.

## Unregister a Hyper-V host in a Hyper-V Site

Hyper-V hosts that aren't managed by VMM are gathered into a Hyper-V site. Remove a host in a Hyper-V site as follows:

1. Disable replication for Hyper-V VMs located on the host.
2. Disassociate policies for the Hyper-V site. In **Site Recovery Infrastructure > For Hyper-V Sites > Replication Policies**, double-click the associated policy. Right-click the site > **Disassociate**.
3. Delete Hyper-V hosts. In **Site Recovery Infrastructure > For Hyper-V Sites > Hyper-V Hosts**, right-click the server > **Delete**.
4. Delete the Hyper-V site after all hosts have been removed from it. In **Site Recovery Infrastructure > For Hyper-V Sites > Hyper-V Sites**, right-click the site > **Delete**.

5. If your Hyper-V host was in a **Disconnected** state, then run the following script on each Hyper-V host that you removed. The script cleans up settings on the server, and unregisters it from the vault.

```

pushd .
try
{
 $windowsIdentity=[System.Security.Principal.WindowsIdentity]::GetCurrent()
 $principal=new-object System.Security.Principal.WindowsPrincipal($windowsIdentity)
 $administrators=[System.Security.Principal.WindowsBuiltInRole]::Administrator
 $isAdmin=$principal.IsInRole($administrators)
 if (!$isAdmin)
 {
 "Please run the script as an administrator in elevated mode."
 $choice = Read-Host
 return;
 }

 $error.Clear()
 "This script will remove the old Azure Site Recovery Provider related properties. Do you want to
continue (Y/N) ?"
 $choice = Read-Host

 if (!($choice -eq 'Y' -or $choice -eq 'y'))
 {
 "Stopping cleanup."
 return;
 }

 $serviceName = "dra"
 $service = Get-Service -Name $serviceName
 if ($service.Status -eq "Running")
 {
 "Stopping the Azure Site Recovery service..."
 net stop $serviceName
 }

 $asrHivePath = "HKLM:\SOFTWARE\Microsoft\Azure Site Recovery"
 $registrationPath = $asrHivePath + '\Registration'
 $proxySettingsPath = $asrHivePath + '\ProxySettings'
 $draIdvalue = 'DraID'
 $idMgmtCloudContainerId='IdMgmtCloudContainerId'

 if (Test-Path $asrHivePath)
 {
 if (Test-Path $registrationPath)
 {
 "Removing registration related registry keys."
 Remove-Item -Recurse -Path $registrationPath
 }

 if (Test-Path $proxySettingsPath)
 {
 "Removing proxy settings"
 Remove-Item -Recurse -Path $proxySettingsPath
 }

 $regNode = Get-ItemProperty -Path $asrHivePath
 if($regNode.DraID -ne $null)
 {
 "Removing DraId"
 Remove-ItemProperty -Path $asrHivePath -Name $draIdValue
 }
 if($regNode.IdMgmtCloudContainerId -ne $null)
 {
 "Removing IdMgmtCloudContainerId"
 Remove-ItemProperty -Path $asrHivePath -Name $idMgmtCloudContainerId
 }
 }
}

```

```

 }
 "Registry keys removed."
 }

 # First retrieve all the certificates to be deleted
 $ASRcerts = Get-ChildItem -Path cert:\localmachine\my | where-object
 {$_.friendlyname.startswith('ASR_SRSAUTH_CERT_KEY_CONTAINER') -or
 $_.friendlyname.startswith('ASR_HYPER_V_HOST_CERT_KEY_CONTAINER')}
 # Open a cert store object
 $store = New-Object System.Security.Cryptography.X509Certificates.X509Store("My", "LocalMachine")
 $store.Open('ReadWrite')
 # Delete the certs
 "Removing all related certificates"
 foreach ($cert in $ASRcerts)
 {
 $store.Remove($cert)
 }
}catch
{
 [system.exception]
 Write-Host "Error occurred" -ForegroundColor "Red"
 $error[0]
 Write-Host "FAILED" -ForegroundColor "Red"
}
popd

```

## Disable protection for a VMware VM or physical server (VMware to Azure)

1. In **Protected Items > Replicated Items**, right-click the machine > **Disable replication**.
2. In **Disable replication** page, select one of these options:
  - **Disable replication and remove (recommended)** - This option removes the replicated item from Azure Site Recovery and the replication for the machine is stopped. Replication configuration on Configuration Server is cleaned up and Site Recovery billing for this protected server is stopped. Note that this option can only be used when Configuration Server is in connected state.
  - **Remove** - This option is supposed to be used only if the source environment is deleted or not accessible (not connected). This removes the replicated item from Azure Site Recovery (billing is stopped). Replication configuration on the Configuration Server **will not** be cleaned up.

### NOTE

In both the options mobility service will not be uninstalled from the protected servers, you need to uninstall it manually. If you plan to protect the server again using the same Configuration server, you can skip uninstalling the mobility service.

### NOTE

If you have already failed over a VM and it is running in Azure, note that disable protection doesn't remove / affect the failed over VM.

## Disable protection for a Azure VM (Azure to Azure)

- In **Protected Items > Replicated Items**, right-click the machine > **Disable replication**.

**NOTE**

mobility service will not be uninstalled from the protected servers, you need to uninstall it manually. If you plan to protect the server again, you can skip uninstalling the mobility service.

## Disable protection for a Hyper-V virtual machine (Hyper-V to Azure)

**NOTE**

Use this procedure if you're replicating Hyper-V VMs to Azure without a VMM server. If you are replicating your virtual machines using the **System Center VMM to Azure** scenario, then follow the instructions Disable protection for a Hyper-V virtual machine replicating using the System Center VMM to Azure scenario

1. In **Protected Items > Replicated Items**, right-click the machine > **Disable replication**.

2. In **Disable replication**, you can select the following options:

- **Disable replication and remove (recommended)** - This option removes the replicated item from Azure Site Recovery and the replication for the machine is stopped. Replication configuration on the on-premises virtual machine will be cleaned up and Site Recovery billing for this protected server is stopped.
- **Remove** - This option is supposed to be used only if the source environment is deleted or not accessible (not connected). This removes the replicated item from Azure Site Recovery (billing is stopped). Replication configuration on the on-premises virtual machine **will not** be cleaned up.

**NOTE**

> If you chose the \*\*Remove\*\* option then run the following set of scripts to clean up the replication settings on-premises Hyper-V Server.

**NOTE**

If you have already failed over a VM and it is running in Azure, note that disable protection doesn't remove / affect the failed over VM.

1. On the source Hyper-V host server, to remove replication for the virtual machine. Replace SQLVM1 with the name of your virtual machine and run the script from an administrative PowerShell

```
$vmName = "SQLVM1"
$vm = Get-WmiObject -Namespace "root\virtualization\v2" -Query "Select * From MsVm_ComputerSystem Where ElementName = '$vmName'"
$replicationService = Get-WmiObject -Namespace "root\virtualization\v2" -Query "Select * From MsVm_ReplicationService"
$replicationService.RemoveReplicationRelationship($vm.__PATH)
```

## Disable protection for a Hyper-V virtual machine replicating to Azure using the System Center VMM to Azure scenario

1. In **Protected Items > Replicated Items**, right-click the machine > **Disable replication**.

2. In **Disable replication**, select one of these options:

- **Disable replication and remove (recommended)** - This option remove the replicated item from Azure Site Recovery and the replication for the machine is stopped. Replication configuration on the on-premises virtual machine is cleaned up and Site Recovery billing for this protected server is stopped.
- **Remove** - This option is supposed to be used only if the source environment is deleted or not accessible (not connected). This removes the replicated item from Azure Site Recovery (billing is stopped). Replication configuration on the on-premises virtual machine **will not** be cleaned up.

**NOTE**

If you chose the **Remove** option, then run the following scripts to clean up the replication settings on-premises VMM Server.

3. Run this script on the source VMM server, using PowerShell (administrator privileges required) from the VMM console. Replace the placeholder **SQLVM1** with the name of your virtual machine.

```
$vm = get-scvirtualmachine -Name "SQLVM1"
Set-SCVirtualMachine -VM $vm -ClearDRProtection
```

4. The above steps clear the replication settings on the VMM server. To stop replication for the virtual machine running on the Hyper-V host server, run this script. Replace SQLVM1 with the name of your virtual machine, and host01.contoso.com with the name of the Hyper-V host server.

```
$vmName = "SQLVM1"
$hostName = "host01.contoso.com"
$vm = Get-WmiObject -Namespace "root\virtualization\v2" -Query "Select * From MsVm_ComputerSystem Where ElementName = '$vmName'" -computername $hostName
$replicationService = Get-WmiObject -Namespace "root\virtualization\v2" -Query "Select * From MsVm_ReplicationService" -computername $hostName
$replicationService.RemoveReplicationRelationship($vm.__PATH)
```

## Disable protection for a Hyper-V virtual machine replicating to secondary VMM Server using the System Center VMM to VMM scenario

1. In **Protected Items > Replicated Items**, right-click the machine > **Disable replication**.
2. In **Disable replication**, select one of these options:
  - **Disable replication and remove (recommended)** - This option remove the replicated item from Azure Site Recovery and the replication for the machine is stopped. Replication configuration on the on-premises virtual machine is cleaned up and Site Recovery billing for this protected server is stopped.
  - **Remove** - This option is supposed to be used only if the source environment is deleted or not accessible (not connected). This removes the replicated item from Azure Site Recovery (billing is stopped). Replication configuration on the on-premises virtual machine **will not** be cleaned up. Run the following set of scripts to clean up the replication settings on-premises virtual machines.

**NOTE**

If you chose the **Remove** option, then run the following scripts to clean up the replication settings on-premises VMM Server.

3. Run this script on the source VMM server, using PowerShell (administrator privileges required) from the VMM console. Replace the placeholder **SQLVM1** with the name of your virtual machine.

```
$vm = get-scvirtualmachine -Name "SQLVM1"
Set-SCVirtualMachine -VM $vm -ClearDRProtection
```

4. On the secondary VMM server, run this script to clean up the settings for the secondary virtual machine:

```
$vm = get-scvirtualmachine -Name "SQLVM1"
Remove-SCVirtualMachine -VM $vm -Force
```

5. On the secondary VMM server, refresh the virtual machines on the Hyper-V host server, so that the secondary VM gets detected again in the VMM console.
6. The above steps clear up the replication settings on the VMM server. If you want to stop replication for the virtual machine, run the following script on the primary and secondary VMs. Replace SQLVM1 with the name of your virtual machine.

```
Remove-VMReplication -VMName "SQLVM1"
```

# Service updates in Site Recovery

9/11/2019 • 4 minutes to read • [Edit Online](#)

This article provides an overview of [Azure Site Recovery](#) updates, and describes how to upgrade Site Recovery components.

Site Recovery publishes service updates on a regular basis. Updates include new features, support improvements, component updates, and bug fixes. In order to take advantage of the latest features and fixes, we recommend running the latest versions of Site Recovery components.

## Updates support

### Support statement for Azure Site Recovery

We recommend always upgrading to the latest component versions:

**With every new version 'N' of an Azure Site Recovery component that's released, all versions below 'N-4' are considered to be out of support.**

#### IMPORTANT

Official support is for upgrading from > N-4 version to N version. For example, if you're running you are on N-6, you need to first upgrade to N-4, and then upgrade to N.

### Links to currently supported update rollups

Review the latest update rollup (version N) in [this article](#). Remember that Site Recovery provides support for N-4 versions.

## Component expiry

Site Recovery notifies you of expired components (or nearing expiry) by email (if you subscribed to email notifications), or on the vault dashboard in the portal.

- In addition, when updates are available, in the infrastructure view for your scenario in the portal, an **Update available** button appears next to the component. This button redirects you to a link for downloading the latest component version.
- Vaults dashboard notifications aren't available if you're replicating Hyper-V VMs.

Emails notifications are sent as follows.

| TIME                            | FREQUENCY      |
|---------------------------------|----------------|
| 60 days before component expiry | Once bi-weekly |
| Next 53 days                    | Once a week    |
| Last 7 days                     | Once a day     |
| After expiry                    | Once bi-weekly |

### Upgrading outside official support

If the difference between your component version and the latest release version is greater than four, this is considered out of support. In this case, upgrade as follows:

1. Upgrade the currently installed component to your current version plus four. For example, if your version is 9.16, then upgrade to 9.20.
2. Then, upgrade to the next compatible version. So in our example, after upgrading 9.16 to 9.20, upgrade to 9.24.

Follow the same process for all relevant components.

## Support for latest operating systems/kernels

### NOTE

If you have a maintenance window scheduled, and a reboot is included in it, we recommend that you first upgrade Site Recovery components, and then proceed with the rest of the scheduled activities in the maintenance window.

1. Before upgrading operating system/kernel versions, verify if the target version is supported Site Recovery.
  - Azure VM support.
  - VMware/physical server support
  - Hyper-V support.
2. Review [available updates](#) to find out what you want to upgrade.
3. Upgrade to the latest Site Recovery version.
4. Upgrade the operating system/kernel to the required versions.
5. Reboot.

This process ensures that the machine operating system/kernel is upgraded to the latest version, and that the latest Site Recovery changes needed to support the new version are loaded on to the machine.

## Azure VM disaster recovery to Azure

In this scenario, we strongly recommend that you [enable automatic updates](#). You can allow Site Recovery to manage updates as follows:

- During the enable replication process.
- By setting the extension update settings inside the vault.

If you want to manually manage updates, do the following:

1. In the vault > **Replicated Items**, click this notification at the top of the screen:  
**New Site Recovery replication agent update is available. Click to install ->**
2. Select the VMs for which you want to apply the update, and then click **OK**.

## VMware VM/physical server disaster recovery to Azure

1. Based on your current version and the [support statement](#), install the update first on the on-premises configuration server, using [these instructions](#).
2. If you have scale-out process servers, update them next, using [these instructions](#).
3. To update the Mobility agent on each protected machine, refer to [this article](#).

### Reboot after Mobility service upgrade

A reboot is recommended after every upgrade of the Mobility service, to ensure that all the latest changes are

loaded on the source machine.

A reboot isn't mandatory, unless the difference between the agent version during last reboot, and the current version, is greater than four.

The example in the table shows how this works.

| AGENT VERSION (LAST REBOOT) | UPGRADE TO | MANDATORY REBOOT?                                                        |
|-----------------------------|------------|--------------------------------------------------------------------------|
| 9.16                        | 9.18       | Not mandatory                                                            |
| 9.16                        | 9.19       | Not mandatory                                                            |
| 9.16                        | 9.20       | Not mandatory                                                            |
| 9.16                        | 9.21       | Mandatory.<br><br>Upgrade to 9.20, then reboot before upgrading to 9.21. |

## Hyper-V VM disaster recovery to Azure

### Between a Hyper-V site and Azure

1. Download the update for the Microsoft Azure Site Recovery Provider.
2. Install the Provider on each Hyper-V server registered in Site Recovery. If you're running a cluster, upgrade on all cluster nodes.

### Between an on-premises VMM site and Azure

1. Download the update for the Microsoft Azure Site Recovery Provider.
2. Install the Provider on the VMM server. If VMM is deployed in a cluster, install the Provider on all cluster nodes.
3. Install the latest Microsoft Azure Recovery Services agent on all Hyper-V hosts or cluster nodes.

### Between two on-premises VMM sites

1. Download the latest update for the Microsoft Azure Site Recovery Provider.
2. Install the latest Provider on the VMM server managing the secondary recovery site. If VMM is deployed in a cluster, install the Provider on all cluster nodes.
3. After the recovery site is updated, install the Provider on the VMM server that's managing the primary site.

## Next steps

Follow our [Azure Updates](#) page to track new updates and releases.

# Delete a Site Recovery Services vault

1/10/2020 • 2 minutes to read • [Edit Online](#)

This article describes how to delete a Recovery Services vault for Site Recovery. To delete a vault used in Azure Backup, see [Delete a Backup vault in Azure](#).

## NOTE

This article has been updated to use the new Azure PowerShell Az module. You can still use the AzureRM module, which will continue to receive bug fixes until at least December 2020. To learn more about the new Az module and AzureRM compatibility, see [Introducing the new Azure PowerShell Az module](#). For Az module installation instructions, see [Install Azure PowerShell](#).

## Before you start

Before you can delete a vault you must remove registered servers, and items in the vault. What you need to remove depends on the replication scenarios you've deployed.

## Delete a vault-Azure VM to Azure

1. Follow [these instructions](#) to delete all protected VMs.
2. Then, delete the vault.

## Delete a vault-VMware VM to Azure

1. Follow [these instructions](#) to delete all protected VMs.
2. Follow [these steps](#) to delete all replication policies.
3. Delete references to vCenter using [these steps](#).
4. Follow [these instructions](#) to decommission a configuration server.
5. Then, delete the vault.

## Delete a vault-Hyper-V VM (with VMM) to Azure

1. Follow [these steps](#) to delete Hyper-V VMs managed by System Center VMM.
2. Disassociate and delete all replication policies. Do this in your vault > **Site Recovery Infrastructure > For System Center VMM > Replication Policies**.
3. Follow [these steps](#) to unregister a connected VMM server.
4. Then, delete the vault.

## Delete a vault-Hyper-V VM to Azure

1. Follow [these steps](#) to delete all protected VMs.
2. Disassociate and delete all replication policies. Do this in your vault > **Site Recovery Infrastructure > For Hyper-V Sites > Replication Policies**.
3. Follow [these instructions](#) to unregister a Hyper-V host.
4. Delete the Hyper-V site.
5. Then, delete the vault.

## Use PowerShell to force delete the vault

### IMPORTANT

If you're testing the product and aren't concerned about data loss, use the force delete method to rapidly remove the vault and all its dependencies. The PowerShell command deletes all the contents of the vault and is **not reversible**.

To delete the Site Recovery vault even if there are protected items, use these commands:

```
Connect-AzAccount

Select-AzSubscription -SubscriptionName "XXXXX"

$vault = Get-AzRecoveryServicesVault -Name "vaultname"

Remove-AzRecoveryServicesVault -Vault $vault
```

Learn more about [Get-AzRecoveryServicesVault](#), and [Remove-AzRecoveryServicesVault](#).

# Replicate Azure Stack VMs to Azure

12/18/2019 • 20 minutes to read • [Edit Online](#)

This article shows you how to set up disaster recovery Azure Stack VMs to Azure, using the [Azure Site Recovery service](#).

Site Recovery contributes to your business continuity and disaster recovery (BCDR) strategy. The service ensures that your VM workloads remain available when expected and unexpected outages occur.

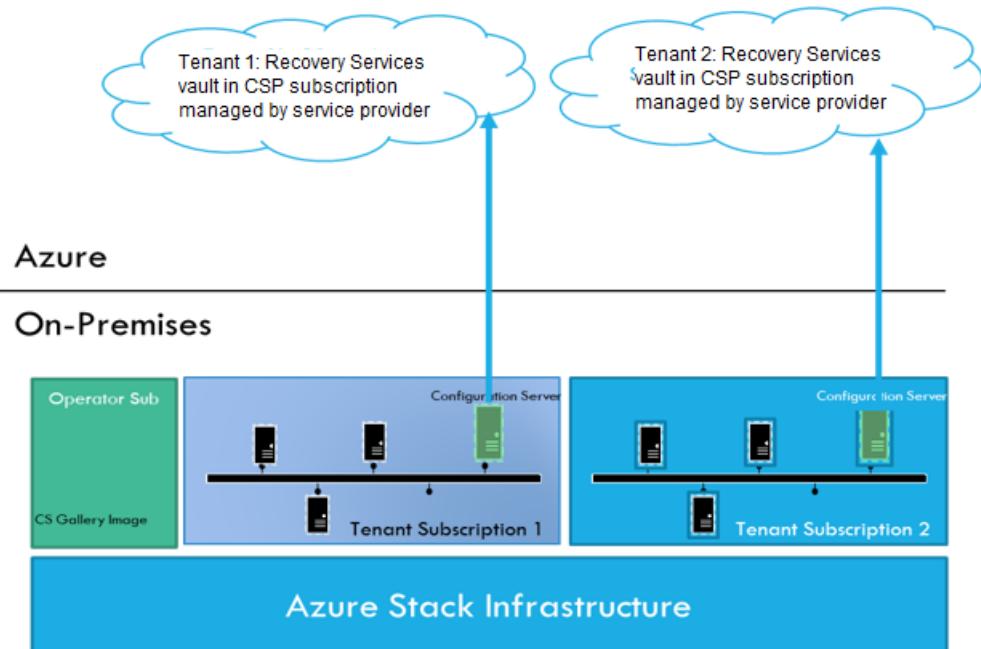
- Site Recovery orchestrates and manages replication of VMs to Azure storage.
- When an outage occurs in your primary site, you use Site Recovery to fail over to Azure.
- On failover, Azure VMs are created from the stored VM data, and users can continue accessing workloads running on those Azure VMs.
- When everything's up and running again, you can fail back Azure VMs to your primary site, and start replicating to Azure storage again.

In this article, you learn how to:

- **Step 1: Prepare Azure stack VMs for replication.** Check that VMs comply with Site Recovery requirements, and prepare for installation of the Site Recovery Mobility service. This service is installed on each VM you want to replicate.
- **Step 2: Set up a Recovery Services vault.** Set up a vault for Site Recovery, and specify what you want to replicate. Site Recovery components and actions are configured and managed in the vault.
- **Step 3: Set up the source replication environment.** Set up a Site Recovery configuration server. The configuration server is a single Azure Stack VM that runs all the components needed by Site Recovery. After you've set up the configuration server, you register it in the vault.
- **Step 4: Set up the target replication environment.** Select your Azure account, and the Azure storage account and network that you want to use. During replication, VM data is copied to Azure storage. After failover, Azure VMs are joined to the specified network.
- **Step 5: Enable replication.** Configure replication settings, and enable replication for VMs. The Mobility service will be installed on a VM when replication is enabled. Site Recovery performs an initial replication of the VM, and then ongoing replication begins.
- **Step 6: Run a disaster recovery drill:** After replication is up and running, you verify that failover will work as expected by running a drill. To initiate the drill, you run a test failover in Site Recovery. The test failover doesn't impact your production environment.

With these steps complete, you can then run a full failover to Azure as and when you need to.

## Architecture



| LOCATION                    | COMPONENT                                                                              | DETAILS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------------------------|----------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Configuration server</b> | Runs on a single Azure Stack VM.                                                       | <p>In each subscription you set up a configuration server VM. This VM runs the following Site Recovery components:</p> <ul style="list-style-type: none"> <li>- Configuration server: Coordinates communications between on-premises and Azure, and manages data replication.</li> <li>- Process server: Acts as a replication gateway. It receives replication data, optimizes with caching, compression, and encryption; and sends it to Azure storage.</li> </ul> <p>If VMs you want to replicate exceed the limits stated below, you can set up a separate standalone process server. <a href="#">Learn more</a>.</p> |
| <b>Mobility service</b>     | Installed on each VM you want to replicate.                                            | <p>In the steps in this article, we prepare an account so that the Mobility service is installed automatically on a VM when replication is enabled. If you don't want to install the service automatically, there are a number of other methods you can use. <a href="#">Learn more</a>.</p>                                                                                                                                                                                                                                                                                                                              |
| <b>Azure</b>                | In Azure you need a Recovery Services vault, a storage account, and a virtual network. | Replicated data is stored in the storage account. Azure VMs are added to the Azure network when failover occurs.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

Replication works as follows:

1. In the vault, you specify the replication source and target, set up the configuration server, create a replication policy, and enable replication.
2. The Mobility service is installed on the machine (if you've used push installation), and machines begin replication in accordance with the replication policy.

3. An initial copy of the server data is replicated to Azure storage.
4. After initial replication finishes, replication of delta changes to Azure begins. Tracked changes for a machine are held in a .hrl file.
5. The configuration server orchestrates replication management with Azure (port HTTPS 443 outbound).
6. The process server receives data from source machines, optimizes and encrypts it, and sends it to Azure storage (port 443 outbound).
7. Replicated machines communicate with the configuration server (port HTTPS 443 inbound, for replication management. Machines send replication data to the process server (port HTTPS 9443 inbound - can be modified).
8. Traffic is replicated to Azure storage public endpoints, over the internet. Alternately, you can use Azure ExpressRoute public peering. Replicating traffic over a site-to-site VPN from an on-premises site to Azure isn't supported.

## Prerequisites

Here's what you need to set up this scenario.

| REQUIREMENT                       | DETAILS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Azure subscription account</b> | If you don't have an Azure subscription, create a <a href="#">free account</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Azure account permissions</b>  | <p>The Azure account you use needs permissions to:</p> <ul style="list-style-type: none"> <li>- Create a Recovery Service vault</li> <li>- Create a virtual machine in the resource group and virtual network you use for the scenario</li> <li>- Write to the storage account you specify</li> </ul> <p>Note that:</p> <ul style="list-style-type: none"> <li>- If you create an account, you're the administrator of your subscription and can perform all actions.</li> <li>- If you use an existing subscription and you're not the administrator, you need to work with the admin to assign you Owner or Contributor permissions.</li> <li>- If you need more granular permissions, review <a href="#">this article</a>.</li> </ul> |
| <b>Azure Stack VM</b>             | You need an Azure Stack VM in the tenant subscription, that will be deployed as the Site Recovery configuration server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

### Prerequisites for the configuration server

#### Configuration/Process server requirements for physical server replication

| COMPONENT                | REQUIREMENT |
|--------------------------|-------------|
| <b>HARDWARE SETTINGS</b> |             |
| CPU cores                | 8           |
| RAM                      | 16 GB       |

| COMPONENT                              | REQUIREMENT                                                                                                                                                                                                                                                                                                                                      |
|----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Number of disks                        | 3, including the OS disk, process server cache disk, and retention drive for failback                                                                                                                                                                                                                                                            |
| Free disk space (process server cache) | 600 GB                                                                                                                                                                                                                                                                                                                                           |
| Free disk space (retention disk)       | 600 GB                                                                                                                                                                                                                                                                                                                                           |
| <b>SOFTWARE SETTINGS</b>               |                                                                                                                                                                                                                                                                                                                                                  |
| Operating system                       | Windows Server 2012 R2<br>Windows Server 2016                                                                                                                                                                                                                                                                                                    |
| Operating system locale                | English (en-us)                                                                                                                                                                                                                                                                                                                                  |
| Windows Server roles                   | Don't enable these roles:<br>- Active Directory Domain Services<br>- Internet Information Services<br>- Hyper-V                                                                                                                                                                                                                                  |
| Group policies                         | Don't enable these group policies:<br>- Prevent access to the command prompt.<br>- Prevent access to registry editing tools.<br>- Trust logic for file attachments.<br>- Turn on Script Execution.<br><a href="#">Learn more</a>                                                                                                                 |
| IIS                                    | - No preexisting default website<br>- No preexisting website/application listening on port 443<br>- Enable <a href="#">anonymous authentication</a><br>- Enable <a href="#">FastCGI</a> setting.                                                                                                                                                 |
| IP address type                        | Static                                                                                                                                                                                                                                                                                                                                           |
| <b>ACCESS SETTINGS</b>                 |                                                                                                                                                                                                                                                                                                                                                  |
| MYSQL                                  | MySQL should be installed on the configuration server. You can install manually, or Site Recovery can install it during deployment. For Site Recovery to install, check that the machine can reach <a href="http://cdn.mysql.com/archives/mysql-5.5/mysql-5.5.37-win32.msi">http://cdn.mysql.com/archives/mysql-5.5/mysql-5.5.37-win32.msi</a> . |

| COMPONENT | REQUIREMENT                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| URLs      | <p>The configuration server needs access to these URLs (directly or via proxy):</p> <p>Azure AD: <code>login.microsoftonline.com</code> ;<br/> <code>login.microsoftonline.us</code> ;<br/> <code>*.accesscontrol.windows.net</code></p> <p>Replication data transfer: <code>*.backup.windowsazure.com</code> ;<br/> <code>*.backup.windowsazure.us</code></p> <p>Replication management:<br/> <code>*.hypervrecoverymanager.windowsazure.com</code> ;<br/> <code>*.hypervrecoverymanager.windowsazure.us</code> ;<br/> <code>https://management.azure.com</code> ;<br/> <code>*.services.visualstudio.com</code></p> <p>Storage access: <code>*.blob.core.windows.net</code> ;<br/> <code>*.blob.core.usgovcloudapi.net</code></p> <p>Time synchronization: <code>time.nist.gov</code> ; <code>time.windows.com</code></p> <p>Telemetry (optional): <code>dc.services.visualstudio.com</code></p>                                                                   |
| Firewall  | <p>IP address-based firewall rules should allow communication to Azure URLs. To simplify and limit the IP ranges, we recommend using URL filtering.</p> <p><b>For commercial IPs:</b></p> <ul style="list-style-type: none"> <li>- Allow the <a href="#">Azure Datacenter IP Ranges</a>, and the HTTPS (443) port.</li> <li>- Allow IP address ranges for the West US (used for Access Control and Identity Management).</li> <li>- Allow IP address ranges for the Azure region of your subscription, to support the URLs needed for Azure Active Directory, backup, replication, and storage.</li> </ul> <p><b>For government IPs:</b></p> <ul style="list-style-type: none"> <li>- Allow the Azure Government Datacenter IP Ranges, and the HTTPS (443) port.</li> <li>- Allow IP address ranges for all US Gov Regions (Virginia, Texas, Arizona, and Iowa), to support the URLs needed for Azure Active Directory, backup, replication, and storage.</li> </ul> |
| Ports     | <p>Allow 443 (Control channel orchestration)</p> <p>Allow 9443 (Data transport)</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

## Configuration/Process server sizing requirements

| CPU                                      | MEMORY | CACHE DISK | DATA CHANGE RATE | REPLICATED MACHINES |
|------------------------------------------|--------|------------|------------------|---------------------|
| 8 vCPUs<br>2 sockets * 4 cores @ 2.5 GHz | 16GB   | 300 GB     | 500 GB or less   | < 100 machines      |
| 12 vCPUs<br>2 socks * 6 cores @ 2.5 GHz  | 18 GB  | 600 GB     | 500 GB-1 TB      | 100 to 150 machines |
| 16 vCPUs<br>2 socks * 8 cores @ 2.5 GHz  | 32 GB  | 1 TB       | 1-2 TB           | 150 -200 machines   |

## Step 1: Prepare Azure Stack VMs

### Verify the operating system

Make sure that the VMs are running one of the operating systems summarized in the table.

| OPERATING SYSTEM      | DETAILS                                                                                             |
|-----------------------|-----------------------------------------------------------------------------------------------------|
| <b>64-bit Windows</b> | Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2 (from SP1) |
| <b>CentOS</b>         | 5.2 to 5.11, 6.1 to 6.9, 7.0 to 7.3                                                                 |
| <b>Ubuntu</b>         | 14.04 LTS server, 16.04 LTS server. Review <a href="#">supported kernels</a>                        |

### Prepare for Mobility service installation

Every VM you want to replicate must have the Mobility service installed. In order for the process server to install the service automatically on the VM when replication is enabled, verify the VM settings.

#### Windows machines

- You need network connectivity between the VM on which you want to enable replication, and the machine running the process server (by default this is the configuration server VM).
- You need an account with admin rights (domain or local) on the machine for which you enable replication.
  - You specify this account when you set up Site Recovery. Then the process server uses this account to install the Mobility service when replication is enabled.
  - This account will only be used by Site Recovery for the push installation, and to update the Mobility service.
  - If you're not using a domain account, you need to disable Remote User Access control on the VM:
    - In the registry, create DWORD value **LocalAccountTokenFilterPolicy** under **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System**.
    - Set the value to 1.
    - To do this at the command prompt, type the following: **REG ADD HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v LocalAccountTokenFilterPolicy /t REG\_DWORD /d 1**.
- In the Windows Firewall on the VM you want to replicate, allow File and Printer Sharing, and WMI.
  - To do this, run **wf.msc** to open the Windows Firewall console. Right click **Inbound Rules > New Rule**. Select **Predefined**, and choose **File and Printer sharing** from the list. Complete the wizard, select to

allow the connection > **Finish**.

- For domain computers, you can use a GPO to do this.

#### Linux machines

- Ensure that there's network connectivity between the Linux computer and the process server.
- On the machine for which you enable replication, you need an account that's a root user on the source Linux server:
  - You specify this account when you set up Site Recovery. Then the process server uses this account to install the Mobility service when replication is enabled.
  - This account will only be used by Site Recovery for the push installation, and to update the Mobility service.
- Check that the /etc/hosts file on the source Linux server has entries that map the local hostname to IP addresses associated with all network adapters.
- Install the latest openssh, openssh-server, and openssl packages on the computer that you want to replicate.
- Ensure that Secure Shell (SSH) is enabled and running on port 22.
- Enable SFTP subsystem and password authentication in the sshd\_config file:
  1. To do this, sign in as root.
  2. Find the line that begins with **PasswordAuthentication**, in the /etc/ssh/sshd\_config file.  
Uncomment the line and change the value to **yes**.
  3. Find the line that begins with **Subsystem** and uncomment the line.

```
override default of no subsystems
Subsystem sftp /usr/libexec.openssh.sftp-server
```

4. Restart the sshd service.

#### Note the VM private IP address

For each machine you want to replicate, find the IP address:

1. In the Azure Stack Portal, click on the VM.
2. On the **Resource** menu, click **Network Interfaces**.
3. Note down the private IP address.

| NAME       | PUBLIC IP ADDRESS | PRIVATE IP ADDRESS | SECURITY GROUP |
|------------|-------------------|--------------------|----------------|
| akvmm01742 | 10.193.133.27     | 10.0.0.4           | akvmm01-nsg    |

## Step 2: Create a vault and select a replication goal

1. In the Azure portal, select **Create a resource** > **Management Tools** > **Backup and Site Recovery**.
2. In **Name**, enter a friendly name to identify the vault.
3. In **Resource group**, create or select a resource group. We're using **contosoRG**.

4. In **Location**, enter the Azure region. We're using **West Europe**.
5. To quickly access the vault from the dashboard, select **Pin to dashboard > Create**.

The screenshot shows the 'Recovery Services vault' creation dialog box. It includes fields for Name (ContosoVMVault), Subscription (Contoso Subscription), Resource group (contosoRG), Location (West Europe), and a 'Pin to dashboard' checkbox which is checked. At the bottom are 'Create' and 'Automation options' buttons.

|                                                      |                                                                                             |
|------------------------------------------------------|---------------------------------------------------------------------------------------------|
| ★ Name                                               | ContosoVMVault                                                                              |
| ★ Subscription                                       | Contoso Subscription                                                                        |
| ★ Resource group                                     | <input type="radio"/> Create new <input checked="" type="radio"/> Use existing<br>contosoRG |
| ★ Location                                           | West Europe                                                                                 |
| <input checked="" type="checkbox"/> Pin to dashboard |                                                                                             |
| <b>Create</b>                                        | Automation options                                                                          |

The new vault appears on **Dashboard > All resources**, and on the main **Recovery Services vaults** page.

#### Select a replication goal

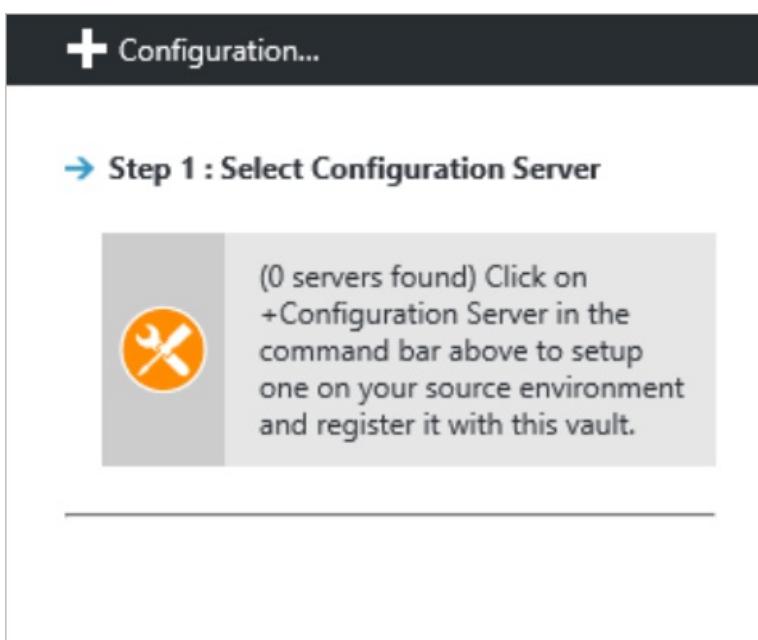
1. In **Recovery Services vaults** > specify a vault name. We're using **ContosoVMVault**.
2. In **Getting Started**, select Site Recovery. Then select **Prepare Infrastructure**.
3. In **Protection goal > Where are your machines located**, select **On-premises**.
4. In **Where do you want to replicate your machines**, select **To Azure**.
5. In **Are your machines virtualized**, select **Not virtualized/Other**. Then select **OK**.

|                                                                     |                                   |
|---------------------------------------------------------------------|-----------------------------------|
| These are long running tasks done on-premises.                      |                                   |
| <b>1</b>                                                            | Protection goal<br>Select >       |
| <b>2</b>                                                            | Source<br>Prepare >               |
| <b>3</b>                                                            | Target<br>Prepare >               |
| <b>4</b>                                                            | Replication settings<br>Prepare > |
| <b>5</b>                                                            | Deployment planning<br>Select >   |
| <input type="button" value="OK"/> <input type="button" value="OK"/> |                                   |

## Step 3: Set up the source environment

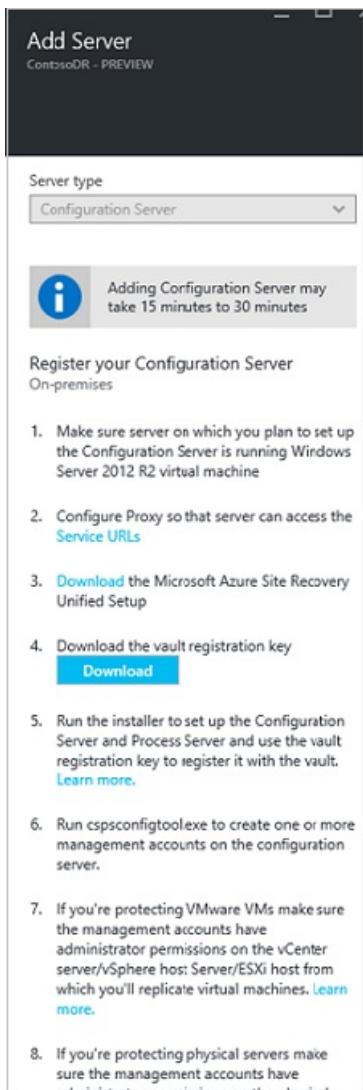
Set up the configuration server machine, register it in the vault, and discover machines you want to replicate.

1. Click **Prepare Infrastructure > Source**.
2. In **Prepare source**, click **+Configuration server**.



3. In **Add Server**, check that **Configuration Server** appears in **Server type**.
4. Download the Site Recovery Unified Setup installation file.

5. Download the vault registration key. You need the registration key when you run Unified Setup. The key is valid for five days after you generate it.



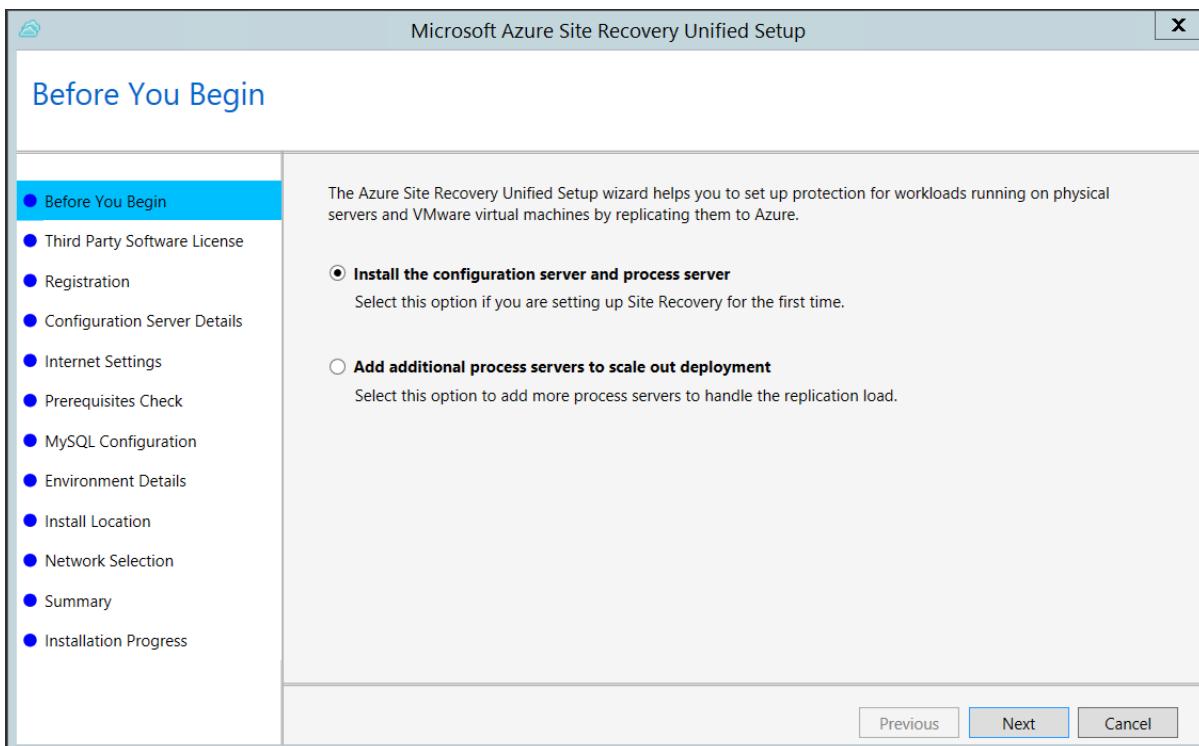
## Run Azure Site Recovery Unified Setup

To install and register the configuration server, do an RDP connection to the VM you want to use for the configuration server, and run Unified Setup.

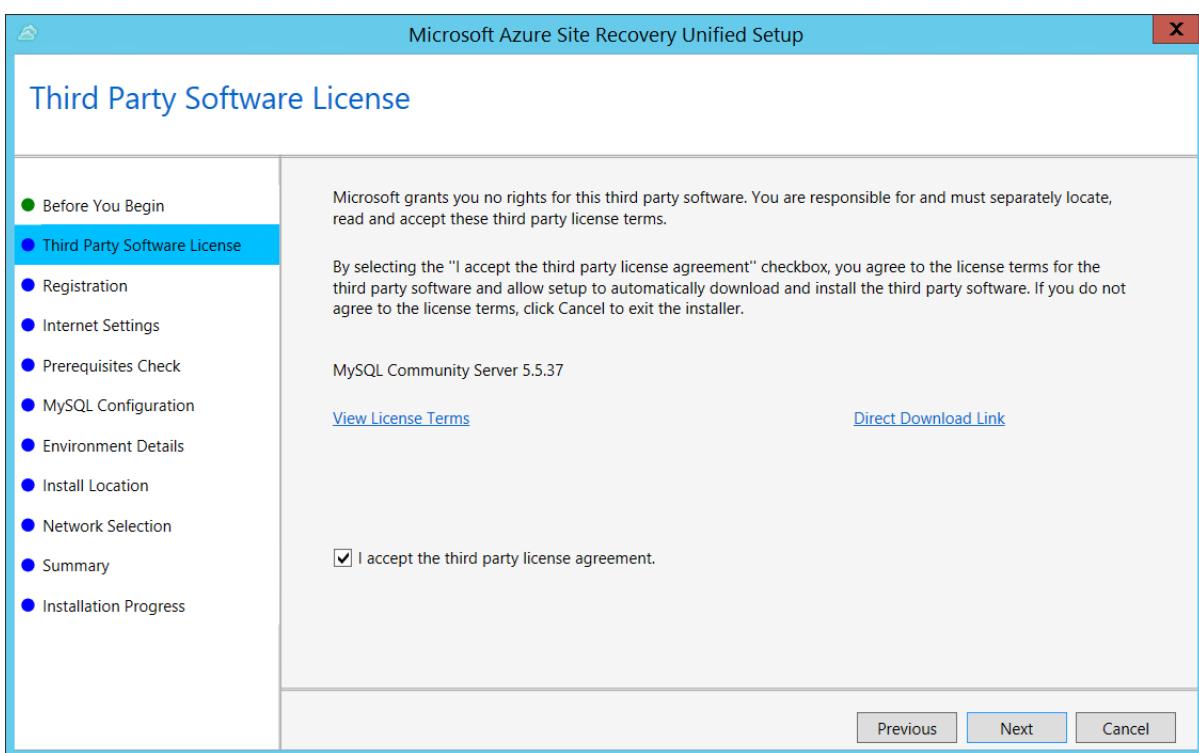
Before you start, make sure that the clock is [synchronized with a time server](#) on the VM before you start. Installation fails if the time is more than five minutes off local time.

Now install the configuration server:

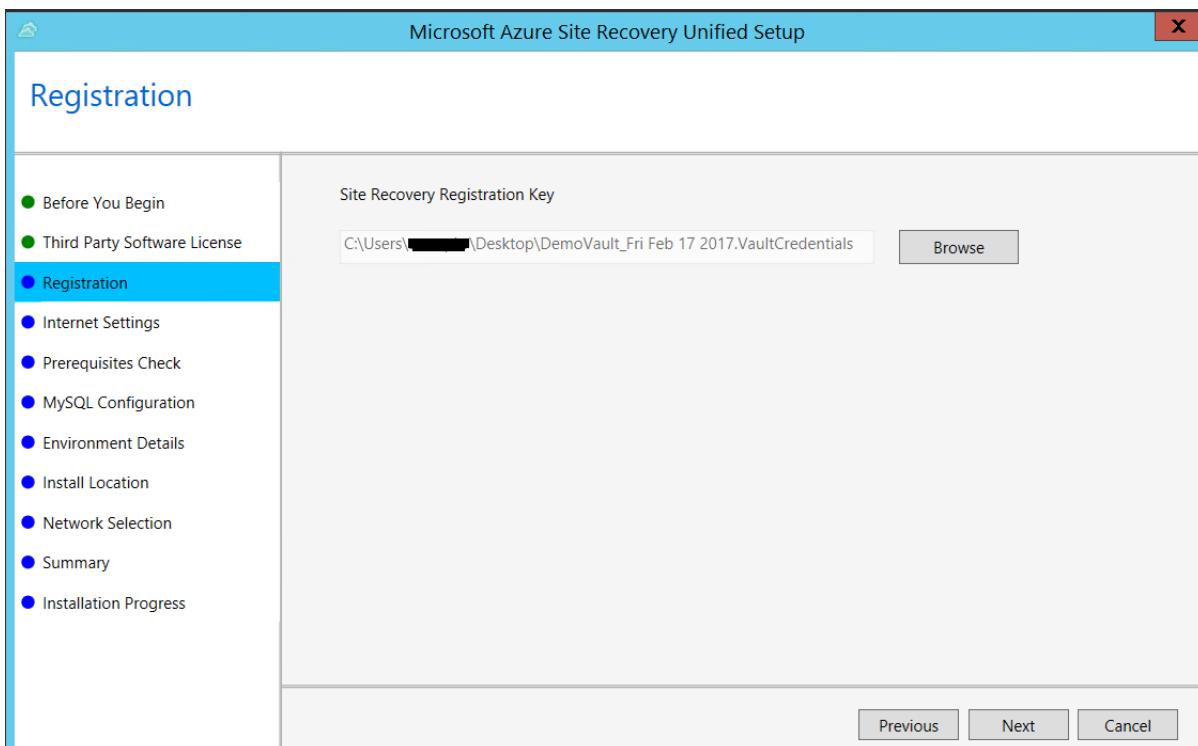
1. Run the Unified Setup installation file.
2. In **Before You Begin**, select **Install the configuration server and process server**.



3. In **Third Party Software License**, click **I Accept** to download and install MySQL.

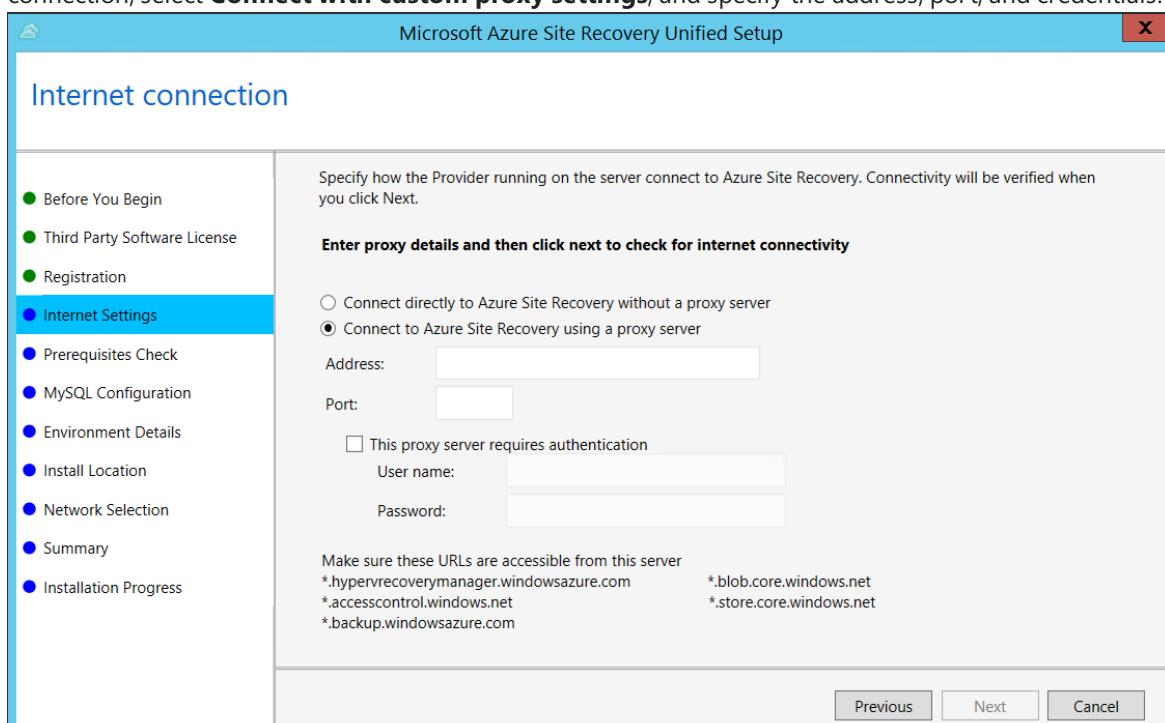


4. In **Registration**, select the registration key you downloaded from the vault.

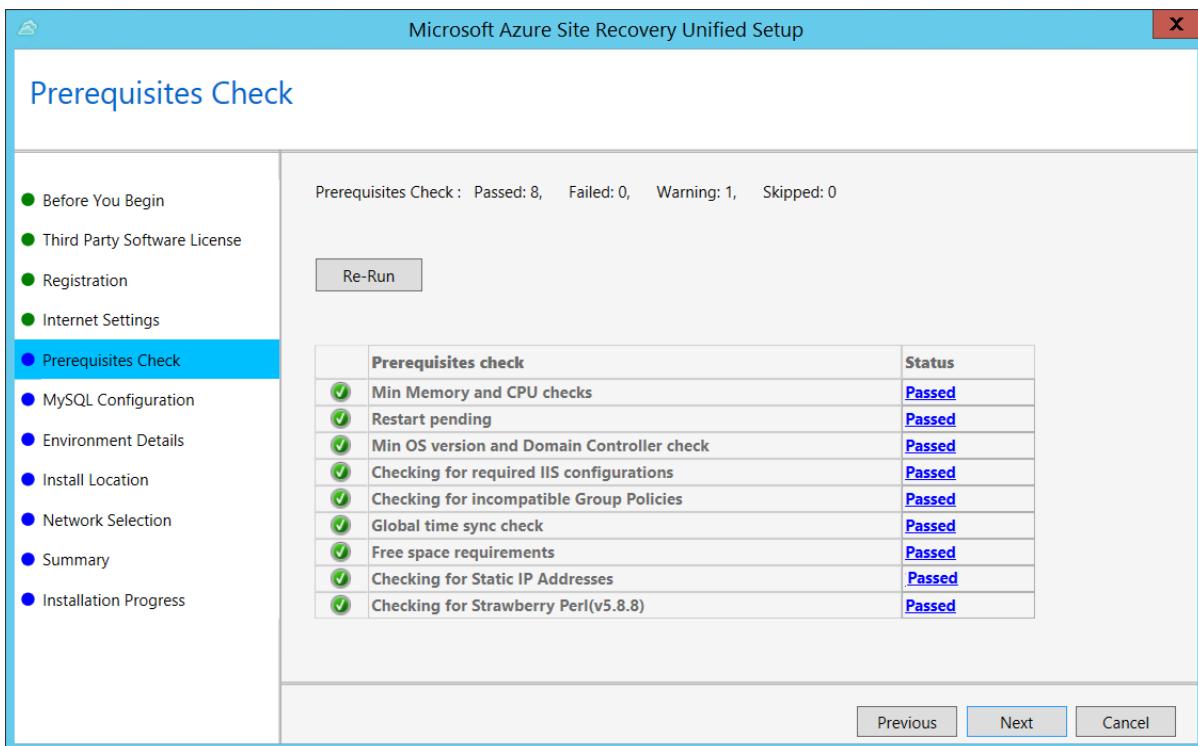


5. In **Internet Settings**, specify how the Provider running on the configuration server connects to Azure Site Recovery over the Internet. Make sure you've allowed the required URLs.

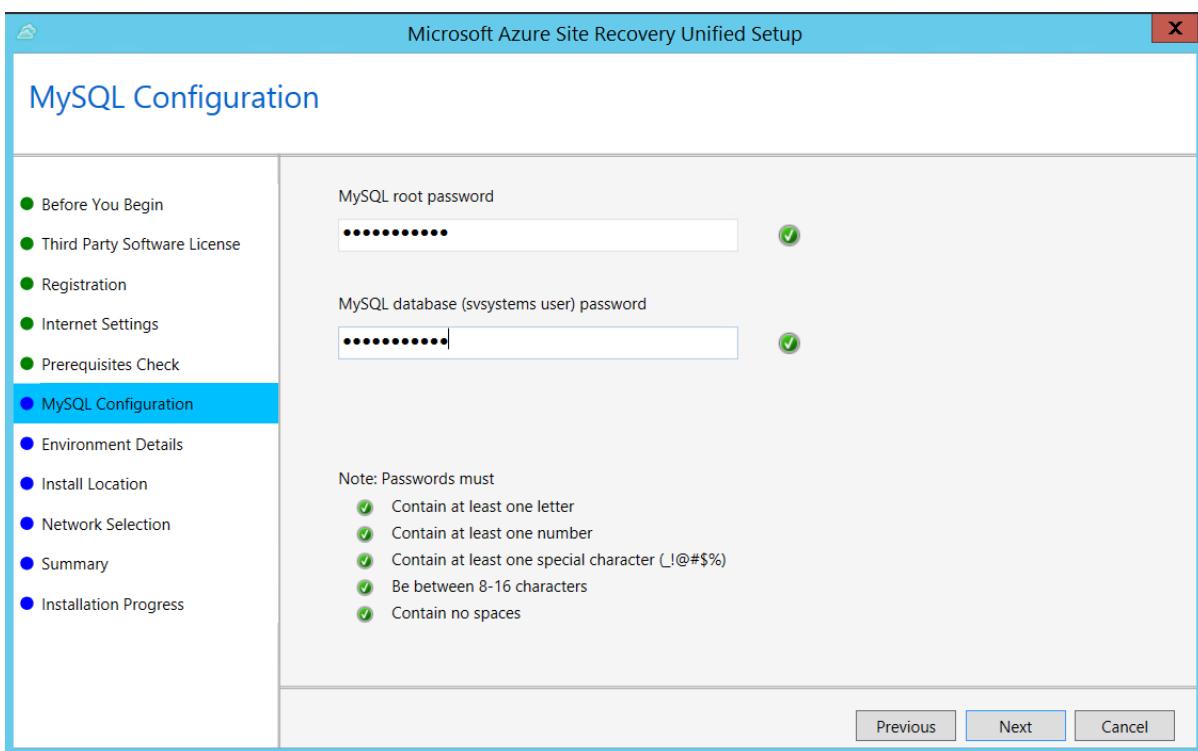
- If you want to connect with the proxy that's currently set up on the machine, select **Connect to Azure Site Recovery using a proxy server**.
- If you want the Provider to connect directly, select **Connect directly to Azure Site Recovery without a proxy server**.
- If the existing proxy requires authentication, or if you want to use a custom proxy for the Provider connection, select **Connect with custom proxy settings**, and specify the address, port, and credentials.



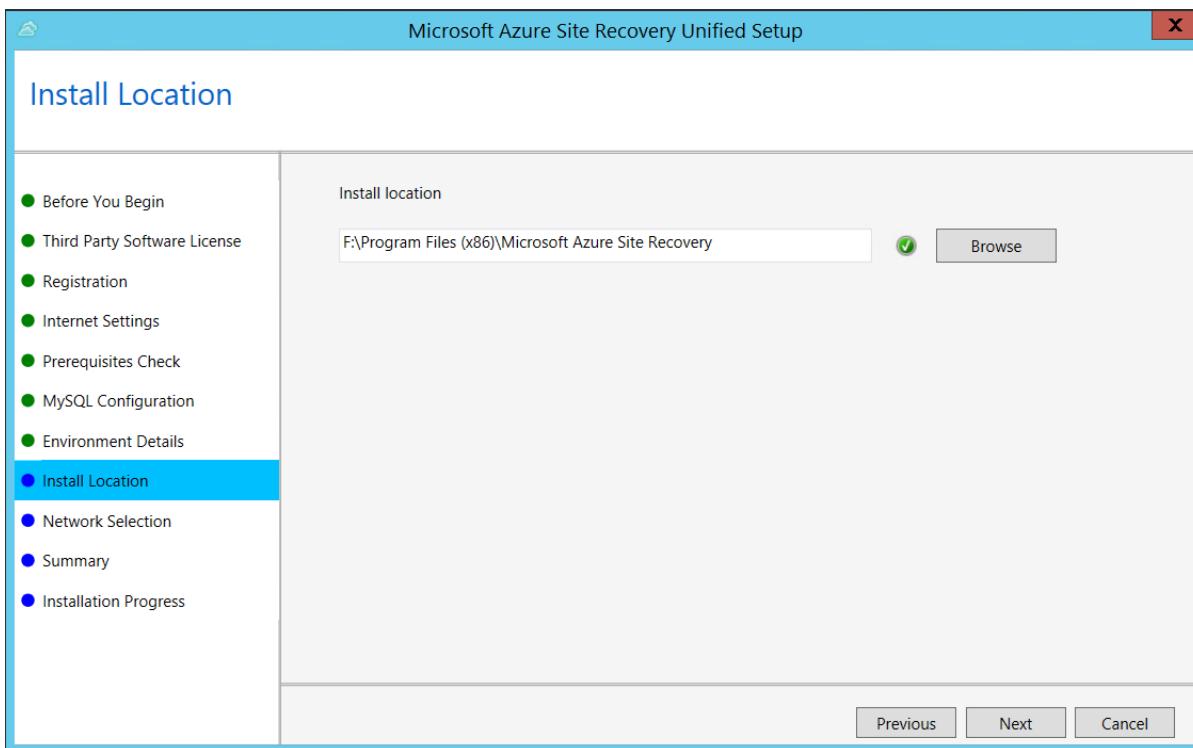
6. In **Prerequisites Check**, Setup runs a check to make sure that installation can run. If a warning appears about the **Global time sync check**, verify that the time on the system clock (**Date and Time** settings) is the same as the time zone.



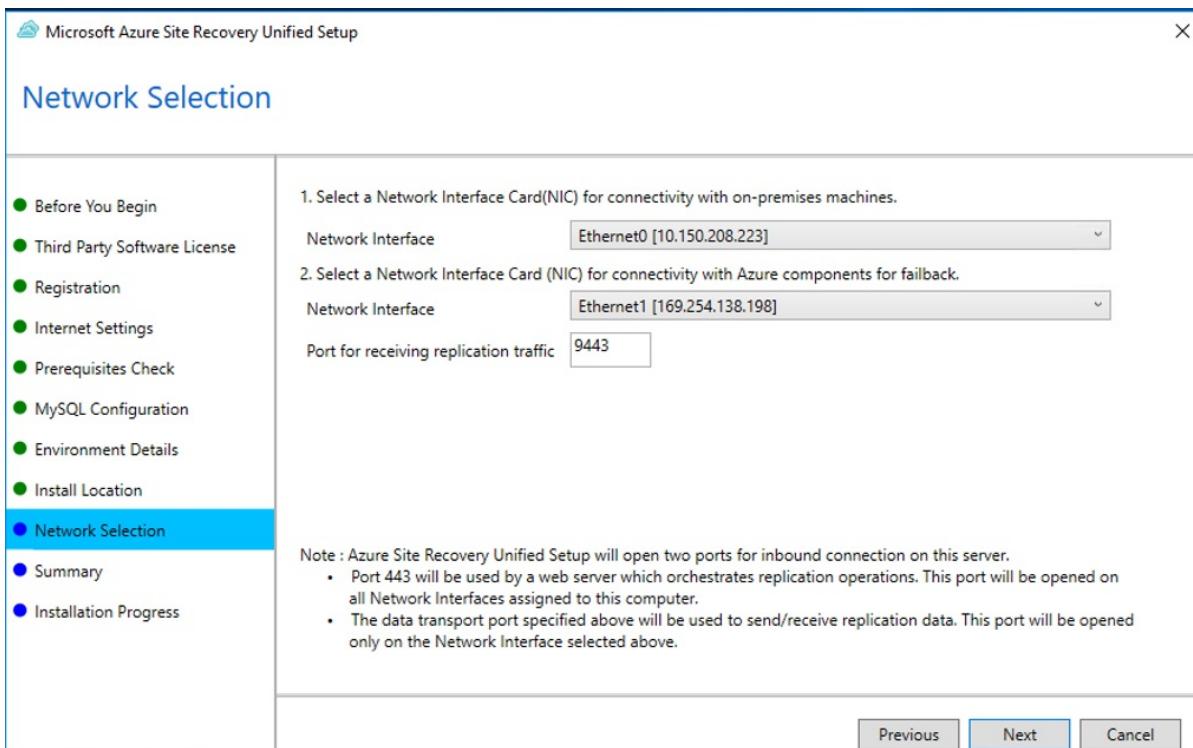
7. In **MySQL Configuration**, create credentials for logging on to the MySQL server instance that is installed.



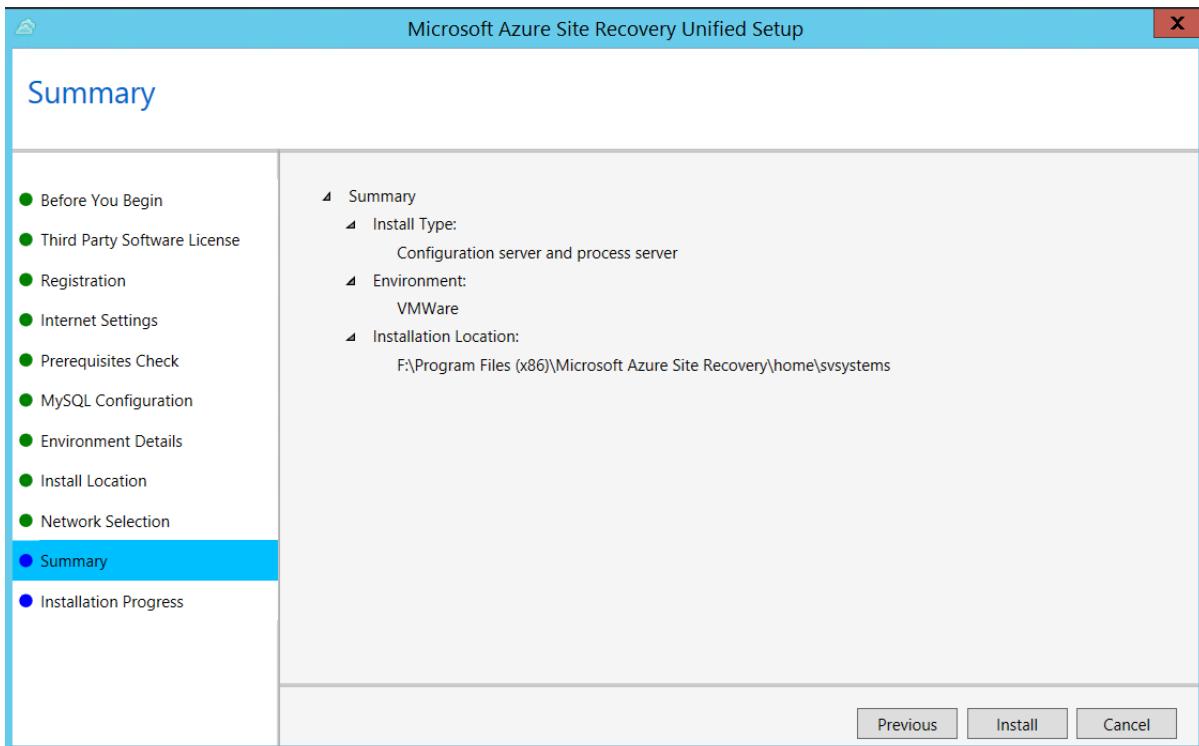
8. In **Environment Details**, select No if you're replicating Azure Stack VMs or physical servers.
9. In **Install Location**, select where you want to install the binaries and store the cache. The drive you select must have at least 5 GB of disk space available, but we recommend a cache drive with at least 600 GB of free space.



10. In **Network Selection**, first select the NIC that the in-built process server uses for discovery and push installation of mobility service on source machines, and then select the NIC that Configuration Server uses for connectivity with Azure. Port 9443 is the default port used for sending and receiving replication traffic, but you can modify this port number to suit your environment's requirements. In addition to the port 9443, we also open port 443, which is used by a web server to orchestrate replication operations. Do not use port 443 for sending or receiving replication traffic.



11. In **Summary**, review the information and click **Install**. When installation finishes, a passphrase is generated. You will need this when you enable replication, so copy it and keep it in a secure location.



After registration finishes, the server is displayed on the **Settings > Servers** blade in the vault.

#### NOTE

The configuration server can also be installed from the command line. [Learn more](#).

It can take 15 minutes or more for the account name to appear in the portal. To update immediately, select **Configuration Servers > server name > Refresh Server**.

## Step 4: Set up the target environment

Select and verify target resources.

1. In **Prepare infrastructure > Target**, select the Azure subscription you want to use.
2. Specify the target deployment model.
3. Site Recovery checks that you have one or more compatible Azure storage accounts and networks. If it doesn't find them, you need to create at least one storage account and virtual network, in order to complete the wizard.

## Step 5: Enable replication

### Create a replication policy

1. Click **Prepare Infrastructure > Replication Settings**.
2. In **Create replication policy**, specify a policy name.
3. In **RPO threshold**, specify the recovery point objective (RPO) limit.
  - Recovery points for replicated data are created in accordance with the time set.
  - This setting does not affect replication, which is continuous. It simply issues an alert if the threshold limit is reached without a recovery point being created.
4. In **Recovery point retention**, specify how long each recovery point is kept. Replicated VMs can be recovered to any point in the specified time window.
5. In **App-consistent snapshot frequency**, specify how often application-consistent snapshots are created.

- An app-consistent snapshot is a point-in-time snapshot of the app data inside the VM.
  - Volume Shadow Copy Service (VSS) ensures that apps on the VM are in a consistent state when the snapshot is taken.
6. Select **OK** to create the policy.

## Confirm deployment planning

You can skip this step right now. In **Deployment Planning** dropdown list, click **Yes, I have done it**.

## Enable replication

Make sure you've completed all the tasks in [Step 1: Prepare machine](#). Then enable replication as follows:

1. Select **Replicate application > Source**.
2. In **Source**, select the configuration server.
3. In **Machine type**, select **Physical machines**.
4. Select the process server (configuration server). Then click **OK**.
5. In **Target**, select the subscription and the resource group in which you want to create the VMs after failover.  
Choose the deployment model that you want to use for the failed-over VMs.
6. Select the Azure storage account in which you want to store the replicated data.
7. Select the Azure network and subnet to which Azure VMs connect when they're created after failover.
8. Select **Configure now for selected machines** to apply the network setting to all machines you select for protection. Select **Configure later** if you want to select the Azure network separately for each machine.
9. In **Physical Machines**, click **+Physical machine**. Specify the name, IP address and OS type of each machine you want to replicate.
  - Use the internal IP address of the machine.
  - If you specify the public IP address, replication may not work as expected.
10. In **Properties > Configure properties**, select the account that the process server will use to automatically install Mobility Service on the machine.
11. In **Replication settings > Configure replication settings**, check that the correct replication policy is selected.
12. Click **Enable Replication**.
13. Track progress of the **Enable Protection** job in **Settings > Jobs > Site Recovery Jobs**. After the **Finalize Protection** job runs, the machine is ready for failover.

### NOTE

Site Recovery installs Mobility Service when replication is enabled for a VM.

It can take 15 minutes or longer for changes to take effect and appear in the portal.

To monitor VMs you add, check the last discovered time for VMs in **Configuration Servers > Last Contact At**. To add VMs without waiting for the scheduled discovery, highlight the configuration server (don't select it) and select **Refresh**.

## Step 6: Run a disaster recovery drill

You run a test failover to Azure to make sure that everything's working as expected. This failover won't affect your production environment.

## Verify machine properties

Before you run a test failover, verify the machine properties, and make sure that they comply with [Azure requirements](#). You can view and modify properties as follows:

1. In **Protected Items**, click **Replicated Items** > VM.
2. In the **Replicated item** pane, there's a summary of VM information, health status, and the latest available recovery points. Click **Properties** to view more details.
3. In **Compute and Network**, modify settings as needed.
  - You can modify the Azure VM name, resource group, target size, [availability set](#), and managed disk settings.
  - You can also view and modify network settings. These include the network/subnet to which the Azure VM is joined after failover, and the IP address that will be assigned to the VM.
4. In **Disks**, view information about the operating system and data disks on the VM.

## Run a test failover

When you run a test failover, the following happens:

1. A prerequisites check runs to make sure all of the conditions required for failover are in place.
2. Failover processes the data using the specified recovery point:
  - **Latest processed**: The machine fails over to the latest recovery point processed by Site Recovery. The time stamp is shown. With this option, no time is spent processing data, so it provides a low RTO (recovery time objective).
  - **Latest app-consistent**: The machine fails over to the latest app-consistent recovery point.
  - **Custom**: Select the recovery point used for failover.
3. An Azure VM is created using the processed data.
4. Test failover can automatically clean up Azure VMs created during the drill.

Run a test failover for a VM as follows:

1. In **Settings** > **Replicated Items**, click the VM > **+Test Failover**.
2. For this walkthrough, we'll select to use the **Latest processed** recovery point.
3. In **Test Failover**, select the target Azure network.
4. Click **OK** to begin the failover.
5. Track progress by clicking on the VM to open its properties. Or, click the **Test Failover** job in *vault name* > **Settings** > **Jobs** > **Site Recovery jobs**.
6. After the failover finishes, the replica Azure VM appears in the Azure portal > **Virtual Machines**. Check that the VM is the appropriate size, connected to the right network, and running.
7. You should now be able to connect to the replicated VM in Azure. [Learn more](#).
8. To delete Azure VMs created during the test failover, click **Cleanup test failover** on the VM. In **Notes**, save any observations associated with the test failover.

## Fail over and fail back

After you've set up replication, and run a drill to make sure everything's working, you can fail machines over to Azure as required.

Before you run a failover, if you want to connect to the machine in Azure after the failover, then[prepare to connect](#) before you start.

Then run a failover as follows:

1. In **Settings > Replicated Items**, click the machine > **Failover**.
2. Select the recovery point that you want to use.
3. In **Test Failover**, select the target Azure network.
4. Select **Shut down machine before beginning failover**. With this setting, Site Recovery tries to shut down the source machine before starting the failover. However failover continues even if shutdown fails.
5. Click **OK** to begin the failover. You can follow the failover progress on the **Jobs** page.
6. After the failover finishes, the replica Azure VM appears in the Azure portal > **Virtual Machines**. If you prepared to connect after failover, check that the VM is the appropriate size, connected to the right network, and running.
7. After verifying the VM, click **Commit** to finish the failover. This deletes all available recovery points.

#### **WARNING**

Don't cancel a failover in progress: Before failover is started, VM replication is stopped. If you cancel a failover in progress, failover stops, but the VM won't replicate again.

### **Fail back to Azure Stack**

When your primary site is up and running again, you can fail back from Azure to Azure Stack. To do this, you need to download the Azure VM VHD, and upload it to Azure Stack.

1. Shut down the Azure VM, so that the VHD can be downloaded.
2. To start downloading the VHD, install [Azure Storage Explorer](#).
3. Navigate to the VM in the Azure Portal (using the VM name).
4. In **Disk**s, click on the disk name, and gather settings.
  - As an example, the VHD URI used in our test:  
<https://502055westcentralus.blob.core.windows.net/wahv9b8d2ceb284fb59287/copied-3676553984.vhd> can be broken down to get the following input parameters that are used to download the VHD.
    - Storage Account: 502055westcentralus
    - Container: wahv9b8d2ceb284fb59287
    - VHD Name: copied-3676553984.vhd
5. Now, use Azure Storage Explorer to download the VHD.
6. Upload the VHD to Azure Stack with [these steps](#).
7. In the existing VM or new VM, attach the uploaded VHDS.
8. Check that the OS Disk is correct, and start the VM.

At this stage failback is complete.

## **Conclusion**

In this article we replicated Azure Stack VMs to Azure. With replication in place, we ran a disaster recovery drill to make sure failover to Azure worked as expected. The article also included steps for running a full failover to Azure, and failing back to Azure Stack.

## **Next steps**

After failing back, you can reprotect the VM and start replicating it to Azure again To do this, repeat the steps in this article.



# Manage VM network interfaces for on-premises disaster recovery to Azure

11/12/2019 • 2 minutes to read • [Edit Online](#)

A virtual machine (VM) in Azure must have at least one network interface attached to it. It can have as many network interfaces attached to it as the VM size supports.

By default, the first network interface attached to an Azure virtual machine is defined as the primary network interface. All other network interfaces in the virtual machine are secondary network interfaces. Also by default, all outbound traffic from the virtual machine is sent out the IP address that's assigned to the primary IP configuration of the primary network interface.

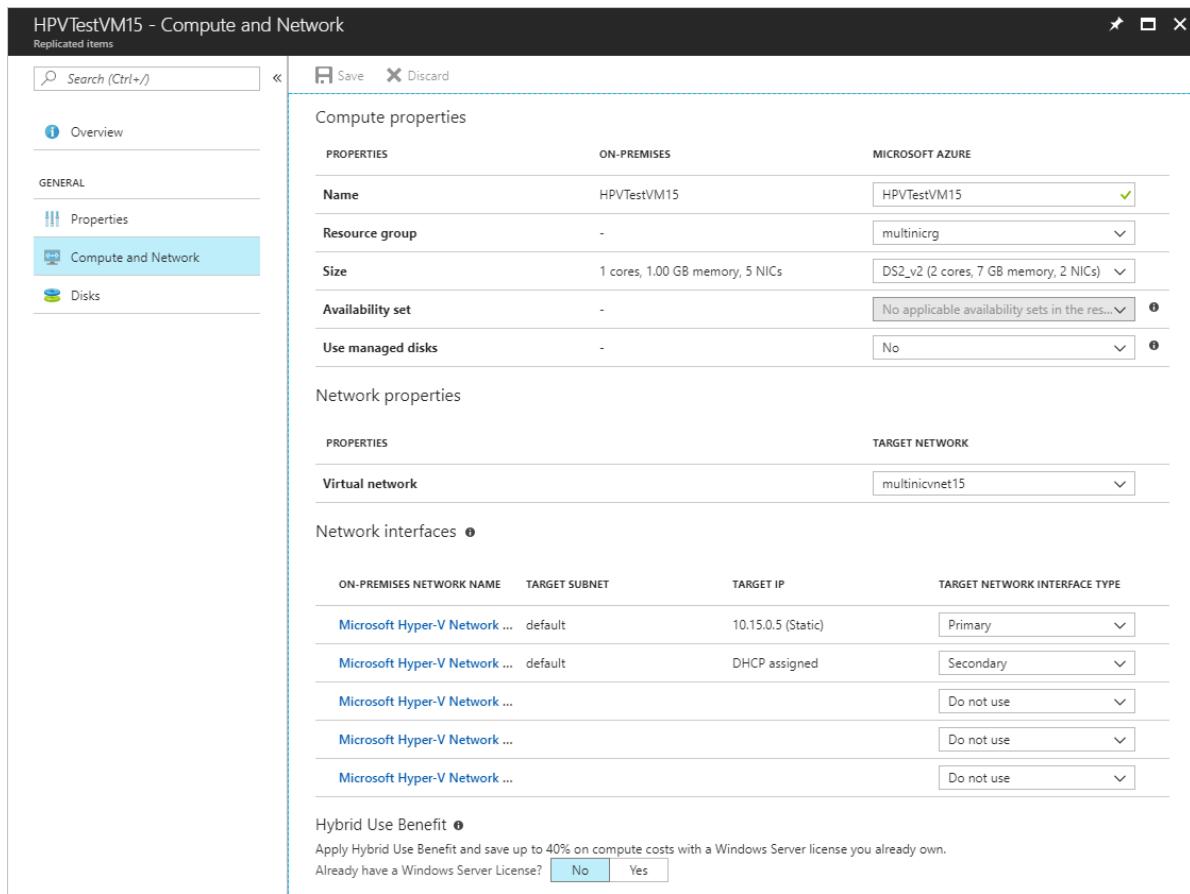
In an on-premises environment, virtual machines or servers can have multiple network interfaces for different networks within the environment. Different networks are typically used for performing specific operations such as upgrades, maintenance, and internet access. When you're migrating or failover to Azure from an on-premises environment, keep in mind that network interfaces in the same virtual machine must all be connected to the same virtual network.

By default, Azure Site Recovery creates as many network interfaces on an Azure virtual machine as are connected to the on-premises server. You can avoid creating redundant network interfaces during migration or failover by editing the network interface settings under the settings for the replicated virtual machine.

## Select the target network

For VMware and physical machines, and for Hyper-V (without System Center Virtual Machine Manager) virtual machines, you can specify the target virtual network for individual virtual machines. For Hyper-V virtual machines managed with Virtual Machine Manager, use [network mapping](#) to map VM networks on a source Virtual Machine Manager server and target Azure networks.

1. Under **Replicated items** in a Recovery Services vault, select any replicated item to access the settings for that replicated item.
2. Select the **Compute and Network** tab to access the network settings for the replicated item.
3. Under **Network properties**, choose a virtual network from the list of available network interfaces.



Modifying the target network affects all network interfaces for that specific virtual machine.

For Virtual Machine Manager clouds, modifying network mapping affects all virtual machines and their network interfaces.

## Select the target interface type

Under the **Network interfaces** section of the **Compute and Network** pane, you can view and edit network interface settings. You can also specify the target network interface type.

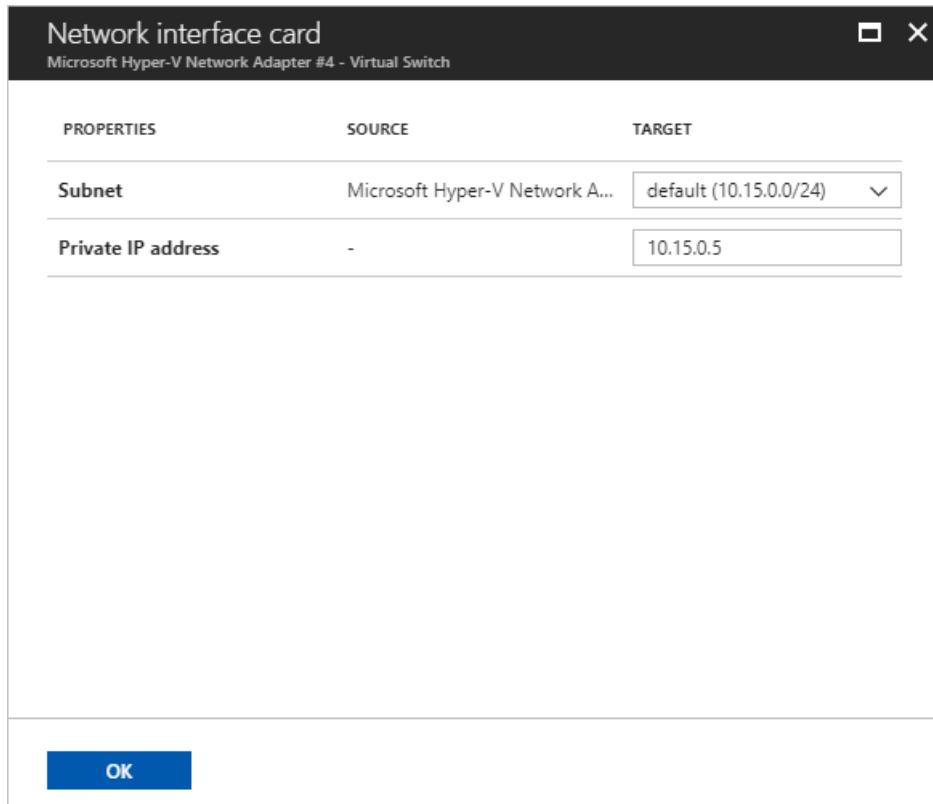
- A **Primary** network interface is required for failover.
- All other selected network interfaces, if any, are **Secondary** network interfaces.
- Select **Do not use** to exclude a network interface from creation at failover.

By default, when you're enabling replication, Site Recovery selects all detected network interfaces on the on-premises server. It marks one as **Primary** and all others as **Secondary**. Any subsequent interfaces added on the on-premises server are marked **Do not use** by default. When you're adding more network interfaces, ensure that the correct Azure virtual machine target size is selected to accommodate all required network interfaces.

## Modify network interface settings

You can modify the subnet and IP address for a replicated item's network interfaces. If an IP address is not specified, Site Recovery will assign the next available IP address from the subnet to the network interface at failover.

1. Select any available network interface to open the network interface settings.
2. Choose the desired subnet from the list of available subnets.
3. Enter the desired IP address (as required).



4. Select **OK** to finish editing and return to the **Compute and Network** pane.
5. Repeat steps 1-4 for other network interfaces.
6. Select **Save** to save all changes.

## Next steps

[Learn more](#) about network interfaces for Azure virtual machines.

# Connect to Azure VMs after failover from on-premises

11/14/2019 • 6 minutes to read • [Edit Online](#)

This article describes how to set up connectivity so that you can successfully connect to Azure VMs after failover.

When you set up disaster recovery of on-premises virtual machines (VMs) and physical servers to Azure, [Azure Site Recovery](#) starts replicating machines to Azure. Then, when outages occur, you can fail over to Azure from your on-premises site. When failover occurs, Site Recovery creates Azure VMs, using replicated on-premises data. As part of disaster recovery planning, you need to figure out how to connect to apps running on these Azure VMs after failover.

In this article you learn how to:

- Prepare on-premises machines before failover.
- Prepare Azure VMs after failover.
- Retain IP addresses on Azure VMs after failover.
- Assign new IP addresses to Azure VMs after failover.

## Prepare on-premises machines

To ensure connectivity to Azure VMs, prepare your on-premises machines before failover.

### Prepare Windows machines

On on-premises Windows machines, do the following:

1. Configure Windows settings. These include removing any static persistent routes or WinHTTP proxy, and setting the disk SAN policy to **OnlineAll**. [Follow](#) these instructions.
2. Make sure [these services](#) are running.
3. Enable remote desktop (RDP) to allow remote connections to the on-premises machine. [Learn how](#) to enable RDP with PowerShell.
4. To access an Azure VM over the internet after failover, in Windows Firewall on the on-premises machine, allow TCP and UDP in the Public profile, and set RDP as an allowed app for all profiles.
5. If you want to access an Azure VM over a site-to-site VPN after failover, in Windows Firewall on the on-premises machine, allow RDP for the Domain and Private profiles. [Learn](#) how to allow RDP traffic.
6. Make sure that there are no Windows updates pending on the on-premises VM when you trigger a failover. If there are, updates might start installing on the Azure VM after failover, and you won't be able to sign into the VM until updates finish.

### Prepare Linux machines

On on-premises Linux machines, do the following:

1. Check that the Secure Shell service is set to start automatically on system boot.
2. Check that firewall rules allow an SSH connection.

## Configure Azure VMs after failover

After failover, do the following on the Azure VMs that are created.

1. To connect to the VM over the internet, assign a public IP address to the VM. You can't use the same public IP address for the Azure VM that you used for your on-premises machine. [Learn more](#)
2. Check that network security group (NSG) rules on the VM allow incoming connections to the RDP or SSH port.
3. Check [Boot diagnostics](#) to view the VM.

**NOTE**

The Azure Bastion service offers private RDP and SSH access to Azure VMs. [Learn more](#) about this service.

## Set a public IP address

As an alternative to assigning a public IP address manually to an Azure VM, you can assign the address during failover using a script or Azure automation runbook in a Site Recovery [recovery plan](#), or you can set up DNS-level routing using Azure Traffic Manager. [Learn more](#) about setting up a public address.

## Assign an internal address

To set the internal IP address of an Azure VM after failover, you have a couple of options:

- **Retain same IP address:** You can use the same IP address on the Azure VM as the one allocated to the on-premises machine.
- **Use different IP address:** You can use a different IP address for the Azure VM.

## Retain IP addresses

Site Recovery lets you retain the same IP addresses when failing over to Azure. Retaining the same IP address avoids potential network issues after failover, but does introduce some complexity.

- If the target Azure VM uses the same IP address/subnet as your on-premises site, you can't connect between them using a site-to-site VPN connection or ExpressRoute, because of the address overlap. Subnets must be unique.
- You need a connection from on-premises to Azure after failover, so that apps are available on Azure VMs. Azure doesn't support stretched VLANs, so if you want to retain IP addresses you need to take the IP space over to Azure by failing over the entire subnet, in addition to the on-premises machine.
- Subnet failover ensures that a specific subnet isn't available simultaneously on-premises and in Azure.

Retaining IP addresses requires the following steps:

- In the Compute & Network properties of the replicated item, set network and IP addressing for the target Azure VM to mirror the on-premises setting.
- Subnets must be managed as part of the disaster recovery process. You need an Azure VNet to match the on-premises network, and after failover network routes must be modified to reflect that the subnet has moved to Azure, and new IP address locations.

## Failover example

Let's look at an example.

- The fictitious company Woodgrove Bank hosts their business apps on-premises. They host their mobile apps in Azure.
- They connect from on-premises to Azure over site-to-site VPN.
- Woodgrove is using Site Recovery to replicate on-premises machines to Azure.

- Their on-premises apps use hard-coded IP addresses, so they want to retain the same IP addresses in Azure.
- On-premises the machines running the apps are running in three subnets:
  - 192.168.1.0/24
  - 192.168.2.0/24
  - 192.168.3.0/24
- Their apps running in Azure are located in the Azure VNet **Azure Network** in two subnets:
  - 172.16.1.0/24
  - 172.16.2.0/24.

In order to retain the addresses, here's what they do.

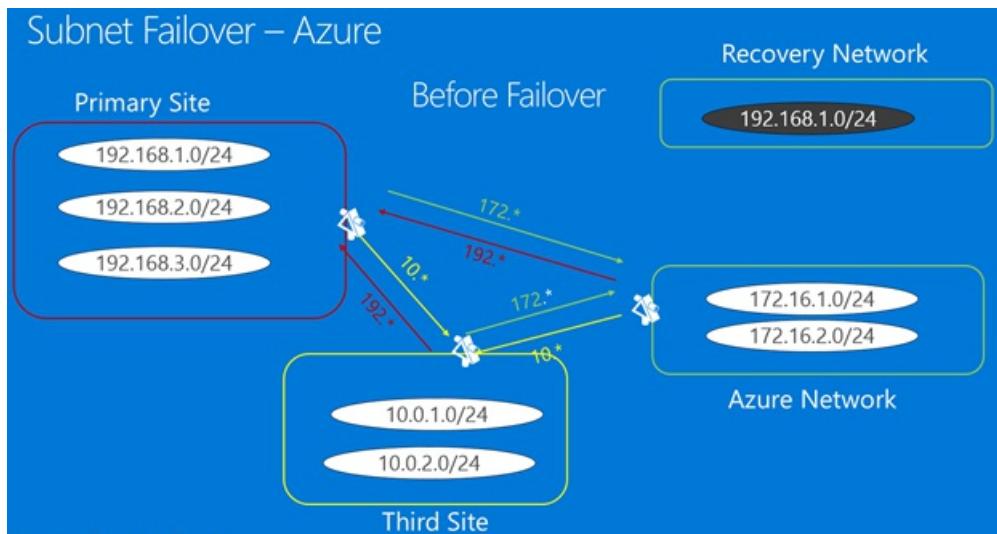
1. When they enable replication, they specify that machines should replicate to the **Azure Network**.
2. They create **Recovery Network** in Azure. This VNet mirrors the 192.168.1.0/24 subnet in their on-premises network.
3. Woodgrove sets up a [VNet-to-VNet connection](#) between the two networks.

#### NOTE

Depending on application requirements, a VNet-to-VNet connection could be set up before failover, as a manual step/scripted step/Azure automation runbook in a Site Recovery [recovery plan](#), or after failover is complete.

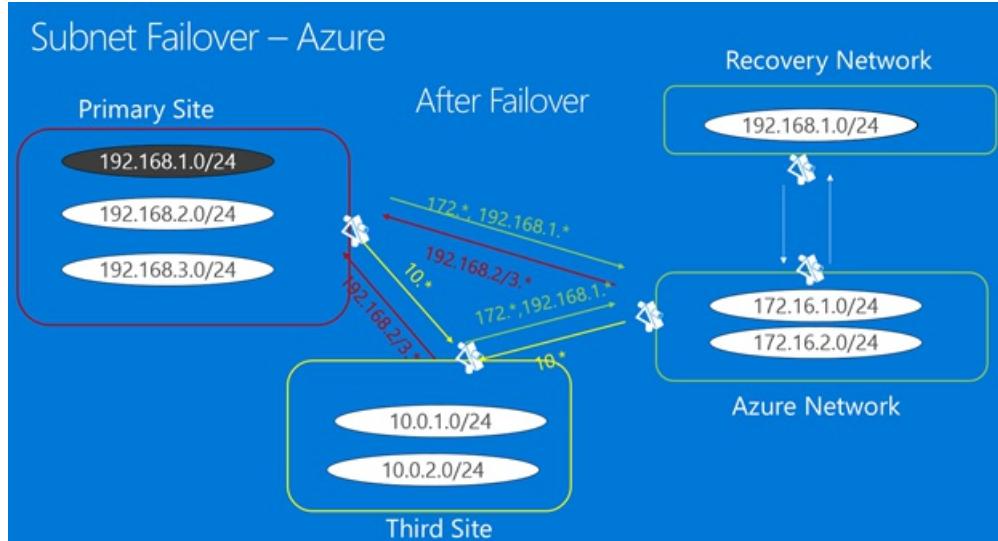
4. Before failover, on the machine properties in Site Recovery, they set the target IP address to the address of the on-premises machine, as described in the next procedure.
5. After failover, the Azure VMs are created with the same IP address. Woodgrove connects from **Azure Network** to **Recovery Network** VNet using VNet peering (with transit connectivity enabled).
6. On-premises, Woodgrove needs to make network changes, including modifying routes to reflect that 192.168.1.0/24 has moved to Azure.

#### Infrastructure before failover



#### Infrastructure after failover

## Subnet Failover – Azure



### Set target network settings

Before failover, specify the network settings and IP address for the target Azure VM.

1. In the Recovery Services vault -> **Replicated items**, select the on-premises machine.
2. In the **Compute and Network** page for the machine, click **Edit**, to configure network and adapter settings for the target Azure VM.
3. In **Network properties**, select the target network in which the Azure VM will be located when it's created after failover.
4. In **Network interfaces**, configure the network adapters in the target network. By default Site Recovery shows all detected NICs on the on-premises machine.
  - In **Target network interface type** you can set each NIC as **Primary**, **Secondary**, or **Do not create** if you don't need that specific NIC in the target network. One network adapter must be set as primary for failover. Note that modifying the target network affects all NICs for the Azure VM.
  - Click the NIC name to specify the subnet in which the Azure VM will be deployed.
  - Overwrite **Dynamic** with the private IP address you want to assign to target Azure VM. If an IP address isn't specified Site Recovery will assign the next available IP address in the subnet to the NIC at failover.
  - [Learn more](#) about managing NICs for on-premises failover to Azure.

### Get new IP addresses

In this scenario, the Azure VM gets a new IP address after failover. A DNS update to update records for failed over machines to point to the IP address of the Azure VM.

### Next steps

[Learn about](#) replicating on-premises Active Directory and DNS to Azure.

# About the Azure Site Recovery Deployment Planner for Hyper-V disaster recovery to Azure

11/12/2019 • 8 minutes to read • [Edit Online](#)

This article is the Azure Site Recovery Deployment Planner user guide for Hyper-V-to-Azure production deployments.

Before you begin protecting any Hyper-V virtual machines (VMs) using Site Recovery, allocate sufficient bandwidth based on your daily data-change rate to meet your desired Recovery Point Objective (RPO), and allocate sufficient free storage space on each volume of Hyper-V storage on-premises.

You also need to create the right type and number of target Azure storage accounts. You create either standard or premium storage accounts, factoring in growth on your source production servers because of increased usage over time. You choose the storage type per VM, based on workload characteristics, for example, read/write I/O operations per second (IOPS), or data churn, and Azure Site Recovery limits.

The Azure Site Recovery deployment planner is a command-line tool for both Hyper-V to Azure and VMware to Azure disaster recovery scenarios. You can remotely profile your Hyper-V VMs present on multiple Hyper-V hosts using this tool (with no production impact whatsoever) to understand the bandwidth and Azure storage requirements for successful replication and test failover / failover. You can run the tool without installing any Azure Site Recovery components on-premises. However, to get accurate achieved throughput results, we recommend that you run the planner on a Windows Server that has the same hardware configuration as that of one of the Hyper-V servers that you will use to enable disaster recovery protection to Azure.

The tool provides the following details:

## Compatibility assessment

- VM eligibility assessment, based on number of disks, disk size, IOPS, churn, and few VM characteristics.

## Network bandwidth need versus RPO assessment

- The estimated network bandwidth that's required for delta replication
- The throughput that Azure Site Recovery can get from on-premises to Azure
- RPO that can be achieved for a given bandwidth
- Impact on the desired RPO if lower bandwidth is provisioned.

## Azure infrastructure requirements

- The storage type (standard or premium storage account) requirement for each VM
- The total number of standard and premium storage accounts to be set up for replication
- Storage-account naming suggestions, based on Azure Storage guidance
- The storage-account placement for all VMs
- The number of Azure cores to be set up before test failover or failover on the subscription
- The Azure VM-recommended size for each on-premises VM

## On-premises infrastructure requirements

- The required free storage space on each volume of Hyper-V storage for successful initial replication and delta replication to ensure that VM replication will not cause any undesirable downtime for your production applications
- Maximum copy frequency to be set for Hyper-V replication

## Initial replication batching guidance

- Number of VM batches to be used for protection
- List of VMs in each batch
- Order in which each batch is to be protected
- Estimated time to complete initial replication of each batch

## Estimated DR cost to Azure

- Estimated total DR cost to Azure: compute, storage, network, and Azure Site Recovery license cost
- Detail cost analysis per VM

### IMPORTANT

Because usage is likely to increase over time, all the preceding tool calculations are performed assuming a 30% growth factor in workload characteristics, and using a 95th percentile value of all the profiling metrics (read/write IOPS, churn, and so forth). Both of these elements (growth factor and percentile calculation) are configurable. To learn more about growth factor, see the "Growth-factor considerations" section. To learn more about percentile value, see the "Percentile value used for the calculation" section.

## Support matrix

|                                                                                                           | VMWARE TO AZURE                                                                           | HYPER-V TO AZURE                                                                | AZURE TO AZURE | HYPER-V TO SECONDARY SITE                                                       | VMWARE TO SECONDARY SITE |
|-----------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|----------------|---------------------------------------------------------------------------------|--------------------------|
| Supported scenarios                                                                                       | Yes                                                                                       | Yes                                                                             | No             | Yes*                                                                            | No                       |
| Supported Version                                                                                         | vCenter 6.7, 6.5, 6.0 or 5.5                                                              | Windows Server 2016, Windows Server 2012 R2                                     | NA             | Windows Server 2016, Windows Server 2012 R2                                     | NA                       |
| Supported configuration                                                                                   | vCenter, ESXi                                                                             | Hyper-V cluster, Hyper-V host                                                   | NA             | Hyper-V cluster, Hyper-V host                                                   | NA                       |
| Number of servers that can be profiled per running instance of the Azure Site Recovery Deployment Planner | Single (VMs belonging to one vCenter Server or one ESXi server can be profiled at a time) | Multiple (VMs across multiple hosts or host clusters can be profiled at a time) | NA             | Multiple (VMs across multiple hosts or host clusters can be profiled at a time) | NA                       |

\*The tool is primarily for the Hyper-V to Azure disaster recovery scenario. For Hyper-V to secondary site disaster recovery, it can be used only to understand source side recommendations like required network bandwidth, required free storage space on each of the source Hyper-V servers, and initial replication batching numbers and batch definitions. Ignore the Azure recommendations and costs from the report. Also, the Get Throughput operation is not applicable for the Hyper-V to secondary site disaster recovery scenario.

## Prerequisites

The tool has three main phases for Hyper-V: get VM list, profiling, and report generation. There is also a fourth option to calculate throughput only. The requirements for the server on which the different phases need to be executed are presented in the following table:

| SERVER REQUIREMENT                                 | DESCRIPTION                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Get VM list, profiling, and throughput measurement | <ul style="list-style-type: none"> <li>Operating system: Microsoft Windows Server 2016 or Microsoft Windows Server 2012 R2</li> <li>Machine configuration: 8 vCPUs, 16 GB RAM, 300 GB HDD</li> <li><a href="#">Microsoft .NET Framework 4.5</a></li> <li><a href="#">Microsoft Visual C++ Redistributable for Visual Studio 2012</a></li> <li>Internet access to Azure from this server</li> <li>Azure storage account</li> <li>Administrator access on the server</li> <li>Minimum 100 GB of free disk space (assuming 1000 VMs with an average of three disks each, profiled for 30 days)</li> <li>The VM from where you are running the Azure Site Recovery deployment planner tool must be added to TrustedHosts list of all the Hyper-V servers.</li> <li>All Hyper-V servers to be profiled must be added to TrustedHosts list of the client VM from where the tool is being run. <a href="#">Learn more to add servers into TrustedHosts list</a>.</li> <li>The tool should be run from Administrative privileges from PowerShell or command-line console on the client</li> </ul> |
| Report generation                                  | A Windows PC or Windows Server with Microsoft Excel 2013 or later                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| User permissions                                   | <p>Administrator account to access Hyper-V cluster/Hyper-V host during get VM list and profiling operations.</p> <p>All the hosts that need to be profiled should have a domain administrator account with the same credentials i.e. user name and password</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

## Steps to add servers into TrustedHosts List

1. The VM from where the tool is to be deployed should have all the hosts to be profiled in its TrustedHosts list. To add the client into Trustedhosts list run the following command from an elevated PowerShell on the VM. The VM can be a Windows Server 2012 R2 or Windows Server 2016.

```
set-item wsman:\localhost\Client\TrustedHosts -value '<ComputerName>[,<ComputerName>]' -Concatenate
```

2. Each Hyper-V Host that needs to be profiled should have:

- a. The VM on which the tool is going to be run in its TrustedHosts list. Run the following command from an elevated PowerShell on the Hyper-V host.

```
set-item wsman:\localhost\Client\TrustedHosts -value '<ComputerName>[,<ComputerName>]' -Concatenate
```

- b. PowerShell remoting enabled.

```
Enable-PSRemoting -Force
```

## Download and extract the deployment planner tool

1. Download the latest version of the [Azure Site Recovery deployment planner](#). The tool is packaged in a .zip folder. The same tool supports both VMware to Azure and Hyper-V to Azure disaster recovery scenarios. You can use this tool for Hyper-V-to secondary site disaster recovery scenario as well but ignore the Azure infrastructure recommendation from the report.
2. Copy the .zip folder to the Windows Server on which you want to run the tool. You can run the tool on a Windows Server 2012 R2 or Windows Server 2016. The server must have network access to connect to the Hyper-V cluster or Hyper-V host that holds the VMs to be profiled. We recommend that you have the same hardware configuration of the VM, where the tool is going to run, as that of the Hyper-V server, which you want to protect. Such a configuration ensures that the achieved throughput that the tool reports matches the actual throughput that Azure Site Recovery can achieve during replication. The throughput calculation depends on available network bandwidth on the server and hardware configuration (CPU, storage, and so forth) of the server. The throughput is calculated from the server where the tool is running to Azure. If the hardware configuration of the server differs from the Hyper-V server, the achieved throughput that the tool reports will be inaccurate. The recommended configuration of the VM: 8 vCPUs, 16 GB RAM, 300 GB HDD.
3. Extract the .zip folder. The folder contains multiple files and subfolders. The executable file is ASRDeploymentPlanner.exe in the parent folder.

Example: Copy the .zip file to E:\ drive and extract it. E:\ASR Deployment Planner\_v2.3.zip

E:\ASR Deployment Planner\_v2.3\ASRDeploymentPlanner.exe

### Updating to the latest version of deployment planner

The latest updates are summarized in the Deployment Planner [version history](#).

If you have previous version of the deployment planner, do either of the following:

- If the latest version doesn't contain a profiling fix and profiling is already in progress on your current version of the planner, continue the profiling.
- If the latest version does contain a profiling fix, we recommend that you stop profiling on your current version and restart the profiling with the new version.

#### NOTE

When you start profiling with the new version, pass the same output directory path so that the tool appends profile data on the existing files. A complete set of profiled data will be used to generate the report. If you pass a different output directory, new files are created, and old profiled data is not used to generate the report.

Each new deployment planner is a cumulative update of the .zip file. You don't need to copy the newest files to the previous folder. You can create and use a new folder.

## Version history

The latest Azure Site Recovery Deployment Planner tool version is 2.5. Refer to [Azure Site Recovery Deployment Planner Version History](#) page for the fixes that are added in each update.

## Next steps

- [Run the deployment planner](#).

# Azure Site Recovery Deployment Planner Version History

10/16/2019 • 4 minutes to read • [Edit Online](#)

This article provides history of all versions of Azure Site Recovery Deployment Planner along with the fixes, known limitations in each and their release dates.

## Version 2.51

**Release Date: August 22, 2019**

**Fixes:**

- Fixed the cost recommendation issue with Deployment Planner version 2.5

## Version 2.5

**Release Date: July 29, 2019**

**Fixes:**

- For VMware virtual machines and physical machines, recommendation is updated to be based on replication to Managed Disks.
- Added support for Windows 10 (x64), Windows 8.1 (x64), Windows 8 (x64), Windows 7 (x64) SP1 or later

## Version 2.4

**Release Date: April 17, 2019**

**Fixes:**

- Improved operating system compatibility, specifically when handling localization-based errors.
- Added VMs with up to 20 Mbps of data change rate (churn) to the compatibility checklist.
- Improved error messages
- Added support for vCenter 6.7.
- Added support for Windows Server 2019 and Red Hat Enterprise Linux (RHEL) workstation.

## Version 2.3

**Release Date: December 3, 2018**

**Fixes:**

- Fixed an issue that prevented the Deployment Planner from generating a report with the provided target location and subscription.

## Version 2.2

**Release Date: April 25, 2018**

**Fixes:**

- GetVMList operations:
  - Fixed an issue that caused GetVMList to fail if the specified folder doesn't exist. It now either creates the default directory, or creates the directory specified in the outputfile parameter.
  - Added more detailed failure reasons for GetVMList.
- Added VM type information as a column in the compatible VMs sheet of the Deployment Planner report.
- Hyper-V to Azure disaster recovery:
  - Excluded VMs with shared VHDs and PassThrough disks from profiling. The Startprofiling operation shows the list of excluded VMs in the console.
  - Added VMs with more than 64 disks to the list of incompatible VMs.
  - Updated the initial replication (IR) and delta replication (DR) compression factor.
  - Added limited support for SMB storage.

## Version 2.1

**Release Date:** January 3, 2018

**Fixes:**

- Updated the Excel report.
- Fixed bugs in the GetThroughput operation.
- Added option to limit the number of VMs to profile or generate the report. The default limit is 1,000 VMs.
- VMware to Azure disaster recovery:
  - Fixed an issue of Windows Server 2016 VM going into the incompatible table.
  - Updated compatibility messages for Extensible Firmware Interface (EFI) Windows VMs.
- Updated the VMware to Azure and Hyper-V to Azure, VM data churn limit per VM.
- Improved reliability of VM list file parsing.

## Version 2.0.1

**Release Date:** December 7, 2017

**Fixes:**

- Added recommendation to optimize the network bandwidth.

## Version 2.0

**Release Date:** November 28, 2017

**Fixes:**

- Added support for Hyper-V to Azure disaster recovery.
- Added cost calculator.
- Added OS version check for VMware to Azure disaster recovery to determine if the VM is compatible or incompatible for the protection. The tool uses the OS version string that is returned by the vCenter server for that VM. It's the guest operating system version that user has selected while creating the VM in VMware.

**Known limitations:**

- For Hyper-V to Azure disaster recovery, VM with name containing the characters like: `,`, `"`, `[`, `]`, and ``` aren't supported. If profiled, report generation will fail or will have an incorrect result.
- For VMware to Azure disaster recovery, VM with name containing comma isn't supported. If profiled, report generation fails or will have an incorrect result.

## Version 1.3.1

**Release Date:** July 19, 2017

### Fixes:

- Added support for large disks (> 1 TB) in report generation. Now you can use Deployment Planner to plan replication for virtual machines that have disk sizes greater than 1 TB (up to 4095 GB). Read more about [Large disk support in Azure Site Recovery](#)

## Version 1.3

**Release Date:** May 9, 2017

### Fixes:

- Added support for managed disk in report generation. The number of VMs that can be placed to a single storage account is calculated based on if the managed disk is selected for Failover/Test Failover.

## Version 1.2

**Release Date:** April 7, 2017

### Fixes:

- Added boot type (BIOS or EFI) checks for each VM to determine if the VM is compatible or incompatible for the protection.
- Added OS type information for each virtual machine in the compatible VMs and incompatible VMs worksheets.
- Added support for GetThroughput operation for the US Government and China Microsoft Azure regions.
- Added few more prerequisite checks for vCenter and ESXi Server.
- Fixed an issue of incorrect report getting generated when locale settings are set to non-English.

## Version 1.1

**Release Date:** March 9, 2017

### Fixes:

- Fixed an issue that prevented profiling VMs when there are two or more VMs with the same name or IP address across various vCenter ESXi hosts.
- Fixed an issue that caused copy and search to be disabled for the compatible VMs and incompatible VMs worksheets.

## Version 1.0

**Release Date:** February 23, 2017

### Known limitations:

- Supports only for VMware to Azure disaster recovery scenarios. For Hyper-V to Azure disaster recovery scenarios, use the [Hyper-V capacity planner tool](#).
- Doesn't support the GetThroughput operation for the US Government and China Microsoft Azure regions.
- The tool can't profile VMs if the vCenter server has two or more VMs with the same name or IP address across various ESXi hosts. In this version, the tool skips profiling for duplicate VM names or IP addresses in the VMListFile. The workaround is to profile the VMs by using an ESXi host instead of the vCenter server.

Ensure to run one instance for each ESXi host.

# Run the Azure Site Recovery deployment planner for Hyper-V disaster recovery to Azure

11/14/2019 • 19 minutes to read • [Edit Online](#)

You can run the Site Recovery deployment planner command-line tool (ASRDeploymentPlanner.exe) in any of these four modes:

- Get the virtual machine (VM) list
- [Profile](#)
- Generate a report
- [Get throughput](#)

First, run the tool to get the list of VMs from a single or multiple Hyper-V hosts. Then run the tool in profiling mode to gather VM data churn and IOPS. Next, run the tool to generate the report to find the network bandwidth and storage requirements.

## Get the VM list for profiling Hyper-V VMs

First, you need a list of the VMs to be profiled. Use the GetVMList mode of the deployment planner tool to generate the list of VMs present on multiple Hyper-V hosts in a single command. After you generate the complete list, you can remove VMs that you don't want to profile from the output file. Then use the output file for all other operations: profiling, report generation, and getting throughput.

You can generate the VM list by pointing the tool to a Hyper-V cluster or a standalone Hyper-V host, or a combination of both.

### Command-line parameters

The following table contains a list of mandatory and optional parameters of the tool to run in GetVMList mode.

```
ASRDeploymentPlanner.exe -Operation GetVMList /?
```

| PARAMETER NAME | DESCRIPTION                                                                                                   |
|----------------|---------------------------------------------------------------------------------------------------------------|
| -Operation     | GetVMList                                                                                                     |
| -User          | The username to connect to the Hyper-V host or Hyper-V cluster. The user needs to have administrative access. |

| PARAMETER NAME  | DESCRIPTION                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -ServerListFile | The file with the list of servers that contain the VMs to be profiled. The file path can be absolute or relative. This file should contain one of the following in each line: <ul style="list-style-type: none"> <li>• Hyper-V host name or IP address</li> <li>• Hyper-V cluster name or IP address</li> </ul> <p><b>Example:</b> ServerList.txt contains the following servers:</p> <ul style="list-style-type: none"> <li>• Host_1</li> <li>• 10.8.59.27</li> <li>• Cluster_1</li> <li>• Host_2</li> </ul> |
| -Directory      | (Optional) The universal naming convention (UNC) or local directory path to store data generated during this operation. If a name is not specified, the directory named ProfiledData under the current path is used as the default directory.                                                                                                                                                                                                                                                                 |
| -OutputFile     | (Optional) The file with the list of VMs fetched from the Hyper-V servers is saved. If a name is not mentioned, the details are stored in VMList.txt. Use the file to start profiling after removing VMs that don't need to be profiled.                                                                                                                                                                                                                                                                      |
| -Password       | (Optional) The password to connect to the Hyper-V host. If you don't specify it as a parameter, you will be prompted for it when you run the command.                                                                                                                                                                                                                                                                                                                                                         |

## GetVMList discovery

- **Hyper-V cluster:** When the Hyper-V cluster name is given in the server's list file, the tool finds all the Hyper-V nodes of the cluster and gets the VMs present on each of the Hyper-V hosts. **Hyper-V host:** When the Hyper-V host name is given, the tool first checks if it belongs to a cluster. If yes, the tool fetches nodes that belong to the cluster. It then gets the VMs from each Hyper-V host.

You can also choose to list in a file the friendly names or IP addresses of the VMs that you want to profile manually.

Open the output file in Notepad, and then copy the names of all VMs that you want to profile to another file (for example, ProfileVMList.txt). Use one VM name per line. This file is used as input to the -VMListFile parameter of the tool for all other operations: profiling, report generation, and getting throughput.

## Examples

### Store the list of VMs in a file

```
ASRDeploymentPlanner.exe -Operation GetVMList -ServerListFile "E:\Hyper-V_ProfiledData\ServerList.txt" -User Hyper-VUser1 -OutputFile "E:\Hyper-V_ProfiledData\VMListFile.txt"
```

### Store the list of VMs at the default location (-Directory path)

```
ASRDeploymentPlanner.exe -Operation GetVMList -Directory "E:\Hyper-V_ProfiledData" -ServerListFile "E:\Hyper-V_ProfiledData\ServerList.txt" -User Hyper-VUser1
```

## Profile Hyper-V VMs

In profiling mode, the deployment planner tool connects to each of the Hyper-V hosts to collect performance data

about the VMs.

Profiling does not affect the performance of the production VMs because no direct connection is made to them. All performance data is collected from the Hyper-V host.

The tool queries the Hyper-V host once every 15 seconds to ensure profiling accuracy. It stores the average of every minute's performance counter data.

The tool seamlessly handles VM migration from one node to another node in the cluster and storage migration within a host.

### Getting the VM list to profile

To create a list of VMs to profile, refer to the GetVMList operation.

After you have the list of VMs to be profiled, you can run the tool in profiling mode.

### Command-line parameters

The following table lists mandatory and optional parameters of the tool to run in profiling mode. The tool is common for scenarios of moving from VMware to Azure and moving from Hyper-V to Azure. These parameters are applicable for Hyper-V.

| ASRDeploymentPlanner.exe -Operation StartProfiling /? |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PARAMETER NAME                                        | DESCRIPTION                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| -Operation                                            | StartProfiling                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| -User                                                 | The username to connect to the Hyper-V host or Hyper-V cluster. The user needs to have administrative access.                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| -VMListFile                                           | The file with the list of VMs to be profiled. The file path can be absolute or relative. For Hyper-V, this file is the output file of the GetVMList operation. If you are preparing manually, the file should contain one server name or IP address, followed by the VM name (separated by a \ per line). The VM name specified in the file should be the same as the VM name on the Hyper-V host.<br><br><b>Example:</b> VMList.txt contains the following VMs: <ul style="list-style-type: none"><li>• Host_1\VM_A</li><li>• 10.8.59.27\VM_B</li><li>• Host_2\VM_C</li></ul> |
| -NoOfMinutesToProfile                                 | The number of minutes for which profiling will run. The minimum is 30 minutes.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| -NoOfHoursToProfile                                   | The number of hours for which profiling will run.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| -NoOfDaysToProfile                                    | The number of days for which profiling will run. We recommend that you run profiling for more than 7 days. That duration helps ensure that the workload pattern in your environment over the specified period is observed and is used to provide an accurate recommendation.                                                                                                                                                                                                                                                                                                   |
| -Virtualization                                       | The virtualization type (VMware or Hyper-V).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

| PARAMETER NAME      | DESCRIPTION                                                                                                                                                                                                                                                                     |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -Directory          | (Optional) The UNC or local directory path to store profiling data generated during profiling. If a name is not specified, the directory named ProfiledData under the current path will be used as the default directory.                                                       |
| -Password           | (Optional) The password to connect to the Hyper-V host. If you don't specify it as a parameter, you will be prompted for it when you run the command.                                                                                                                           |
| -StorageAccountName | (Optional) The storage-account name that's used to find the throughput achievable for replication of data from on-premises to Azure. The tool uploads test data to this storage account to calculate throughput. The storage account must be General-purpose v1 (GPv1) type.    |
| -StorageAccountKey  | (Optional) The key that's used to access the storage account. Go to the Azure portal > <b>Storage accounts</b> > <i>storage-account name</i> > <b>Settings</b> > <b>Access Keys</b> > <b>Key1</b> (or the primary access key for a classic storage account).                    |
| -Environment        | (Optional) Your target environment for the Azure storage account. It can be one of three values: AzureCloud, AzureUSGovernment, or AzureChinaCloud. The default is AzureCloud. Use the parameter when your target region is either Azure US Government or Azure China 21Vianet. |

We recommend that you profile your VMs for more than 7 days. If churn pattern varies in a month, we recommend that you profile during the week when you see the maximum churn. The best way is to profile for 31 days, to get a better recommendation.

During the profiling period, ASRDeploymentPlanner.exe keeps running. The tool takes profiling time input in days. For a quick test of the tool or for proof of concept, you can profile for a few hours or minutes. The minimum allowed profiling time is 30 minutes.

During profiling, you can optionally pass a storage-account name and key to find the throughput that Azure Site Recovery can achieve at the time of replication from the Hyper-V server to Azure. If the storage-account name and key are not passed during profiling, the tool does not calculate achievable throughput.

You can run multiple instances of the tool for various sets of VMs. Ensure that the VM names are not repeated in any of the profiling sets. For example, let's say that you have profiled 10 VMs (VM1 through VM10). After a few days, you want to profile another 5 VMs (VM11 through VM15). You can run the tool from another command-line console for the second set of VMs (VM11 through VM15).

Ensure that the second set of VMs does not have any VM names from the first profiling instance, or that you use a different output directory for the second run. If two instances of the tool are used for profiling the same VMs and use the same output directory, the generated report will be incorrect.

By default, the tool is configured to profile and generate reports for up to 1,000 VMs. You can change the limit by changing the MaxVMsSupported key value in the ASRDeploymentPlanner.exe.config file.

```
<!-- Maximum number of VMs supported-->
<add key="MaxVmSupported" value="1000"/>
```

With the default settings, to profile (for example) 1,500 VMs, create two VMList.txt files. One has 1,000 VMs, and other has 500 VMs. Run the two instances of Azure Site Recovery deployment planner: one with VMList1.txt, and

other with VMList2.txt. You can use the same directory path to store the profiled data of both the VMList VMs.

Based on the hardware configuration (especially RAM size) of the server from where the tool is run to generate the report, the operation might fail with insufficient memory. If you have good hardware, you can change MaxVMsSupported to any higher value.

VM configurations are captured once at the beginning of the profiling operation and stored in a file called VMDetailList.xml. This information is used when the report is generated. Any change in VM configuration (for example, an increased number of cores, disks, or NICs) from the beginning to the end of profiling is not captured. If a profiled VM configuration has changed during profiling, here is the workaround to get the latest VM details when you're generating the report:

- Back up VMdetailList.xml, and delete the file from its current location.
- Pass -User and -Password arguments at the time of report generation.

The profiling command generates several files in the profiling directory. Do not delete any of the files, because doing so affects report generation.

## Examples

### Profile VMs for 30 days, and find the throughput from on-premises to Azure

```
ASRDeploymentPlanner.exe -Operation StartProfiling -Virtualization Hyper-V -Directory "E:\Hyper-V_ProfiledData" -VMListFile "E:\Hyper-V_ProfiledData\ProfileVMList1.txt" -NoOfDaysToProfile 30 -User Contoso\HyperVUser1 -StorageAccountName asrspfarm1 -StorageAccountKey Eby8vdM02xNOcqFlqUwJPLlmEt1CDXJ10UzFT50uSRZ6IFsuFq2UVErCz4I6tq/K1SZFPT0tr/KBHBeksoGMGw==
```

### Profile VMs for 15 days

```
ASRDeploymentPlanner.exe -Operation StartProfiling -Virtualization Hyper-V -Directory "E:\Hyper-V_ProfiledData" -VMListFile "E:\vCenter1_ProfiledData\ProfileVMList1.txt" -NoOfDaysToProfile 15 -User contoso\HyperVUser1
```

### Profile VMs for 60 minutes for a quick test of the tool

```
ASRDeploymentPlanner.exe -Operation StartProfiling -Virtualization Hyper-V -Directory "E:\Hyper-V_ProfiledData" -VMListFile "E:\Hyper-V_ProfiledData\ProfileVMList1.txt" -NoOfMinutesToProfile 60 -User Contoso\HyperVUser1
```

### Profile VMs for 2 hours for a proof of concept

```
ASRDeploymentPlanner.exe -Operation StartProfiling -Virtualization Hyper-V -Directory "E:\Hyper-V_ProfiledData" -VMListFile "E:\Hyper-V_ProfiledData\ProfileVMList1.txt" -NoOfHoursToProfile 2 -User Contoso\HyperVUser1
```

## Considerations for profiling

If the server that the tool is running on is rebooted or has crashed, or if you close the tool by using Ctrl+C, the profiled data is preserved. However, there is a chance of missing the last 15 minutes of profiled data. In such cases, rerun the tool in profiling mode after the server restarts.

When the storage-account name and key are passed, the tool measures the throughput at the last step of profiling. If the tool is closed before profiling is completed, the throughput is not calculated. To find the throughput before generating the report, you can run the GetThroughput operation from the command-line console. Otherwise, the generated report will not contain throughput information.

Azure Site Recovery doesn't support VMs that have iSCSI and pass-through disks. The tool can't detect and profile iSCSI and pass-through disks that are attached to VMs.

# Generate a report

The tool generates a macro-enabled Microsoft Excel file (XLSM file) as the report output. It summarizes all the deployment recommendations. The report is named DeploymentPlannerReport\_*unique numeric identifier*.xslm and placed in the specified directory.

After profiling is complete, you can run the tool in report-generation mode.

## Command-line parameters

The following table contains a list of mandatory and optional tool parameters to run in report-generation mode. The tool is common for moving from VMware to Azure and for moving from Hyper-V to Azure. The following parameters are applicable for Hyper-V.

ASRDeploymentPlanner.exe -Operation GenerateReport /?	
PARAMETER NAME	DESCRIPTION
-Operation	GenerateReport
-VMListFile	<p>The file that contains the list of profiled VMs that the report will be generated for. The file path can be absolute or relative. For Hyper-V, this file is the output file of the GetVMList operation. If you are preparing manually, the file should contain one server name or IP address, followed by the VM name (separated by a \ per line). The VM name specified in the file should be the same as the VM name on the Hyper-V host.</p> <p><b>Example:</b> VMList.txt contains the following VMs:</p> <ul style="list-style-type: none"><li>• Host_1\VM_A</li><li>• 10.8.59.27\VM_B</li><li>• Host_2\VM_C</li></ul>
-Virtualization	The virtualization type (VMware or Hyper-V).
-Directory	(Optional) The UNC or local directory path where the profiled data (files generated during profiling) is stored. This data is required for generating the report. If a name is not specified, the directory named ProfiledData under the current path will be used as the default directory.
-User	(Optional) The username to connect to the Hyper-V host or Hyper-V cluster. The user needs to have administrative access. The user and password are used to fetch the latest configuration information of the VMs (like the number of disks, number of cores, and number of NICs) to use in the report. If this value is not provided, configuration information collected during profiling is used.
-Password	(Optional) The password to connect to the Hyper-V host. If you don't specify it as a parameter, you will be prompted for it when you run the command.
-DesiredRPO	(Optional) The desired recovery point objective (RPO), in minutes. The default is 15 minutes.

PARAMETER NAME	DESCRIPTION
-Bandwidth	(Optional) The bandwidth in megabits per second. Use this parameter to calculate the RPO that can be achieved for the specified bandwidth.
-StartDate	(Optional) The start date and time in MM-DD-YYYY:HH:MM (24-hour) format. StartDate must be specified along with EndDate. When StartDate is specified, the report is generated for the profiled data that's collected between StartDate and EndDate.
-EndDate	(Optional) The end date and time in MM-DD-YYYY:HH:MM (24-hour) format. EndDate must be specified along with StartDate. When EndDate is specified, the report is generated for the profiled data that's collected between StartDate and EndDate.
-GrowthFactor	(Optional) The growth factor, expressed as a percentage. The default is 30 percent.
-UseManagedDisks	(Optional) UseManagedDisks: Yes/No. The default is Yes. The number of virtual machines that can be placed in a single storage account is calculated based on whether failover/test failover of virtual machines is done on a managed disk instead of an unmanaged disk.
-SubscriptionId	(Optional) The subscription GUID. Use this parameter to generate the cost estimation report with the latest price based on your subscription, the offer that is associated with your subscription, and your target Azure region in the specified currency.
-TargetRegion	(Optional) The Azure region where replication is targeted. Because Azure has different costs per region, to generate a report with a specific target Azure region, use this parameter. The default is WestUS2 or the last-used target region. Refer to the list of <a href="#">supported target regions</a> .
-OfferId	(Optional) The offer associated with the subscription. The default is MS-AZR-0003P (Pay-As-You-Go).
-Currency	(Optional) The currency in which cost is shown in the generated report. The default is US Dollar (\$) or the last-used currency. Refer to the list of <a href="#">supported currencies</a> .

By default, the tool is configured to profile and generate reports for up to 1,000 VMs. You can change the limit by changing the MaxVMsSupported key value in the ASRDeploymentPlanner.exe.config file.

```
<!-- Maximum number of VMs supported-->
<add key="MaxVmsSupported" value="1000"/>
```

## Examples

Generate a report with default values when the profiled data is on the local drive

```
ASRDeploymentPlanner.exe -Operation GenerateReport -virtualization Hyper-V -Directory "E:\Hyper-V_ProfiledData" -VMListFile "E:\Hyper-V_ProfiledData\ProfileVMList1.txt"
```

#### Generate a report when the profiled data is on a remote server

You should have read/write access on the remote directory.

```
ASRDeploymentPlanner.exe -Operation GenerateReport -Virtualization Hyper-V -Directory "\\\PS1-W2K12R2\Hyper-V_ProfiledData" -VMListFile "\\\PS1-W2K12R2\vCenter1_ProfiledData\ProfileVMList1.txt"
```

#### Generate a report with a specific bandwidth that you will provision for the replication

```
ASRDeploymentPlanner.exe -Operation GenerateReport -Virtualization Hyper-V -Directory "E:\Hyper-V_ProfiledData" -VMListFile "E:\Hyper-V_ProfiledData\ProfileVMList1.txt" -Bandwidth 100
```

#### Generate a report with a 5 percent growth factor instead of the default 30 percent

```
ASRDeploymentPlanner.exe -Operation GenerateReport -Virtualization Hyper-V -Directory "E:\Hyper-V_ProfiledData" -VMListFile "E:\Hyper-V_ProfiledData\ProfileVMList1.txt" -GrowthFactor 5
```

#### Generate a report with a subset of profiled data

For example, you have 30 days of profiled data and want to generate a report for only 20 days.

```
ASRDeploymentPlanner.exe -Operation GenerateReport -virtualization Hyper-V -Directory "E:\Hyper-V_ProfiledData" -VMListFile "E:\Hyper-V_ProfiledData\ProfileVMList1.txt" -StartDate 01-10-2017:12:30 -EndDate 01-19-2017:12:30
```

#### Generate a report for a 5-minute RPO

```
ASRDeploymentPlanner.exe -Operation GenerateReport -Virtualization Hyper-V -Directory "E:\Hyper-V_ProfiledData" -VMListFile "E:\Hyper-V_ProfiledData\ProfileVMList1.txt" -DesiredRPO 5
```

#### Generate a report for the South India Azure region with Indian Rupee and a specific offer ID

```
ASRDeploymentPlanner.exe -Operation GenerateReport -Virtualization Hyper-V -Directory "E:\Hyper-V_ProfiledData" -VMListFile "E:\Hyper-V_ProfiledData\ProfileVMList1.txt" -SubscriptionID 4d19f16b-3e00-4b89-a2ba-8645edf42fe5 -OfferID MS-AZR-0148P -TargetRegion southindia -Currency INR
```

#### Percentile value used for the calculation

When the tool generates a report, it defaults to the percentile value of 95 for read/write IOPS, write IOPS, and data churn. These values are collected during profiling of all the VMs. This metric ensures that the percentile spike of 100 that your VMs might see because of temporary events is not used to determine your target storage account and source bandwidth requirements. For example, a temporary event might be a backup job running once a day, a periodic database indexing or analytics report generation activity, or another short-lived, point-in-time event.

Using a percentile value of 95 gives a true picture of real workload characteristics, and it gives you the best performance when the workloads are running on Azure. We do not anticipate that you'll need to change this number. If you do change the value (to a percentile of 90, for example), you can update the configuration file ASRDeploymentPlanner.exe.config in the default folder and save it to generate a new report on the existing profiled data.

```

<add key="WriteIOPSPercentile" value="95" />
<add key="ReadWriteIOPSPercentile" value="95" />
<add key="DataChurnPercentile" value="95" />

```

## Considerations for growth factor

It's critical to account for growth in your workload characteristics, assuming a potential increase in usage over time. After protection is in place, if your workload characteristics change, you cannot switch to a different storage account for protection without disabling and re-enabling the protection.

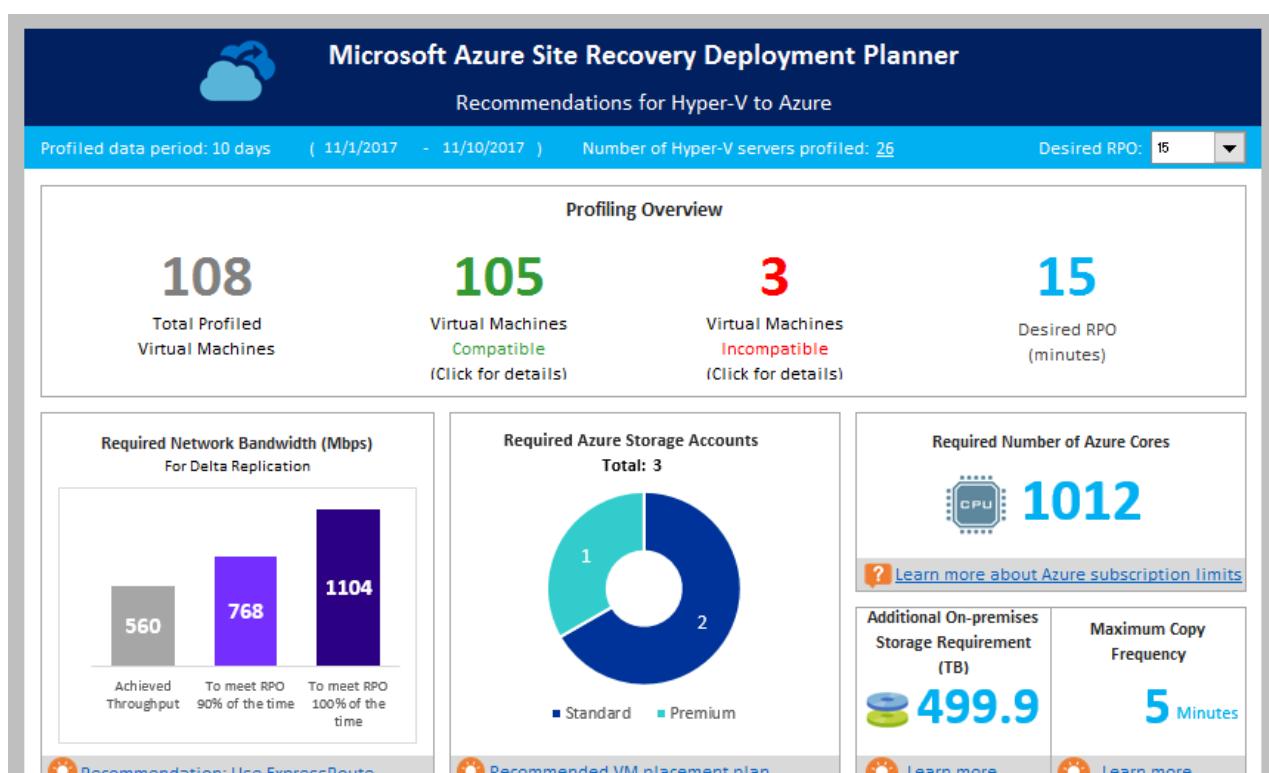
For example, let's say that today your VM fits in a standard storage replication account. Over the next three months, these changes are likely to occur:

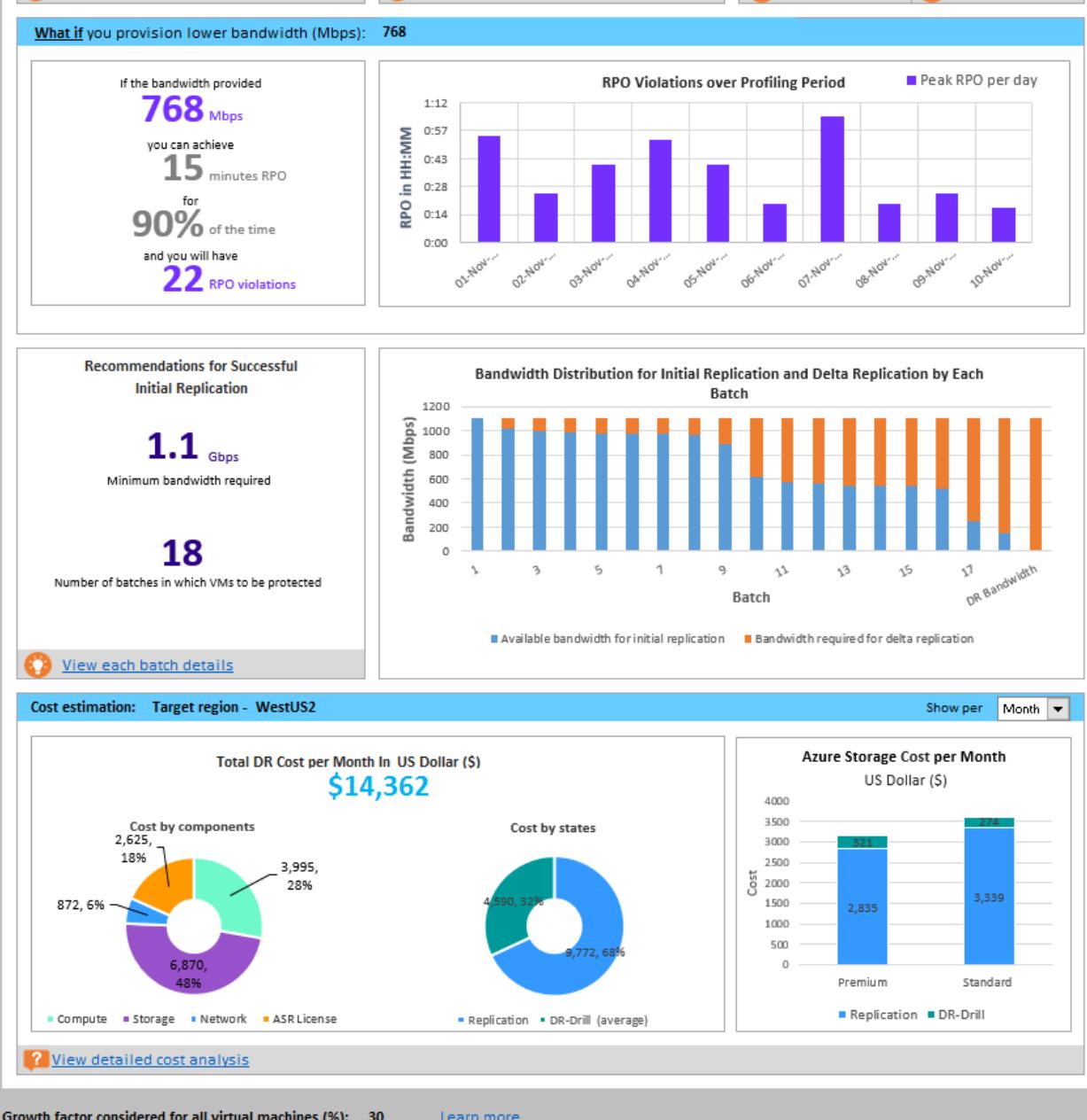
1. The number of users of the application that runs on the VM will increase.
2. The increased churn on the VM will require the VM to go to premium storage so that Azure Site Recovery replication can keep pace.
3. You will have to disable and re-enable protection to a premium storage account.

We strongly recommend that you plan for growth during deployment planning. Although the default value is 30 percent, you are the expert on your application usage pattern and growth projections. You can change this number accordingly while you're generating a report. Moreover, you can generate multiple reports with various growth factors with the same profiled data. You can then determine what target storage and source bandwidth recommendations work best for you.

The generated Microsoft Excel report contains the following information:

- On-premises summary
- Recommendations
- VM-storage placement
- Compatible VMs
- Incompatible VMs
- On-premises storage requirement
- IR batching
- Cost estimation





Growth factor considered for all virtual machines (%): 30 [Learn more](#)

Max value of IOPS and data churn of the profiled data considered for calculating bandwidth and Azure storage type: [Learn more](#)

Write IOPS percentile: 95

Read/Write IOPS percentile: 95

Data churn percentile: 95

**Note:**

- Recommended network bandwidth should be dedicated for Azure Site Recovery replication
- Desired RPO implies acceptable delay of data transfer from on-premises to Azure
- Number of RPO violations identified are spread across the total duration of profiling days and not just for one day
- There may be multiple RPO violations occurred on a day - the RPO violations graph shows the peak RPO hit every day

On-Premises Summary
**Recommendations**
VM<->Storage Placement
Compatible VMs
Incompatible VMs
...
[+](#)

## Get throughput

To estimate the throughput that Azure Site Recovery can achieve from on-premises to Azure during replication, run the tool in GetThroughput mode. The tool calculates the throughput from the server that the tool is running on. Ideally, this server is the Hyper-V server whose VMs will be protected.

### Command-line parameters

Open a command-line console and go to the folder for the Azure Site Recovery deployment planning tool. Run ASRDeploymentPlanner.exe with the following parameters.

```
ASRDeploymentPlanner.exe -Operation GetThroughput /?
```

PARAMETER NAME	DESCRIPTION
-Operation	GetThroughput
-Virtualization	The virtualization type (VMware or Hyper-V).
-Directory	(Optional) The UNC or local directory path where the profiled data (files generated during profiling) is stored. This data is required for generating the report. If a name is not specified, the directory named ProfiledData under the current path will be used as the default directory.
-StorageAccountName	The storage-account name that's used to find the bandwidth consumed for replication of data from on-premises to Azure. The tool uploads test data to this storage account to find the bandwidth consumed. The storage account must be General-purpose v1 (GPv1) type.
-StorageAccountKey	The storage-account key that's used to access the storage account. Go to the Azure portal > <b>Storage accounts</b> > <i>storage-account name</i> > <b>Settings</b> > <b>Access Keys</b> > <b>Key1</b> .
-VMListFile	The file that contains the list of VMs to be profiled for calculating the bandwidth consumed. The file path can be absolute or relative. For Hyper-V, this file is the output file of the GetVMList operation. If you are preparing manually, the file should contain one server name or IP address, followed by the VM name (separated by a \ per line). The VM name specified in the file should be the same as the VM name on the Hyper-V host.  <b>Example:</b> VMList.txt contains the following VMs: <ul style="list-style-type: none"> <li>• Host_1\VM_A</li> <li>• 10.8.59.27\VM_B</li> <li>• Host_2\VM_C</li> </ul>
-Environment	(Optional) Your target environment for the Azure storage account. It can be one of three values: AzureCloud, AzureUSGovernment, or AzureChinaCloud. The default is AzureCloud. Use the parameter when your target Azure region is either Azure US Government or Azure China 21Vianet.

## Example

```
ASRDeploymentPlanner.exe -Operation GetThroughput -Virtualization Hyper-V -Directory "E:\Hyper-V_ProfiledData"
-VMListFile "E:\Hyper-V_ProfiledData\ProfileVMList1.txt" -StorageAccountName asrspfarm1 -StorageAccountKey
by8vdM02xN0cqFlqUwJPLlmEt1CDXJ10UzFT50uSRZ6IFsuFq2UVErCz4I6tq/K1SZFPT0tr/KBHBeksoGMGw==
```

## Throughput considerations

The tool creates several 64-MB `asrvhdfilenumber.vhd` files (where *number* is the number of files) on the specified directory. The tool uploads the files to the storage account to find the throughput. After the throughput is measured, the tool deletes all the files from the storage account and from the local server. If the tool is terminated for any reason while it is calculating throughput, it doesn't delete the files from the storage account or from the

local server. You have to delete them manually.

The throughput is measured at a specified point in time. It's the maximum throughput that Azure Site Recovery can achieve during replication, if all other factors remain the same. For example, if any application starts consuming more bandwidth on the same network, the actual throughput varies during replication. The result of the measured throughput is different if the GetThroughput operation is run when the protected VMs have high data churn.

To understand what throughput levels can be achieved at various times, we recommend that you run the tool at various points in time during profiling. In the report, the tool shows the last measured throughput.

**NOTE**

Run the tool on a server that has the same storage and CPU characteristics as a Hyper-V server.

For replication, set the recommended bandwidth to meet the RPO 100 percent of the time. After you set the right bandwidth, if you don't see an increase in the achieved throughput reported by the tool, do the following:

1. Check to determine whether a network Quality of Service (QoS) problem is limiting Azure Site Recovery throughput.
2. Check to determine whether your Azure Site Recovery vault is in the nearest physically supported Microsoft Azure region to minimize network latency.
3. Check your local storage characteristics to determine whether you can improve the hardware (for example, HDD to SSD).

## Next steps

- [Analyze the generated report](#)

# Analyze the Azure Site Recovery Deployment Planner report

11/14/2019 • 23 minutes to read • [Edit Online](#)

This article discusses the sheets contained in the Excel report generated by Azure Site Recovery Deployment Planner for a Hyper-V to Azure scenario.

## On-premises summary

The on-premises summary worksheet provides an overview of the profiled Hyper-V environment.



Microsoft Azure Site Recovery Deployment Planner Report	
<b>Profiled Report for</b>	<b>Hyper-V to Azure</b>
Start date	11/1/2017
End date	11/10/2017
Total number of profiling days	10
<b>Source Environment Summary</b>	
Deployment planning recommendation has been generated based on following source environment details and desired replication inputs	
Total number of profiled virtual machines	108
Number of compatible virtual machines	105
Total number of disks across all compatible virtual machines	604
Average number of disks per compatible virtual machine	5.75
Average disk size (GB)	145
Total data to be replicated for initial replication (GB)	87,580
Desired RPO (minutes)	15
Desired bandwidth (Mbps)	NA
Observed typical data churn per day (GB)	5,087

**Start date** and **End date**: The start and end dates of the profiling data considered for report generation. By default, the start date is the date when profiling starts, and the end date is the date when profiling stops. This information can be the "StartDate" and "EndDate" values if the report is generated with these parameters.

**Total number of profiling days**: The total number of days of profiling between the start and end dates for which the report is generated.

**Number of compatible virtual machines**: The total number of compatible VMs for which the required network bandwidth, required number of storage accounts, and Azure cores are calculated.

**Total number of disks across all compatible virtual machines**: The total number of disks across all compatible VMs.

**Average number of disks per compatible virtual machine**: The average number of disks calculated across all compatible VMs.

**Average disk size (GB)**: The average disk size calculated across all compatible VMs.

**Desired RPO (minutes)**: Either the default recovery point objective or the value passed for the "DesiredRPO" parameter at the time of report generation to estimate required bandwidth.

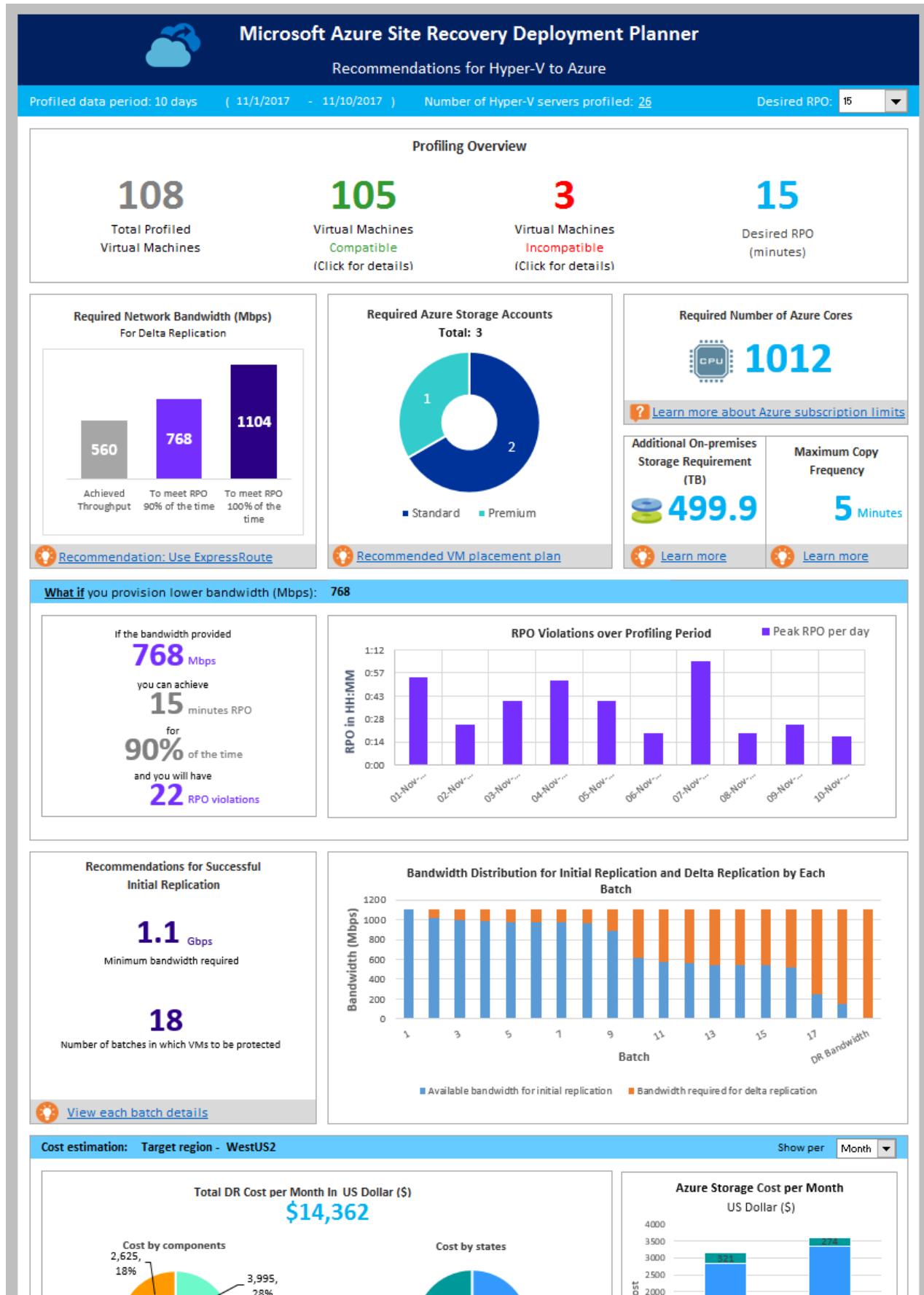
**Desired bandwidth (Mbps)**: The value that you passed for the "Bandwidth" parameter at the time of report

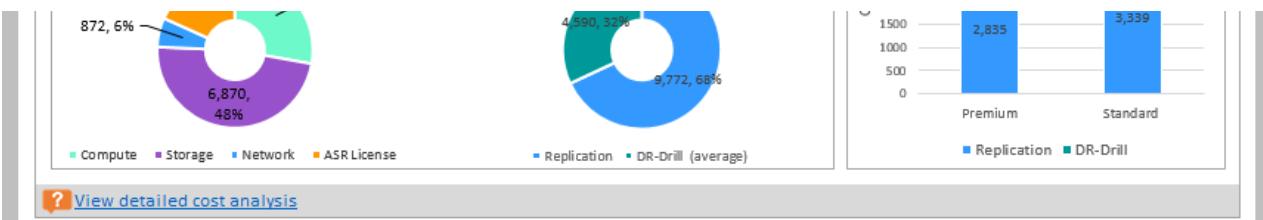
generation to estimate achievable recovery point objective (RPO).

**Observed typical data churn per day (GB):** The average data churn observed across all profiling days.

## Recommendations

The recommendations sheet of the Hyper-V to Azure report has the following details as per the selected desired RPO:





Growth factor considered for all virtual machines (%): 30 [Learn more](#)

Max value of IOPS and data churn of the profiled data considered for calculating bandwidth and Azure storage type: [Learn more](#)

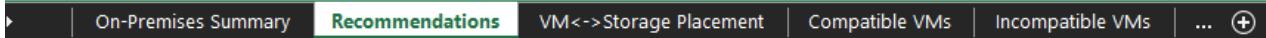
Write IOPS percentile: 95

Read/Write IOPS percentile: 95

Data churn percentile: 95

#### Note:

- Recommended network bandwidth should be dedicated for Azure Site Recovery replication
- Desired RPO implies acceptable delay of data transfer from on-premises to Azure
- Number of RPO violations identified are spread across the total duration of profiling days and not just for one day
- There may be multiple RPO violations occurred on a day - the RPO violations graph shows the peak RPO hit every day



## Profile data

**Microsoft Azure Site Recovery Deployment Planner**

Recommendations for Hyper-V to Azure

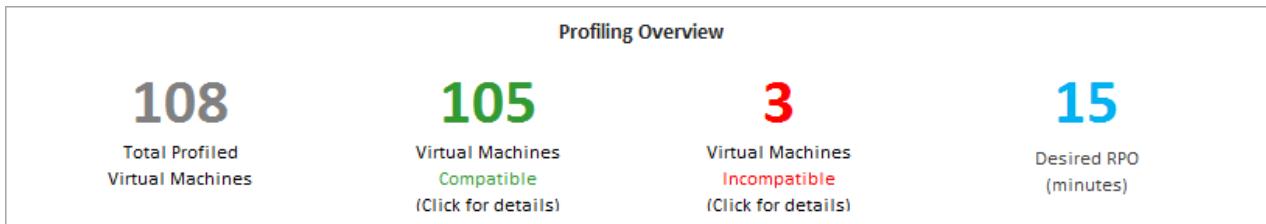
Profiled data period: 10 days ( 11/1/2017 - 11/10/2017 ) Number of Hyper-V servers profiled: 26 Desired RPO: 15

**Profiled data period:** The period during which the profiling was run. By default, the tool includes all profiled data in the calculation. If you used the StartDate and EndDate option in report generation, it generates the report for the specific period.

**Number of Hyper-V servers profiled:** The number of Hyper-V servers whose VMs' report is generated. Select the number to view the name of the Hyper-V servers. The On-premises Storage Requirement sheet opens to show all the servers along with their storage requirements.

**Desired RPO:** The recovery point objective for your deployment. By default, the required network bandwidth is calculated for RPO values of 15, 30, and 60 minutes. Based on the selection, the affected values are updated on the sheet. If you used the DesiredRPOinMin parameter while generating the report, that value is shown in the Desired RPO result.

## Profiling overview



**Total Profiled Virtual Machines:** The total number of VMs whose profiled data is available. If the VMListFile has names of any VMs that weren't profiled, those VMs aren't considered in the report generation and are excluded from the total profiled VMs count.

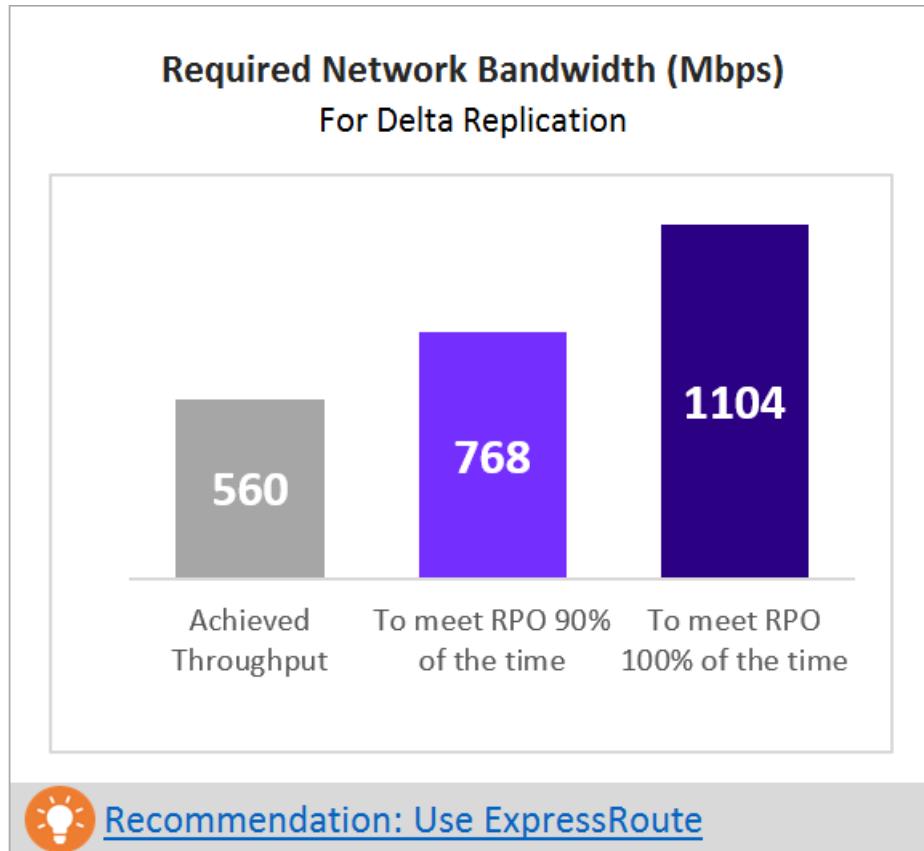
**Compatible Virtual Machines:** The number of VMs that can be protected to Azure by using Azure Site Recovery. It's the total number of compatible VMs for which the required network bandwidth, number of storage accounts, and number of Azure cores are calculated. The details of every compatible VM are available in the "Compatible VMs" section.

**Incompatible Virtual Machines:** The number of profiled VMs that are incompatible for protection with Site Recovery. The reasons for incompatibility are noted in the "Incompatible VMs" section. If the VMListFile has

names of any VMs that weren't profiled, those VMs are excluded from the incompatible VMs count. These VMs are listed as "Data not found" at the end of the "Incompatible VMs" section.

**Desired RPO:** Your desired recovery point objective, in minutes. The report is generated for three RPO values: 15 (default), 30, and 60 minutes. The bandwidth recommendation in the report is changed based on your selection in the **Desired RPO** drop-down list on the upper right of the sheet. If you generated the report by using the -DesiredRPO parameter with a custom value, this custom value shows as the default in the **Desired RPO** drop-down list.

#### Required network bandwidth (Mbps)



**To meet RPO 100% of the time:** The recommended bandwidth in Mbps to be allocated to meet your desired RPO 100 percent of the time. This amount of bandwidth must be dedicated for steady-state delta replication of all your compatible VMs to avoid any RPO violations.

**To meet RPO 90% of the time:** Perhaps because of broadband pricing or another reason you can't set the bandwidth needed to meet your desired RPO 100 percent of the time. If this is the case, you can use a lower bandwidth setting that can meet your desired RPO 90 percent of the time. To understand the implications of setting this lower bandwidth, the report provides a what-if analysis on the number and duration of RPO violations to expect.

**Achieved Throughput:** The throughput from the server on which you run the GetThroughput command to the Azure region where the storage account is located. This throughput number indicates the estimated level that you can achieve when you protect the compatible VMs by using Site Recovery. The Hyper-V server storage and network characteristics must remain the same as that of the server from which you run the tool.

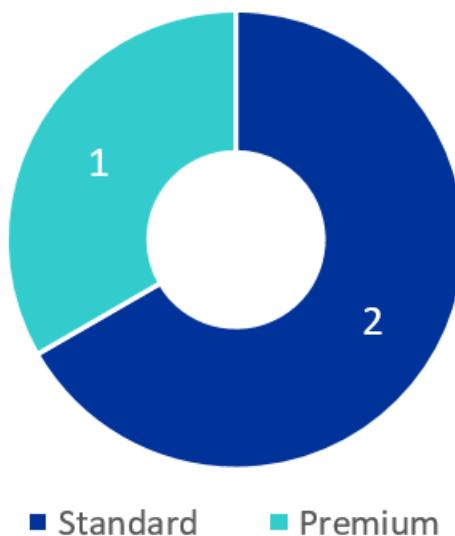
For all enterprise Site Recovery deployments, we recommend that you use [ExpressRoute](#).

#### Required storage accounts

The following chart shows the total number of storage accounts (standard and premium) that are required to protect all the compatible VMs. To learn which storage account to use for each VM, see the "VM-storage placement" section.

## Required Azure Storage Accounts

Total: 3

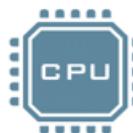


### [Recommended VM placement plan](#)

## Required number of Azure cores

This result is the total number of cores to be set up before failover or test failover of all the compatible VMs. If too few cores are available in the subscription, Site Recovery fails to create VMs at the time of test failover or failover.

## Required Number of Azure Cores



**1012**



### [Learn more about Azure subscription limits](#)

## Additional on-premises storage requirement

The total free storage required on Hyper-V servers for successful initial replication and delta replication to ensure that the VM replication doesn't cause any undesirable downtime for your production applications. More information on each volume requirement is available in [on-premises storage requirement](#).

To understand why free space is required for the replication, see the [On-premises storage requirement](#) section.

## Additional On-premises Storage Requirement (TB)

 **499.9**

## Maximum Copy Frequency

**5** Minutes



[Learn more](#)

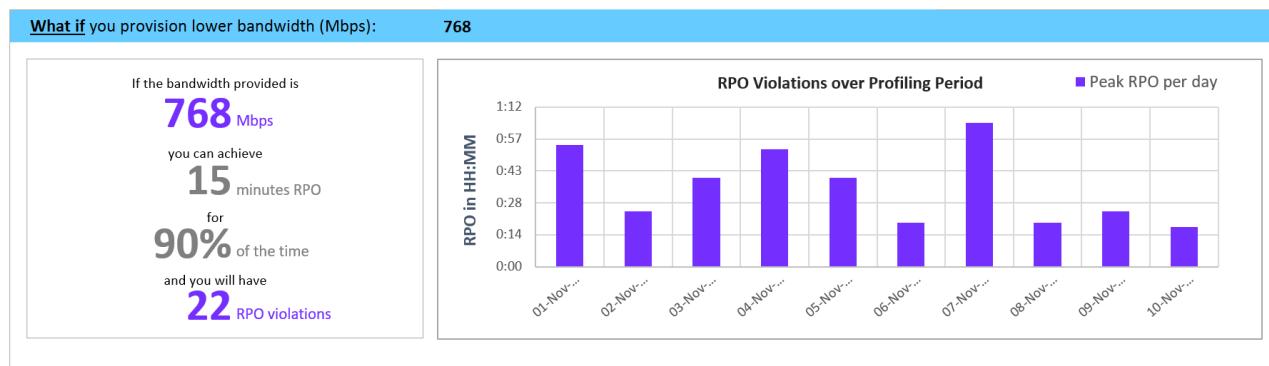


[Learn more](#)

### Maximum copy frequency

The recommended maximum copy frequency must be set for the replication to achieve the desired RPO. Default is five minutes. You can set the copy frequency to 30 seconds to achieve better RPO.

### What-if analysis



This analysis outlines how many violations might occur during the profiling period when you set a lower bandwidth for the desired RPO to be met only 90 percent of the time. One or more RPO violations can occur on any given day. The graph shows the peak RPO of the day. Based on this analysis, you can decide if the number of RPO violations across all days and peak RPO hit per day is acceptable with the specified lower bandwidth. If it's acceptable, you can allocate the lower bandwidth for replication. If it's unacceptable, allocate higher bandwidth as suggested to meet the desired RPO 100 percent of the time.

### Recommendation for successful initial replication

This section discusses the number of batches in which the VMs are to be protected and the minimum bandwidth required to finish initial replication (IR) successfully.

#### Recommendations for Successful Initial Replication

**1.1** Gbps

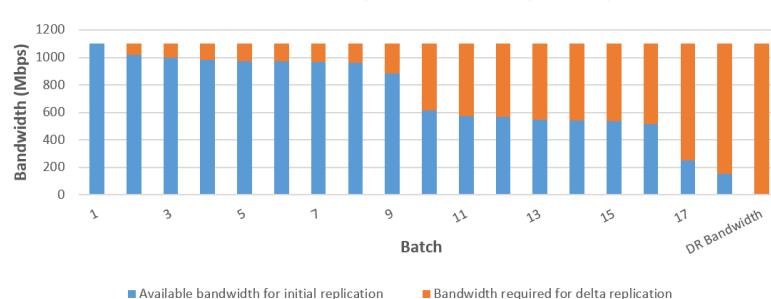
Minimum bandwidth required

**18**

Number of batches in which VMs to be protected

[View each batch details](#)

#### Bandwidth Distribution for Initial Replication and Delta Replication by Each Batch



VMs must be protected in the given batch order. Each batch has a specific list of VMs. Batch 1 VMs must be protected before Batch 2 VMs. Batch 2 VMs must be protected before Batch 3 VMs, and so on. After initial replication of the Batch 1 VMs is finished, you can enable replication for Batch 2 VMs. Similarly, after initial replication of Batch 2 VMs is finished, you can enable replication for Batch 3 VMs, and so on.

If the batch order isn't followed, sufficient bandwidth for initial replication might not be available for the VMs that

are protected later. The result is that either VMs never finish initial replication or a few protected VMs might go into resync mode. IR batching for the selected RPO sheet has the detailed information about which VMs should be included in each batch.

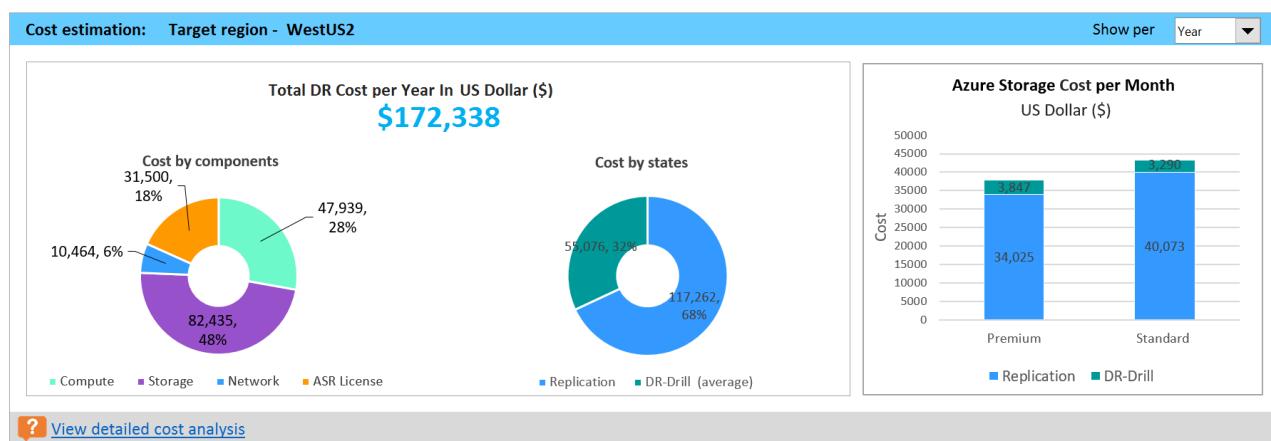
The graph here shows the bandwidth distribution for initial replication and delta replication across batches in the given batch order. When you protect the first batch of VMs, full bandwidth is available for initial replication. After initial replication is finished for the first batch, part of the bandwidth is required for delta replication. The remaining bandwidth is available for initial replication of the second batch of VMs.

The Batch 2 bar shows the required delta replication bandwidth for Batch 1 VMs and the bandwidth available for initial replication for Batch 2 VMs. Similarly, the Batch 3 bar shows the bandwidth required for delta replication for previous batches (Batch 1 and Batch 2 VMs) and the bandwidth available for initial replication for Batch 3, and so on. After initial replication of all the batches is finished, the last bar shows the bandwidth required for delta replication for all the protected VMs.

**Why do I need initial replication batching?** The completion time of the initial replication is based on the VM disk size, used disk space, and available network throughput. The detail is available in IR batching for a selected RPO sheet.

## Cost estimation

The graph shows the summary view of the estimated total disaster recovery (DR) cost to Azure of your chosen target region and the currency that you specified for report generation.



The summary helps you to understand the cost that you need to pay for storage, compute, network, and licensing when you protect all your compatible VMs to Azure by using Site Recovery. The cost is calculated for compatible VMs and not on all the profiled VMs.

You can view the cost either monthly or yearly. Learn more about [supported target regions](#) and [supported currencies](#).

**Cost by components:** The total DR cost is divided into four components: compute, storage, network, and Site Recovery license cost. The cost is calculated based on the consumption that is incurred during replication and at DR drill time. Compute, storage (premium and standard), the ExpressRoute/VPN that is configured between the on-premises site and Azure, and the Site Recovery license are used for the calculations.

**Cost by states:** The total disaster recovery cost is categorized based on two different states: replication and DR drill.

**Replication cost:** The cost that is incurred during replication. It covers the cost of storage, network, and the Site Recovery license.

**DR-Drill cost:** The cost that is incurred during test failovers. Site Recovery spins up VMs during test failover. The DR drill cost covers the running VMs' compute and storage cost.

**Azure Storage Cost per Month/Year:** The bar chart shows the total storage cost that is incurred for premium

and standard storage for replication and DR drill. You can view detailed cost analysis per VM in the [Cost Estimation](#) sheet.

### Growth factor and percentile values used

This section at the bottom of the sheet shows the percentile value used for all the performance counters of the profiled VMs (default is 95th percentile). It also shows the growth factor (default is 30 percent) that's used in all the calculations.

Growth factor considered for all virtual machines (%): 30 [Learn more](#)

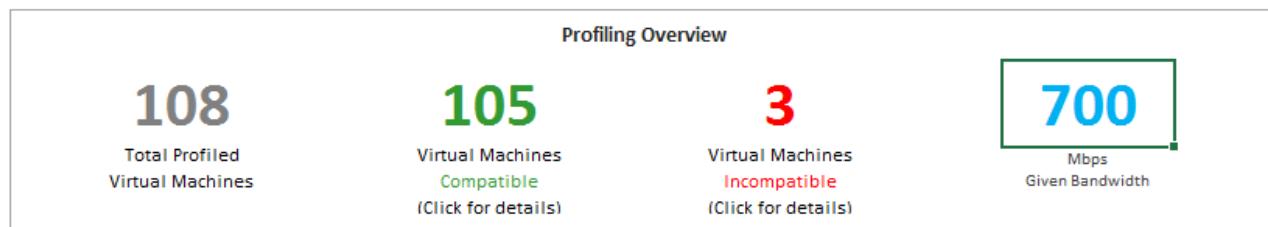
Max value of IOPS and data churn of the profiled data considered for calculating bandwidth and Azure storage type: [Learn more](#)

Write IOPS percentile:	95
Read/Write IOPS percentile:	95
Data churn percentile:	95

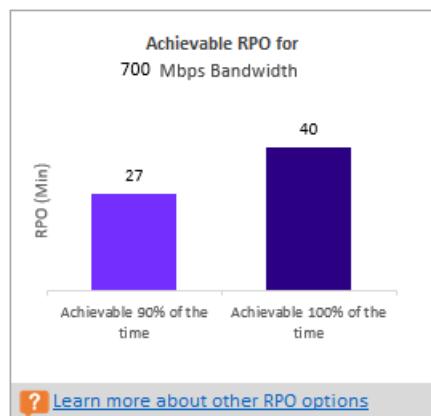
**Note:**

- Recommended network bandwidth should be dedicated for Azure Site Recovery replication
- Desired RPO implies acceptable delay of data transfer from on-premises to Azure
- Number of RPO violations identified are spread across the total duration of profiling days and not just for one day
- There may be multiple RPO violations occurred on a day - the RPO violations graph shows the peak RPO hit every day

## Recommendations with available bandwidth as input



You might have a situation where you know that you can't set a bandwidth of more than x Mbps for Site Recovery replication. You can use the tool to input available bandwidth (by using the -Bandwidth parameter during report generation) and get the achievable RPO in minutes. With this achievable RPO value, you can decide whether you need to provision additional bandwidth or you're satisfied with a disaster recovery solution with this RPO.



## VM-storage placement recommendation

Replication Storage Type	Suggested Prefix	Suggested Account Name	Log Storage Account Type	Suggested Prefix	Suggested Log Account Name	Placement Summary	VMs to Place
Premium	hlr	hlr<premium>	Standard	yni	yni<standard2>	Total number of VMs: 14 Total read/write IOPS: 13083 Total write IOPS: 12530 Total provisioned size across all disks: 28.74 TB  Total disk: 71 P10:26 P15:10 P20:14 P30:9 P40:2 P50:1	co1-01-01 (CO1-CU-SV-FR000), co1-02-01 (CO1-CU-SV-FR000), co1-03-01 (CO1-CU-SV-FR000), co1-04-01 (CO1-CU-SV-FR000), co1-05-01 (CO1-CU-SV-FR000), co1-06-01 (CO1-CU-SV-FR000), co1-07-01 (CO1-CU-SV-FR000), co1-08-01 (CO1-CU-SV-FR000), co1-09-01 (CO1-CU-SV-FR000), co1-10-01 (CO1-CU-SV-FR000), co1-11-01 (CO1-CU-SV-FR000), co1-12-01 (CO1-CU-SV-FR000), co1-13-01 (CO1-CU-SV-FR000), co1-14-01 (CO1-CU-SV-FR000), co1-15-01 (CO1-CU-SV-FR000), co1-16-01 (CO1-CU-SV-FR000), co1-17-01 (CO1-CU-SV-FR000), co1-18-01 (CO1-CU-SV-FR000), co1-19-01 (CO1-CU-SV-FR000), co1-20-01 (CO1-CU-SV-FR000), co1-21-01 (CO1-CU-SV-FR000), co1-22-01 (CO1-CU-SV-FR000), co1-23-01 (CO1-CU-SV-FR000), co1-24-01 (CO1-CU-SV-FR000), co1-25-01 (CO1-CU-SV-FR000), co1-26-01 (CO1-CU-SV-FR000), co1-27-01 (CO1-CU-SV-FR000), co1-28-01 (CO1-CU-SV-FR000), co1-29-01 (CO1-CU-SV-FR000), co1-30-01 (CO1-CU-SV-FR000), co1-31-01 (CO1-CU-SV-FR000), co1-32-01 (CO1-CU-SV-FR000), co1-33-01 (CO1-CU-SV-FR000), co1-34-01 (CO1-CU-SV-FR000), co1-35-01 (CO1-CU-SV-FR000), co1-36-01 (CO1-CU-SV-FR000), co1-37-01 (CO1-CU-SV-FR000), co1-38-01 (CO1-CU-SV-FR000), co1-39-01 (CO1-CU-SV-FR000), co1-40-01 (CO1-CU-SV-FR000), co1-41-01 (CO1-CU-SV-FR000), co1-42-01 (CO1-CU-SV-FR000), co1-43-01 (CO1-CU-SV-FR000), co1-44-01 (CO1-CU-SV-FR000), co1-45-01 (CO1-CU-SV-FR000), co1-46-01 (CO1-CU-SV-FR000), co1-47-01 (CO1-CU-SV-FR000), co1-48-01 (CO1-CU-SV-FR000), co1-49-01 (CO1-CU-SV-FR000), co1-50-01 (CO1-CU-SV-FR000), co1-51-01 (CO1-CU-SV-FR000), co1-52-01 (CO1-CU-SV-FR000), co1-53-01 (CO1-CU-SV-FR000), co1-54-01 (CO1-CU-SV-FR000), co1-55-01 (CO1-CU-SV-FR000), co1-56-01 (CO1-CU-SV-FR000), co1-57-01 (CO1-CU-SV-FR000), co1-58-01 (CO1-CU-SV-FR000), co1-59-01 (CO1-CU-SV-FR000), co1-60-01 (CO1-CU-SV-FR000), co1-61-01 (CO1-CU-SV-FR000), co1-62-01 (CO1-CU-SV-FR000), co1-63-01 (CO1-CU-SV-FR000), co1-64-01 (CO1-CU-SV-FR000), co1-65-01 (CO1-CU-SV-FR000), co1-66-01 (CO1-CU-SV-FR000), co1-67-01 (CO1-CU-SV-FR000), co1-68-01 (CO1-CU-SV-FR000), co1-69-01 (CO1-CU-SV-FR000), co1-70-01 (CO1-CU-SV-FR000), co1-71-01 (CO1-CU-SV-FR000)
Standard	xlc	xlc<standard1>	Standard	NA	NA	Total number of VMs: 91 Total read/write IOPS: 4290 Total write IOPS: 3539 Total provisioned size across all disks: 81.00 TB Total disk: 133 S4-24 S6-84 S10:130 S15:41 S20:33 S30:27 S40:3 S50:1	co1-01-01 (CO1-CU-SV-FR000), co1-02-01 (CO1-CU-SV-FR000), co1-03-01 (CO1-CU-SV-FR000), co1-04-01 (CO1-CU-SV-FR000), co1-05-01 (CO1-CU-SV-FR000), co1-06-01 (CO1-CU-SV-FR000), co1-07-01 (CO1-CU-SV-FR000), co1-08-01 (CO1-CU-SV-FR000), co1-09-01 (CO1-CU-SV-FR000), co1-10-01 (CO1-CU-SV-FR000), co1-11-01 (CO1-CU-SV-FR000), co1-12-01 (CO1-CU-SV-FR000), co1-13-01 (CO1-CU-SV-FR000), co1-14-01 (CO1-CU-SV-FR000), co1-15-01 (CO1-CU-SV-FR000), co1-16-01 (CO1-CU-SV-FR000), co1-17-01 (CO1-CU-SV-FR000), co1-18-01 (CO1-CU-SV-FR000), co1-19-01 (CO1-CU-SV-FR000), co1-20-01 (CO1-CU-SV-FR000), co1-21-01 (CO1-CU-SV-FR000), co1-22-01 (CO1-CU-SV-FR000), co1-23-01 (CO1-CU-SV-FR000), co1-24-01 (CO1-CU-SV-FR000), co1-25-01 (CO1-CU-SV-FR000), co1-26-01 (CO1-CU-SV-FR000), co1-27-01 (CO1-CU-SV-FR000), co1-28-01 (CO1-CU-SV-FR000), co1-29-01 (CO1-CU-SV-FR000), co1-30-01 (CO1-CU-SV-FR000), co1-31-01 (CO1-CU-SV-FR000), co1-32-01 (CO1-CU-SV-FR000), co1-33-01 (CO1-CU-SV-FR000), co1-34-01 (CO1-CU-SV-FR000), co1-35-01 (CO1-CU-SV-FR000), co1-36-01 (CO1-CU-SV-FR000), co1-37-01 (CO1-CU-SV-FR000), co1-38-01 (CO1-CU-SV-FR000), co1-39-01 (CO1-CU-SV-FR000), co1-40-01 (CO1-CU-SV-FR000), co1-41-01 (CO1-CU-SV-FR000), co1-42-01 (CO1-CU-SV-FR000), co1-43-01 (CO1-CU-SV-FR000), co1-44-01 (CO1-CU-SV-FR000), co1-45-01 (CO1-CU-SV-FR000), co1-46-01 (CO1-CU-SV-FR000), co1-47-01 (CO1-CU-SV-FR000), co1-48-01 (CO1-CU-SV-FR000), co1-49-01 (CO1-CU-SV-FR000), co1-50-01 (CO1-CU-SV-FR000), co1-51-01 (CO1-CU-SV-FR000), co1-52-01 (CO1-CU-SV-FR000), co1-53-01 (CO1-CU-SV-FR000), co1-54-01 (CO1-CU-SV-FR000), co1-55-01 (CO1-CU-SV-FR000), co1-56-01 (CO1-CU-SV-FR000), co1-57-01 (CO1-CU-SV-FR000), co1-58-01 (CO1-CU-SV-FR000), co1-59-01 (CO1-CU-SV-FR000), co1-60-01 (CO1-CU-SV-FR000), co1-61-01 (CO1-CU-SV-FR000), co1-62-01 (CO1-CU-SV-FR000), co1-63-01 (CO1-CU-SV-FR000), co1-64-01 (CO1-CU-SV-FR000), co1-65-01 (CO1-CU-SV-FR000), co1-66-01 (CO1-CU-SV-FR000), co1-67-01 (CO1-CU-SV-FR000), co1-68-01 (CO1-CU-SV-FR000), co1-69-01 (CO1-CU-SV-FR000), co1-70-01 (CO1-CU-SV-FR000), co1-71-01 (CO1-CU-SV-FR000)

**Disk Storage Type:** Either a standard or premium storage account, which is used to replicate all the corresponding VMs mentioned in the **VMs to Place** column.

**Suggested Prefix:** The suggested three-character prefix that can be used for naming the storage account. You can use your own prefix, but the tool's suggestion follows the [partition naming convention for storage accounts](#).

**Suggested Account Name:** The storage-account name after you include the suggested prefix. Replace the name within the angle brackets (< and >) with your custom input.

**Log Storage Account:** All the replication logs are stored in a standard storage account. For VMs that replicate to a premium storage account, set up an additional standard storage account for log storage. A single standard log-storage account can be used by multiple premium replication storage accounts. VMs that are replicated to standard storage accounts use the same storage account for logs.

**Suggested Log Account Name:** Your storage log account name after you include the suggested prefix. Replace the name within the angle brackets (< and >) with your custom input.

**Placement Summary:** A summary of the total VMs' load on the storage account at the time of replication and test failover or failover. The summary includes the:

- Total number of VMs mapped to the storage account.
  - Total read/write IOPS across all VMs being placed in this storage account.
  - Total write (replication) IOPS.
  - Total setup size across all disks.
  - Total number of disks.

**VMs to Place:** A list of all the VMs that should be placed on the given storage account for optimal performance and use.

## Compatible VMs

The Excel report generated by Site Recovery Deployment Planner provides all compatible VMs' details in the "Compatible VMs" sheet.

VM Name	VM Compatibility	Storage Type	Suggested Prefix	Storage Account	Peak R/W IOPS (with Growth Factor)	Peak Data Churn (MBps) (with Growth Factor)	Azure VM Size	Number of Disks	Disk Size (GB)	Cores	Memory (MB)	NICs	Boot Type
co1magicsql1 (CO1-CU-SV-E0001)	Yes	Premium	hr	hr>premium1>	1922	25.02	Standard_DS5_v2	8	2949	16	0	1	BIOS
C-ClusterStorage-Volume4<co1magicsql1_d.vhdx		P10			0	0.00				50			
C-ClusterStorage-Volume4<co1magicsql1_E.vhdx		P20			0	0.00				360			
C-ClusterStorage-Volume4<co1magicsql1_F.vhdx		P10			0	0.00				6			
C-ClusterStorage-Volume4<co1magicsql1_G.vhdx		P40			273	24.17				1832			
C-ClusterStorage-Volume4<co1magicsql1_H.vhdx		P10			0	0.00				51			
C-ClusterStorage-Volume4<co1magicsql1_I.vhdx		P20			1789	1.93				500			
C-ClusterStorage-Volume4<co1magicsql1_J.vhdx		P10			0	0.00				50			
c-clusterstorage-volume<co1magicsql1<co1magicsql1_vm2012r2sp0.vhdx		P10			86	1.58				100			
co1ecitweb05 (CO1-CU-SV-E0003)	Yes*	Premium	hr	hr>premium1>	1428	5.78	Standard_DS3_v2	3	652	4	0	2	BIOS
C-ClusterStorage-Volume3<co1ecitweb05_c.vhdx		P10			17	0.09				51			
C-ClusterStorage-Volume3<co1ecitweb05_CO1ECITWEB05_H.vhdx		P20			0	0.00				501			
Source disk size maps to P10 disk but workload IOPS/churn goes beyond the P10 maximum IOPS/throughput limit. It is recommended that you either increase the source disk size before VM replication or increase the target disk size after VM failover to 128 GB to 512 GB (so that the disk maps to the P20 disk size).													
C-ClusterStorage-Volume3<co1ecitweb05_vm-w2012fsp0_new.vhd		P20*			1428	5.78				100			
co1ecitweb07 (CO1-CU-SV-E0004)	Yes	Standard	xtc	xtc>standard1>	43	0.33	Standard_A3	3	652	4	0	2	BIOS
C-ClusterStorage-Volume2<co1ecitweb07_co1ecitweb07_d.vhdx		S6			12	0.09				51			
C-ClusterStorage-Volume2<co1ecitweb07_Co1ecitweb07_H.vhdx		S20			0	0.00				501			
C-ClusterStorage-Volume2<co1ecitweb07_c01ecitweb07_vhdx		S10			36	0.32				100			
co1plappsm02 (CO1-CU-SV-E0004)	Yes	Standard	xtc	xtc>standard1>	26	0.34	Standard_A2	3	200	2	0	1	BIOS
C-ClusterStorage-Volume2<co1plappsm02_c01plappsm02_C.vhdx		S10			19	0.33				100			
C-ClusterStorage-Volume2<co1plappsm02_c01plappsm02_d.vhdx		S6			8	0.05				50			

**VM Name:** The VM name that's used in the VMListFile when a report is generated. This column also lists the disks (VHDs) that are attached to the VMs. The names include the Hyper-V host names where the VMs were placed when the tool discovered them during the profiling period.

**VM Compatibility:** Values are **Yes** and **Yes\***. **Yes\*** is for instances in which the VM is a fit for [premium SSDs](#). Here, the profiled high churn or IOPS disk fits in higher premium disk size than the size mapped to the disk. The storage account decides which premium storage disk type to map a disk to, based on its size:

- <128 GB is a P10.
- 128 GB to 256 GB is a P15.
- 256 GB to 512 GB is a P20.
- 512 GB to 1,024 GB is a P30.
- 1,025 GB to 2,048 GB is a P40.
- 2,049 GB to 4,095 GB is a P50.

For example, if the workload characteristics of a disk put it in the P20 or P30 category, but the size maps it down to a lower premium storage disk type, the tool marks that VM as **Yes\***. The tool also recommends that you either change the source disk size to fit into the recommended premium storage disk type or change the target disk type post-failover.

**Storage Type:** Standard or premium.

**Suggested Prefix:** The three-character storage-account prefix.

**Storage Account:** The name that uses the suggested storage-account prefix.

**Peak R/W IOPS (with Growth Factor):** The peak workload read/write IOPS on the disk (default is 95th percentile) along with the future growth factor (default is 30 percent). The total read/write IOPS of a VM isn't always the sum of the VM's individual disks' read/write IOPS. The peak read/write IOPS of the VM are the peak of the sum of its individual disks' read/write IOPS during every minute of the profiling period.

**Peak Data Churn in MB/s (with Growth Factor):** The peak churn rate on the disk (default is 95th percentile) along with the future growth factor (default is 30 percent). The total data churn of the VM isn't always the sum of the VM's individual disks' data churn. The peak data churn of the VM is the peak of the sum of its individual disks' churn during every minute of the profiling period.

**Azure VM Size:** The ideal mapped Azure Cloud Services VM size for this on-premises VM. The mapping is based on the on-premises VM's memory, number of disks/cores/NICs, and read/write IOPS. The recommendation is always the lowest Azure VM size that matches all the on-premises VM characteristics.

**Number of Disks:** The total number of virtual machine disks (VHDs) on the VM.

**Disk Size (GB):** The total size of all disks of the VM. The tool also shows the disk size for the individual disks in the

VM.

**Cores:** The number of CPU cores on the VM.

**Memory (MB):** The RAM on the VM.

**NICs:** The number of NICs on the VM.

**Boot Type:** The boot type of the VM. It can be either BIOS or EFI.

## Incompatible VMs

The Excel report generated by the Site Recovery Deployment Planner provides all incompatible VMs' details in the "Incompatible VMs" sheet.

VM Name	VM Compatibility	Peak R/W IOPS (with Growth Factor)	Peak Data Churn (MBps) (with Growth Factor)	Number of Disks	Disk Size (GB)	Cores	Memory (MB)	NICs	Boot Type
co1mpagent03 (CO1-CU-SV-EE002)	No	16	0.30	2	5220	4	0	1	BIOS
C:\ClusterStorage\Volume1\co1mpagent03.co1mpagent03_C.vhdx		16	0.30		100				
C:\ClusterStorage\Volume1\co1mpagent03.co1mpagent03_d.vhdx	Not Supported (Disk size > 4095 GB)	0	0.00		5120				
co1vellumsql10 (CO1-CU-SV-EC007)	No	64	0.87	12	50283	32	0	2	BIOS
C:\ClusterStorage\Volume4\co1vellumsql10\co1vellumsql10_d.vhdx		8	0.06		101				
C:\ClusterStorage\Volume4\co1vellumsql10\co1vellumsql10_disk_1.M.vhdx	Not Supported (Disk size > 4095 GB)	0	0.00		4098				
C:\ClusterStorage\Volume4\co1vellumsql10\co1vellumsql10_disk_2.vhdx	Not Supported (Disk size > 4095 GB)	0	0.00		10240				
C:\ClusterStorage\Volume4\co1vellumsql10\co1vellumsql10_disk_3.vhdx	Not Supported (Disk size > 4095 GB)	0	0.00		5120				
C:\ClusterStorage\Volume4\co1vellumsql10\co1vellumsql10_disk_Lvhdx		0	0.00		4096				
C:\ClusterStorage\Volume4\co1vellumsql10\co1vellumsql10_e.vhdx	Not Supported (Disk size > 4095 GB)	0	0.00		8192				
C:\ClusterStorage\Volume4\co1vellumsql10\co1vellumsql10_h.vhdx	Not Supported (Disk size > 4095 GB)	3	0.01		5120				
C:\ClusterStorage\Volume4\co1vellumsql10\co1vellumsql10_j.vhdx	Not Supported (Disk size > 4095 GB)	0	0.00		4096				
C:\ClusterStorage\Volume4\co1vellumsql10\co1vellumsql10_o.vhdx	Not Supported (Disk size > 4095 GB)	0	0.00		4096				
C:\ClusterStorage\Volume4\co1vellumsql10\co1vellumsql10_t.vhdx	Not Supported (Disk size > 4095 GB)	0	0.00		4096				
C:\ClusterStorage\Volume4\co1vellumsql10\co1vellumsql10_v.vhdx		0	0.00		1024				
C:\ClusterStorage\Volume4\co1vellumsql10\vm-w2012fsp0.vhd		62	0.85		100				
co1ecitweb15 (CO1-CU-SV-E8001)	No	2307	9.18	3	620	4	0	2	BIOS
C:\ClusterStorage\Volume3\CO1ECITWEB15-co1ecitweb15.vhd	Not supported (Average effective write IOPS exceeds supported ASR IOPS limit (840) for disk)	2304	9.18		100				
C:\ClusterStorage\Volume3\CO1ECITWEB15-co1ecitweb15_d.vhdx		10	0.08		20				
C:\ClusterStorage\Volume3\CO1ECITWEB15-CO1ECITWEB15_disk_1.vhdx		0	0.00		500				

**VM Name:** The VM name that's used in the VMListFile when a report is generated. This column also lists the disks (VHDs) that are attached to the VMs. The names include the Hyper-V host names where the VMs were placed when the tool discovered them during the profiling period.

**VM Compatibility:** Indicates why the given VM is incompatible for use with Site Recovery. The reasons are described for each incompatible disk of the VM and, based on published [storage limits](#), can be any of the following:

- Disk size is greater than 4,095 GB. Azure Storage currently doesn't support data disk sizes greater than 4,095 GB.
- OS disk is greater than 2,047 GB for generation 1 (BIOS boot type) VM. Site Recovery doesn't support OS disk size greater than 2,047 GB for generation 1 VMs.
- OS disk is greater than 300 GB for generation 2 (EFI boot type) VM. Site Recovery doesn't support OS disk size greater than 300 GB for generation 2 VMs.
- A VM name isn't supported with any of the following characters: "" [] ` . The tool can't get profiled data for VMs that have any of these characters in their names.
- A VHD is shared by two or more VMs. Azure doesn't support VMs with a shared VHD.
- A VM with Virtual Fiber Channel isn't supported. Site Recovery doesn't support VMs with Virtual Fiber Channel.
- A Hyper-V cluster doesn't contain a replication broker. Site Recovery doesn't support a VM in a Hyper-V cluster if the Hyper-V Replica Broker isn't configured for the cluster.
- A VM isn't highly available. Site Recovery doesn't support a VM of a Hyper-V cluster node whose VHDs are stored on the local disk instead of on the cluster disk.
- Total VM size (replication + test failover) exceeds the supported premium storage-account size limit (35 TB). This incompatibility usually occurs when a single disk in the VM has a performance characteristic that exceeds the maximum supported Azure or Site Recovery limits for standard storage. Such an instance pushes the VM into the premium storage zone. However, the maximum supported size of a premium

storage account is 35 TB. A single protected VM can't be protected across multiple storage accounts.

When a test failover executes on a protected VM and if an unmanaged disk is configured for test failover, it runs in the same storage account where replication is progressing. In this instance, the additional same amount of storage space is required as that of replication. It ensures replication to progress and test failover to succeed in parallel. When a managed disk is configured for test failover, no additional space needs to be accounted for with the test failover VM.

- Source IOPS exceeds the supported storage IOPS limit of 7,500 per disk.
- Source IOPS exceeds the supported storage IOPS limit of 80,000 per VM.
- Source VM average data churn exceeds the supported Site Recovery data churn limit of 20 MB/s for average I/O size.
- Source VM average effective write IOPS exceeds the supported Site Recovery IOPS limit of 840.
- Calculated snapshot storage exceeds the supported snapshot storage limit of 10 TB.

**Peak R/W IOPS (with Growth Factor):** The peak workload IOPS on the disk (default is 95th percentile) along with the future growth factor (default is 30 percent). The total read/write IOPS of the VM isn't always the sum of the VM's individual disks' read/write IOPS. The peak read/write IOPS of the VM is the peak of the sum of its individual disks' read/write IOPS during every minute of the profiling period.

**Peak Data Churn (MB/s) (with Growth Factor):** The peak churn rate on the disk (default is 95th percentile) along with the future growth factor (default is 30 percent). Note that the total data churn of the VM isn't always the sum of the VM's individual disks' data churn. The peak data churn of the VM is the peak of the sum of its individual disks' churn during every minute of the profiling period.

**Number of Disks:** The total number of VHDs on the VM.

**Disk Size (GB):** The total setup size of all disks of the VM. The tool also shows the disk size for the individual disks in the VM.

**Cores:** The number of CPU cores on the VM.

**Memory (MB):** The amount of RAM on the VM.

**NICs:** The number of NICs on the VM.

**Boot Type:** The boot type of the VM. It can be either BIOS or EFI.

## Azure Site Recovery limits

The following table provides the Site Recovery limits. These limits are based on tests, but they can't cover all possible application I/O combinations. Actual results can vary based on your application I/O mix. For best results, even after deployment planning, perform extensive application testing by issuing a test failover to get the true performance picture of the application.

REPLICATION STORAGE TARGET	SOURCE VM AVERAGE I/O SIZE	SOURCE VM AVERAGE DATA CHURN	TOTAL SOURCE VM DATA CHURN PER DAY
Standard storage	8 KB	2 MB/s per VM	168 GB per VM
Premium storage	8 KB	5 MB/s per VM	421 GB per VM
Premium storage	16 KB or higher	20 MB/s per VM	1684 GB per VM

These limits are average numbers assuming a 30 percent I/O overlap. Site Recovery is capable of handling higher

throughput based on overlap ratio, larger write sizes, and actual workload I/O behavior. The preceding numbers assume a typical backlog of approximately five minutes. That is, after data is uploaded, it's processed and a recovery point is created within five minutes.

## On-premises storage requirement

The worksheet provides the total free storage space requirement for each volume of the Hyper-V servers (where VHDs reside) for successful initial replication and delta replication. Before you enable replication, add required storage space on the volumes to ensure that the replication doesn't cause any undesirable downtime of your production applications.

Site Recovery Deployment Planner identifies the optimal storage space requirement based on the VHD's size and the network bandwidth used for replication.



## Microsoft Azure Site Recovery Deployment Planner

Additional storage requirement for on-premises Hyper-V server

Following table shows the storage required on each volume for successful initial replication and delta replication to ensure that the replication will not cause any undesirable downtime for your production applications

[Learn more about additional on-premises storage space requirement](#)

Additional storage requirement on each Hyper-V host for successful replication				
Hyper-V host	Volume (VHD path)	Free space available (GB)	Total storage space required on the volume (GB)	Total additional storage to be provisioned on the volume for successful replication (GB)
CO1-CU-SV-EB001 CO1-CU-SV-EB002 CO1-CU-SV-EB003 CO1-CU-SV-EB004 CO1-CU-SV-EB005 CO1-CU-SV-EB006 CO1-CU-SV-EB007 CO1-CU-SV-EB008	C-ClusterStorage-DedicatedStandard_CSv7_1407_0BEE	1875.14	2199	324
	C-ClusterStorage-Volume1	23441.93	1595	0
	C-ClusterStorage-Volume2	32668.83	8105.5	0
	C-ClusterStorage-Volume3	35315.98	9932.5	0
	C-ClusterStorage-Volume4	39001.14	5054	0
	C-ClusterStorage-Volume5	28359.98	1822	0
	C-ClusterStorage-Volume6	922.26	3846	2,924
	C:	24.46	300	276
	C:	31.69	4299	4,267
CO1-CU-SV-EC001	C:	28.89	52644	52,615
CO1-CU-SV-EC001 CO1-CU-SV-EC002 CO1-CU-SV-EC003 CO1-CU-SV-EC004 CO1-CU-SV-EC005 CO1-CU-SV-EC006 CO1-CU-SV-EC007 CO1-CU-SV-EC008	C-ClusterStorage-DedicatedStandardPlus_CSv1_1237_00090	13232.56	79113	65,880
	C-ClusterStorage-SharedStandardPlus_CSv2_1237_000A6	30224.49	79113	48,889
	C-ClusterStorage-SharedStandardPlus_CSv3_1237_010D	19499.06	105386	85,887
	C-ClusterStorage-volume2	33306.85	105386	72,079
	C-ClusterStorage-Volume4	11486.19	52742	41,256
	C-ClusterStorage-Volume5	43198.25	7408	0
	C:	18.22	52742	52,724
	C:	28.29	26273	26,245
	C:	25.66	10557	10,531
CO1-CU-SV-ED002 CO1-CU-SV-ED003 CO1-CU-SV-ED004 CO1-CU-SV-ED005 CO1-CU-SV-ED006 CO1-CU-SV-ED007 CO1-CU-SV-ED008	C-ClusterStorage-SharedHighPerf_CSv1_0360_0003	15126.88	36036.5	20,910
	C-ClusterStorage-Volume1	43214.07	16285.5	0
	C-ClusterStorage-Volume2	38061.88	16297.5	0
	C-ClusterStorage-Volume4	41217.33	7681.5	0
	C-ClusterStorage-Volume5	36878.18	16296	0
	C:	18.45	10557	10,539
	C:	30.35	10865	10,835
	C:	31.76	2949	2,917
	C-ClusterStorage-Volume1	46275.67	4712	0
CO1-CU-SV-EE002 CO1-CU-SV-EE003 CO1-CU-SV-EE004 CO1-CU-SV-EE005	C-ClusterStorage-Volume2	31216.22	9786.5	0
	C-ClusterStorage-Volume3	35059.27	1909.5	0
	C-ClusterStorage-Volume4	43809.86	6920	0
	C:	32.95	2691.5	2,659
	C:	29.62	200	170
CO1-CU-SV-GA001 CO1-CU-SV-GA002 CO1-CU-SV-GA003 CO1-CU-SV-GA004 CO1-CU-SV-GA005 CO1-CU-SV-GA006 CO1-CU-SV-GA007 CO1-CU-SV-GA008	C-ClusterStorage-SharedStandardPlus_CSv1_1640_0105	34584.97	13102	0
<b>Total additional storage to be provisioned (GB)</b>				<b>511,925</b>

### Why do I need free space on the Hyper-V server for the replication?

- When you enable replication of a VM, Site Recovery takes a snapshot of each VHD of the VM for initial replication. While initial replication is going on, new changes are written to the disks by the application. Site Recovery tracks these delta changes in the log files, which require additional storage space. Until initial replication is finished, the log files are stored locally.

If sufficient space isn't available for the log files and snapshot (AVHDX), replication goes into resynchronization mode and replication is never finished. In the worst case, you need 100 percent additional

free space of the VHD size for initial replication.

- After initial replication is finished, delta replication starts. Site Recovery tracks these delta changes in the log files, which are stored on the volume where the VHDs of the VM reside. These log files get replicated to Azure at a configured copy frequency. Based on the available network bandwidth, the log files take some time to get replicated to Azure.

If sufficient free space isn't available to store the log files, replication is paused. Then the replication status of the VM goes into "resynchronization required."

- If network bandwidth isn't enough to push the log files into Azure, the log files get piled up on the volume. In a worst-case scenario, when the log files' size is increased to 50 percent of the VHD size, the replication of the VM goes into "resynchronization required." In the worst case, you need 50 percent additional free space of the VHD size for delta replication.

**Hyper-V host:** The list of profiled Hyper-V servers. If a server is part of a Hyper-V cluster, all the cluster nodes are grouped together.

**Volume (VHD path):** Each volume of a Hyper-V host where VHDs/VHDXs are present.

**Free space available (GB):** The free space available on the volume.

**Total storage space required on the volume (GB):** The total free storage space required on the volume for successful initial replication and delta replication.

**Total additional storage to be provisioned on the volume for successful replication (GB):** It recommends the total additional space that must be provisioned on the volume for successful initial replication and delta replication.

## Initial replication batching

### Why do I need initial replication batching?

If all the VMs are protected at the same time, the free storage requirement is much higher. If enough storage isn't available, the replication of the VMs goes into resynchronization mode. Also, the network bandwidth requirement is much higher to finish initial replication of all VMs together successfully.

### Initial replication batching for a selected RPO

This worksheet provides the detail view of each batch for IR. For each RPO, a separate IR batching sheet is created.

After you followed the on-premises storage requirement recommendation for each volume, the main information that you need to replicate is the list of VMs that can be protected in parallel. These VMs are grouped together in a batch, and there can be multiple batches. Protect the VMs in the given batch order. First protect Batch 1 VMs. After initial replication is finished, protect Batch 2 VMs, and so on. You can get the list of batches and corresponding VMs from this sheet.

Microsoft Azure Site Recovery Deployment Planner											
Initial Replication (IR) batching guidance for Hyper-V to Azure											
Protect Hyper-V virtual machines in the given batches and in the given order as suggested in this page to ensure that the replication will not cause any undesirable downtime for your production applications											
<a href="#">Learn more about initial replication batching for Hyper-V to Azure</a>											
Summary											
[A] Minimum bandwidth required for successful initial replication and delta replication of all VMs in the given batch order (Mbps)				1104							
[B] Number of batches in which VMs need to be protected as given below				30							
Batch 1 (Number of VMs: 17)			Storage requirements								
Hyper-V host	Virtual Machine	Comments	Volume (VHD path)	Free space available on the volume (GB)	Storage required on the volume for initial replication (GB)	Storage required on the volume for delta replication (GB)	Additional storage required based on deficit to avoid replication failure (GB)	Minimum bandwidth required for initial replication (Mbps)	Minimum bandwidth required for delta replication (Mbps)		
CO1-CU-SV-EB001	mssx01		C:\ClusterStorage\Volume5	28,360	1,822	911	0	0.11	6.18		
CO1-CU-SV-EB004	co1s1u1407	Add additional storage to protect this VM	C:	24	300	150	276	0.32	35.21		
CO1-CU-SV-EB005	test-offsite02		C:\ClusterStorage\Volume3	35,316	300	150	0	0.00	0.52		
CO1-CU-SV-EB006	co1vmbg1tco0e02		C:\ClusterStorage\Volume6	922	121	61	0	0.30	16.78		
CO1-CU-SV-EB007	mssx01	Add additional storage to protect this VM	C:	32	4,299	2,150	4,267	0.23	66.14		
CO1-CU-SV-EB008	co1nps-sgrp-01		C:\ClusterStorage\Volume1	39,001	250	125	0	0.03	4.82		
CO1-CU-SV-EB008	co1gptrvsn01		C:\ClusterStorage\Volume2	32,669	1,001	501	0	0.06	3.09		
CO1-CU-SV-EC001	co1scnrvqxp01a	Add additional storage to protect this VM	C:\ClusterStorage\Volume2	33,307	52,742	26,371	19,435				
			C:\ClusterStorage\SharedStandardPlus_CSV2_1237_00046	29	52,742	26,371	52,713				
			C:\ClusterStorage\DedicatedStandardPlus_CSV1_1237_00090	30,224	52,742	26,371	22,518				
			C:\ClusterStorage\SharedStandardPlus_CSV2_1237_010	13,233	52,742	26,371	39,509				
			C:\ClusterStorage\SharedStandardPlus_CSV1_1237_010	19,499	52,742	26,371	33,243	0.47	12.29		
			C:\ClusterStorage\Volume3	43,198	7,408	3,704	0	0.26	26.71		
CO1-CU-SV-EC005	co1converge001		C:\ClusterStorage\Volume1	41,217	10,557	5,279	0	0.16	37.42		
CO1-CU-SV-ED001	co1-sfsq-07	Add additional storage to protect this VM	C:	26	10,557	5,279	10,531				
CO1-CU-SV-ED004	co1-sfsq-03	Add additional storage to protect this VM	C:\ClusterStorage\Volume2	38,062	10,865	5,433	0	0.11	10.70		
CO1-CU-SV-ED004	co1-sfsq-03	Add additional storage to protect this VM	C:	30	10,865	5,433	10,835				
CO1-CU-SV-ED006	co1-sfsq-02		C:\ClusterStorage\Volume1	43,214	10,857	5,429	0	0.11	10.70		
CO1-CU-SV-EE002	co1-corp-a-01		C:\ClusterStorage\SharedHighPerf_CSV1_0360_0003	15,127	10,857	5,429	0	0.08	5.84		
CO1-CU-SV-EE003	co1pdmuets01		C:\ClusterStorage\Volume2	31,216	5,037	2,519	0	0.02	3.44		
CO1-CU-SV-EE004	co1etprodwe02		C:\ClusterStorage\Volume3	35,059	2,619	1,310	0	0.93	57.15		
CO1-CU-SV-EE005	co1-dsake-03		C:\ClusterStorage\Volume1	46,276	250	125	0	0.01	15.92		
CO1-CU-SV-GA001	co1vmfseddt01		C:\ClusterStorage\SharedStandardPlus_CSV1_1640_0105	34,585	13,102	6,551	0	0.03	5.39		
Network Utilization Details for Batch 1			Storage requirements						Bandwidth requirements		
Bandwidth available for batch 1 (Mbps)	1,104.00										
Approximate bandwidth available for initial replication of batch 1 (Mbps)	1,104.00										
Approximate bandwidth consumed for delta replication upto batch 1 (Mbps)	87.37										
Estimated initial replication time for batch 1 (HH:MM)	22:51										
Batch 2 (Number of VMs: 10)			Storage requirements						Bandwidth requirements		
Hyper-V host	Virtual Machine	Comments	Volume (VHD path)	Free space available on the volume (GB)	Storage required on the volume for initial replication (GB)	Storage required on the volume for delta replication (GB)	Additional storage required based on deficit to avoid replication failure (GB)	Minimum bandwidth required for initial replication (Mbps)	Minimum bandwidth required for delta replication (Mbps)		
CO1-CU-SV-EB002	co1ofsf0101		C:\ClusterStorage\Volume4	58,876	615	308	0	0.25	6.54		
CO1-CU-SV-EB002	co1dssq010	Add additional storage to protect this VM	C:\ClusterStorage\Volume5	862	2,102	1,051	1,240	0.22	25.52		
CO1-CU-SV-EB004	co1ectheweb1		C:\ClusterStorage\Volume3	53,356	650	325	0	0.01	3.10		
CO1-CU-SV-EB004	co1ppamps02		C:\ClusterStorage\Volume2	31,558	200	100	0	0.05	5.94		
CO1-CU-SV-EC007	co1cesqj09	Add additional storage to protect this VM	C:\ClusterStorage\Volume2	4,516	26,273	13,137	19,337				
			C:	28	26,273	13,137	26,245				
Each batch provides the following information											
<b>Hyper-V host:</b> The Hyper-V host of the VM to be protected.											
<b>Virtual Machine:</b> The VM to be protected.											
<b>Comments:</b> If any action is required for a specific volume of a VM, the comment is provided here. For example, if sufficient free space isn't available on a volume, the comment says, "Add additional storage to protect this VM."											
<b>Volume (VHD path):</b> The volume name where the VM's VHDs reside.											
<b>Free space available on the volume (GB):</b> The free disk space available on the volume for the VM. While calculating available free space on the volumes, it considers the disk space used for delta replication by the VMs of the previous batches whose VHDs are on the same volume.											
For example, VM1, VM2, and VM3 reside on a volume, say, E:\VHDpath. Before replication, free space on the volume is 500 GB. VM1 is part of Batch 1, VM2 is part of Batch 2, and VM3 is part of Batch3. For VM1, the free space available is 500 GB. For VM2, the free space available is 500 – disk space required for delta replication for VM1. If VM1 requires 300 GB space for delta replication, the free space available for VM2 is 500 GB – 300 GB = 200 GB. Similarly, VM2 requires 300 GB for delta replication. The free space available for VM3 is 200 GB - 300 GB = -100 GB.											
<b>Storage required on the volume for initial replication (GB):</b> The free storage space required on the volume for the VM for initial replication.											
<b>Storage required on the volume for delta replication (GB):</b> The free storage space required on the volume for the VM for delta replication.											
<b>Additional storage required based on deficit to avoid replication failure (GB):</b> The additional storage space											

**Storage required on the volume for initial replication (GB):** The free storage space required on the volume for the VM for initial replication.

**Storage required on the volume for delta replication (GB):** The free storage space required on the volume for the VM for delta replication.

**Additional storage required based on deficit to avoid replication failure (GB):** The additional storage space

required on the volume for the VM. It's the max of initial replication and delta replication storage space requirement minus the free space available on the volume.

**Minimum bandwidth required for initial replication (Mbps):** The minimum bandwidth required for initial replication for the VM.

**Minimum bandwidth required for delta replication (Mbps):** The minimum bandwidth required for delta replication for the VM.

#### **Network utilization details for each batch**

Each batch table provides a summary of network utilization of the batch.

**Bandwidth available for batch:** The bandwidth available for the batch after considering the previous batch's delta replication bandwidth.

**Approximate bandwidth available for initial replication of batch:** The bandwidth available for initial replication of the VMs of the batch.

**Approximate bandwidth consumed for delta replication of batch:** The bandwidth needed for delta replication of the VMs of the batch.

**Estimated initial replication time for batch (HH:MM):** The estimated initial replication time in Hours:Minutes.

## Next steps

Learn more about [cost estimation](#).

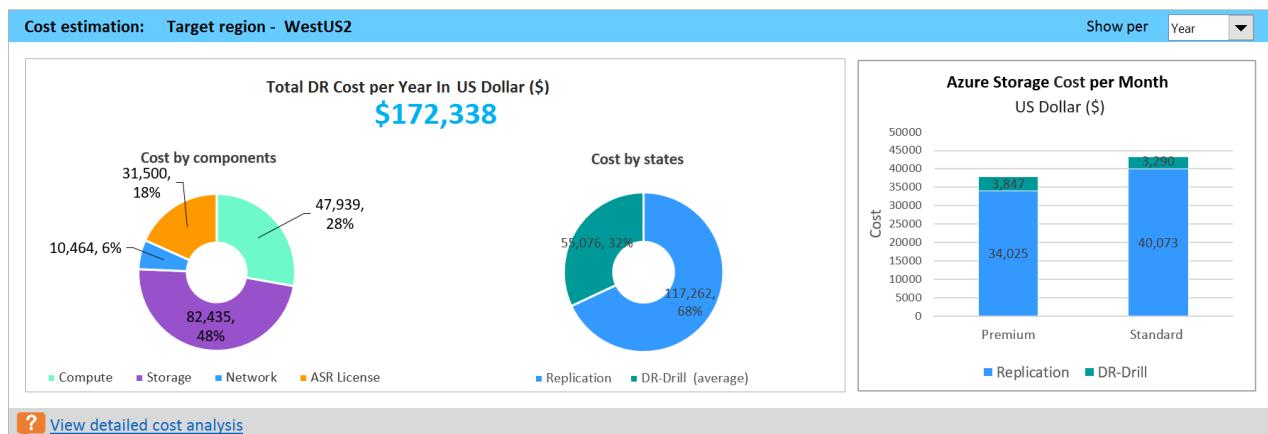
# Cost estimation report by Azure Site Recovery Deployment Planner

4/9/2019 • 8 minutes to read • [Edit Online](#)

The Azure Site Recovery Deployment Planner Report provides the cost estimation summary in [Recommendations](#) sheets and detailed cost analysis in the Cost Estimation sheet. It has the detailed cost analysis per VM.

## Cost estimation summary

The graph shows the summary view of the estimated total disaster recovery (DR) cost to Azure of your chosen target region and the currency that you specified for report generation.



The summary helps you to understand the cost that you need to pay for storage, compute, network, and license when you protect your compatible VMs by using Azure Site Recovery. The cost is calculated for compatible VMs and not on all the profiled VMs.

You can view the cost either monthly or yearly. Learn more about [supported target regions](#) and [supported currencies](#).

**Cost by components:** The total DR cost is divided into four components: compute, storage, network, and Site Recovery license cost. The cost is calculated based on the consumption that is incurred during replication and at DR-drill time. Compute, storage (premium and standard), the ExpressRoute/VPN that is configured between the on-premises site and Azure, and the Site Recovery license are used for the calculations.

**Cost by states:** The total disaster recovery (DR) cost category is based on two different states: replication and DR drill.

**Replication cost:** The cost that is incurred during replication. It covers the cost of storage, network, and the Site Recovery license.

**DR-Drill cost:** The cost that is incurred during test failovers. Site Recovery spins up VMs during test failover. The DR-drill cost covers the running VMs' compute and storage costs.

**Azure storage cost per Month/Year:** The total storage cost that is incurred for premium and standard storage for replication and DR drill.

## Detailed cost analysis

Azure prices for compute, storage, and network vary across Azure regions. You can generate a cost estimation report with the latest Azure prices based on your subscription, the offer associated with your subscription, and the specified target Azure region in a specified currency. By default, the tool uses West US 2 Azure region and US

dollar (USD) currency. If you use any other region and currency, the next time you generate a report without subscription ID, offer ID, target region, and currency, the tool uses prices of the last-used target region and currency for cost estimation.

This section shows the subscription ID and offer ID that you used for report generation. If they're not used, it's blank.

In the whole report, the cells marked in gray are read-only. Cells in white can be modified according to your requirements.

Overall DR costs by components			Overall DR costs by States				
	Month	Year		Month	Year		
<b>Compute</b>	\$3,995	\$47,939	<b>Replication</b>	\$9,772	\$117,262		
<b>Storage</b>	\$6,870	\$82,435	<b>DR-Drill (average)</b>	\$4,590	\$55,076		
<b>Network</b>	\$872	\$10,464	<b>Total</b>	<b>\$14,362</b>	<b>\$172,338</b>		
<b>ASR License</b>	\$2,625	\$31,500					
<b>Total</b>	<b>\$14,362</b>	<b>\$172,338</b>					
<b>Storage cost - Year (without discount)</b>			<b>Storage cost - Year (with discount)</b>				
<b>Replication</b>		<b>DR-Drill</b>	<b>Replication</b>	<b>DR-Drill</b>	<b>Replication</b>		
Premium	\$34,025	\$3,847	\$34,025	\$3,847	\$2,835		
Standard	\$40,073	\$3,290	\$40,073	\$3,290	\$3,339		
<b>Total</b>	<b>\$74,098</b>	<b>\$7,137</b>	<b>\$74,098</b>	<b>\$7,137</b>	<b>\$6,175</b>		
<b>Site to Azure Network</b>			<b>Number of virtual machines type and compute cost (per year)</b>				
ExpressRoute	ExpressRoute - 2 Gbps (Metered)		<b>OS type</b>	<b>Number of VMs</b>	<b>DR-Drill compute cost</b>		
VPN Gateway type	NA		Windows	105	\$47,939		
Target region	WestUS2		Non-Windows	0	\$0		
<b>VM running on Azure</b>			<b>Settings</b>				
Domain controller/DNS	<b>Number of VMs</b>	<b>IaaS size</b>	<b>Using Managed disk</b>	Yes			
SQL Always On	0	Standard_D3	Currency	US Dollar (\$)			
<b>Apply overall discount if applicable</b>			Cost duration	Year			
Discount in (%)	0						
<b>Detailed cost analysis</b>							
The below table lists cost breakup for each compatible VM of the profiled virtual machines. You can also use this table to get estimated Azure DR cost of non-profiled virtual machines by manually adding virtual machines. To manually add virtual machines: 1. Click on 'Insert row' button below to insert a new row between Start and End rows 2. Fill the following columns based on approximate virtual machine size and number of virtual machines that match this configuration - Number of VMs, IaaS size (Your selection), Storage T VM total storage size (GB), Number of DR-Drills in a year, Each DR-Drill duration (Days), OS Type, Data redundancy and Azure Hybrid Use Benefit 3. You can apply the same value to all the virtual machines in the table by clicking 'Apply to all' button for Number of DR-Drills in a year, Each DR-Drill duration (Days), Data redundancy and 4. Click 'Re-calculate cost' to update cost							
<a href="#">Learn more about cost estimation</a>							
<b>Insert row</b>	<b>Re-calculate cost</b>						
					<b>IaaS characteristics</b>		
<b>VM Name</b>	<b>Number of VMs</b>	<b>IaaS size (Recommended)</b>	<b>IaaS size (Your selection)</b>	<b>Storage type</b> Standard/Premium	<b>VM total storage size (GB) (Replication)</b>	<b>Number of DR-Drills in a year</b>	<b>Each DR-Drill duration (Days)</b>
<b>**START:INSERT A ROW BELOW TO ADD A NEW ENTRY**</b>							
co1magicsq1 (C01-CU-SV-E001)	1	Standard_D5_v2	Standard_D5_v2	Premium	2949.00	4	Apply to all 7
co1ecitweb05 (C01-CU-SV-EB003)	1	Standard_DS3_v2	Standard_DS3_v2	Premium	652.00	4	7
co1ecitweb07 (C01-CU-SV-EB004)	1	Standard_A3	Standard_A3	Standard	652.00	4	7
co1piappsm02 (C01-CU-SV-EB004)	1	Standard_A2	Standard_A2	Standard	200.00	4	7
co1su1407 (C01-CU-SV-EB004)	1	Standard_A4	Standard_A4	Standard	300.00	4	7
co1xitexsqla (C01-CU-SV-EB004)	1	Standard_D5_v2	Standard_D5_v2	Standard	1194.00	4	7
co1bimsspolp01 (C01-CU-SV-EB00)	1	Standard_A4	Standard_A4	Standard	550.00	4	7

## Overall DR costs by components

The first section shows the overall DR cost by components and DR cost by states.

**Compute:** The cost of IaaS VMs that run on Azure for DR needs. It includes VMs that are created by Site Recovery during DR drills (test failovers). It also includes VMs running on Azure, such as SQL Server with Always On availability groups and domain controllers or domain name servers.

**Storage:** The cost of Azure storage consumption for DR needs. It includes storage consumption for replication and during DR drills.

**Network:** ExpressRoute and site-to-site VPN cost for DR needs.

**Azure Site Recovery license:** The Site Recovery license cost for all compatible VMs. If you manually entered a VM in the detailed cost analysis table, the Site Recovery license cost also is included for that VM.

### Overall DR costs by states

The total DR cost is categorized based on two different states: replication and DR drill.

**Replication:** The cost incurred at the time of replication. It covers the cost of storage, network, and the Site Recovery license.

**DR-Drill:** The cost incurred at the time of DR drills. Site Recovery spins up VMs during DR drills. The DR-drill cost covers compute and storage cost of the running VMs.

- Total DR-drill duration in a year = number of DR drills x each DR drill duration (days)
- Average DR-drill cost (per month) = total DR-drill cost / 12

### Storage cost table

This table shows premium and standard storage costs incurred for replication and DR drills with and without discounts.

### Site to Azure network

Select the appropriate setting according to your requirements.

**ExpressRoute:** By default, the tool selects the nearest ExpressRoute plan that matches with the required network bandwidth for delta replication. You can change the plan according to your requirements.

**VPN Gateway type:** Select the Azure VPN Gateway if you have any in your environment. By default, it is NA.

**Target region:** Specified Azure region for DR. The price used in the report for compute, storage, network, and license is based on the Azure pricing for that region.

### VM running on Azure

Perhaps you have a domain controller or DNS VM or SQL Server VM with Always On availability groups running on Azure for DR. You can provide the number of VMs and the size to consider their computing cost in the total DR cost.

### Apply overall discount if applicable

If you're an Azure partner or a customer and are entitled to any discount on overall Azure pricing, you can use this field. The tool applies the discount (in percent) on all components.

### Number of virtual machines type and compute cost (per year)

This table shows the number of Windows and non-Windows VMs and the DR-drill compute cost for them.

### Settings

**Using Managed disk:** This setting specifies whether a managed disk is used at the time of DR drills. The default is **Yes**. If you set **-UseManagedDisks** to **No**, the unmanaged disk price is used for cost calculation.

**Currency:** The currency in which the report is generated.

**Cost duration:** You can view all costs either for the month or for the whole year.

## Detailed cost analysis table

Detailed cost analysis													
Cost breakdown for each compatible VM of the profiled virtual machines.													
You can use this table to get estimated Azure DR cost of non-profiled virtual machines by manually adding virtual machines.													
To manually add virtual machines:													
1. Click on <b>Insert row</b> button below to insert a new row between <b>Start</b> and <b>End</b> rows.													
2. Fill in the following columns based on approximate virtual machine size and number of virtual machines that match this configuration - Number of VMs, IaaS size (Your selection), Storage Type (Standard/Premium), VM total storage size (GB), Number of DR-Drills in a year, Each DR-Drill duration (Days), OS Type, Data redundancy and Azure Hybrid Use Benefit													
3. You can apply the same value to all the virtual machines in the table by clicking 'Apply to all' button for Number of DR-Drills in a year, Each DR-Drill duration (Days), Data redundancy and Azure Hybrid Use Benefit													
4. Click <b>Re-calculate cost</b> to update the cost.													
Learn more about cost estimation													
<a href="#">Insert row</a>		<a href="#">Re-calculate cost</a>											
IaaS characteristics													
												Cost breakup	

total DR-drill cost is calculated.

**Each DR-Drill duration (Days):** The duration of each DR drill. By default, it's 7 days every 90 days according to the [Disaster Recovery Software Assurance benefit](#). You can modify the period for specific VMs, or you can apply a new value to all VMs. Enter a new value in the top row, and select **Apply to all**. The total DR-drill cost is calculated based on the number of DR drills in a year and each DR-drill duration period.

**OS Type:** The operating system (OS) type of the VM. It's either Windows or Linux. If the OS type is Windows, the Azure Hybrid Use Benefit can be applied to that VM.

**Data redundancy:** It can be locally redundant storage, geo-redundant storage, or read-access geo-redundant storage. The default is locally redundant storage. You can change the type based on your storage account for specific VMs, or you can apply the new type to all VMs. Change the type of the top row, and select **Apply to all**. The cost of storage for replication is calculated based on the price of data redundancy that you selected.

**Azure Hybrid Use Benefit:** You can apply the Azure Hybrid Use Benefit to Windows VMs, if applicable. The default is **Yes**. You can change the setting for specific VMs, or you can update all VMs. Select **Apply to all**.

**Total Azure consumption:** The compute, storage, and Site Recovery license cost for your DR. Based on your selection, it shows the cost either monthly or yearly.

**Steady state replication cost:** The storage cost for replication.

**Total DR-Drill cost (average):** The compute and storage cost for DR drills.

**Azure Site Recovery license cost:** The Site Recovery license cost.

## Supported target regions

Site Recovery Deployment Planner provides cost estimation for the following Azure regions. If your region isn't listed here, you can use any of the following regions whose pricing is nearest to your region:

eastus, eastus2, westus, centralus, northcentralus, southcentralus, northeurope, westeurope, eastasia, southeastasia, japaneast, japanwest, australiaeast, australiasoutheast, brazilsouth, southindia, centralindia, westindia, canadacentral, canadaeast, westus2, westcentralus, uksouth, ukwest, koreacentral, koreasouth

## Supported currencies

Site Recovery Deployment Planner can generate the cost report with any of the following currencies.

CURRENCY	NAME	CURRENCY	NAME	CURRENCY	NAME
ARS	Argentine peso (\$)	AUD	Australian dollar (\$)	BRL	Brazilian real (R\$)
CAD	Canadian dollar (\$)	CHF	Swiss franc (chf)	DKK	Danish krone (kr)
EUR	Euro (€)	GBP	British pound (£)	HKD	Hong Kong dollar (HK\$)
IDR	Indonesia rupiah (Rp)	INR	Indian rupee (₹)	JPY	Japanese yen (¥)
KRW	Korean won (₩)	MXN	Mexican peso (MX\$)	MYR	Malaysian ringgit (RM\$)

CURRENCY	NAME		CURRENCY	NAME		CURRENCY	NAME
NOK	Norwegian krone (kr)		NZD	New Zealand dollar (\$)		RUB	Russian ruble (py6)
SAR	Saudi riyal (SR)		SEK	Swedish krona (kr)		TWD	Taiwanese dollar (NT\$)
TRY	Turkish lira (TL)		USD	US dollar (\$)		ZAR	South African rand (R)

## Next steps

Learn more about how to protect [Hyper-V VMs to Azure by using Site Recovery](#).

# Prepare network mapping for Hyper-V VM disaster recovery to Azure

11/14/2019 • 4 minutes to read • [Edit Online](#)

This article helps you to understand and prepare for network mapping when you replicate Hyper-V VMs in System Center Virtual Machine Manager (VMM) clouds to Azure, or to a secondary site, using the [Azure Site Recovery](#) service.

## Prepare network mapping for replication to Azure

When you're replicating to Azure, network mapping maps between VM networks on a source VMM server, and target Azure virtual networks. Mapping does the following:

- **Network connection**—Ensures that replicated Azure VMs are connected to the mapped network. All machines which fail over on the same network can connect to each other, even if they failed over in different recovery plans.
- **Network gateway**—If a network gateway is set up on the target Azure network, VMs can connect to other on-premises virtual machines.

Network mapping works as follows:

- You map a source VMM VM network to an Azure virtual network.
- After failover Azure VMs in the source network will be connected to the mapped target virtual network.
- New VMs added to the source VM network are connected to the mapped Azure network when replication occurs.
- If the target network has multiple subnets, and one of those subnets has the same name as subnet on which the source virtual machine is located, then the replica virtual machine connects to that target subnet after failover.
- If there's no target subnet with a matching name, the virtual machine connects to the first subnet in the network.

## Prepare network mapping for replication to a secondary site

When you're replicating to a secondary site, network mapping maps between VM networks on a source VMM server, and VM networks on a target VMM server. Mapping does the following:

- **Network connection**—Connects VMs to appropriate networks after failover. The replica VM will be connected to the target network that's mapped to the source network.
- **Optimal VM placement**—Optimally places the replica VMs on Hyper-V host servers. Replica VMs are placed on hosts that can access the mapped VM networks.
- **No network mapping**—If you don't configure network mapping, replica VMs won't be connected to any VM networks after failover.

Network mapping works as follows:

- Network mapping can be configured between VM networks on two VMM servers, or on a single VMM server if two sites are managed by the same server.
- When mapping is configured correctly and replication is enabled, a VM at the primary location will be connected to a network, and its replica at the target location will be connected to its mapped network.
- When you select a target VM network during network mapping in Site Recovery, the VMM source clouds that

use the source VM network will be displayed, along with the available target VM networks on the target clouds that are used for protection.

- If the target network has multiple subnets and one of those subnets has the same name as the subnet on which the source virtual machine is located, then the replica VM will be connected to that target subnet after failover. If there's no target subnet with a matching name, the VM will be connected to the first subnet in the network.

## Example

Here's an example to illustrate this mechanism. Let's take an organization with two locations in New York and Chicago.

LOCATION	VMM SERVER	VM NETWORKS	MAPPED TO
New York	VMM-NewYork	VMNetwork1-NewYork	Mapped to VMNetwork1-Chicago
	VMNetwork2-NewYork	Not mapped	
Chicago	VMM-Chicago	VMNetwork1-Chicago	Mapped to VMNetwork1-NewYork
	VMNetwork2-Chicago	Not mapped	

In this example:

- When a replica VM is created for any VM that's connected to VMNetwork1-NewYork, it will be connected to VMNetwork1-Chicago.
- When a replica VM is created for VMNetwork2-NewYork or VMNetwork2-Chicago, it won't be connected to any network.

Here's how VMM clouds are set up in our example organization, and the logical networks associated with the clouds.

### Cloud protection settings

PROTECTED CLOUD	PROTECTING CLOUD	LOGICAL NETWORK (NEW YORK)
GoldCloud1	GoldCloud2	
SilverCloud1	SilverCloud2	
GoldCloud2	NA	LogicalNetwork1-NewYork LogicalNetwork1-Chicago
SilverCloud2	NA	LogicalNetwork1-NewYork LogicalNetwork1-Chicago

### Logical and VM network settings

LOCATION	LOGICAL NETWORK	ASSOCIATED VM NETWORK
New York	LogicalNetwork1-NewYork	VMNetwork1-NewYork

LOCATION	LOGICAL NETWORK	ASSOCIATED VM NETWORK
Chicago	LogicalNetwork1-Chicago	VMNetwork1-Chicago
LogicalNetwork2Chicago	VMNetwork2-Chicago	

## Target network settings

Based on these settings, when you select the target VM network, the following table shows the choices that will be available.

SELECT	PROTECTED CLOUD	PROTECTING CLOUD	TARGET NETWORK AVAILABLE
VMNetwork1-Chicago	SilverCloud1	SilverCloud2	Available
GoldCloud1	GoldCloud2	Available	
VMNetwork2-Chicago	SilverCloud1	SilverCloud2	Not available
GoldCloud1	GoldCloud2	Available	

If the target network has multiple subnets and one of those subnets has the same name as the subnet on which the source virtual machine is located, then the replica virtual machine will be connected to that target subnet after failover. If there's no target subnet with a matching name, the virtual machine will be connected to the first subnet in the network.

## Fallback behavior

To see what happens in the case of fallback (reverse replication), let's assume that VMNetwork1-NewYork is mapped to VMNetwork1-Chicago, with the following settings.

VM	CONNECTED TO VM NETWORK
VM1	VMNetwork1-Network
VM2 (replica of VM1)	VMNetwork1-Chicago

With these settings, let's review what happens in a couple of possible scenarios.

SCENARIO	OUTCOME
No change in the network properties of VM-2 after failover.	VM-1 remains connected to the source network.
Network properties of VM-2 are changed after failover and is disconnected.	VM-1 is disconnected.
Network properties of VM-2 are changed after failover and is connected to VMNetwork2-Chicago.	If VMNetwork2-Chicago isn't mapped, VM-1 will be disconnected.
Network mapping of VMNetwork1-Chicago is changed.	VM-1 will be connected to the network now mapped to VMNetwork1-Chicago.

## Next steps

- [Learn about](#) IP addressing after failover to a secondary VMM site.

- [Learn about](#) IP addressing after failover to Azure.

# Exclude disks from replication

12/26/2019 • 2 minutes to read • [Edit Online](#)

This article describes how to exclude disks when replicating Hyper-V VMs to Azure. You might want to exclude disks from replication for a number of reasons:

- Ensure that unimportant data churned on the excluded disk doesn't get replicated.
- Optimize the consumed replication bandwidth, or the target-side resources, by excluding disks you don't need to replicate.
- Save storage and network resources by not replicating data you don't need.

Before you exclude disks from replication:

- [Learn more](#) about excluding disks.
- Review [typical exclude scenarios](#) and [examples](#) that show how excluding a disk affects replication, failover, and fallback.

## Before you start

Note the following before you start:

- **Replication:** By default all disks on a machine are replicated.
- **Disk type:**
  - You can exclude basic disks from replication.
  - You can't exclude operating system disks.
  - We recommend that you don't exclude dynamic disks. Site Recovery can't identify which VHD is basic or dynamic in the guest VM. If you don't exclude all dependent dynamic volume disks, the protected dynamic disk becomes a failed disk on a failed over VM, and the data on that disk isn't accessible.
- **Add/remove/exclude disks:** After you enable replication, you can't add/remove/exclude disks for replication. If you want to add/remove or exclude a disk, you need to disable protection for the VM, and then enable it again.
- **Failover:** After failover, if failed over apps need exclude disks in order to work, you need to create those disks manually. Alternatively, you can integrate Azure automation into a recovery plan, to create the disk during failover of the machine.
- **Fallback:** When you fail back to your on-premises site after failover, disks that you created manually in Azure aren't failed back. For example, if you fail over three disks and create two disks directly on an Azure VM, only three disks that were failed over are then failed back. You can't include disks that were created manually in fallback, or in reverse replication of VMs.

## Exclude disks

1. To exclude disks when you [enable replication](#) for a Hyper-V VM, after selecting the VMs you want to replicate, in the **Enable replication > Properties > Configure properties** page, review the **Disks to Replicate** column. By default all disks are selected for replication.
2. If you don't want to replicate a specific disk, in **Disks to replicate** clear the selection for any disks you want to exclude.

## Configure properties

 Selected Virtual Machines (2) has non supported name format. Please enter a valid name.

NAME	OS TYPE	OS DISK	DISKS TO REPLICATE	TARGET NAME	...
Defaults	Windows	Need to select per VM.	Need to select per VM.	Fix per VM	...
Sales_BackendDB1	Windows	SalesDB-Disk1-OS	Selected 6 out of 10	SalesBackendDB1	...
Sales_Frontend1	Windows	Sales_Frontend1-...	Selected 3 out of 4	SalesFrontend1	...

Sales\_FE1-Disk2 [40 GB]  
 Sales\_FE1-Disk3 [100 GB]  
 Sales\_FE1-Disk4 [100 GB]  
 Sales\_Frontend1-Disk1-OS [60 GB]

## Next steps

After your deployment is set up and running, [learn more](#) about different types of failover.

# Create and customize recovery plans

1/23/2020 • 4 minutes to read • [Edit Online](#)

This article describes how to create and customize a recovery plan for failover in [Azure Site Recovery](#). Before you start, [learn more](#) about recovery plans.

## Create a recovery plan

1. In the Recovery Services vault, select **Recovery Plans (Site Recovery)** > **+Recovery Plan**.
2. In **Create recovery plan**, specify a name for the plan.
3. Choose a source and target based on the machines in the plan, and select **Resource Manager** for the deployment model. The source location must have machines that are enabled for failover and recovery.

FAILOVER	SOURCE	TARGET
Azure to Azure	Select the Azure region	Select the Azure region
VMware to Azure	Select the configuration server	Select Azure
Physical machines to Azure	Select the configuration server	Select Azure
Hyper-V to Azure	Select the Hyper-V site name	Select Azure
Hyper-V (managed by VMM) to Azure	Select the VMM server	Select Azure

Note the following:

- You can only use a recovery plan for failover from the source location to Azure. You can't use a recovery plan for fallback from Azure.
  - The source location must have machines that are enabled for failover and recovery.
  - A recovery plan can contain machines with the same source and target.
  - You can include VMware VMs and Hyper-V VMs managed by VMM, in the same plan.
  - VMware VMs and physical servers can be in the same plan.
4. In **Select items virtual machines**, select the machines (or replication group) that you want to add to the plan. Then click **OK**.
    - Machines are added default group (Group 1) in the plan. After failover, all machines in this group start at the same time.
    - You can only select machines are in the source and target locations that you specified.
  5. Click **OK** to create the plan.

## Add a group to a plan

You create additional groups, and add machines to different groups so that you can specify different behavior on a group-by-group basis. For example, you can specify when machines in a group should start after failover, or specify customized actions per group.

1. In **Recovery Plans**, right-click the plan > **Customize**. By default, after creating a plan all the machines you added to it are located in default Group 1.
2. Click **+Group**. By default a new group is numbered in the order in which it's added. You can have up to seven groups.
3. Select the machine you want to move to the new group, click **Change group**, and then select the new group. Alternatively, right-click the group name > **Protected item**, and add machines to the group. A machine or replication group can only belong to one group in a recovery plan.

## Add a script or manual action

You can customize a recovery plan by adding a script or manual action. Note that:

- If you're replicating to Azure you can integrate Azure automation runbooks into your recovery plan. [Learn more](#).
- If you're replicating Hyper-V VMs managed by System Center VMM, you can create a script on the on-premises VMM server, and include it in the recovery plan.
- When you add a script, it adds a new set of actions for the group. For example, a set of pre-steps for Group 1 is created with the name *Group 1: pre-steps*. All pre-steps are listed inside this set. You can add a script on the primary site only if you have a VMM server deployed.
- If you add a manual action, when the recovery plan runs, it stops at the point at which you inserted the manual action. A dialog box prompts you to specify that the manual action was completed.
- To create a script on the VMM server, follow the instructions in [this article](#).
- Scripts can be applied during failover to the secondary site, and during fallback from the secondary site to the primary. Support depends on your replication scenario:

SCENARIO	FAILOVER	FAILBACK
Azure to Azure	Runbook	Runbook
VMware to Azure	Runbook	NA
Hyper-V with VMM to Azure	Runbook	Script
Hyper-V site to Azure	Runbook	NA
VMM to secondary VMM	Script	Script

1. In the recovery plan, click the step to which the action should be added, and specify when the action should occur:
  - a. If you want the action to occur before the machines in the group are started after failover, select **Add pre-action**.
  - b. If you want the action to occur after the machines in the group start after failover, select **Add post action**. To move the position of the action, select the **Move Up** or **Move Down** buttons.
2. In **Insert action**, select **Script** or **Manual action**.
3. If you want to add a manual action, do the following:
  - a. Type in a name for the action, and type in action instructions. The person running the failover will see these instructions.
  - b. Specify whether you want to add the manual action for all types of failover (Test, Failover, Planned failover (if relevant)). Then click **OK**.

4. If you want to add a script, do the following:
  - a. If you're adding a VMM script, select **Failover to VMM script**, and in **Script Path** type the relative path to the share. For example, if the share is located at \\<VMMServerName>\MSSCVMMLibrary\RPScripts, specify the path: \\RPScripts\RPScript.PS1.
  - b. If you're adding an Azure automation run book, specify the **Azure Automation Account** in which the runbook is located, and select the appropriate **Azure Runbook Script**.
5. Run a test failover of the recovery plan to ensure that the script works as expected.

## Watch a video

Watch a video that demonstrates how to build a recovery plan.

## Next steps

Learn more about [running failovers](#).

# Add a VMM script to a recovery plan

11/14/2019 • 4 minutes to read • [Edit Online](#)

This article describes how to create a System Center Virtual Machine Manager (VMM) script and add it to a recovery plan in [Azure Site Recovery](#).

Post any comments or questions at the bottom of this article, or on the [Azure Recovery Services forum](#).

## Prerequisites

You can use PowerShell scripts in your recovery plans. To be accessible from the recovery plan, you must author the script and place the script in the VMM library. Keep the following considerations in mind while you write the script:

- Ensure that scripts use try-catch blocks, so that exceptions are handled gracefully.
  - If an exception occurs in the script, the script stops running, and the task shows as failed.
  - If an error occurs, the remainder of the script doesn't run.
  - If an error occurs when you run an unplanned failover, the recovery plan continues.
  - If an error occurs when you run a planned failover, the recovery plan stops. Fix the script, check that it runs as expected, and then run the recovery plan again.
  - The `Write-Host` command doesn't work in a recovery plan script. If you use the `Write-Host` command in a script, the script fails. To create output, create a proxy script that in turn runs your main script. To ensure that all output is piped out, use the `>>` command.
  - The script times out if it doesn't return within 600 seconds.
  - If anything is written to `STDERR`, the script is classified as failed. This information is displayed in the script execution details.
- Scripts in a recovery plan run in the context of the VMM service account. Ensure that this account has read permissions for the remote share on which the script is located. Test the script to run with the same level of user rights as the VMM service account.
- VMM cmdlets are delivered in a Windows PowerShell module. The module is installed when you install the VMM console. To load the module into your script, use the following command in the script:

```
Import-Module -Name virtualmachinemanager
```

For more information, see [Get started with Windows PowerShell and VMM](#).

- Ensure that you have at least one library server in your VMM deployment. By default, the library share path for a VMM server is located locally on the VMM server. The folder name is `MSCVMMLibrary`.

If your library share path is remote (or if it's local but not shared with `MSCVMMLibrary`), configure the share as follows, using `\libserver2.contoso.com\share\` as an example:

1. Open the Registry Editor, and then go to  
**`HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\Azure Site Recovery\Registration`**.
2. Change the value for **ScriptLibraryPath** to `\libserver2.contoso.com\share\`. Specify the full FQDN. Provide permissions to the share location. This is the root node of the share. To check for the root node, in VMM, go to the root node in the library. The path that opens is the root of the path. This is the path that you must use in the variable.

3. Test the script by using a user account that has the same level of user rights as the VMM service account. Using these user rights verifies that standalone, tested scripts run the same way that they run in recovery plans. On the VMM server, set the execution policy to bypass, as follows:

- a. Open the **64-bit Windows PowerShell** console as an administrator.
- b. Enter **Set-executionpolicy bypass**. For more information, see [Using the Set-ExecutionPolicy cmdlet](#).

**IMPORTANT**

Set **Set-executionpolicy bypass** only in the 64-bit PowerShell console. If you set it for the 32-bit PowerShell console, the scripts don't run.

## Add the script to the VMM library

If you have a VMM source site, you can create a script on the VMM server. Then, include the script in your recovery plan.

1. In the library share, create a new folder. For example, <VMM server name>\MSSCVMMLibrary\RPScripts. Place the folder on the source and target VMM servers.
2. Create the script. For example, name the script RPScript. Verify that the script works as expected.
3. Place the script in the <VMM server name>\MSSCVMMLibrary folder on the source and target VMM servers.

## Add the script to a recovery plan

After you've added VMs or replication groups to a recovery plan and created the plan, you can add the script to the group.

1. Open the recovery plan.
2. In the **Step** list, select an item. Then, select either **Script** or **Manual Action**.
3. Specify whether to add the script or action before or after the selected item. To move the position of the script up or down, select the **Move Up** and **Move Down** buttons.
4. If you add a VMM script, select **Failover to VMM script**. In **Script Path**, enter the relative path to the share. For example, enter **\RPScripts\RPScript.PS1**.
5. If you add an Azure Automation runbook, specify the Automation account in which the runbook is located. Then, select the Azure runbook script that you want to use.
6. To ensure that the script works as expected, do a test failover of the recovery plan.

## Next steps

- Learn more about [running failovers](#).

# Run a test failover (disaster recovery drill) to Azure

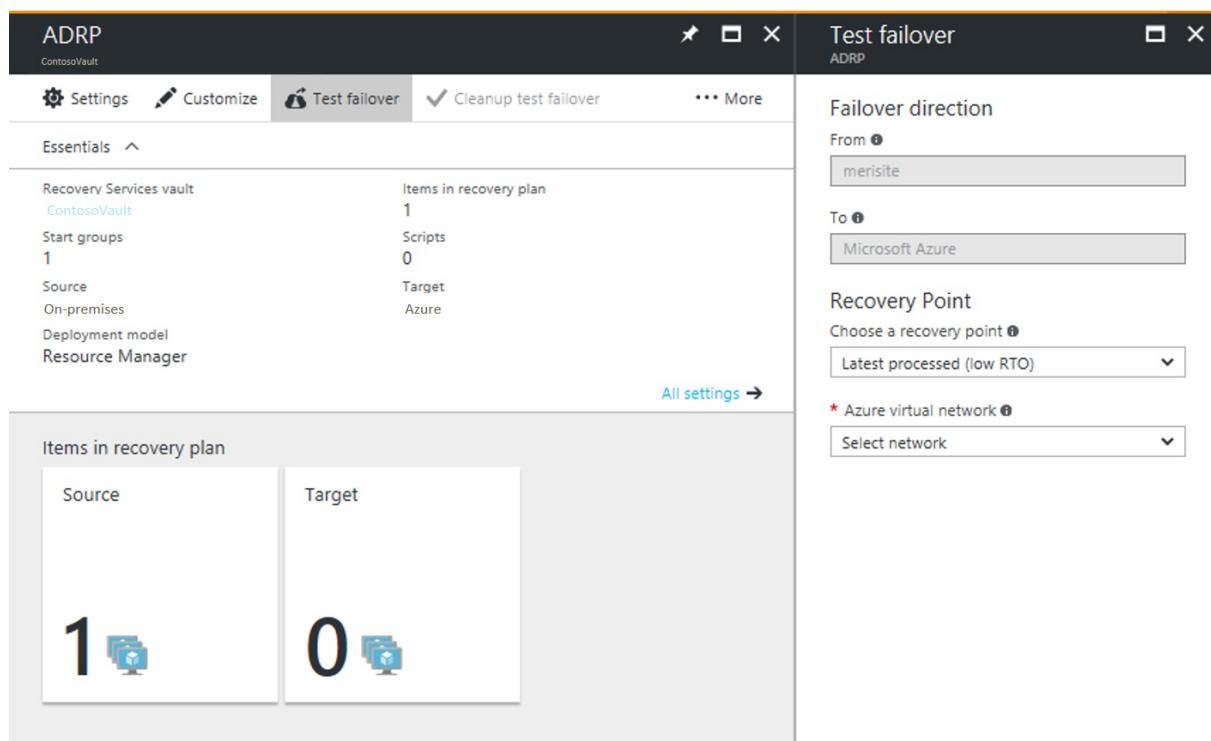
11/14/2019 • 7 minutes to read • [Edit Online](#)

This article describes how to run a disaster recovery drill to Azure, using a Site Recovery test failover.

You run a test failover to validate your replication and disaster recovery strategy, without any data loss or downtime. A test failover doesn't impact ongoing replication, or your production environment. You can run a test failover on a specific virtual machine (VM), or on a [recovery plan](#) containing multiple VMs.

## Run a test failover

This procedure describes how to run a test failover for a recovery plan. If you want to run a test failover for a single VM, follow the steps described [here](#)



1. In Site Recovery in the Azure portal, click **Recovery Plans** > *recoveryplan\_name* > **Test Failover**.
2. Select a **Recovery Point** to which to fail over. You can use one of the following options:
  - **Latest processed:** This option fails over all VMs in the plan to the latest recovery point processed by Site Recovery. To see the latest recovery point for a specific VM, check **Latest Recovery Points** in the VM settings. This option provides a low RTO (Recovery Time Objective), because no time is spent processing unprocessed data.
  - **Latest app-consistent:** This option fails over all the VMs in the plan to the latest application-consistent recovery point processed by Site Recovery. To see the latest recovery point for a specific VM, check **Latest Recovery Points** in the VM settings.
  - **Latest:** This option first processes all the data that has been sent to Site Recovery service, to create a recovery point for each VM before failing over to it. This option provides the lowest RPO (Recovery Point Objective), because the VM created after failover will have all the data replicated to Site Recovery when the failover was triggered.
  - **Latest multi-VM processed:** This option is available for recovery plans with one or more VMs that have multi-VM consistency enabled. VMs with the setting enabled fail over to the latest

common multi-VM consistent recovery point. Other VMs fail over to the latest processed recovery point.

- **Latest multi-VM app-consistent:** This option is available for recovery plans with one or more VMs that have multi-VM consistency enabled. VMs that are part of a replication group fail over to the latest common multi-VM application-consistent recovery point. Other VMs fail over to their latest application-consistent recovery point.
- **Custom:** Use this option to fail over a specific VM to a particular recovery point.

3. Select an Azure virtual network in which test VMs will be created.
  - Site Recovery attempts to create test VMs in a subnet with the same name and same IP address as that provided in the **Compute and Network** settings of the VM.
  - If a subnet with the same name isn't available in the Azure virtual network used for test failover, then the test VM is created in the first subnet alphabetically.
  - If same IP address isn't available in the subnet, then the VM receives another available IP address in the subnet. [Learn more](#).
4. If you're failing over to Azure and data encryption is enabled, in **Encryption Key**, select the certificate that was issued when you enabled encryption during Provider installation. You can ignore this step if encryption isn't enabled.
5. Track failover progress on the **Jobs** tab. You should be able to see the test replica machine in the Azure portal.
6. To initiate an RDP connection to the Azure VM, you need to [add a public IP address](#) on the network interface of the failed over VM.
7. When everything is working as expected, click **Cleanup test failover**. This deletes the VMs that were created during test failover.
8. In **Notes**, record and save any observations associated with the test failover.

## Job

NAME	STATUS	START TIME	DURATION	...
Prerequisites check for the recovery plan	✓ Successful	5/3/2017 3:48:14 PM	00:00:04	...
Create the test environment	✓ Successful	5/3/2017 3:48:19 PM	00:00:01	...
▼ Recovery plan failover	✓ Successful	5/3/2017 3:48:20 PM	00:01:14	...
SQLServer	✓ Successful	5/3/2017 3:48:20 PM	00:01:14	...
▼ Group 1: Start (1)	✓ Successful	5/3/2017 3:49:35 PM	00:01:40	...
SQLServer	✓ Successful	5/3/2017 3:49:35 PM	00:01:40	...
Finalizing the recovery plan	✓ Successful	5/3/2017 3:51:16 PM	00:00:00	...

When a test failover is triggered, the following occurs:

1. **Prerequisites:** A prerequisites check runs to make sure that all conditions required for failover are met.
2. **Failover:** The failover processes and prepared the data, so that an Azure VM can be created from it.
3. **Latest:** If you have chosen the latest recovery point, a recovery point is created from the data that's been sent to the service.
4. **Start:** This step creates an Azure virtual machine using the data processed in the previous step.

## Failover timing

In the following scenarios, failover requires an extra intermediate step that usually takes around 8 to 10 minutes to complete:

- VMware VMs running a version of the Mobility service older than 9.8
- Physical servers
- VMware Linux VMs
- Hyper-V VM protected as physical servers
- VMware VM where the following drivers aren't boot drivers:
  - storvsc
  - vmbus
  - storflt
  - intelide
  - atapi
- VMware VM that don't have DHCP enabled , irrespective of whether they are using DHCP or static IP addresses.

In all the other cases, no intermediate step is not required, and failover takes significantly less time.

## Create a network for test failover

We recommended that for test failover, you choose a network that's isolated from the production recovery site network specific in the **Compute and Network** settings for each VM. By default, when you create an Azure virtual network, it is isolated from other networks. The test network should mimic your production network:

- The test network should have same number of subnets as your production network. Subnets should have the same names.
- The test network should use the same IP address range.
- Update the DNS of the test network with the IP address specified for the DNS VM in **Compute and Network** settings. Read [test failover considerations for Active Directory](#) for more details.

## Test failover to a production network in the recovery site

Although we recommended that you use a test network separate from your production network, if you do want to test a disaster recovery drill into your production network, note the following:

- Make sure that the primary VM is shut down when you run the test failover. Otherwise there will be two VMs with the same identity, running in the same network at the same time. This can lead to unexpected consequences.
- Any changes to VMs created for test failover are lost when you clean up the failover. These changes are not replicated back to the primary VM.
- Testing in your production environment leads to a downtime of your production application. Users shouldn't use apps running on VMs when the test failover is in progress.

## Prepare Active Directory and DNS

To run a test failover for application testing, you need a copy of your production Active Directory environment in your test environment. Read [test failover considerations for Active Directory](#) to learn more.

## Prepare to connect to Azure VMs after failover

If you want to connect to Azure VMs using RDP/SSH after failover, follow the requirements summarized in the table.

FAILOVER	LOCATION	ACTIONS
<b>Azure VM running Windows</b>	On-premises machine before failover	<p>To access the Azure VM over the internet, enable RDP, and make sure that TCP and UDP rules are added for <b>Public</b>, and that RDP is allowed for all profiles in <b>Windows Firewall &gt; Allowed Apps</b>.</p> <p>To access the Azure VM over a site-to-site connection, enable RDP on the machine, and ensure that RDP is allowed in the <b>Windows Firewall -&gt; Allowed apps and features</b>, for <b>Domain and Private</b> networks.</p> <p>Make sure the operating system SAN policy is set to <b>OnlineAll</b>. <a href="#">Learn more</a>.</p> <p>Make sure there are no Windows updates pending on the VM when you trigger a failover. Windows update might start when you fail over, and you won't be able to log onto the VM until the update completes.</p>
<b>Azure VM running Windows</b>	Azure VM after failover	<p><a href="#">Add a public IP address</a> for the VM.</p> <p>The network security group rules on the failed over VM (and the Azure subnet to which it is connected) need to allow incoming connections to the RDP port.</p> <p>Check <b>Boot diagnostics</b> to verify a screenshot of the VM.</p> <p>If you can't connect, check that the VM is running, and review these <a href="#">troubleshooting tips</a>.</p>
<b>Azure VM running Linux</b>	On-premises machine before failover	<p>Ensure that the Secure Shell service on the VM is set to start automatically on system boot.</p> <p>Check that firewall rules allow an SSH connection to it.</p>
<b>Azure VM running Linux</b>	Azure VM after failover	<p>The network security group rules on the failed over VM (and the Azure subnet to which it is connected) need to allow incoming connections to the SSH port.</p> <p><a href="#">Add a public IP address</a> for the VM.</p> <p>Check <b>Boot diagnostics</b> for a screenshot of the VM.</p>

Follow the steps described [here](#) to troubleshoot any connectivity issues post failover.

## Next steps

After you've completed a disaster recovery drill, learn more about other types of [failover](#).

# Run a failover from on-premises to Azure

1/2/2020 • 7 minutes to read • [Edit Online](#)

This article describes how to fail over on-premises machines to Azure in [Azure Site Recovery](#)

## Before you start

- [Learn](#) about the failover process in disaster recovery.
- If you want to fail over multiple machines, [learn](#) how to gather machines together in a recovery plan.
- Before you do a full failover, run a [disaster recovery drill](#) to ensure that everything is working as expected.

## Prepare to connect after failover

To make sure you can connect to the Azure VMs that are created after failover, here are a number of things you need to do on-premises before failover.

### Prepare on-premises to connect after failover

If you want to connect to Azure VMs using RDP/SSH after failover, there are a number of things you need to do on-premises before failover.

AFTER FAILOVER	LOCATION	ACTIONS
<b>Azure VM running Windows</b>	On-premises machine before failover	<p>To access the Azure VM over the internet, enable RDP, and make sure that TCP and UDP rules are added for <b>Public</b>, and that RDP is allowed for all profiles in <b>Windows Firewall</b> &gt; <b>Allowed Apps</b>.</p> <p>To access the Azure VM over a site-to-site connection, enable RDP on the machine, and ensure that RDP is allowed in the <b>Windows Firewall</b> -&gt; <b>Allowed apps and features</b>, for <b>Domain and Private</b> networks.</p> <p>Remove any static persistent routes and WinHTTP proxy. Make sure the operating system SAN policy is set to <b>OnlineAll</b>. <a href="#">Learn more</a>.</p> <p>Make sure there are no Windows updates pending on the VM when you trigger a failover. Windows update might start when you fail over, and you won't be able to log onto the VM until the update completes.</p>

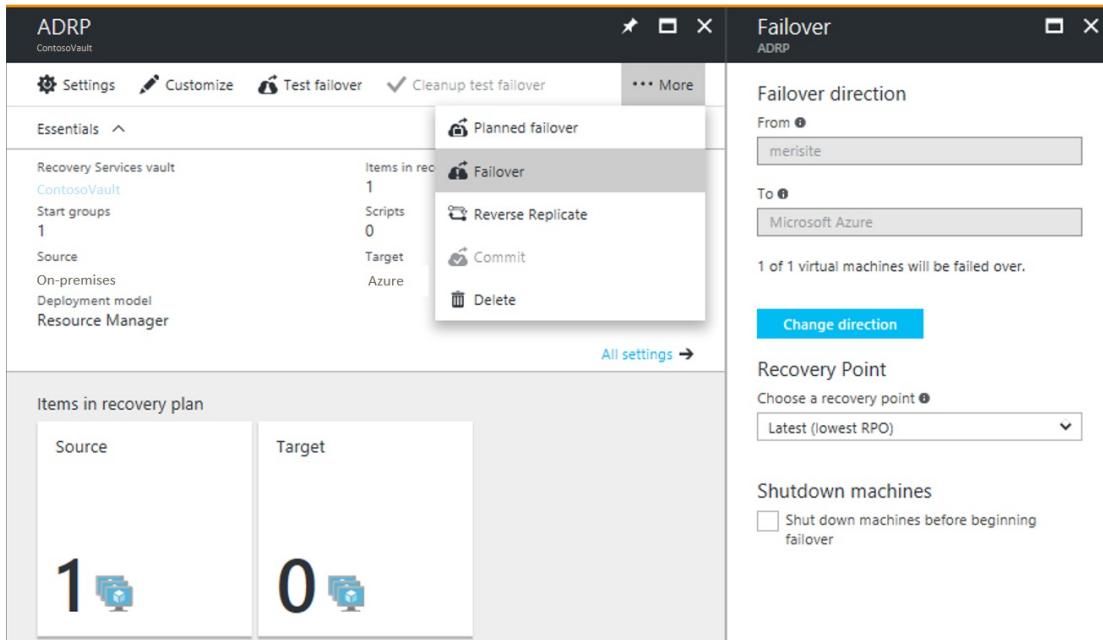
AFTER FAILOVER	LOCATION	ACTIONS
<b>Azure VM running Linux</b>	On-premises machine before failover	<p>Ensure that the Secure Shell service on the VM is set to start automatically on system boot.</p> <p>Check that firewall rules allow an SSH connection to it.</p>

## Run a failover

This procedure describes how to run a failover for a [recovery plan](#). If you want to run a failover for a single VM, follow the instructions for a [VMware VM](#), a [physical server](#), or a [Hyper-V VM](#).

Run the recovery plan failover as follows:

1. In the Site Recovery vault, select **Recovery Plans** > *recoveryplan\_name*.
2. Click **Failover**.



3. In **Failover > Failover direction**, leave the default if you're replicating to Azure.
4. In **Failover**, select a **Recovery Point** to which to fail over.
  - **Latest:** Use the latest point. This processes all the data that's been sent to Site Recovery service, and creates a recovery point for each machine. This option provides the lowest RPO (Recovery Point Objective) because the VM created after failover has all the data that's been replicated to Site Recovery when the failover was triggered.
  - **Latest processed:** Use this option to fail over VMs to the latest recovery point already processed by Site Recovery. You can see the latest processed recovery point in the VM **Latest Recovery Points**. This option provides a low RTO as no time is spent to processing the unprocessed data
  - **Latest app-consistent:** Use this option to fail VMs over to the latest application consistent recovery point that's been processed by Site Recovery.
  - **Latest multi-VM processed:** With this option VMs that are part of a replication group failover to the latest common multi-VM consistent recovery point. Other virtual machines fail over to their latest processed recovery point. This option is only for recovery plans that have at least one VM with multi-VM consistency enabled.

- **Latest multi-VM app-consistent:** With this option VMs that are part of a replication group fail over to the latest common multi-VM application-consistent recovery point. Other virtual machines failover to their latest application-consistent recovery point. Only for recovery plans that have at least one VM with multi-VM consistency enabled.
  - **Custom:** Not available for recovery plans. This option is only for failover of individual VMs.
5. Select **Shut-down machine before beginning failover** if you want Site Recovery shut down source VMs before starting the failover. Failover continues even if shutdown fails.

#### NOTE

If you fail over Hyper-V VMs, shutdown tries to synchronize and replicate the on-premises data that hasn't yet been sent to the service, before triggering the failover.

6. Follow failover progress on the **Jobs** page. Even if errors occurs, the recovery plan runs until it is complete.
7. After the failover, sign into the VM to validate it.
8. If you want to switch to different recovery point to use for the failover, use **Change recovery point**.
9. When you're ready, you can commit the failover. The **Commit** action deletes all the recovery points available with the service. The **Change recovery point** option will no longer be available.

## Run a planned failover (Hyper-V)

You can run a planned failover for Hyper-V VMs.

- A planned failover is a zero data loss failover option.
- When a planned failover is triggered, first the source virtual machines are shut-down, the latest data is synchronized and then a failover is triggered.
- You run a planned failover using the **Planned failover** option. It runs in a similar way to a regular failover.

## Track failovers

There are a number of jobs associated with failover.

### Job

NAME	STATUS	START TIME	DURATION	...
Prerequisites check for the recovery plan	✓ Successful	5/3/2017 4:01:19 PM	00:00:02	...
Create the environment	✓ Successful	5/3/2017 4:01:22 PM	00:00:00	...
▼ All groups shutdown (1)	✓ Successful	5/3/2017 4:01:23 PM	00:01:54	...
Shutdown: Group 1 (1)	✓ Successful	5/3/2017 4:01:23 PM	00:01:54	...
▼ Recovery plan failover	✓ Successful	5/3/2017 4:03:18 PM	00:01:38	...
SQLServer	✓ Successful	5/3/2017 4:03:18 PM	00:01:38	...
▼ Group 1: Start (1)	✓ Successful	5/3/2017 4:04:57 PM	00:01:45	...
SQLServer	✓ Successful	5/3/2017 4:04:57 PM	00:01:45	...
Finalizing the recovery plan	✓ Successful	5/3/2017 4:06:43 PM	00:00:00	...

- **Prerequisites check:** Ensures that all conditions required for failover are met.

- **Failover:** Processes the data so that an Azure VM can be created from it. If you have chosen **Latest** recovery point, a recovery point is created from the data that's been sent to the service.
- **Start:** Creates an Azure VM using the data processed in the previous step.

#### **WARNING**

**Don't cancel a failover in progress:** Before failover is started, replication stops for the VM. If you cancel an in-progress job, failover stops, but the VM will not start to replicate. Replication can't be started again.

#### **Extra failover time**

In some cases, VM failover requires intermediate step that usually takes around eight to 10 minutes to complete. These are the machines that are affected by this additional step/time:

- VMware virtual machines running a Mobility service version older than 9.8.
- Physical servers, and Hyper-V VMs protected as physical servers.
- VMware Linux VMs.
- VMware VMs on which these drivers aren't present as boot drivers:
  - storvsc
  - vmbus
  - storflt
  - intelide
  - atapi
- VMware VMs that don't have DHCP enabled, irrespective of whether they're using DHCP or static IP addresses.

## Automate actions during failover

You might want to automate actions during failover. To do this, you can use scripts or Azure automation runbooks in recovery plans.

- [Learn about creating and customizing recovery plans, including adding scripts.](#)
- [Learn about adding Azure Automation runbooks to recovery plans.](#)

## Configure settings after failover

#### **Retain drive letters after failover**

Site Recovery handles retention of drive letters. If you're excluding disks during VM replication, [review an example](#) of how this works.

#### **Prepare in Azure to connect after failover**

If you want to connect to Azure VMs that are created after failover using RDP or SSH, follow the requirements summarized in the table.

FAILOVER	LOCATION	ACTIONS
----------	----------	---------

FAILOVER	LOCATION	ACTIONS
<b>Azure VM running Windows</b>	Azure VM after failover	<p><a href="#">Add a public IP address</a> for the VM.</p> <p>The network security group rules on the failed over VM (and the Azure subnet to which it is connected) need to allow incoming connections to the RDP port.</p> <p>Check <b>Boot diagnostics</b> to verify a screenshot of the VM.</p> <p>If you can't connect, check that the VM is running, and review these <a href="#">troubleshooting tips</a>.</p>
<b>Azure VM running Linux</b>	Azure VM after failover	<p>The network security group rules on the failed over VM (and the Azure subnet to which it is connected) need to allow incoming connections to the SSH port.</p> <p><a href="#">Add a public IP address</a> for the VM.</p> <p>Check <b>Boot diagnostics</b> for a screenshot of the VM.</p>

Follow the steps described [here](#) to troubleshoot any connectivity issues post failover.

## Set up IP addressing

- **Internal IP addresses:** To set the internal IP address of an Azure VM after failover, you have a couple of options:
  - Retain same IP address: You can use the same IP address on the Azure VM as the one allocated to the on-premises machine.
  - Use different IP address: You can use a different IP address for the Azure VM.
  - [Learn more](#) about setting up internal IP addresses.
- **External IP addresses:** You can retain public IP addresses on failover. Azure VMs created as part of the failover process must be assigned an Azure public IP address available in the Azure region. You can assign a public IP address either manually or by automating the process with a recovery plan. [Learn more](#).

## Next steps

After you've failed over, you need to reprotect to start replicating the Azure VMs back to the on-premises site. After replication is up and running, you can fail back on-premises when you're ready.

- [Learn more](#) about reprotection and failback.
- [Prepare](#) for VMware reprotection and failback.
- [Fail back](#) Hyper-V VMs.
- [Learn about](#) the failover and failback process for physical servers.

# Run a failback for Hyper-V VMs

12/26/2019 • 5 minutes to read • [Edit Online](#)

This article describes how to fail back Azure VMs that were created after failover of Hyper-V VMs from an on-premises site to Azure, with [Azure Site Recovery](#).

- You fail back Hyper-V VMs from Azure by running a planned failover from Azure to the on-premises site. If the failover direction is from Azure to on-premises, it's considered a failback.
- Since Azure is a highly available environment and VMs are always available, failback from Azure is a planned activity. You can plan for a small downtime so that workloads can start running on-premises again.
- Planned failback turns off the VMs in Azure, and downloads the latest changes. No data loss is expected.

## Before you start

1. [Review the types of failback](#) you can use - original location recovery and alternate location recovery.
2. Ensure that the Azure VMs are using a storage account and not managed disks. Failback of Hyper-V VMs replicated using managed disks isn't supported.
3. Check that the on-premises Hyper-V host (or System Center VMM server if you're using with Site Recovery) is running and connected to Azure.
4. Make sure that failover and commit are complete for the VMs. You don't need to set up any specific Site Recovery components for failback of Hyper-V VMs from Azure.
5. The time needed to complete data synchronization and start the on-premises VM will depend on a number of factors. To speed up data download, you can configure the Microsoft Recovery Services agent to use more threads to parallelize the download. [Learn more](#).

## Fail back to the original location

To fail back Hyper-V VMs in Azure to the original on-premises VM, run a planned failover from Azure to the on-premises site as follows:

1. In the vault > **Replicated items**, select the VM. Right-click the VM > **Planned Failover**. If you're failing back a recovery plan, select the plan name and click **Failover** > **Planned Failover**.
2. In **Confirm Planned Failover**, choose the source and target locations. Note the failover direction. If the failover from primary worked as expected and all virtual machines are in the secondary location this is for information only.
3. In **Data Synchronization**, select an option:
  - **Synchronize data before failover (synchronize delta changes only)**—This option minimizes downtime for VMs as it synchronizes without shutting them down.
    - **Phase 1:** Takes a snapshot of Azure VM and copies it to the on-premises Hyper-V host. The machine continues running in Azure.
    - **Phase 2:** Shuts down the Azure VM so that no new changes occur there. The final set of delta changes is transferred to the on-premises server and the on-premises VM is started.
  - **Synchronize data during failover only (full download)**—This option is faster because we presume that most of the disk has changed, and don't want to spend time calculating checksums. This option doesn't perform any checksum calculations.
    - It performs a download of the disk.
    - We recommend you use this option if you've been running Azure for a while (a month or more)

or if the on-premises VM is deleted.

4. For VMM only, if data encryption is enabled for the cloud, in **Encryption Key**, select the certificate that was issued when you enabled data encryption during Provider installation on the VMM server.
5. Initiate the failover. You can follow the failover progress on the **Jobs** tab.
6. If you selected the option to synchronize the data before the failover, after the initial data synchronization is complete and you're ready to shut down the virtual machines in Azure, click **Jobs** > job name > **Complete Failover**. This does the following:
  - Shuts down the Azure machine.
  - Transfers the latest changes to the on-premises VM.
  - Starts the on-premises VM.
7. You can now sign into the on-premises VM machine to check that it's available as expected.
8. The virtual machine is in a commit pending state. Click **Commit** to commit the failover.
9. To complete the failback, click **Reverse Replicate** to start replicating the on-premises VM to Azure again.

## Fail back to an alternate location

Fail back to an alternate location as follows:

1. If you're setting up new hardware, install a [supported version of Windows](#), and the Hyper-V role on the machine.
2. Create a virtual network switch with the same name that you had on the original server.
3. In **Protected Items** > **Protection Group** > <ProtectionGroupName> -> <VirtualMachineName>, select the VM you want to fail back, and then select **Planned Failover**.
4. In **Confirm Planned Failovers**, elect **Create on-premises virtual machine if it does not exist**.
5. In **Host Name**, select the new Hyper-V host server on which you want to place the VM.
6. In **Data Synchronization**, we recommend you select the option to synchronize the data before the failover. This minimizes downtime for VMs as it synchronizes without shutting them down. It does the following:
  - **Phase 1**: Takes snapshot of the Azure VM and copies it to the on-premises Hyper-V host. The machine continues running in Azure.
  - **Phase 2**: Shuts down the Azure VM so that no new changes occur there. The final set of changes is transferred to the on-premises server and the on-premises virtual machine is started up.
7. Click the checkmark to begin the failover (failback).
8. After the initial synchronization finishes and you're ready to shut down the Azure VM, click **Jobs** > <planned failover job> > **Complete Failover**. This shuts down the Azure machine, transfers the latest changes to the on-premises VM, and starts it.
9. You can sign into the on-premises VM to verify that everything is working as expected.
10. Click **Commit** to finish the failover. Commit deletes the Azure VM and its disks, and prepares the on-premises VM to be protected again.
11. Click **Reverse Replicate** to start replicating the on-premises VM to Azure. Only the delta changes since the VM was turned off in Azure will be replicated.

**NOTE**

If you cancel the failback job during data synchronization, the on-premises VM will be in a corrupted state. This is because data synchronization copies the latest data from Azure VM disks to the on-premises data disks, and until the synchronization completes, the disk data may not be in a consistent state. If the on-premises VM starts after data synchronization is canceled, it might not boot. In this case, rerun the failover to complete data synchronization.

## Next steps

After the on-premises VM is replicating to Azure, you can [run another failover](#) to Azure as needed.

# Deprecation of Site Recovery data encryption feature

11/15/2019 • 2 minutes to read • [Edit Online](#)

This document describes the deprecation details and the remediation action you need to take if you are using the Site Recovery data encryption feature while configuring disaster recovery of Hyper-V virtual machines to Azure.

## Deprecation information

The Site Recovery data encryption feature was available for customers protecting Hyper-V vms to ensure that the replicated data was protected against security threats. this feature will be deprecated by **December 30, 2019**. It is being replaced by the more advanced [Encryption at Rest](#) feature, which uses [Storage Service Encryption](#) (SSE). With SSE, data is encrypted before persisting to storage and decrypted on retrieval, and, upon failover to Azure, your VMs will run from the encrypted storage accounts, allowing for an improved recovery time objective (RTO).

Please note that if you are an existing customer using this feature, you would have received communications with the deprecation details and remediation steps.

## What are the implications?

After **December 30, 2019**, any VMs that still use the retired encryption feature will not be allowed to perform failover.

## Required action

To continue successful failover operations, and replications follow the steps mentioned below:

Follow these steps for each VM:

1. [Disable replication](#).
2. [Create a new replication policy](#).
3. [Enable replication](#) and select a storage account with SSE enabled.

After completing the initial replication to storage accounts with SSE enabled, your VMs will be using Encryption at Rest with Azure Site Recovery.

## Next steps

Plan for performing the remediation steps, and execute them at the earliest. In case you have any queries regarding this deprecation, please reach out to Microsoft Support. To read more about Hyper-V to Azure scenario, refer [here](#).

# Upgrade Windows Server Server/System Center 2012 R2 VMM to Windows Server/VMM 2016

11/12/2019 • 5 minutes to read • [Edit Online](#)

This article shows you how to upgrade Windows Server 2012 R2 hosts & SCVMM 2012 R2 that are configured with Azure Site Recovery, to Windows Server 2016 & SCVMM 2016

Site Recovery contributes to your business continuity and disaster recovery (BCDR) strategy. The service ensures that your VM workloads remain available when expected and unexpected outages occur.

## IMPORTANT

When you upgrade Windows Server 2012 R2 hosts that are already configured for replication with Azure Site Recovery, you must follow the steps mentioned in this document. Any alternate path chosen for upgrade can result in unsupported states and can result in a break in replication or ability to perform failover.

In this article, you learn how to upgrade the following configurations in your environment:

- **Windows Server 2012 R2 hosts which aren't managed by SCVMM**
- **Windows Server 2012 R2 hosts which are managed by a standalone SCVMM 2012 R2 server**
- **Windows Server 2012 R2 hosts which are managed by highly available SCVMM 2012 R2 server**

## Prerequisites & factors to consider

Before you upgrade, note the following:-

- If you have Windows Server 2012 R2 hosts that are not managed by SCVMM, and its a stand-alone environment setup, there will be a break in replication if you try to perform the upgrade.
- If you had selected "*not store my Keys in Active Directory under Distributed Key Management*" while installing SCVMM 2012 R2 in the first place, the upgrades will not complete successfully.
- If you are using System Center 2012 R2 VMM,
  - Check the database information on VMM: **VMM console -> settings -> General -> Database connection**
  - Check the service accounts being used for System Center Virtual Machine Manager Agent service
  - Make sure that you have a backup of the VMM Database.
  - Note down the database name of the SCVMM servers involved. This can be done by navigating to **VMM console -> Settings -> General -> Database connection**
  - Note down the VMM ID of both the 2012R2 primary and recovery VMM servers. VMM ID can be found from the registry "HKLM:\SOFTWARE\Microsoft\Microsoft System Center Virtual Machine Manager Server\Setup".
  - Ensure that you the new SCVMMs that you add to the cluster has the same names as was before.
- If you are replicating between two of your sites managed by SCVMMs on both sides, ensure that you upgrade your recovery side first before you upgrade the primary side.

**WARNING**

While upgrading the SCVMM 2012 R2, under Distributed Key Management, select to **store encryption keys in Active Directory**. Choose the settings for the service account and distributed key management carefully. Based on your selection, encrypted data such as passwords in templates might not be available after the upgrade, and can potentially affect replication with Azure Site Recovery

**IMPORTANT**

Please refer to the detailed SCVMM documentation of [prerequisites](#)

## Windows Server 2012 R2 hosts which aren't managed by SCVMM

The list of steps mentioned below applies to the user configuration from [Hyper-V hosts to Azure](#) executed by following this [tutorial](#)

**WARNING**

As mentioned in the prerequisites, these steps only apply to a clustered environment scenario, and not in a stand-alone Hyper-V host configuration.

1. Follow the steps to perform the [rolling cluster upgrade](#) to execute the rolling cluster upgrade process.
2. With every new Windows Server 2016 host that is introduced in the cluster, remove the reference of a Windows Server 2012 R2 host from Azure Site Recovery by following steps mentioned [here]. This should be the host you chose to drain & evict from the cluster.
3. Once the *Update-VMVersion* command has been executed for all virtual machines, the upgrades have been completed.
4. Use the steps mentioned [here](#) to register the new Windows Server 2016 host to Azure Site Recovery. Please note that the Hyper-V site is already active and you just need to register the new host in the cluster.
5. Go to Azure portal and verify the replicated health status inside the Recovery Services

## Upgrade Windows Server 2012 R2 hosts managed by stand-alone SCVMM 2012 R2 server

Before you upgrade your Windows Server 2012 R2 hosts, you need to upgrade the SCVMM 2012 R2 to SCVMM 2016. Follow the below steps:-

### Upgrade standalone SCVMM 2012 R2 to SCVMM 2016

1. Uninstall ASR provider by navigating to Control Panel -> Programs -> Programs and Features -> Microsoft Azure Site Recovery , and click on Uninstall
2. [Retain the SCVMM database and upgrade the operating system](#)
3. In **Add remove programs**, select **VMM > Uninstall**. b. Select **Remove Features**, and then select **VMM management Server and VMM Console**. c. In **Database Options**, select **Retain database**. d. Review the summary and click **Uninstall**.
4. [Install VMM 2016](#)
5. Launch SCVMM and check status of each hosts under **Fabrics** tab. Click **Refresh** to get the most recent status. You should see status as "Needs Attention".

6. Install the latest [Microsoft Azure Site Recovery Provider](#) on the SCVMM.
7. Install the latest [Microsoft Azure Recovery Service \(MARS\) agent](#) on each host of the cluster. Refresh to ensure SCVMM is able to successfully query the hosts.

### **Upgrade Windows Server 2012 R2 hosts to Windows Server 2016**

1. Follow the steps mentioned [here](#) to execute the rolling cluster upgrade process.
2. After adding the new host to the cluster, refresh the host from the SCVMM console to install the VMM Agent on this updated host.
3. Execute *Update-VMVersion* to update the VM versions of the Virtual machines.
4. Go to Azure portal and verify the replicated health status of the virtual machines inside the Recovery Services Vault.

## **Upgrade Windows Server 2012 R2 hosts are managed by highly available SCVMM 2012 R2 server**

Before you upgrade your Windows Server 2012 R2 hosts, you need to upgrade the SCVMM 2012 R2 to SCVMM 2016. The following modes of upgrade are supported while upgrading SCVMM 2012 R2 servers configured with Azure Site Recovery - Mixed mode with no additional VMM servers & Mixed mode with additional VMM servers.

### **Upgrade SCVMM 2012 R2 to SCVMM 2016**

1. Uninstall ASR provider by navigating to Control Panel -> Programs -> Programs and Features -> Microsoft Azure Site Recovery , and click on Uninstall
2. Follow the steps mentioned [here](#) based on the mode of upgrade you wish to execute.
3. Launch SCVMM console and check status of each hosts under **Fabrics** tab. Click **Refresh** to get the most recent status. You should see status as "Needs Attention".
4. Install the latest [Microsoft Azure Site Recovery Provider](#) on the SCVMM.
5. Update the latest [Microsoft Azure Recovery Service \(MARS\) agent](#) on each host of the cluster. Refresh to ensure SC VMM is able to successfully query the hosts.

### **Upgrade Windows Server 2012 R2 hosts to Windows Server 2016**

1. Follow the steps mentioned [here](#) to execute the rolling cluster upgrade process.
2. After adding the new host to the cluster, refresh the host from the SCVMM console to install the VMM Agent on this updated host.
3. Execute *Update-VMVersion* to update the VM versions of the Virtual machines.
4. Go to Azure portal and verify the replicated health status of the virtual machines inside the Recovery Services Vault.

## **Next steps**

Once the upgrade of the hosts is performed, you can perform a [test failover](#) to test the health of your replication and disaster recovery status.

# Remove servers and disable protection

7/14/2019 • 8 minutes to read • [Edit Online](#)

This article describes how to unregister servers from a Recovery Services vault, and how to disable protection for machines protected by Site Recovery.

## Unregister a configuration server

If you replicate VMware VMs or Windows/Linux physical servers to Azure, you can unregister an unconnected configuration server from a vault as follows:

1. [Disable protection of virtual machines](#).
2. [Disassociate or delete replication policies](#).
3. [Delete the configuration server](#)

## Unregister a VMM server

1. Stop replicating virtual machines in clouds on the VMM server you want to remove.
2. Delete any network mappings used by clouds on the VMM server that you want to delete. In **Site Recovery Infrastructure > For System Center VMM > Network Mapping**, right-click the network mapping > **Delete**.
3. Note the ID of the VMM server.
4. Disassociate replication policies from clouds on the VMM server you want to remove. In **Site Recovery Infrastructure > For System Center VMM > Replication Policies**, double-click the associated policy. Right-click the cloud > **Disassociate**.
5. Delete the VMM server or active node. In **Site Recovery Infrastructure > For System Center VMM > VMM Servers**, right-click the server > **Delete**.
6. If your VMM server was in a Disconnected state, then download and run the [cleanup script](#) on the VMM server. Open PowerShell with the **Run as Administrator** option, to change the execution policy for the default (LocalMachine) scope. In the script, specify the ID of the VMM server you want to remove. The script removes registration and cloud pairing information from the server.
7. Run the cleanup script on any secondary VMM server.
8. Run the cleanup script on any other passive VMM cluster nodes that have the Provider installed.
9. Uninstall the Provider manually on the VMM server. If you have a cluster, remove from all nodes.
10. If your virtual machines were replicating to Azure, you need to uninstall the Microsoft Recovery Services agent from Hyper-V hosts in the deleted clouds.

## Unregister a Hyper-V host in a Hyper-V Site

Hyper-V hosts that aren't managed by VMM are gathered into a Hyper-V site. Remove a host in a Hyper-V site as follows:

1. Disable replication for Hyper-V VMs located on the host.
2. Disassociate policies for the Hyper-V site. In **Site Recovery Infrastructure > For Hyper-V Sites > Replication Policies**, double-click the associated policy. Right-click the site > **Disassociate**.
3. Delete Hyper-V hosts. In **Site Recovery Infrastructure > For Hyper-V Sites > Hyper-V Hosts**, right-click the server > **Delete**.
4. Delete the Hyper-V site after all hosts have been removed from it. In **Site Recovery Infrastructure > For Hyper-V Sites**, right-click the site > **Delete**.

**Hyper-V Sites > Hyper-V Sites**, right-click the site > **Delete**.

5. If your Hyper-V host was in a **Disconnected** state, then run the following script on each Hyper-V host that you removed. The script cleans up settings on the server, and unregisters it from the vault.

```
pushd .
try
{
 $windowsIdentity=[System.Security.Principal.WindowsIdentity]::GetCurrent()
 $principal=new-object System.Security.Principal.WindowsPrincipal($windowsIdentity)
 $administrators=[System.Security.Principal.WindowsBuiltInRole]::Administrator
 $isAdmin=$principal.IsInRole($administrators)
 if (!$isAdmin)
 {
 "Please run the script as an administrator in elevated mode."
 $choice = Read-Host
 return;
 }

 $error.Clear()
 "This script will remove the old Azure Site Recovery Provider related properties. Do you want to continue (Y/N) ?"
 $choice = Read-Host

 if (!($choice -eq 'Y' -or $choice -eq 'y'))
 {
 "Stopping cleanup."
 return;
 }

 $serviceName = "dra"
 $service = Get-Service -Name $serviceName
 if ($service.Status -eq "Running")
 {
 "Stopping the Azure Site Recovery service..."
 net stop $serviceName
 }

 $asrHivePath = "HKLM:\SOFTWARE\Microsoft\Azure Site Recovery"
 $registrationPath = $asrHivePath + '\Registration'
 $proxySettingsPath = $asrHivePath + '\ProxySettings'
 $draIdvalue = 'DraID'
 $idMgmtCloudContainerId='IdMgmtCloudContainerId'

 if (Test-Path $asrHivePath)
 {
 if (Test-Path $registrationPath)
 {
 "Removing registration related registry keys."
 Remove-Item -Recurse -Path $registrationPath
 }

 if (Test-Path $proxySettingsPath)
 {
 "Removing proxy settings"
 Remove-Item -Recurse -Path $proxySettingsPath
 }

 $regNode = Get-ItemProperty -Path $asrHivePath
 if($regNode.DraID -ne $null)
 {
 "Removing DraId"
 Remove-ItemProperty -Path $asrHivePath -Name $draIdValue
 }
 if($regNode.IdMgmtCloudContainerId -ne $null)
 {
 "Removing IdMgmtCloudContainerId"
 }
 }
}
```

```

 Remove-ItemProperty -Path $asrHivePath -Name $idMgmtCloudContainerId
 }
 "Registry keys removed."
}

First retrieve all the certificates to be deleted
$ASRcerts = Get-ChildItem -Path cert:\localmachine\my | where-object
{$_.friendlyname.startswith('ASR_SRSAUTH_CERT_KEY_CONTAINER') -or
$_.friendlyname.startswith('ASR_HYPER_V_HOST_CERT_KEY_CONTAINER')}
Open a cert store object
$store = New-Object System.Security.Cryptography.X509Certificates.X509Store("My","LocalMachine")
$store.Open('ReadWrite')
Delete the certs
"Removing all related certificates"
foreach ($cert in $ASRcerts)
{
 $store.Remove($cert)
}
}catch
{
 [system.exception]
 Write-Host "Error occurred" -ForegroundColor "Red"
 $error[0]
 Write-Host "FAILED" -ForegroundColor "Red"
}
popd

```

## Disable protection for a VMware VM or physical server (VMware to Azure)

1. In **Protected Items > Replicated Items**, right-click the machine > **Disable replication**.
2. In **Disable replication** page, select one of these options:
  - **Disable replication and remove (recommended)** - This option removes the replicated item from Azure Site Recovery and the replication for the machine is stopped. Replication configuration on Configuration Server is cleaned up and Site Recovery billing for this protected server is stopped. Note that this option can only be used when Configuration Server is in connected state.
  - **Remove** - This option is supposed to be used only if the source environment is deleted or not accessible (not connected). This removes the replicated item from Azure Site Recovery (billing is stopped). Replication configuration on the Configuration Server **will not** be cleaned up.

### NOTE

In both the options mobility service will not be uninstalled from the protected servers, you need to uninstall it manually. If you plan to protect the server again using the same Configuration server, you can skip uninstalling the mobility service.

### NOTE

If you have already failed over a VM and it is running in Azure, note that disable protection doesn't remove / affect the failed over VM.

## Disable protection for a Azure VM (Azure to Azure)

- In **Protected Items > Replicated Items**, right-click the machine > **Disable replication**.

**NOTE**

mobility service will not be uninstalled from the protected servers, you need to uninstall it manually. If you plan to protect the server again, you can skip uninstalling the mobility service.

## Disable protection for a Hyper-V virtual machine (Hyper-V to Azure)

**NOTE**

Use this procedure if you're replicating Hyper-V VMs to Azure without a VMM server. If you are replicating your virtual machines using the **System Center VMM to Azure** scenario, then follow the instructions Disable protection for a Hyper-V virtual machine replicating using the System Center VMM to Azure scenario

1. In **Protected Items > Replicated Items**, right-click the machine > **Disable replication**.
2. In **Disable replication**, you can select the following options:
  - **Disable replication and remove (recommended)** - This option removes the replicated item from Azure Site Recovery and the replication for the machine is stopped. Replication configuration on the on-premises virtual machine will be cleaned up and Site Recovery billing for this protected server is stopped.
  - **Remove** - This option is supposed to be used only if the source environment is deleted or not accessible (not connected). This removes the replicated item from Azure Site Recovery (billing is stopped). Replication configuration on the on-premises virtual machine **will not** be cleaned up.

**NOTE**

> If you chose the \*\*Remove\*\* option then run the following set of scripts to clean up the replication settings on-premises Hyper-V Server.

**NOTE**

If you have already failed over a VM and it is running in Azure, note that disable protection doesn't remove / affect the failed over VM.

1. On the source Hyper-V host server, to remove replication for the virtual machine. Replace SQLVM1 with the name of your virtual machine and run the script from an administrative PowerShell

```
$vmName = "SQLVM1"
$vm = Get-WmiObject -Namespace "root\virtualization\v2" -Query "Select * From MsVm_ComputerSystem Where ElementName = '$vmName'"
$replicationService = Get-WmiObject -Namespace "root\virtualization\v2" -Query "Select * From MsVm_ReplicationService"
$replicationService.RemoveReplicationRelationship($vm.__PATH)
```

## Disable protection for a Hyper-V virtual machine replicating to Azure using the System Center VMM to Azure scenario

1. In **Protected Items > Replicated Items**, right-click the machine > **Disable replication**.
2. In **Disable replication**, select one of these options:

- **Disable replication and remove (recommended)** - This option remove the replicated item from Azure Site Recovery and the replication for the machine is stopped. Replication configuration on the on-premises virtual machine is cleaned up and Site Recovery billing for this protected server is stopped.
- **Remove** - This option is supposed to be used only if the source environment is deleted or not accessible (not connected). This removes the replicated item from Azure Site Recovery (billing is stopped). Replication configuration on the on-premises virtual machine **will not** be cleaned up.

**NOTE**

If you chose the **Remove** option, then run the following scripts to clean up the replication settings on-premises VMM Server.

3. Run this script on the source VMM server, using PowerShell (administrator privileges required) from the VMM console. Replace the placeholder **SQLVM1** with the name of your virtual machine.

```
$vm = get-scvirtualmachine -Name "SQLVM1"
Set-SCVirtualMachine -VM $vm -ClearDRProtection
```

4. The above steps clear the replication settings on the VMM server. To stop replication for the virtual machine running on the Hyper-V host server, run this script. Replace SQLVM1 with the name of your virtual machine, and host01.contoso.com with the name of the Hyper-V host server.

```
$vmName = "SQLVM1"
$hostName = "host01.contoso.com"
$vm = Get-WmiObject -Namespace "root\virtualization\v2" -Query "Select * From MsVm_ComputerSystem Where ElementName = '$vmName'" -computername $hostName
$replicationService = Get-WmiObject -Namespace "root\virtualization\v2" -Query "Select * From MsVm_ReplicationService" -computername $hostName
$replicationService.RemoveReplicationRelationship($vm.__PATH)
```

## Disable protection for a Hyper-V virtual machine replicating to secondary VMM Server using the System Center VMM to VMM scenario

1. In **Protected Items > Replicated Items**, right-click the machine > **Disable replication**.
2. In **Disable replication**, select one of these options:
  - **Disable replication and remove (recommended)** - This option remove the replicated item from Azure Site Recovery and the replication for the machine is stopped. Replication configuration on the on-premises virtual machine is cleaned up and Site Recovery billing for this protected server is stopped.
  - **Remove** - This option is supposed to be used only if the source environment is deleted or not accessible (not connected). This removes the replicated item from Azure Site Recovery (billing is stopped). Replication configuration on the on-premises virtual machine **will not** be cleaned up. Run the following set of scripts to clean up the replication settings on-premises virtual machines.

**NOTE**

If you chose the **Remove** option, then run the following scripts to clean up the replication settings on-premises VMM Server.

3. Run this script on the source VMM server, using PowerShell (administrator privileges required) from the VMM console. Replace the placeholder **SQLVM1** with the name of your virtual machine.

```
$vm = get-scvirtualmachine -Name "SQLVM1"
Set-SCVirtualMachine -VM $vm -ClearDRProtection
```

4. On the secondary VMM server, run this script to clean up the settings for the secondary virtual machine:

```
$vm = get-scvirtualmachine -Name "SQLVM1"
Remove-SCVirtualMachine -VM $vm -Force
```

5. On the secondary VMM server, refresh the virtual machines on the Hyper-V host server, so that the secondary VM gets detected again in the VMM console.

6. The above steps clear up the replication settings on the VMM server. If you want to stop replication for the virtual machine, run the following script on the primary and secondary VMs. Replace SQLVM1 with the name of your virtual machine.

```
Remove-VMReplication -VMName "SQLVM1"
```

# Service updates in Site Recovery

9/11/2019 • 4 minutes to read • [Edit Online](#)

This article provides an overview of [Azure Site Recovery](#) updates, and describes how to upgrade Site Recovery components.

Site Recovery publishes service updates on a regular basis. Updates include new features, support improvements, component updates, and bug fixes. In order to take advantage of the latest features and fixes, we recommend running the latest versions of Site Recovery components.

## Updates support

### Support statement for Azure Site Recovery

We recommend always upgrading to the latest component versions:

**With every new version 'N' of an Azure Site Recovery component that's released, all versions below 'N-4' are considered to be out of support.**

#### IMPORTANT

Official support is for upgrading from > N-4 version to N version. For example, if you're running you are on N-6, you need to first upgrade to N-4, and then upgrade to N.

### Links to currently supported update rollups

Review the latest update rollup (version N) in [this article](#). Remember that Site Recovery provides support for N-4 versions.

## Component expiry

Site Recovery notifies you of expired components (or nearing expiry) by email (if you subscribed to email notifications), or on the vault dashboard in the portal.

- In addition, when updates are available, in the infrastructure view for your scenario in the portal, an **Update available** button appears next to the component. This button redirects you to a link for downloading the latest component version.
- Vaults dashboard notifications aren't available if you're replicating Hyper-V VMs.

Emails notifications are sent as follows.

TIME	FREQUENCY
60 days before component expiry	Once bi-weekly
Next 53 days	Once a week
Last 7 days	Once a day
After expiry	Once bi-weekly

### Upgrading outside official support

If the difference between your component version and the latest release version is greater than four, this is considered out of support. In this case, upgrade as follows:

1. Upgrade the currently installed component to your current version plus four. For example, if your version is 9.16, then upgrade to 9.20.
2. Then, upgrade to the next compatible version. So in our example, after upgrading 9.16 to 9.20, upgrade to 9.24.

Follow the same process for all relevant components.

### Support for latest operating systems/kernels

#### NOTE

If you have a maintenance window scheduled, and a reboot is included in it, we recommend that you first upgrade Site Recovery components, and then proceed with the rest of the scheduled activities in the maintenance window.

1. Before upgrading operating system/kernel versions, verify if the target version is supported Site Recovery.
  - [Azure VM support](#).
  - [VMware/physical server support](#)
  - [Hyper-V support](#).
2. Review [available updates](#) to find out what you want to upgrade.
3. Upgrade to the latest Site Recovery version.
4. Upgrade the operating system/kernel to the required versions.
5. Reboot.

This process ensures that the machine operating system/kernel is upgraded to the latest version, and that the latest Site Recovery changes needed to support the new version are loaded on to the machine.

## Azure VM disaster recovery to Azure

In this scenario, we strongly recommend that you [enable automatic updates](#). You can allow Site Recovery to manage updates as follows:

- During the enable replication process.
- By setting the extension update settings inside the vault.

If you want to manually manage updates, do the following:

1. In the vault > **Replicated Items**, click this notification at the top of the screen:

**New Site Recovery replication agent update is available. Click to install ->**

2. Select the VMs for which you want to apply the update, and then click **OK**.

## VMware VM/physical server disaster recovery to Azure

1. Based on your current version and the [support statement](#), install the update first on the on-premises configuration server, using [these instructions](#).
2. If you have scale-out process servers, update them next, using [these instructions](#).
3. To update the Mobility agent on each protected machine, refer to [this article](#).

### Reboot after Mobility service upgrade

A reboot is recommended after every upgrade of the Mobility service, to ensure that all the latest changes are loaded on the source machine.

A reboot isn't mandatory, unless the difference between the agent version during last reboot, and the current version, is greater than four.

The example in the table shows how this works.

AGENT VERSION (LAST REBOOT)	UPGRADE TO	MANDATORY REBOOT?
9.16	9.18	Not mandatory
9.16	9.19	Not mandatory
9.16	9.20	Not mandatory
9.16	9.21	Mandatory.  Upgrade to 9.20, then reboot before upgrading to 9.21.

## Hyper-V VM disaster recovery to Azure

### Between a Hyper-V site and Azure

1. Download the update for the Microsoft Azure Site Recovery Provider.
2. Install the Provider on each Hyper-V server registered in Site Recovery. If you're running a cluster, upgrade on all cluster nodes.

### Between an on-premises VMM site and Azure

1. Download the update for the Microsoft Azure Site Recovery Provider.
2. Install the Provider on the VMM server. If VMM is deployed in a cluster, install the Provider on all cluster nodes.
3. Install the latest Microsoft Azure Recovery Services agent on all Hyper-V hosts or cluster nodes.

### Between two on-premises VMM sites

1. Download the latest update for the Microsoft Azure Site Recovery Provider.
2. Install the latest Provider on the VMM server managing the secondary recovery site. If VMM is deployed in a cluster, install the Provider on all cluster nodes.
3. After the recovery site is updated, install the Provider on the VMM server that's managing the primary site.

## Next steps

Follow our [Azure Updates](#) page to track new updates and releases.

# Delete a Site Recovery Services vault

1/10/2020 • 2 minutes to read • [Edit Online](#)

This article describes how to delete a Recovery Services vault for Site Recovery. To delete a vault used in Azure Backup, see [Delete a Backup vault in Azure](#).

## NOTE

This article has been updated to use the new Azure PowerShell Az module. You can still use the AzureRM module, which will continue to receive bug fixes until at least December 2020. To learn more about the new Az module and AzureRM compatibility, see [Introducing the new Azure PowerShell Az module](#). For Az module installation instructions, see [Install Azure PowerShell](#).

## Before you start

Before you can delete a vault you must remove registered servers, and items in the vault. What you need to remove depends on the replication scenarios you've deployed.

## Delete a vault-Azure VM to Azure

1. Follow [these instructions](#) to delete all protected VMs.
2. Then, delete the vault.

## Delete a vault-VMware VM to Azure

1. Follow [these instructions](#) to delete all protected VMs.
2. Follow [these steps](#) to delete all replication policies.
3. Delete references to vCenter using [these steps](#).
4. Follow [these instructions](#) to decommission a configuration server.
5. Then, delete the vault.

## Delete a vault-Hyper-V VM (with VMM) to Azure

1. Follow [these steps](#) to delete Hyper-V VMs managed by System Center VMM.
2. Disassociate and delete all replication policies. Do this in your vault > **Site Recovery Infrastructure > For System Center VMM > Replication Policies**.
3. Follow [these steps](#) to unregister a connected VMM server.
4. Then, delete the vault.

## Delete a vault-Hyper-V VM to Azure

1. Follow [these steps](#) to delete all protected VMs.
2. Disassociate and delete all replication policies. Do this in your vault > **Site Recovery Infrastructure > For Hyper-V Sites > Replication Policies**.
3. Follow [these instructions](#) to unregister a Hyper-V host.
4. Delete the Hyper-V site.
5. Then, delete the vault.

## Use PowerShell to force delete the vault

### IMPORTANT

If you're testing the product and aren't concerned about data loss, use the force delete method to rapidly remove the vault and all its dependencies. The PowerShell command deletes all the contents of the vault and is **not reversible**.

To delete the Site Recovery vault even if there are protected items, use these commands:

```
Connect-AzAccount

Select-AzSubscription -SubscriptionName "XXXXX"

$vault = Get-AzRecoveryServicesVault -Name "vaultname"

Remove-AzRecoveryServicesVault -Vault $vault
```

Learn more about [Get-AzRecoveryServicesVault](#), and [Remove-AzRecoveryServicesVault](#).

# About disaster recovery for on-premises apps

10/10/2019 • 8 minutes to read • [Edit Online](#)

This article describes on-premises workloads and apps you can protect for disaster recovery with the [Azure Site Recovery](#) service.

## Overview

Organizations need a business continuity and disaster recovery (BCDR) strategy to keep workloads and data safe and available during planned and unplanned downtime, and recover to regular working conditions as soon as possible.

Site Recovery is an Azure service that contributes to your BCDR strategy. Using Site Recovery, you can deploy application-aware replication to the cloud, or to a secondary site. Whether your apps are Windows or Linux-based, running on physical servers, VMware or Hyper-V, you can use Site Recovery to orchestrate replication, perform disaster recovery testing, and run failovers and failback.

Site Recovery integrates with Microsoft applications, including SharePoint, Exchange, Dynamics, SQL Server, and Active Directory. Microsoft also works closely with leading vendors including Oracle, SAP, and Red Hat. You can customize replication solutions on an app-by-app basis.

## Why use Site Recovery for application replication?

Site Recovery contributes to application-level protection and recovery as follows:

- App-agnostic, providing replication for any workloads running on a supported machine.
- Near-synchronous replication, with RPOs as low as 30 seconds to meet the needs of most critical business apps.
- App-consistent snapshots, for single or multi-tier applications.
- Integration with SQL Server AlwaysOn, and partnership with other application-level replication technologies, including AD replication, SQL AlwaysOn, Exchange Database Availability Groups (DAGs).
- Flexible recovery plans, that enable you to recover an entire application stack with a single click, and to include external scripts and manual actions in the plan.
- Advanced network management in Site Recovery and Azure to simplify app network requirements, including the ability to reserve IP addresses, configure load-balancing, and integration with Azure Traffic Manager, for low RTO network switchovers.
- A rich automation library that provides production-ready, application-specific scripts that can be downloaded and integrated with recovery plans.

## Workload summary

Site Recovery can replicate any app running on a supported machine. In addition, we've partnered with product teams to carry out additional testing for the apps specified in the table.

WORKLOAD	REPLICATE AZURE VMS TO AZURE	REPLICATE HYPER-V VMS TO A SECONDARY SITE	REPLICATE HYPER-V VMS TO AZURE	REPLICATE VMWARE VMS TO A SECONDARY SITE	REPLICATE VMWARE VMS TO AZURE
Active Directory, DNS	Y	Y	Y	Y	Y

WORKLOAD	REPLICATE AZURE VMS TO AZURE	REPLICATE HYPER-V VMS TO A SECONDARY SITE	REPLICATE HYPER-V VMS TO AZURE	REPLICATE VMWARE VMS TO A SECONDARY SITE	REPLICATE VMWARE VMS TO AZURE
Web apps (IIS, SQL)	Y	Y	Y	Y	Y
System Center Operations Manager	Y	Y	Y	Y	Y
SharePoint	Y	Y	Y	Y	Y
SAP Replicate SAP site to Azure for non-cluster	Y (tested by Microsoft)	Y (tested by Microsoft)	Y (tested by Microsoft)	Y (tested by Microsoft)	Y (tested by Microsoft)
Exchange (non-DAG)	Y	Y	Y	Y	Y
Remote Desktop/VDI	Y	Y	Y	Y	Y
Linux (operating system and apps)	Y (tested by Microsoft)	Y (tested by Microsoft)	Y (tested by Microsoft)	Y (tested by Microsoft)	Y (tested by Microsoft)
Dynamics AX	Y	Y	Y	Y	Y
Windows File Server	Y	Y	Y	Y	Y
Citrix XenApp and XenDesktop	Y	N/A	Y	N/A	Y

## Replicate Active Directory and DNS

An Active Directory and DNS infrastructure are essential to most enterprise apps. During disaster recovery, you'll need to protect and recover these infrastructure components, before recovering your workloads and apps.

You can use Site Recovery to create a complete automated disaster recovery plan for Active Directory and DNS. For example, if you want to fail over SharePoint and SAP from a primary to a secondary site, you can set up a recovery plan that fails over Active Directory first, and then an additional app-specific recovery plan to fail over the other apps that rely on Active Directory.

[Learn more](#) about protecting Active Directory and DNS.

## Protect SQL Server

SQL Server provides a data services foundation for data services for many business apps in an on-premises data center. Site Recovery can be used together with SQL Server HA/DR technologies, to protect multi-tiered enterprise apps that use SQL Server. Site Recovery provides:

- A simple and cost-effective disaster recovery solution for SQL Server. Replicate multiple versions and editions of SQL Server standalone servers and clusters, to Azure or to a secondary site.

- Integration with SQL AlwaysOn Availability Groups, to manage failover and failback with Azure Site Recovery recovery plans.
- End-to-end recovery plans for the all tiers in an application, including the SQL Server databases.
- Scaling of SQL Server for peak loads with Site Recovery, by “bursting” them into larger IaaS virtual machine sizes in Azure.
- Easy testing of SQL Server disaster recovery. You can run test failovers to analyze data and run compliance checks, without impacting your production environment.

[Learn more](#) about protecting SQL server.

## Protect SharePoint

Azure Site Recovery helps protect SharePoint deployments, as follows:

- Eliminates the need and associated infrastructure costs for a stand-by farm for disaster recovery. Use Site Recovery to replicate an entire farm (Web, app and database tiers) to Azure or to a secondary site.
- Simplifies application deployment and management. Updates deployed to the primary site are automatically replicated, and are thus available after failover and recovery of a farm in a secondary site. Also lowers the management complexity and costs associated with keeping a stand-by farm up-to-date.
- Simplifies SharePoint application development and testing by creating a production-like copy on-demand replica environment for testing and debugging.
- Simplifies transition to the cloud by using Site Recovery to migrate SharePoint deployments to Azure.

[Learn more](#) about protecting SharePoint.

## Protect Dynamics AX

Azure Site Recovery helps protect your Dynamics AX ERP solution, by:

- Orchestrating replication of your entire Dynamics AX environment (Web and AOS tiers, database tiers, SharePoint) to Azure, or to a secondary site.
- Simplifying migration of Dynamics AX deployments to the cloud (Azure).
- Simplifying Dynamics AX application development and testing by creating a production-like copy on-demand, for testing and debugging.

[Learn more](#) about protecting Dynamic AX.

## Protect RDS

Remote Desktop Services (RDS) enables virtual desktop infrastructure (VDI), session-based desktops, and applications, allowing users to work anywhere. With Azure Site Recovery you can:

- Replicate managed or unmanaged pooled virtual desktops to a secondary site, and remote applications and sessions to a secondary site or Azure.
- Here's what you can replicate:

RDS	REPLICATE AZURE VMS TO AZURE	REPLICATE HYPER-V VMs TO A SECONDARY SITE	REPLICATE HYPER-V VMs TO AZURE	REPLICATE VMWARE VMs TO A SECONDARY SITE	REPLICATE VMWARE VMs TO AZURE	REPLICATE PHYSICAL SERVERS TO A SECONDARY SITE	REPLICATE PHYSICAL SERVERS TO AZURE
<b>Pooled Virtual Desktop (unmanaged)</b>	No	Yes	No	Yes	No	Yes	No
<b>Pooled Virtual Desktop (managed and without UPD)</b>	No	Yes	No	Yes	No	Yes	No
<b>Remote applications and Desktop sessions (without UPD)</b>	Yes	Yes	Yes	Yes	Yes	Yes	Yes

[Set up disaster recovery for RDS using Azure Site Recovery.](#)

[Learn more](#) about protecting RDS.

## Protect Exchange

Site Recovery helps protect Exchange, as follows:

- For small Exchange deployments, such as a single or standalone server, Site Recovery can replicate and fail over to Azure or to a secondary site.
- For larger deployments, Site Recovery integrates with Exchange DAGs.
- Exchange DAGs are the recommended solution for Exchange disaster recovery in an enterprise. Site Recovery recovery plans can include DAGs, to orchestrate DAG failover across sites.

[Learn more](#) about protecting Exchange.

## Protect SAP

Use Site Recovery to protect your SAP deployment, as follows:

- Enable protection of SAP NetWeaver and non-NetWeaver Production applications running on-premises, by replicating components to Azure.
- Enable protection of SAP NetWeaver and non-NetWeaver Production applications running Azure, by replicating components to another Azure datacenter.
- Simplify cloud migration, by using Site Recovery to migrate your SAP deployment to Azure.
- Simplify SAP project upgrades, testing, and prototyping, by creating a production clone on-demand for testing SAP applications.

[Learn more](#) about protecting SAP.

## Protect IIS

Use Site Recovery to protect your IIS deployment, as follows:

Azure Site Recovery provides disaster recovery by replicating the critical components in your environment to a cold remote site or a public cloud like Microsoft Azure. Since the virtual machines with the web server and the database are being replicated to the recovery site, there is no requirement to backup configuration files or certificates separately. The application mappings and bindings dependent on environment variables that are changed post failover can be updated through scripts integrated into the disaster recovery plans. Virtual machines are brought up on the recovery site only in the event of a failover. Not only this, Azure Site Recovery also helps you orchestrate the end to end failover by providing you the following capabilities:

- Sequencing the shutdown and startup of virtual machines in the various tiers.
- Adding scripts to allow update of application dependencies and bindings on the virtual machines after they have been started up. The scripts can also be used to update the DNS server to point to the recovery site.
- Allocate IP addresses to virtual machines pre-failover by mapping the primary and recovery networks and hence use scripts that do not need to be updated post failover.
- Ability for a one-click failover for multiple web applications on the web servers, thus eliminating the scope for confusion in the event of a disaster.
- Ability to test the recovery plans in an isolated environment for DR drills.

[Learn more](#) about protecting IIS web farm.

## Protect Citrix XenApp and XenDesktop

Use Site Recovery to protect your Citrix XenApp and XenDesktop deployments, as follows:

- Enable protection of the Citrix XenApp and XenDesktop deployment, by replicating different deployment layers including (AD DNS server, SQL database server, Citrix Delivery Controller, StoreFront server, XenApp Master (VDA), Citrix XenApp License Server) to Azure.
- Simplify cloud migration, by using Site Recovery to migrate your Citrix XenApp and XenDesktop deployment to Azure.
- Simplify Citrix XenApp/XenDesktop testing, by creating a production-like copy on-demand for testing and debugging.
- This solution is only applicable for Windows Server operating system virtual desktops and not client virtual desktops as client virtual desktops are not yet supported for licensing in Azure. [Learn More](#) about licensing for client/server desktops in Azure.

[Learn more](#) about protecting Citrix XenApp and XenDesktop deployments. Alternatively, you can refer the [whitepaper from Citrix](#) detailing the same.

## Next steps

[Get started](#) with Azure VM replication.

# Set up disaster recovery for Active Directory and DNS

11/14/2019 • 10 minutes to read • [Edit Online](#)

Enterprise applications such as SharePoint, Dynamics AX, and SAP depend on Active Directory and a DNS infrastructure to function correctly. When you set up disaster recovery for applications, you often need to recover Active Directory and DNS before you recover other application components, to ensure correct application functionality.

You can use [Site Recovery](#) to create a disaster recovery plan for Active Directory. When a disruption occurs, you can initiate a failover. You can have Active Directory up and running in a few minutes. If you have deployed Active Directory for multiple applications in your primary site, for example, for SharePoint and SAP, you might want to fail over the complete site. You can first fail over Active Directory using Site Recovery. Then, fail over the other applications, using application-specific recovery plans.

This article explains how to create a disaster recovery solution for Active Directory. It includes prerequisites, and failover instructions. You should be familiar with Active Directory and Site Recovery before you begin.

## Prerequisites

- If you're replicating to Azure, [prepare Azure resources](#), including a subscription, an Azure Virtual Network, a storage account, and a Recovery Services vault.
- Review the [support requirements](#) for all components.

## Replicate the domain controller

- You must set up Site Recovery replication, on at least one VM that hosts a domain controller or DNS.
- If you have multiple domain controllers in your environment, you also must set up an additional domain controller on the target site. The additional domain controller can be in Azure, or in a secondary on-premises datacenter.
- If you have only a few applications and one domain controller, you might want to fail over the entire site together. In this case, we recommend using Site Recovery to replicate the domain controller to the target site (either in Azure or in a secondary on-premises datacenter). You can use the same replicated domain controller or DNS virtual machine for [test failover](#).
- If you have many applications and more than one domain controller in your environment, or if you plan to fail over a few applications at a time, in addition to replicating the domain controller virtual machine with Site Recovery, we recommend that you set up an additional domain controller on the target site (either in Azure or in a secondary on-premises datacenter). For [test failover](#), you can use domain controller that's replicated by Site Recovery. For failover, you can use the additional domain controller on the target site.

## Enable protection with Site Recovery

You can use Site Recovery to protect the virtual machine that hosts the domain controller or DNS.

### Protect the VM

The domain controller that is replicated by using Site Recovery is used for [test failover](#). Ensure that it meets the following requirements:

1. The domain controller is a global catalog server.
2. The domain controller should be the FSMO role owner for roles that are needed during a test failover.  
Otherwise, these roles will need to be [seized](#) after the failover.

## Configure VM network settings

For the virtual machine that hosts the domain controller or DNS, in Site Recovery, configure network settings under the **Compute and Network** settings of the replicated virtual machine. This ensures that the virtual machine is attached to the correct network after failover.

# Protect Active Directory

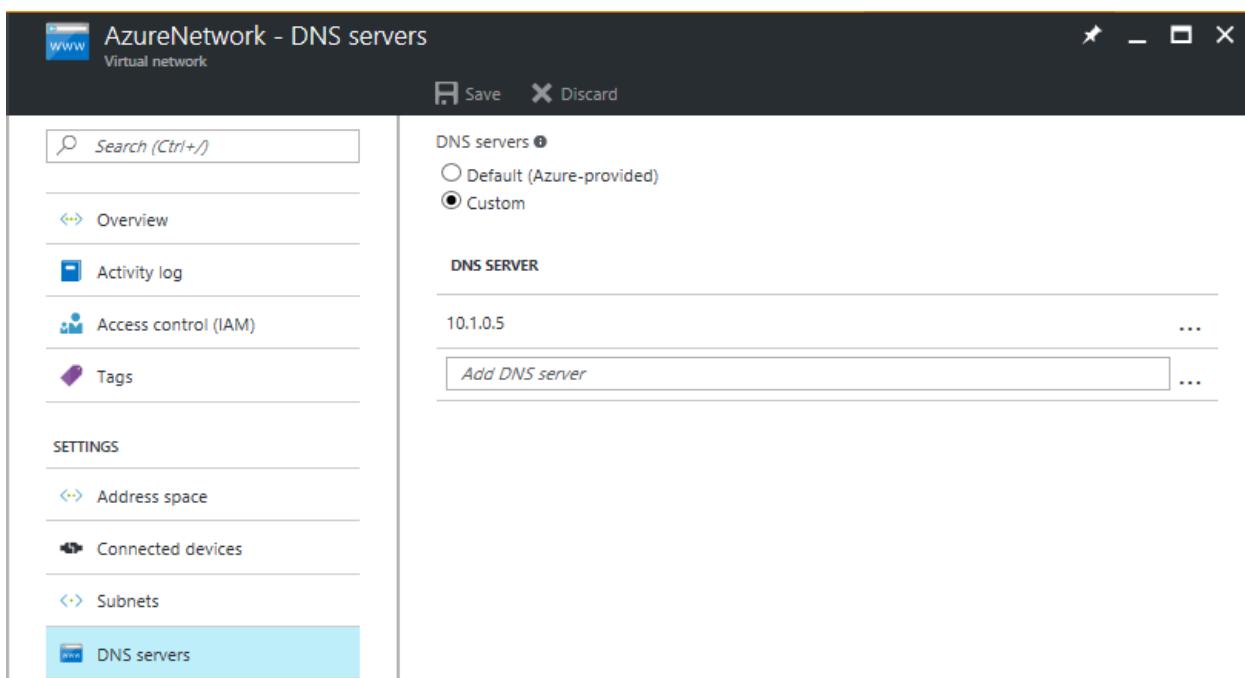
## Site-to-site protection

Create a domain controller on the secondary site. When you promote the server to a domain controller role, specify the name of the same domain that is being used on the primary site. You can use the **Active Directory Sites and Services** snap-in to configure settings on the site link object to which the sites are added. By configuring settings on a site link, you can control when replication occurs between two or more sites, and how often it occurs. For more information, see [Scheduling replication between sites](#).

## Site-to-Azure protection

First, create a domain controller in an Azure virtual network. When you promote the server to a domain controller role, specify the same domain name that's used on the primary site.

Then, reconfigure the DNS server for the virtual network to use the DNS server in Azure.



## Azure-to-Azure protection

First, create a domain controller in an Azure virtual network. When you promote the server to a domain controller role, specify the same domain name that's used on the primary site.

Then, reconfigure the DNS server for the virtual network to use the DNS server in Azure.

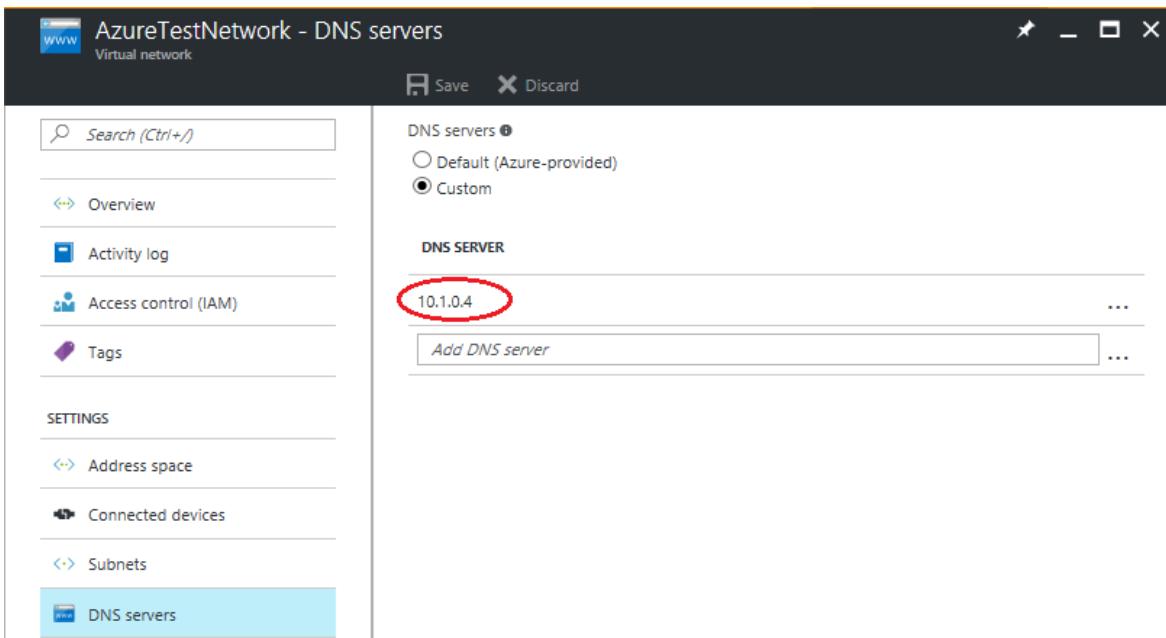
# Test failover considerations

To avoid impact on production workloads, test failover occurs in a network that's isolated from the production network.

Most applications require the presence of a domain controller or a DNS server. Therefore, before the application

fails over, you must create a domain controller in the isolated network to be used for test failover. The easiest way to do this is to use Site Recovery to replicate a virtual machine that hosts a domain controller or DNS. Then, run a test failover of the domain controller virtual machine before you run a test failover of the recovery plan for the application. Here's how you do that:

1. Use Site Recovery to [replicate](#) the virtual machine that hosts the domain controller or DNS.
2. Create an isolated network. Any virtual network that you create in Azure is isolated from other networks by default. We recommend that you use the same IP address range for this network that you use in your production network. Don't enable site-to-site connectivity on this network.
3. Provide a DNS IP address in the isolated network. Use the IP address that you expect the DNS virtual machine to get. If you're replicating to Azure, provide the IP address for the virtual machine that's used on failover. To enter the IP address, in the replicated virtual machine, in the **Compute and Network** settings, select the **Target IP** settings.



The screenshot shows the Azure portal interface for managing a virtual network. The left sidebar lists several options: Overview, Activity log, Access control (IAM), Tags, Address space, Connected devices, Subnets, and DNS servers. The 'DNS servers' option is highlighted with a blue background. The main pane shows the configuration for 'AzureTestNetwork - DNS servers'. It has a 'Save' and 'Discard' button at the top. Under 'DNS servers', there are two options: 'Default (Azure-provided)' (radio button) and 'Custom' (radio button, which is selected). Below this is a list of 'DNS SERVER' entries, where '10.1.0.4' is listed and circled in red. There is also a 'Add DNS server' button.

#### TIP

Site Recovery attempts to create test virtual machines in a subnet of the same name and by using the same IP address that's provided in the **Compute and Network** settings of the virtual machine. If a subnet of the same name isn't available in the Azure virtual network that's provided for test failover, the test virtual machine is created in the alphabetically first subnet.

If the target IP address is part of the selected subnet, Site Recovery tries to create the test failover virtual machine by using the target IP address. If the target IP isn't part of the selected subnet, the test failover virtual machine is created by using the next available IP in the selected subnet.

## Test failover to a secondary site

1. If you're replicating to another on-premises site and you use DHCP, [set up DNS and DHCP for test failover](#).
2. Do a test failover of the domain controller virtual machine that runs in the isolated network. Use the latest available *application consistent* recovery point of the domain controller virtual machine to do the test failover.
3. Run a test failover for the recovery plan that contains virtual machines that the application runs on.
4. When testing is complete, *clean up the test failover* on the domain controller virtual machine. This step deletes the domain controller that was created for test failover.

## Remove references to other domain controllers

When you initiate a test failover, don't include all the domain controllers in the test network. To remove

references to other domain controllers that exist in your production environment, you might need to [seize FSMO Active Directory roles](#) and do [metadata cleanup](#) for missing domain controllers.

## Issues caused by virtualization safeguards

### IMPORTANT

Some of the configurations described in this section are not standard or default domain controller configurations. If you don't want to make these changes to a production domain controller, you can create a domain controller that's dedicated for Site Recovery to use for test failover. Make these changes only to that domain controller.

Beginning with Windows Server 2012, [additional safeguards are built into Active Directory Domain Services \(AD DS\)](#). These safeguards help protect virtualized domain controllers against USN rollbacks if the underlying hypervisor platform supports **VM-GenerationID**. Azure supports **VM-GenerationID**. Because of this, domain controllers that run Windows Server 2012 or later on Azure virtual machines have these additional safeguards.

When **VM-GenerationID** is reset, the **InvocationID** value of the AD DS database is also reset. In addition, the RID pool is discarded, and sysvol folder is marked as non-authoritative. For more information, see [Introduction to Active Directory Domain Services virtualization](#) and [Safely virtualizing DFSR](#).

Failing over to Azure might cause **VM-GenerationID** to reset. Resetting **VM-GenerationID** triggers additional safeguards when the domain controller virtual machine starts in Azure. This might result in a *significant delay* in being able to sign in to the domain controller virtual machine.

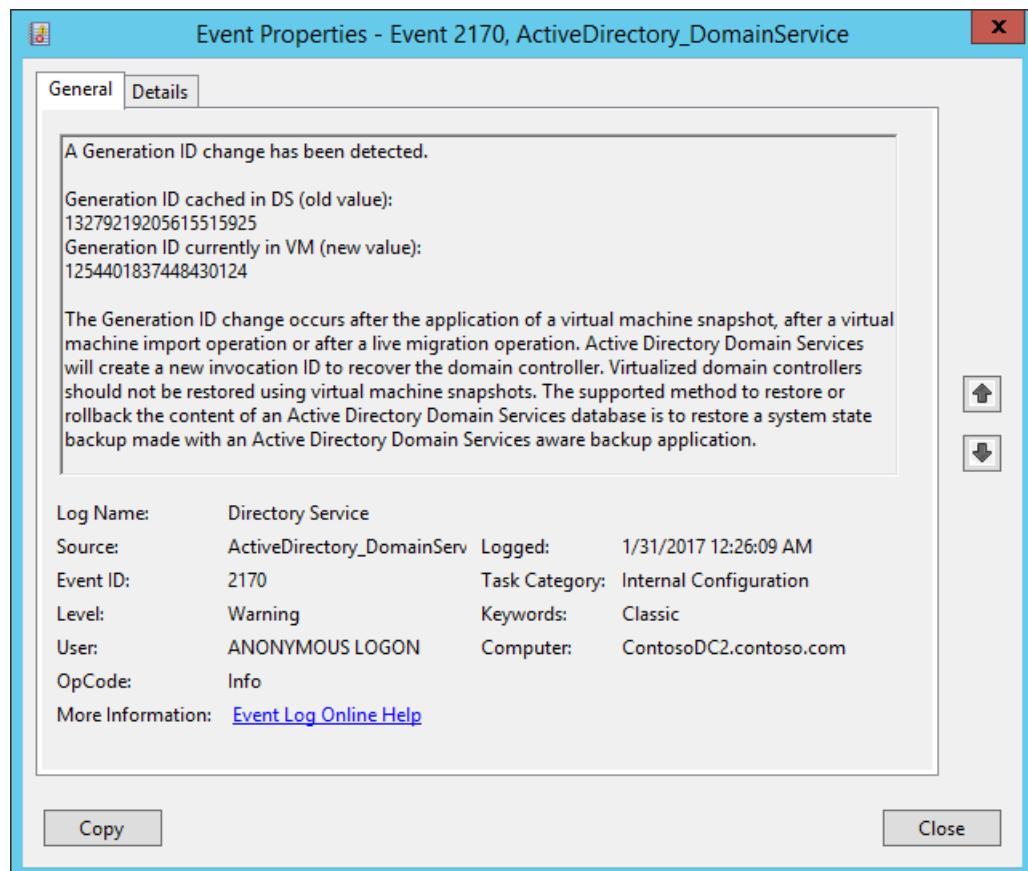
Because this domain controller is used only in a test failover, virtualization safeguards aren't necessary. To ensure that the **VM-GenerationID** value for the domain controller virtual machine doesn't change, you can change the value of following DWORD to **4** in the on-premises domain controller:

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\gencounter\Start`

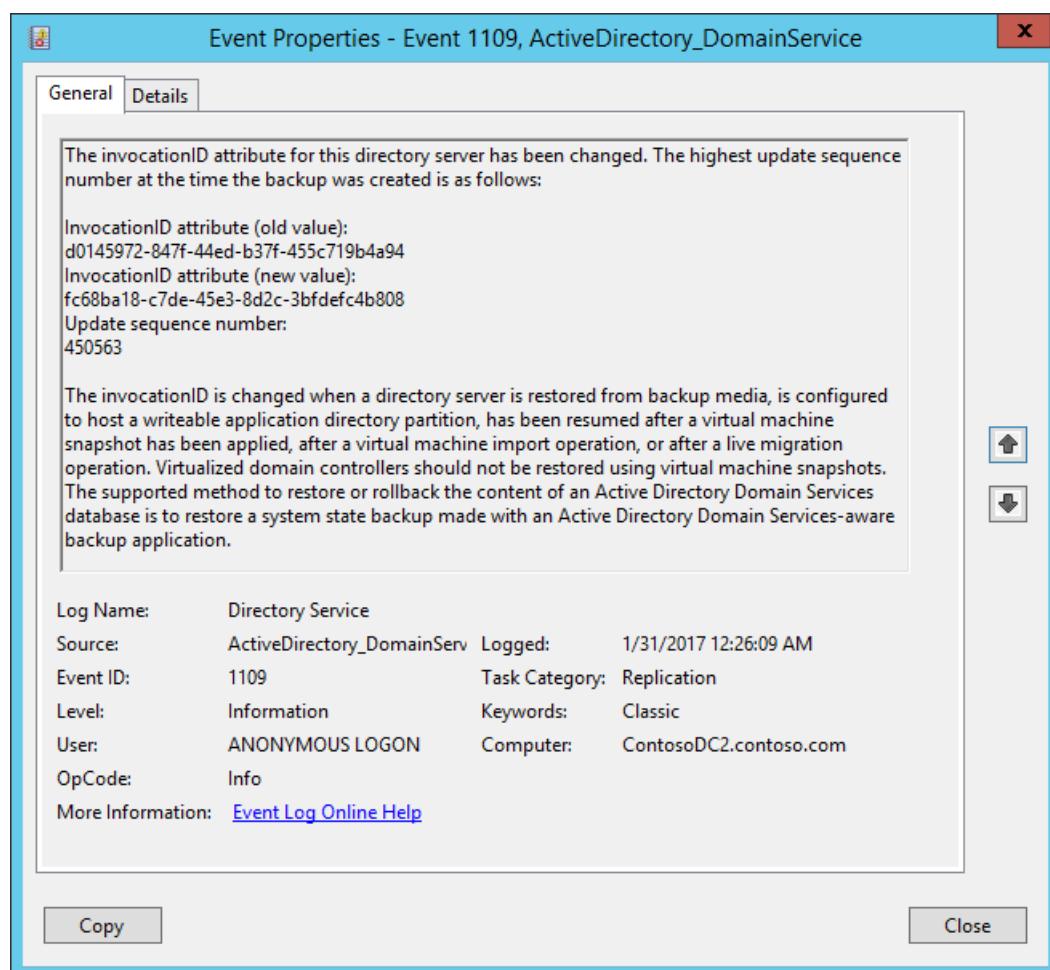
### Symptoms of virtualization safeguards

If virtualization safeguards are triggered after a test failover, you might see one or more of following symptoms:

- The **GenerationID** value changes.

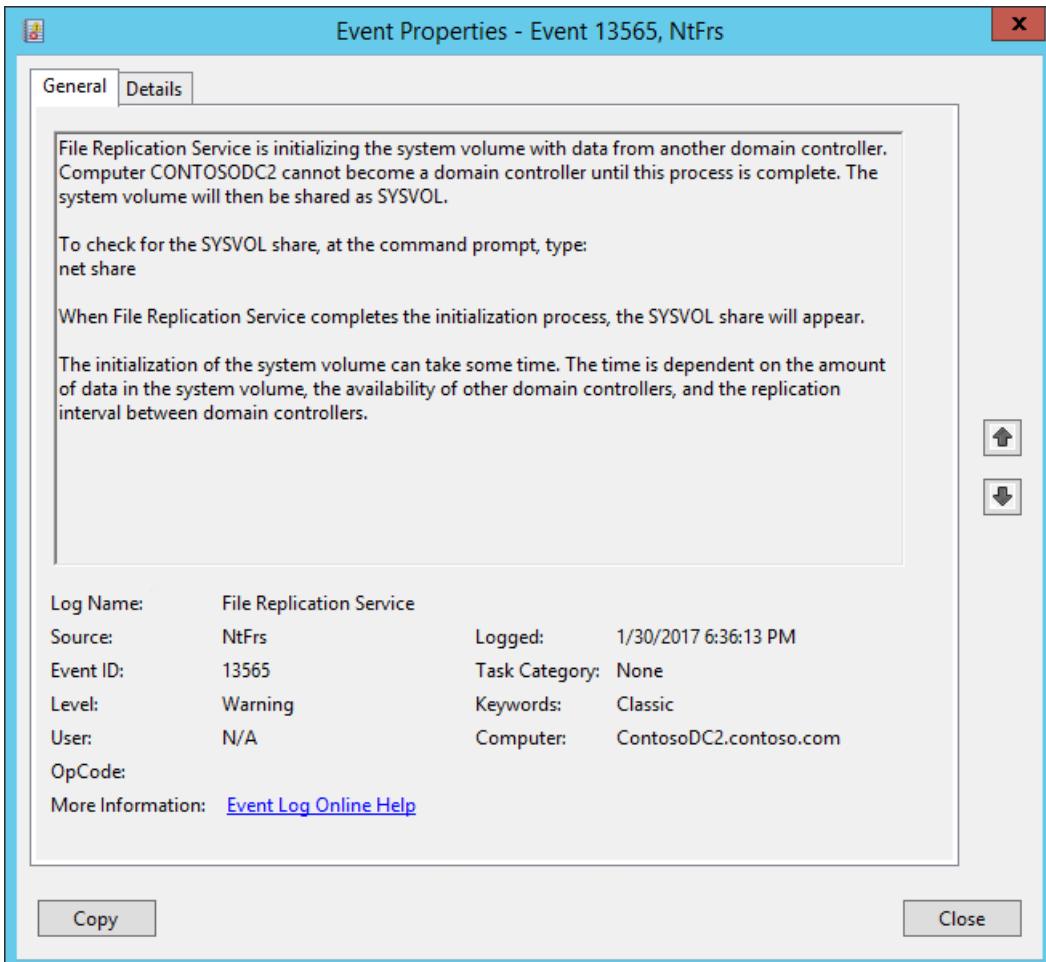


- The **InvocationID** value changes.

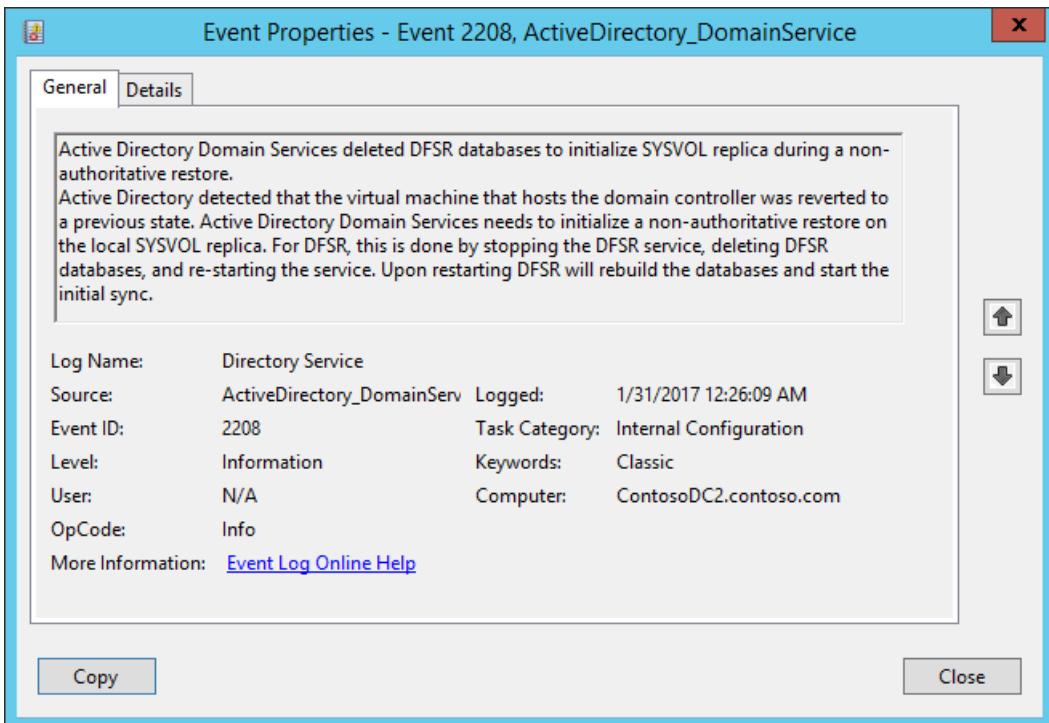


- Sysvol folder and NETLOGON shares aren't available.

```
Select Administrator: C:\Windows\system32\cmd.exe
C:\Users\Administrator.CONTOSO>net share
Share name Resource Remark
----- -----
C$ C:\\
D$ D:\\
IPC$ Remote IPC
ADMIN$ C:\Windows
The command completed successfully.
```



- DFS R databases are deleted.



## Troubleshoot domain controller issues during test failover

### IMPORTANT

Some of the configurations described in this section aren't standard or default domain controller configurations. If you don't want to make these changes to a production domain controller, you can create a domain controller that's dedicated for Site Recovery test failover. Make the changes only to that dedicated domain controller.

- At the command prompt, run the following command to check whether sysvol folder and NETLOGON folder are shared:

`NET SHARE`

- At the command prompt, run the following command to ensure that the domain controller is functioning properly:

`dcdiag /v > dcdiag.txt`

- In the output log, look for the following text. The text confirms that the domain controller is functioning correctly.
  - "passed test Connectivity"
  - "passed test Advertising"
  - "passed test MachineAccount"

If the preceding conditions are satisfied, it's likely that the domain controller is functioning correctly. If it's not, complete the following steps:

- Do an authoritative restore of the domain controller. Keep the following information in mind:
    - Although we don't recommend [FRS replication](#), if you use FRS replication, follow the steps for an authoritative restore. The process is described in [Using the BurFlags registry key to reinitialize File Replication Service](#).
- For more information about BurFlags, see the blog post [D2 and D4: What is it for?](#).
- If you use DFSR replication, complete the steps for an authoritative restore. The process is

described in [Force an authoritative and non-authoritative sync for DFSR-replicated sysvol folder \(like "D4/D2" for FRS\)](#).

You can also use the PowerShell functions. For more information, see [DFSR-SYSVOL authoritative/non-authoritative restore PowerShell functions](#).

2. Bypass the initial sync requirement by setting the following registry key to **0** in the on-premises domain controller. If the DWORD doesn't exist, you can create it under the **Parameters** node.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters\Repl Perform Initial Synchronizations
```

For more information, see [Troubleshoot DNS Event ID 4013: The DNS server was unable to load AD integrated DNS zones](#).

3. Disable the requirement that a global catalog server be available to validate the user login. To do this, in the on-premises domain controller, set the following registry key to **1**. If the DWORD doesn't exist, you can create it under the **Lsa** node.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\IgnoreGCFailures
```

For more information, see [Disable the requirement that a global catalog server be available to validate user logons](#).

### DNS and domain controller on different machines

If you're running the domain controller and DNs on the same VM, you can skip this procedure.

If DNS isn't on the same VM as the domain controller, you need to create a DNS VM for the test failover. You can use a fresh DNS server, and create all the required zones. For example, if your Active Directory domain is contoso.com, you can create a DNS zone with the name contoso.com. The entries that correspond to Active Directory must be updated in DNS as follows:

1. Ensure that these settings are in place before any other virtual machine in the recovery plan starts:
  - The zone must be named after the forest root name.
  - The zone must be file-backed.
  - The zone must be enabled for secure and nonsecure updates.
  - The resolver of the virtual machine that hosts the domain controller should point to the IP address of the DNS virtual machine.
2. Run the following command on the VM that hosts the domain controller:

```
nltest /dsregdns
```

3. Run the following commands to add a zone on the DNS server, allow nonsecure updates, and add an entry for the zone to DNS:

```
dnscmd /zoneadd contoso.com /Primary
```

```
dnscmd /recordadd contoso.com contoso.com. SOA %computername%.contoso.com. hostmaster. 1 15 10 1 1
```

```
dnscmd /recordadd contoso.com %computername% A <IP_OF_DNS_VM>
```

```
dnscmd /config contoso.com /allowupdate 1
```

## Next steps

Learn more about [protecting enterprise workloads with Azure Site Recovery](#).

# Set up disaster recovery for SQL Server

11/14/2019 • 8 minutes to read • [Edit Online](#)

This article describes how to help protect the SQL Server back end of an application. You do so by using a combination of SQL Server business continuity and disaster recovery (BCDR) technologies and [Azure Site Recovery](#).

Before you start, make sure you understand SQL Server disaster recovery capabilities. These capabilities include:

- Failover clustering
- Always On availability groups
- Database mirroring
- Log shipping
- Active geo-replication
- Auto-failover groups

## Combining BCDR technologies with Site Recovery

Your choice of a BCDR technology to recover SQL Server instances should be based on your recovery time objective (RTO) and recovery point objective (RPO) needs as described in the following table. Combine Site Recovery with the failover operation of your chosen technology to orchestrate recovery of your entire application.

DEPLOYMENT TYPE	BCDR TECHNOLOGY	EXPECTED RTO FOR SQL SERVER	EXPECTED RPO FOR SQL SERVER
SQL Server on an Azure infrastructure as a service (IaaS) virtual machine (VM) or at on-premises.	<a href="#">Always On availability group</a>	The time taken to make the secondary replica as primary.	Because replication to the secondary replica is asynchronous, there's some data loss.
SQL Server on an Azure IaaS VM or at on-premises.	<a href="#">Failover clustering (Always On FCI)</a>	The time taken to fail over between the nodes.	Because Always On FCI uses shared storage, the same view of the storage instance is available on failover.
SQL Server on an Azure IaaS VM or at on-premises.	<a href="#">Database mirroring (high-performance mode)</a>	The time taken to force the service, which uses the mirror server as a warm standby server.	Replication is asynchronous. The mirror database might lag somewhat behind the principal database. The lag is typically small. But it can become large if the principal or mirror server's system is under a heavy load.  Log shipping can be a supplement to database mirroring. It's a favorable alternative to asynchronous database mirroring.

Deployment type	BCDR technology	Expected RTO for SQL Server	Expected RPO for SQL Server
SQL as platform as a service (PaaS) on Azure.  This deployment type includes elastic pools and Azure SQL Database servers.	Active geo-replication	30 seconds after failover is triggered.  When failover is activated for one of the secondary databases, all other secondaries are automatically linked to the new primary.	RPO of five seconds.  Active geo-replication uses the Always On technology of SQL Server. It asynchronously replicates committed transactions on the primary database to a secondary database by using snapshot isolation.  The secondary data is guaranteed to never have partial transactions.
SQL as PaaS configured with active geo-replication on Azure.  This deployment type includes a SQL Database managed instance, elastic pools, and SQL Database servers.	Auto-failover groups	RTO of one hour.	RPO of five seconds.  Auto-failover groups provide the group semantics on top of active geo-replication. But the same asynchronous replication mechanism is used.
SQL Server on an Azure IaaS VM or at on-premises.	Replication with Azure Site Recovery	RTO is typically less than 15 minutes. To learn more, read the <a href="#">RTO SLA provided by Site Recovery</a> .	One hour for application consistency and five minutes for crash consistency. If you are looking for lower RPO, use other BCDR technologies.

#### NOTE

A few important considerations when you're helping to protect SQL workloads with Site Recovery:

- Site Recovery is application agnostic. Site Recovery can help protect any version of SQL Server that is deployed on a supported operating system. To learn more, see the [support matrix for recovery](#) of replicated machines.
- You can choose to use Site Recovery for any deployment at Azure, Hyper-V, VMware, or physical infrastructure. Please follow the guidance at the end of this article on [how to help protect a SQL Server cluster](#) with Site Recovery.
- Ensure that the data change rate observed on the machine is within [Site Recovery limits](#). The change rate is measured in write bytes per second. For machines running Windows, you can view this change rate by selecting the **Performance** tab in Task Manager. Observe the write speed for each disk.
- Site Recovery supports replication of Failover Cluster Instances on Storage Spaces Direct. To learn more, see [how to enable Storage Spaces Direct replication](#).

## Disaster recovery of an application

Site Recovery orchestrates the test failover and the failover of your entire application with the help of recovery plans.

There are some prerequisites to ensure your recovery plan is fully customized according to your need. Any SQL Server deployment typically needs an Active Directory deployment. It also needs connectivity for your application tier.

## Step 1: Set up Active Directory

Set up Active Directory in the secondary recovery site for SQL Server to run properly.

- **Small enterprise:** You have a small number of applications and a single domain controller for the on-premises site. If you want to fail over the entire site, use Site Recovery replication. This service replicates the domain controller to the secondary datacenter or to Azure.
- **Medium to large enterprise:** You might need to set up additional domain controllers.
  - If you have a large number of applications, have an Active Directory forest, and want to fail over by application or workload, set up another domain controller in the secondary datacenter or in Azure.
  - If you're using Always On availability groups to recover to a remote site, set up another domain controller on the secondary site or in Azure. This domain controller is used for the recovered SQL Server instance.

The instructions in this article assume that a domain controller is available in the secondary location. To learn more, see the procedures for [helping to protect Active Directory with Site Recovery](#).

## Step 2: Ensure connectivity with other tiers

After the database tier is running in the target Azure region, ensure that you have connectivity with the application and web tiers. Take the necessary steps in advance to validate connectivity with test failover.

To understand how you can design applications for connectivity considerations, see these examples:

- [Design an application for cloud disaster recovery](#)
- [Elastic pool Disaster Recovery strategies](#)

## Step 3: Interoperate with Always On, active geo-replication, and auto-failover groups

BCDR technologies Always On, active geo-replication, and auto-failover groups have secondary replicas of SQL Server running in the target Azure region. The first step for your application failover is to specify this replica as primary. This step assumes you already have a domain controller in the secondary. The step may not be necessary if you choose to do an auto-failover. Fail over your web and application tiers only after the database failover is completed.

### NOTE

If you have helped to protect the SQL machines with Site Recovery, you just need to create a recovery group of these machines and add their failover in the recovery plan.

[Create a recovery plan](#) with application and web tier virtual machines. The following steps show how to add failover of the database tier:

1. Import the scripts to fail over SQL Availability Group in both a [Resource Manager virtual machine](#) and a [classic virtual machine](#). Import the scripts into your Azure Automation account.



[Deploy to Azure](#)

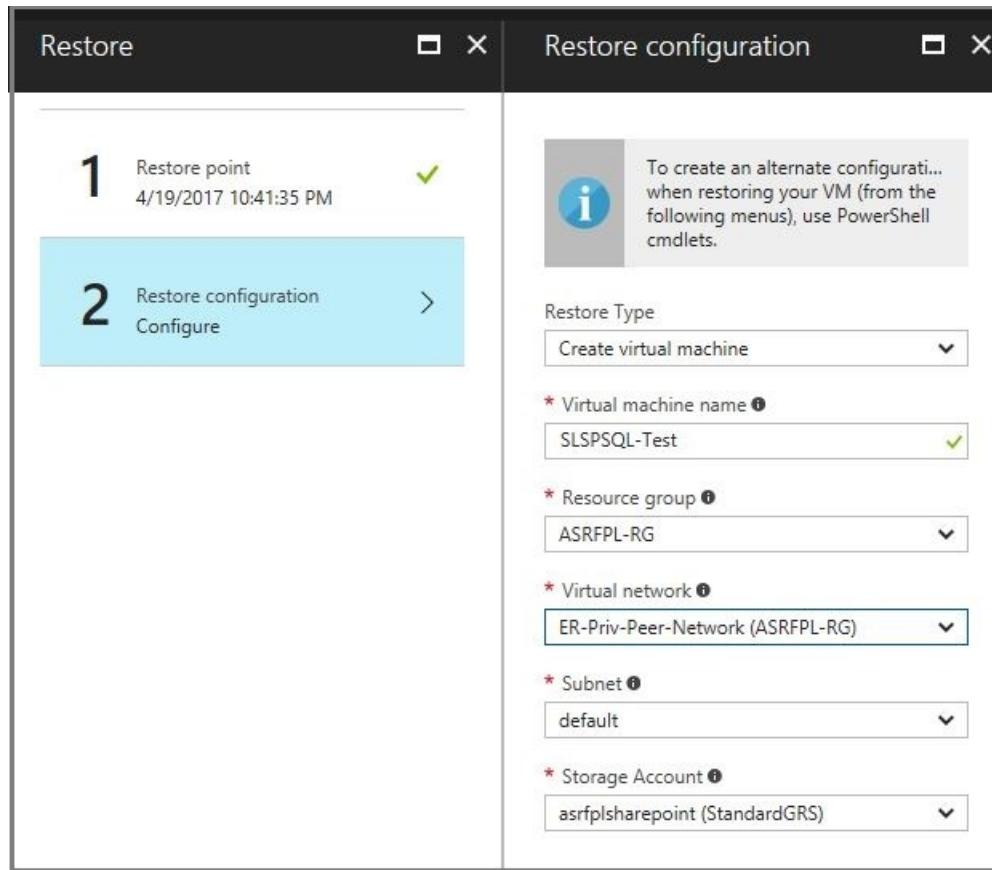
2. Add the ASR-SQL-FailoverAG script as a pre-action of the first group of the recovery plan.
3. Follow the instructions available in the script to create an automation variable. This variable provides the name of the availability groups.

## Step 4: Conduct a test failover

Some BCDR technologies such as SQL Always On don't natively support test failover. We recommend the following approach *only when using such technologies*.

1. Set up [Azure Backup](#) on the VM that hosts the availability group replica in Azure.

2. Before triggering test failover of the recovery plan, recover the VM from the backup taken in the previous step.



3. [Force a quorum](#) in the VM that was restored from backup.
4. Update the IP address of the listener to be an address available in the test failover network.

**Roles (2)**

Name	Status	Type	Owner Node	Priority	Information
Content_AG	Stopped	Other	FW12R2LSP16D3-2	Medium	
FPL-AG	Stopped	Other	FW12R2LSP16D3-2	Medium	

**IP Address: 10.151.139.120 Properties**

General		Dependencies	Policies	Advanced Policies
	Name: Content_AG_10.151.139.120	Type: IP Address		
	Status: Offline			
Network:		10.3.0.0/20		
Subnet mask:		255.255.240.0		
IP Address		<input type="radio"/> DHCP Enabled Address: 0.0.0.0 Lease Obtained: <not configured> Lease Expires: <not configured>		
		<input checked="" type="radio"/> Static IP Address Address: 10 . 3 . 0 . 20		
<input checked="" type="checkbox"/> Enable NetBIOS for this address				
		OK	Cancel	Apply

**Content\_AG**

Name	Status	Information
<b>Other Resources</b>		
Content_AG	Offline	
<b>Server Name</b>		
Name: FPL-LIS0	Offline	
IP Address: 10.151.139.120	Offline	

5. Bring the listener online.

**Content\_AG**

Name	Status	Information
<b>Other Resources</b>		
Content_AG	Offline	
<b>Server Name</b>		
Name: FPL-LIS0	Online	
IP Address: 10.3.0.20	Online	
IP Address: 10.150.8.130	Offline	

6. Ensure that the load balancer in the failover network has one IP address, from the front-end IP address pool that corresponding to each availability group listener, and with the SQL Server VM in the back-end pool.

NAME	IP ADDRESS
FPL-AG	10.3.0.10
Content-AG	10.3.0.20

VIRTUAL MACHINE	STATUS	NETWORK INTERFACE	PRIVATE IP ADDRESS
pool1 (1 virtual machine)			
SLSQL-Test	Running	SLSQL-Test-nic-efe654ea23934d8585dd82fe...	10.3.0.6

7. In later recovery groups, add failover of your application tier followed by your web tier for this recovery plan.
8. Do a test failover of the recovery plan to test end-to-end failover of your application.

## Steps to do a failover

After you add the script in Step 3 and validate it in Step 4, you can do a failover of the recovery plan created in Step 3.

The failover steps for application and web tiers should be the same in both test failover and failover recovery plans.

## How to help protect a SQL Server cluster

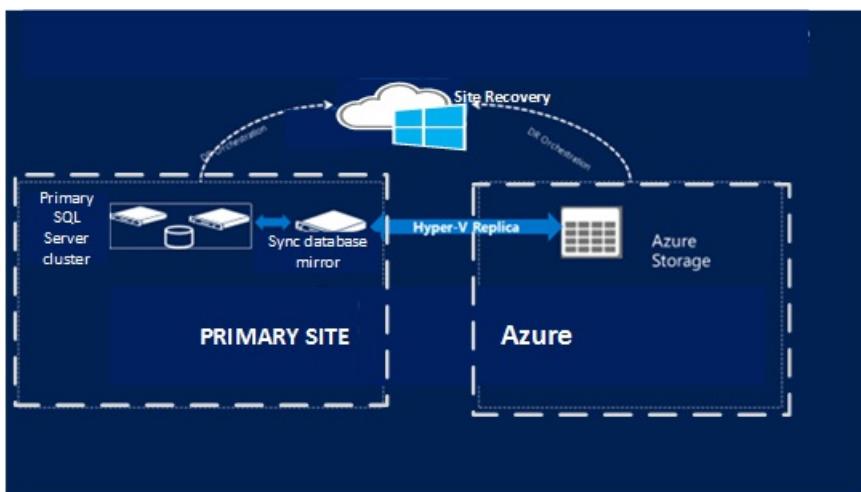
For a cluster running SQL Server Standard edition or SQL Server 2008 R2, we recommend you use Site Recovery replication to help protect SQL Server.

### Azure to Azure and On-premises to Azure

Site Recovery doesn't provide guest cluster support when replicating to an Azure region. SQL Server Standard edition also doesn't provide a low-cost disaster recovery solution. In this scenario, we recommend you protect the SQL Server cluster to a standalone SQL Server instance in the primary location and recover it in the secondary.

1. Configure an additional standalone SQL Server instance on the primary Azure region or at on-premises site.
2. Configure the instance to serve as a mirror for the databases you want to help protect. Configure mirroring in high-safety mode.

3. Configure Site Recovery on the primary site for [Azure](#), [Hyper-V](#), or [VMware VMs and physical servers](#).
4. Use Site Recovery replication to replicate the new SQL Server instance to the secondary site. As it's a high-safety mirror copy, it will be synchronized with the primary cluster but replicated using Site Recovery replication.



### **Fallback considerations**

For SQL Server Standard clusters, fallback after an unplanned failover requires a SQL Server backup and restore. This operation is done from the mirror instance to the original cluster with re-establishment of the mirror.

## Frequently asked questions

### **How does SQL Server get licensed when used with Site Recovery?**

Site Recovery replication for SQL Server is covered under the Software Assurance disaster recovery benefit. This coverage applies to all Site Recovery scenarios: on-premises to Azure disaster recovery and cross-region Azure IaaS disaster recovery. See [Azure Site Recovery pricing](#) for more.

### **Will Site Recovery support my SQL Server version?**

Site Recovery is application agnostic. Site Recovery can help protect any version of SQL Server that is deployed on a supported operating system. For more, see the [support matrix for recovery](#) of replicated machines.

## Next steps

- Learn more about [Site Recovery architecture](#).
- For SQL Server in Azure, learn more about [high availability solutions](#) for recovery in a secondary Azure region.
- For SQL Database, learn more about the [business continuity](#) and [high availability](#) options for recovery in a secondary Azure region.
- For SQL Server machines at on-premises, learn more about the [high availability options](#) for recovery in Azure Virtual Machines.

# Set up disaster recovery for a multi-tier SharePoint application for disaster recovery using Azure Site Recovery

12/2/2019 • 9 minutes to read • [Edit Online](#)

This article describes in detail how to protect a SharePoint application using [Azure Site Recovery](#).

## Overview

Microsoft SharePoint is a powerful application that can help a group or department organize, collaborate, and share information. SharePoint can provide intranet portals, document and file management, collaboration, social networks, extranets, websites, enterprise search, and business intelligence. It also has system integration, process integration, and workflow automation capabilities. Typically, organizations consider it as a Tier-1 application sensitive to downtime and data loss.

Today, Microsoft SharePoint does not provide any out-of-the-box disaster recovery capabilities. Regardless of the type and scale of a disaster, recovery involves the use of a standby data center that you can recover the farm to. Standby data centers are required for scenarios where local redundant systems and backups cannot recover from the outage at the primary data center.

A good disaster recovery solution should allow modeling of recovery plans around the complex application architectures such as SharePoint. It should also have the ability to add customized steps to handle application mappings between various tiers and hence providing a single-click failover with a lower RTO in the event of a disaster.

This article describes in detail how to protect a SharePoint application using [Azure Site Recovery](#). This article will cover best practices for replicating a three tier SharePoint application to Azure, how you can do a disaster recovery drill, and how you can failover the application to Azure.

You can watch the below video about recovering a multi-tier application to Azure.

## Prerequisites

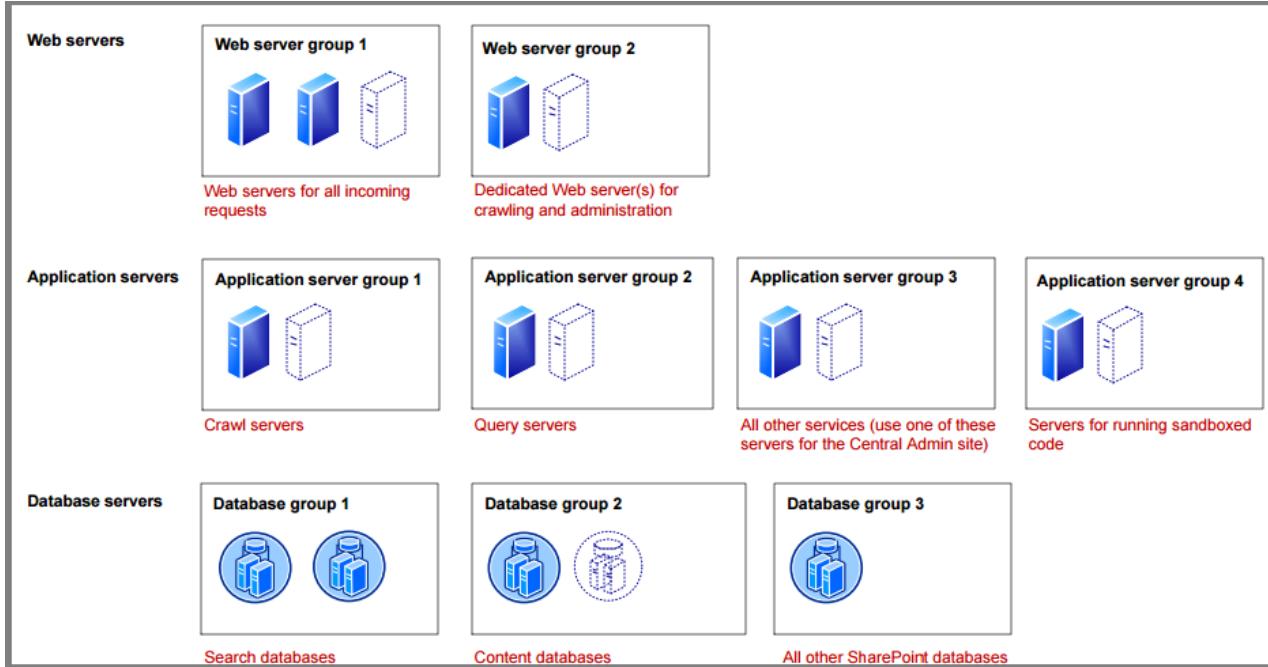
Before you start, make sure you understand the following:

1. [Replicating a virtual machine to Azure](#)
2. How to [design a recovery network](#)
3. [Doing a test failover to Azure](#)
4. [Doing a failover to Azure](#)
5. How to [replicate a domain controller](#)
6. How to [replicate SQL Server](#)

## SharePoint architecture

SharePoint can be deployed on one or more servers using tiered topologies and server roles to implement a farm design that meets specific goals and objectives. A typical large, high-demand SharePoint server farm that supports

a high number of concurrent users and a large number of content items use service grouping as part of their scalability strategy. This approach involves running services on dedicated servers, grouping these services together, and then scaling out the servers as a group. The following topology illustrates the service and server grouping for a three tier SharePoint server farm. Please refer to SharePoint documentation and product line architectures for detailed guidance on different SharePoint topologies. You can find more details about SharePoint 2013 deployment in [this document](#).



## Site Recovery support

Site Recovery is application-agnostic and should work with any version of SharePoint running on a supported machine. For creating this article, VMware virtual machines with Windows Server 2012 R2 Enterprise were used. SharePoint 2013 Enterprise edition and SQL server 2014 Enterprise edition were used.

### Source and target

SCENARIO	TO A SECONDARY SITE	TO AZURE
<b>Hyper-V</b>	Yes	Yes
<b>VMware</b>	Yes	Yes
<b>Physical server</b>	Yes	Yes
<b>Azure</b>	NA	Yes

### Things to keep in mind

If you are using a shared disk-based cluster as any tier in your application then you will not be able to use Site Recovery replication to replicate those virtual machines. You can use native replication provided by the application and then use a [recovery plan](#) to failover all tiers.

## Replicating virtual machines

Follow [this guidance](#) to start replicating the virtual machine to Azure.

- Once the replication is complete, make sure you go to each virtual machine of each tier and select same availability set in 'Replicated item > Settings > Properties > Compute and Network'. For example, if your

web tier has 3 VMs, ensure all the 3 VMs are configured to be part of same availability set in Azure.

The screenshot shows the Azure portal interface for managing a virtual machine. On the left, there's a sidebar with 'Settings' and 'Replication' sections. The main area is titled 'Compute and Network' for 'FW12R2LSP16A3-2'. It displays 'Compute properties' including 'Name' (FW12R2LSP16A3-2), 'Resource group' (ASRPL-RG), 'Size' (2 cores, 2.00 GB memory, 1 NICs), and 'Availability set' (highlighted with a red box). Below these are 'Network properties' and a 'Hybrid Use Benefit' section.

- For guidance on protecting Active Directory and DNS, refer to [Protect Active Directory and DNS](#) document.
- For guidance on protecting database tier running on SQL server, refer to [Protect SQL Server](#) document.

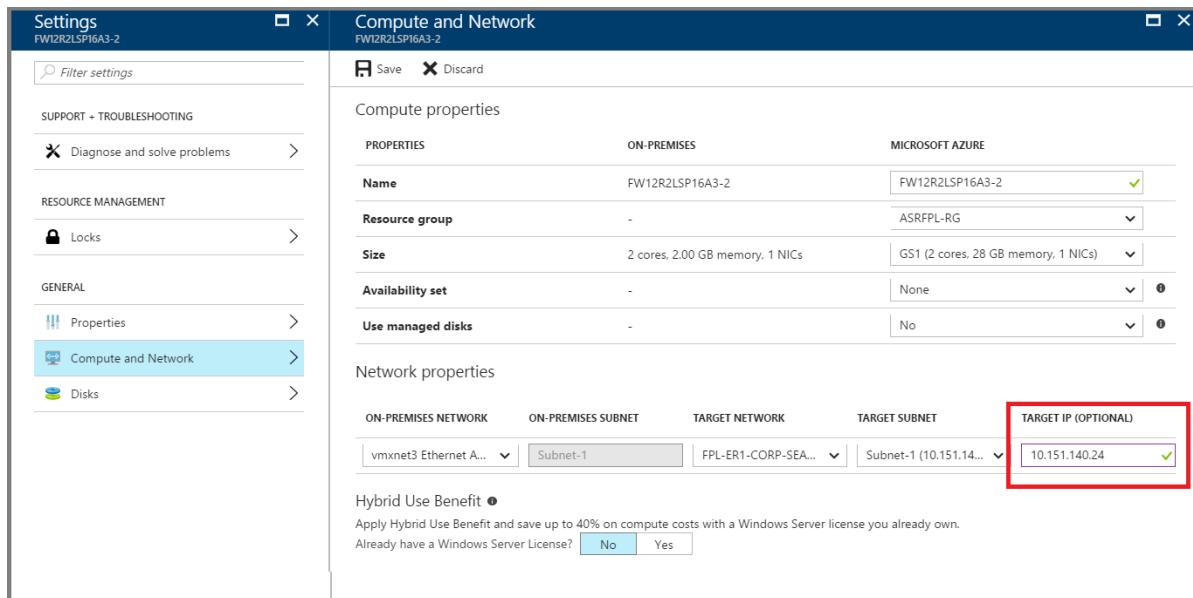
## Networking configuration

### Network properties

- For the App and Web tier VMs, configure network settings in Azure portal so that the VMs get attached to the right DR network after failover.

This screenshot shows the 'Compute and Network' settings for the same VM. The 'Compute properties' section is identical. In the 'Network properties' section, the 'TARGET NETWORK' dropdown is highlighted with a red box, showing options like 'vmxnet3 Ethernet A...' and 'FPL-ER1-CORP-SEA...'. The 'TARGET SUBNET' dropdown also has a red box around it, showing 'Subnet-1 (10.151.14...)'.

- If you are using a static IP, then specify the IP that you want the virtual machine to take in the **Target IP** field



## DNS and Traffic Routing

For internet facing sites, [create a Traffic Manager profile of 'Priority' type](#) in the Azure subscription. And then configure your DNS and Traffic Manager profile in the following manner.

WHERE	SOURCE	TARGET
Public DNS	Public DNS for SharePoint sites Ex: sharepoint.contoso.com	Traffic Manager contososharepoint.trafficmanager.net
On-premises DNS	sharepointonprem.contoso.com	Public IP on the on-premises farm

In the Traffic Manager profile, [create the primary and recovery endpoints](#). Use the external endpoint for on-premises endpoint and public IP for Azure endpoint. Ensure that the priority is set higher to on-premises endpoint.

Host a test page on a specific port (for example, 800) in the SharePoint web tier in order for Traffic Manager to automatically detect availability post failover. This is a workaround in case you cannot enable anonymous authentication on any of your SharePoint sites.

[Configure the Traffic Manager profile](#) with the below settings.

- Routing method - 'Priority'
- DNS time to live (TTL) - '30 seconds'
- Endpoint monitor settings - If you can enable anonymous authentication, you can give a specific website endpoint. Or, you can use a test page on a specific port (for example, 800).

## Creating a recovery plan

A recovery plan allows sequencing the failover of various tiers in a multi-tier application, hence, maintaining application consistency. Follow the below steps while creating a recovery plan for a multi-tier web application.

[Learn more about creating a recovery plan.](#)

### Adding virtual machines to failover groups

1. Create a recovery plan by adding the App and Web tier VMs.
2. Click on 'Customize' to group the VMs. By default, all VMs are part of 'Group 1'.

The screenshot shows two windows side-by-side. The left window is titled 'AlwaysOnSP-Test' and shows the 'ASRFPI-vault' details. It lists 'Start groups' as 2, 'Source' as FPL-CS2, and 'Deployment model' as Resource Manager. The right window is titled 'AlwaysOnSP-Test Recovery plan' and shows a table of replication groups. The table has columns 'STAGE NAME' and 'DETAILS'. It contains 9 rows, with the first row being 'All groups shutdown' and the last row being 'FW12R2LSP16W3-2'.

STAGE NAME	DETAILS
All groups shutdown	0 machines in 2 groups.
▶ All groups failover	...
▼ Group 1: Start	3 Machines
FW12R2LSP16A3-2	Machine
FW12R2LSP16A1-2	Machine
FW12R2LSP16A2-2	Machine
▼ Group 2: Start	3 Machines
FW12R2LSP16W1-2	Machine
FW12R2LSP16W2-2	Machine
FW12R2LSP16W3-2	Machine

3. Create another Group (Group 2) and move the Web tier VMs into the new group. Your App tier VMs should be part of 'Group 1' and Web tier VMs should be part of 'Group 2'. This is to ensure that the App tier VMs boot up first followed by Web tier VMs.

#### **Adding scripts to the recovery plan**

You can deploy the most commonly used Azure Site Recovery scripts into your Automation account clicking the 'Deploy to Azure' button below. When you are using any published script, ensure you follow the guidance in the script.



1. Add a pre-action script to 'Group 1' to failover SQL Availability group. Use the 'ASR-SQL-FailoverAG' script published in the sample scripts. Ensure you follow the guidance in the script and make the required changes in the script appropriately.

**AlwaysOnSP-Test**  
Recovery plan

**Group** **Save** **Discard** **Change group**

This recovery plan contains 1 replication group(s).

STAGE NAME	DETAILS	
All groups shutdown	0 machines in 2 groups.	...
▶ All groups failover		...
▼ Group 1: Start	3 Machines	<b>Delete</b> <b>Add protected items</b> <b>Add pre action</b> <b>Add post action</b>
FW12R2LSP16A3-2	Machine	...
FW12R2LSP16A1-2	Machine	...
FW12R2LSP16A2-2	Machine	...
▼ Group 2: Start	3 Machines	...
FW12R2LSP16W1-2	Machine	...
FW12R2LSP16W2-2	Machine	...
FW12R2LSP16W3-2	Machine	...

**AlwaysOnSP-Test**

Recovery plan

Group Save Discard Change group

This recovery plan contains 1 replication group(s).

STAGE NAME	DETAILS
All groups shutdown	0 machines in 2 groups.
▶ All groups failover	
▼ Group 1: Start	3 Machines
FW12R2LSP16A3-2	Machine
FW12R2LSP16A1-2	Machine
FW12R2LSP16A2-2	Machine
▼ Group 2: Start	3 Machines
FW12R2LSP16W1-2	Machine
FW12R2LSP16W2-2	Machine
FW12R2LSP16W3-2	Machine

**Insert action**

Insert

Script Manual action

\* Name Failover SQL Availability Group

Failover to azure script

\* Automation account name ASRAutomation

\* Runbook name ASR-SQL-FailoverAG

OK

2. Add a post action script to attach a load balancer on the failed over virtual machines of Web tier (Group 2). Use the 'ASR-AddSingleLoadBalancer' script published in the sample scripts. Ensure you follow the guidance in the script and make the required changes in the script appropriately.

AlwaysOnSP-Test

Recovery plan

+ Group    Save    Discard    Change group

**i** You have unsaved changes.

This recovery plan contains 1 replication group(s).

STAGE NAME	DETAILS	
All groups shutdown	0 machines in 2 groups.	...
▶ All groups failover		...
▶ Group 1: Pre-steps	1 Step	...
▶ Script: Failover SQL Availability Gro...	Script	...
▼ Group 1: Start	3 Machines	...
FW12R2LSP16A3-2	Machine	...
FW12R2LSP16A1-2	Machine	...
FW12R2LSP16A2-2	Machine	...
▼ Group 2: Start	3 Machines	Delete group Add protected items Add pre action Add post action
FW12R2LSP16W1-2	Machine	
FW12R2LSP16W2-2	Machine	
FW12R2LSP16W3-2	Machine	

STAGE NAME	DETAILS
All groups shutdown	0 machines in 2 groups.
▶ All groups failover	
▀ ▾ Group 1: Pre-steps	1 Step
▀ Script: Failover SQL Availability Gro...	Script
▀ ▾ Group 1: Start	3 Machines
FW12R2LSP16A3-2	Machine
FW12R2LSP16A1-2	Machine
FW12R2LSP16A2-2	Machine
▀ ▾ Group 2: Start	3 Machines
FW12R2LSP16W1-2	Machine
FW12R2LSP16W2-2	Machine
FW12R2LSP16W3-2	Machine

3. Add a manual step to update the DNS records to point to the new farm in Azure.
  - For internet facing sites, no DNS updates are required post failover. Follow the steps described in the 'Networking guidance' section to configure Traffic Manager. If the Traffic Manager profile has been set up as described in the previous section, add a script to open dummy port (800 in the example) on the Azure VM.
  - For internal facing sites, add a manual step to update the DNS record to point to the new Web tier VM's load balancer IP.
4. Add a manual step to restore search application from a backup or start a new search service.
5. For restoring Search service application from a backup, follow below steps.
  - This method assumes that a backup of the Search Service Application was performed before the catastrophic event and that the backup is available at the DR site.
  - This can easily be achieved by scheduling the backup (for example, once daily) and using a copy procedure to place the backup at the DR site. Copy procedures could include scripted programs such as AzCopy (Azure Copy) or setting up DFSR (Distributed File Services Replication).
  - Now that the SharePoint farm is running, navigate the Central Administration, 'Backup and Restore' and

select Restore. The restore interrogates the backup location specified (you may need to update the value). Select the Search Service Application backup you would like to restore.

- Search is restored. Keep in mind that the restore expects to find the same topology (same number of servers) and same hard drive letters assigned to those servers. For more information, see '[Restore Search service application in SharePoint 2013](#)' document.

## 6. For starting with a new Search service application, follow below steps.

- This method assumes that a backup of the "Search Administration" database is available at the DR site.
- Since the other Search Service Application databases are not replicated, they need to be re-created. To do so, navigate to Central Administration and delete the Search Service Application. On any servers which host the Search Index, delete the index files.
- Re-create the Search Service Application and this re-creates the databases. It is recommended to have a prepared script that re-creates this service application since it is not possible to perform all actions via the GUI. For example, setting the index drive location and configuring the search topology are only possible by using SharePoint PowerShell cmdlets. Use the Windows PowerShell cmdlet `Restore-SPEnterpriseSearchServiceApplication` and specify the log-shipped and replicated Search Administration database, `Search_Service__DB`. This cmdlet gives the search configuration, schema, managed properties, rules, and sources and creates a default set of the other components.
- Once the Search Service Application has been re-created, you must start a full crawl for each content source to restore the Search Service. You lose some analytics information from the on-premises farm, such as search recommendations.

## 7. Once all the steps are completed, save the recovery plan and the final recovery plan will look like following.

The screenshot shows two windows side-by-side. The left window is titled 'AlwaysOnSP-Test ASRFPL-vault' and displays a comparison between 'Source' (containing 6 items) and 'Target' (containing 0 items). The right window is titled 'AlwaysOnSP-Test Recovery plan' and shows a detailed list of recovery steps, including groups for shutdown, failover, and start, along with specific machine details and scripts.

STAGE NAME	DETAILS
All groups shutdown	0 machines in 2 groups.
▶ All groups failover	...
▼ Group 1: Pre-steps	1 Step
Script: Failover SQL Availability Gro...	Script
▼ Group 1: Start	3 Machines
FW12R2LSP16A3-2	Machine
FW12R2LSP16A1-2	Machine
FW12R2LSP16A2-2	Machine
▼ Group 2: Start	3 Machines
FW12R2LSP16W1-2	Machine
FW12R2LSP16W2-2	Machine
FW12R2LSP16W3-2	Machine
▼ Group 2: Post-steps	3 Steps
Script: Add Frontend Load Balancer	Script
Manual: Update DNS	Manual action
Manual: Restore Search Service	Manual action

## Doing a test failover

Follow [this guidance](#) to do a test failover.

1. Go to Azure portal and select your Recovery Service vault.
2. Click on the recovery plan created for SharePoint application.
3. Click on 'Test Failover'.
4. Select recovery point and Azure virtual network to start the test failover process.

5. Once the secondary environment is up, you can perform your validations.
6. Once the validations are complete, you can click 'Cleanup test failover' on the recovery plan and the test failover environment is cleaned.

For guidance on doing test failover for AD and DNS, refer to [Test failover considerations for AD and DNS](#) document.

For guidance on doing test failover for SQL Always ON availability groups, refer to [Performing Application DR with Azure Site Recovery and doing Test failover](#) document.

## Doing a failover

Follow [this guidance](#) for doing a failover.

1. Go to Azure portal and select your Recovery Services vault.
2. Click on the recovery plan created for SharePoint application.
3. Click on 'Failover'.
4. Select recovery point to start the failover process.

## Next steps

You can learn more about [replicating other applications using Site Recovery](#).

# Set up disaster recovery for a multitier Dynamics AX application

1/14/2020 • 6 minutes to read • [Edit Online](#)

Dynamics AX is one of the most popular ERP solutions used by enterprises to standardize processes across locations, manage resources, and simplify compliance. Because the application is critical to an organization, in the event of a disaster, the application should be up and running in minimum time.

Today, Dynamics AX doesn't provide any out-of-the-box disaster recovery capabilities. Dynamics AX consists of many server components, such as Windows Application Object Server, Azure Active Directory, Azure SQL Database, SharePoint Server, and Reporting Services. To manage the disaster recovery of each of these components manually is not only expensive but also error prone.

This article explains how you can create a disaster recovery solution for your Dynamics AX application by using [Azure Site Recovery](#). It also covers planned/unplanned test failovers by using a one-click recovery plan, supported configurations, and prerequisites.

## Prerequisites

Implementing disaster recovery for Dynamics AX application by using Site Recovery requires the following prerequisites:

- Set up an on-premises Dynamics AX deployment.
- Create a Site Recovery vault in an Azure subscription.
- If Azure is your recovery site, run the Azure Virtual Machine Readiness Assessment tool on the VMs. They must be compatible with the Azure Virtual Machines and Site Recovery services.

## Site Recovery support

For the purpose of creating this article, we used VMware virtual machines with Dynamics AX 2012 R3 on Windows Server 2012 R2 Enterprise. Because Site Recovery replication is application agnostic, we expect the recommendations provided here to hold for the following scenarios.

### Source and target

SCENARIO	TO A SECONDARY SITE	TO AZURE
Hyper-V	Yes	Yes
VMware	Yes	Yes
Physical server	Yes	Yes

## Enable disaster recovery of the Dynamics AX application by using Site Recovery

### Protect your Dynamics AX application

To enable the complete application replication and recovery, each component of Dynamics AX must be protected.

## 1. Set up Active Directory and DNS replication

Active Directory is required on the disaster recovery site for the Dynamics AX application to function. We recommend the following two choices based on the complexity of the customer's on-premises environment.

### Option 1

The customer has a small number of applications and a single domain controller for the entire on-premises site and plans to fail over the entire site together. We recommend that you use Site Recovery replication to replicate the domain controller machine to a secondary site (applicable for both site-to-site and site-to-Azure scenarios).

### Option 2

The customer has a large number of applications and is running an Active Directory forest and plans to fail over a few applications at a time. We recommend that you set up an additional domain controller on the disaster recovery site (a secondary site or in Azure).

For more information, see [Make a domain controller available on a disaster recovery site](#). For the remainder of this document, we assume that a domain controller is available on the disaster recovery site.

## 2. Set up SQL Server replication

For technical guidance on the recommended option for protecting the SQL tier, see [Replicate applications with SQL Server and Azure Site Recovery](#).

## 3. Enable protection for the Dynamics AX client and Application Object Server VMs

Perform relevant Site Recovery configuration based on whether the VMs are deployed on [Hyper-V](#) or [VMware](#).

### TIP

We recommend that you configure the crash-consistent frequency to 15 minutes.

The following snapshot shows the protection status of Dynamics-component VMs in a VMware site-to-Azure protection scenario.

The screenshot shows the 'Replicated items' blade in the Site Recovery interface. At the top, there are buttons for Refresh, Replicate, and Columns. A prominent orange banner displays a warning: '⚠️ New Mobility Service Update is available. Push install latest update on every physical and virtual machine →'. Below the banner, a message says 'Last refreshed at: 3/13/2017, 1:00:48 PM'. A blue info icon indicates 'Finished loading data from service'. A search bar labeled 'Filter items...' is present. The main table lists two VMs:

NAME	HEALTH	STATUS	ACTIVE LOCATION
DynamicsAOS	✔️ OK	Protected	Contoso-CSPS
DynamicsClient	✔️ OK	Protected	Contosos-CSPS

## 4. Configure networking

### Configure VM compute and network settings

For the Dynamics AX client and Application Object Server VMs, configure network settings in Site Recovery so that the VM networks get attached to the right disaster recovery network after failover. Ensure that the disaster recovery network for these tiers is routable to the SQL tier.

You can select the VM in the replicated items to configure the network settings, as shown in the following

snapshot:

- For Application Object Server servers, select the correct availability set.
- If you're using a static IP, specify the IP that you want the VM to take in the **Target IP** text box.

The screenshot shows the 'Compute and Network' blade for a VM named 'DynamicsAOSVM1'. It has tabs for 'Compute properties' and 'Network properties'. Under 'Compute properties', there are sections for 'PROPERTIES', 'ON-PREMISES', and 'MICROSOFT AZURE'. Under 'Network properties', there are sections for 'ON-PREMISES NETWORK', 'ON-PREMISES SUBNET', 'TARGET NETWORK', 'TARGET SUBNET', and 'TARGET IP (OPTIONAL)'. The 'Name' field is set to 'DynamicsAOSVM1' in the Microsoft Azure section. The 'Resource group' dropdown shows 'DynamicsAX'. The 'Size' dropdown shows 'D1\_v2 (1 cores, 3.5 GB memory, 1 NICs)'. The 'Availability set' dropdown shows 'AOSAVset'. In the 'Network properties' section, the 'ON-PREMISES NETWORK' dropdown shows 'Intel(R) PRO/1000 M...'. The 'ON-PREMISES SUBNET' dropdown shows 'Subnet-1'. The 'TARGET NETWORK' dropdown shows 'AzureNetwork'. The 'TARGET SUBNET' dropdown shows 'default (10.38.0.0/24)'. The 'TARGET IP (OPTIONAL)' dropdown shows 'Defaulted to DHCP'.

## 5. Create a recovery plan

You can create a recovery plan in Site Recovery to automate the failover process. Add an app tier and a web tier in the recovery plan. Order them in different groups so that the front-end shuts down before the app tier.

1. Select the Site Recovery vault in your subscription, and select the **Recovery Plans** tile.
2. Select **+ Recovery plan**, and specify a name.
3. Select the **Source** and **Target**. The target can be Azure or a secondary site. If you choose Azure, you must specify the deployment model.

The screenshot shows the 'Create recovery plan' dialog box. It has fields for 'Name' (set to 'dynamicsaxrecoveryplan'), 'Source' (set to 'Contosos-CSPS'), 'Target' (set to 'Microsoft Azure'), 'Allow items with deployment model' (set to 'Resource Manager'), and 'Select items' (set to '0').

4. Select the Application Object Server and the client VMs for the recovery plan, and select the **✓**.

### Create recovery plan

★ Name: dynamicsaxrecoveryplan ✓

★ Source: Contoso-CSPS

★ Target: Microsoft Azure

★ Allow items with deployment model: Resource Manager

★ Select items: 0 >

### Select items

Finished retrieving data.

Filter items...

PROTECTED ITEM	TYPE
DynamicsAOSVM1	Machine
DynamicsAOSVM2	Machine
DynamicsAXClient	Machine

Selected items: 3 >

Recovery plan example:

dynamicsaxrecoveryplan  
Recovery plan

+ Group    Save    Discard    Change group

**i** You have unsaved changes.

STAGE NAME	DETAILS	
All groups shutdown	3 machines in 2 groups.	...
▼ All groups failover		...
▼ Machines	3 Machines	...
DynamicsAOSVM1	Machine	...
DynamicsAOSVM2	Machine	...
DynamicsAXClient	Machine	...
Replication groups	0 Replication Groups	...
▼ Group 1: Pre-steps	1 Step	...
Script: SQLAGFailover	Script	...
▼ Group 1: Start	2 Machines	...
DyanmicsAOSVM1	Machine	...
DynamicsAOSVM2	Machine	...
▼ Group 1: Post-steps	2 Steps	...
Script: Update DNS	Script	...
Script: AddLoadbalancer	Script	...
▼ Group 2: Start	1 Machine	...
DynamicsAXClient	Machine	...

You can customize the recovery plan for the Dynamics AX application by adding the following steps. The previous snapshot shows the complete recovery plan after you add all the steps.

- **SQL Server failover steps:** For information about recovery steps specific to SQL server, see [Replication applications with SQL Server and Azure Site Recovery](#).
- **Failover Group 1:** Fail over the Application Object Server VMs. Make sure that the recovery point selected is as close as possible to the database PIT, but not ahead of it.
- **Script:** Add load balancer (only E-A). Add a script (via Azure Automation) after the Application Object Server VM group comes up to add a load balancer to it. You can use a script to do this task. For more information, see [How to add a load balancer for multitier application disaster recovery](#).
- **Failover Group 2:** Fail over the Dynamics AX client VMs. Fail over the web tier VMs as part of the recovery plan.

## Perform a test failover

For more information specific to Active Directory during test failover, see the "Active Directory disaster recovery solution" companion guide.

For more information specific to SQL server during test failover, see [Replicate applications with SQL Server and Azure Site Recovery](#).

1. Go to the Azure portal, and select your Site Recovery vault.
2. Select the recovery plan created for Dynamics AX.
3. Select **Test Failover**.
4. Select the virtual network to start the test failover process.
5. After the secondary environment is up, you can perform your validations.
6. After the validations are complete, select **Validations complete** and the test failover environment is cleaned.

For more information on performing a test failover, see [Test failover to Azure in Site Recovery](#).

### Perform a failover

1. Go to the Azure portal, and select your Site Recovery vault.
2. Select the recovery plan created for Dynamics AX.
3. Select **Failover**, and select **Failover**.
4. Select the target network, and select  to start the failover process.

For more information on doing a failover, see [Failover in Site Recovery](#).

### Perform a failback

For considerations specific to SQL Server during failback, see [Replicate applications with SQL Server and Azure Site Recovery](#).

1. Go to the Azure portal, and select your Site Recovery vault.
2. Select the recovery plan created for Dynamics AX.
3. Select **Failover**, and select **Failover**.
4. Select **Change Direction**.
5. Select the appropriate options: data synchronization and VM creation.
6. Select  to start the failback process.

For more information on doing a failback, see [Failback VMware VMs from Azure to on-premises](#).

## Summary

By using Site Recovery, you can create a complete automated disaster recovery plan for your Dynamics AX application. In the event of a disruption, you can initiate the failover within seconds from anywhere and get the application up and running in minutes.

## Next steps

To learn more about protecting enterprise workloads with Site Recovery, see [What workloads can I protect?](#).

# About disaster recovery for on-premises apps

10/10/2019 • 8 minutes to read • [Edit Online](#)

This article describes on-premises workloads and apps you can protect for disaster recovery with the [Azure Site Recovery](#) service.

## Overview

Organizations need a business continuity and disaster recovery (BCDR) strategy to keep workloads and data safe and available during planned and unplanned downtime, and recover to regular working conditions as soon as possible.

Site Recovery is an Azure service that contributes to your BCDR strategy. Using Site Recovery, you can deploy application-aware replication to the cloud, or to a secondary site. Whether your apps are Windows or Linux-based, running on physical servers, VMware or Hyper-V, you can use Site Recovery to orchestrate replication, perform disaster recovery testing, and run failovers and failback.

Site Recovery integrates with Microsoft applications, including SharePoint, Exchange, Dynamics, SQL Server, and Active Directory. Microsoft also works closely with leading vendors including Oracle, SAP, and Red Hat. You can customize replication solutions on an app-by-app basis.

## Why use Site Recovery for application replication?

Site Recovery contributes to application-level protection and recovery as follows:

- App-agnostic, providing replication for any workloads running on a supported machine.
- Near-synchronous replication, with RPOs as low as 30 seconds to meet the needs of most critical business apps.
- App-consistent snapshots, for single or multi-tier applications.
- Integration with SQL Server AlwaysOn, and partnership with other application-level replication technologies, including AD replication, SQL AlwaysOn, Exchange Database Availability Groups (DAGs).
- Flexible recovery plans, that enable you to recover an entire application stack with a single click, and to include external scripts and manual actions in the plan.
- Advanced network management in Site Recovery and Azure to simplify app network requirements, including the ability to reserve IP addresses, configure load-balancing, and integration with Azure Traffic Manager, for low RTO network switchovers.
- A rich automation library that provides production-ready, application-specific scripts that can be downloaded and integrated with recovery plans.

## Workload summary

Site Recovery can replicate any app running on a supported machine. In addition, we've partnered with product teams to carry out additional testing for the apps specified in the table.

WORKLOAD	REPLICATE AZURE VMS TO AZURE	REPLICATE HYPER-V VMS TO A SECONDARY SITE	REPLICATE HYPER-V VMS TO AZURE	REPLICATE VMWARE VMS TO A SECONDARY SITE	REPLICATE VMWARE VMS TO AZURE
Active Directory, DNS	Y	Y	Y	Y	Y

WORKLOAD	REPLICATE AZURE VMS TO AZURE	REPLICATE HYPER-V VMS TO A SECONDARY SITE	REPLICATE HYPER-V VMS TO AZURE	REPLICATE VMWARE VMS TO A SECONDARY SITE	REPLICATE VMWARE VMS TO AZURE
Web apps (IIS, SQL)	Y	Y	Y	Y	Y
System Center Operations Manager	Y	Y	Y	Y	Y
SharePoint	Y	Y	Y	Y	Y
SAP Replicate SAP site to Azure for non-cluster	Y (tested by Microsoft)	Y (tested by Microsoft)	Y (tested by Microsoft)	Y (tested by Microsoft)	Y (tested by Microsoft)
Exchange (non-DAG)	Y	Y	Y	Y	Y
Remote Desktop/VDI	Y	Y	Y	Y	Y
Linux (operating system and apps)	Y (tested by Microsoft)	Y (tested by Microsoft)	Y (tested by Microsoft)	Y (tested by Microsoft)	Y (tested by Microsoft)
Dynamics AX	Y	Y	Y	Y	Y
Windows File Server	Y	Y	Y	Y	Y
Citrix XenApp and XenDesktop	Y	N/A	Y	N/A	Y

## Replicate Active Directory and DNS

An Active Directory and DNS infrastructure are essential to most enterprise apps. During disaster recovery, you'll need to protect and recover these infrastructure components, before recovering your workloads and apps.

You can use Site Recovery to create a complete automated disaster recovery plan for Active Directory and DNS. For example, if you want to fail over SharePoint and SAP from a primary to a secondary site, you can set up a recovery plan that fails over Active Directory first, and then an additional app-specific recovery plan to fail over the other apps that rely on Active Directory.

[Learn more](#) about protecting Active Directory and DNS.

## Protect SQL Server

SQL Server provides a data services foundation for data services for many business apps in an on-premises data center. Site Recovery can be used together with SQL Server HA/DR technologies, to protect multi-tiered enterprise apps that use SQL Server. Site Recovery provides:

- A simple and cost-effective disaster recovery solution for SQL Server. Replicate multiple versions and editions of SQL Server standalone servers and clusters, to Azure or to a secondary site.

- Integration with SQL AlwaysOn Availability Groups, to manage failover and failback with Azure Site Recovery recovery plans.
- End-to-end recovery plans for the all tiers in an application, including the SQL Server databases.
- Scaling of SQL Server for peak loads with Site Recovery, by “bursting” them into larger IaaS virtual machine sizes in Azure.
- Easy testing of SQL Server disaster recovery. You can run test failovers to analyze data and run compliance checks, without impacting your production environment.

[Learn more](#) about protecting SQL server.

## Protect SharePoint

Azure Site Recovery helps protect SharePoint deployments, as follows:

- Eliminates the need and associated infrastructure costs for a stand-by farm for disaster recovery. Use Site Recovery to replicate an entire farm (Web, app and database tiers) to Azure or to a secondary site.
- Simplifies application deployment and management. Updates deployed to the primary site are automatically replicated, and are thus available after failover and recovery of a farm in a secondary site. Also lowers the management complexity and costs associated with keeping a stand-by farm up-to-date.
- Simplifies SharePoint application development and testing by creating a production-like copy on-demand replica environment for testing and debugging.
- Simplifies transition to the cloud by using Site Recovery to migrate SharePoint deployments to Azure.

[Learn more](#) about protecting SharePoint.

## Protect Dynamics AX

Azure Site Recovery helps protect your Dynamics AX ERP solution, by:

- Orchestrating replication of your entire Dynamics AX environment (Web and AOS tiers, database tiers, SharePoint) to Azure, or to a secondary site.
- Simplifying migration of Dynamics AX deployments to the cloud (Azure).
- Simplifying Dynamics AX application development and testing by creating a production-like copy on-demand, for testing and debugging.

[Learn more](#) about protecting Dynamic AX.

## Protect RDS

Remote Desktop Services (RDS) enables virtual desktop infrastructure (VDI), session-based desktops, and applications, allowing users to work anywhere. With Azure Site Recovery you can:

- Replicate managed or unmanaged pooled virtual desktops to a secondary site, and remote applications and sessions to a secondary site or Azure.
- Here's what you can replicate:

RDS	REPLICATE AZURE VMS TO AZURE	REPLICATE HYPER-V VMs TO A SECONDARY SITE	REPLICATE HYPER-V VMs TO AZURE	REPLICATE VMWARE VMs TO A SECONDARY SITE	REPLICATE VMWARE VMs TO AZURE	REPLICATE PHYSICAL SERVERS TO A SECONDARY SITE	REPLICATE PHYSICAL SERVERS TO AZURE
<b>Pooled Virtual Desktop (unmanaged)</b>	No	Yes	No	Yes	No	Yes	No
<b>Pooled Virtual Desktop (managed and without UPD)</b>	No	Yes	No	Yes	No	Yes	No
<b>Remote applications and Desktop sessions (without UPD)</b>	Yes	Yes	Yes	Yes	Yes	Yes	Yes

[Set up disaster recovery for RDS using Azure Site Recovery.](#)

[Learn more](#) about protecting RDS.

## Protect Exchange

Site Recovery helps protect Exchange, as follows:

- For small Exchange deployments, such as a single or standalone server, Site Recovery can replicate and fail over to Azure or to a secondary site.
- For larger deployments, Site Recovery integrates with Exchange DAGs.
- Exchange DAGs are the recommended solution for Exchange disaster recovery in an enterprise. Site Recovery recovery plans can include DAGs, to orchestrate DAG failover across sites.

[Learn more](#) about protecting Exchange.

## Protect SAP

Use Site Recovery to protect your SAP deployment, as follows:

- Enable protection of SAP NetWeaver and non-NetWeaver Production applications running on-premises, by replicating components to Azure.
- Enable protection of SAP NetWeaver and non-NetWeaver Production applications running Azure, by replicating components to another Azure datacenter.
- Simplify cloud migration, by using Site Recovery to migrate your SAP deployment to Azure.
- Simplify SAP project upgrades, testing, and prototyping, by creating a production clone on-demand for testing SAP applications.

[Learn more](#) about protecting SAP.

## Protect IIS

Use Site Recovery to protect your IIS deployment, as follows:

Azure Site Recovery provides disaster recovery by replicating the critical components in your environment to a cold remote site or a public cloud like Microsoft Azure. Since the virtual machines with the web server and the database are being replicated to the recovery site, there is no requirement to backup configuration files or certificates separately. The application mappings and bindings dependent on environment variables that are changed post failover can be updated through scripts integrated into the disaster recovery plans. Virtual machines are brought up on the recovery site only in the event of a failover. Not only this, Azure Site Recovery also helps you orchestrate the end to end failover by providing you the following capabilities:

- Sequencing the shutdown and startup of virtual machines in the various tiers.
- Adding scripts to allow update of application dependencies and bindings on the virtual machines after they have been started up. The scripts can also be used to update the DNS server to point to the recovery site.
- Allocate IP addresses to virtual machines pre-failover by mapping the primary and recovery networks and hence use scripts that do not need to be updated post failover.
- Ability for a one-click failover for multiple web applications on the web servers, thus eliminating the scope for confusion in the event of a disaster.
- Ability to test the recovery plans in an isolated environment for DR drills.

[Learn more](#) about protecting IIS web farm.

## Protect Citrix XenApp and XenDesktop

Use Site Recovery to protect your Citrix XenApp and XenDesktop deployments, as follows:

- Enable protection of the Citrix XenApp and XenDesktop deployment, by replicating different deployment layers including (AD DNS server, SQL database server, Citrix Delivery Controller, StoreFront server, XenApp Master (VDA), Citrix XenApp License Server) to Azure.
- Simplify cloud migration, by using Site Recovery to migrate your Citrix XenApp and XenDesktop deployment to Azure.
- Simplify Citrix XenApp/XenDesktop testing, by creating a production-like copy on-demand for testing and debugging.
- This solution is only applicable for Windows Server operating system virtual desktops and not client virtual desktops as client virtual desktops are not yet supported for licensing in Azure. [Learn More](#) about licensing for client/server desktops in Azure.

[Learn more](#) about protecting Citrix XenApp and XenDesktop deployments. Alternatively, you can refer the [whitepaper from Citrix](#) detailing the same.

## Next steps

[Get started](#) with Azure VM replication.

# About disaster recovery for on-premises apps

10/10/2019 • 8 minutes to read • [Edit Online](#)

This article describes on-premises workloads and apps you can protect for disaster recovery with the [Azure Site Recovery](#) service.

## Overview

Organizations need a business continuity and disaster recovery (BCDR) strategy to keep workloads and data safe and available during planned and unplanned downtime, and recover to regular working conditions as soon as possible.

Site Recovery is an Azure service that contributes to your BCDR strategy. Using Site Recovery, you can deploy application-aware replication to the cloud, or to a secondary site. Whether your apps are Windows or Linux-based, running on physical servers, VMware or Hyper-V, you can use Site Recovery to orchestrate replication, perform disaster recovery testing, and run failovers and failback.

Site Recovery integrates with Microsoft applications, including SharePoint, Exchange, Dynamics, SQL Server, and Active Directory. Microsoft also works closely with leading vendors including Oracle, SAP, and Red Hat. You can customize replication solutions on an app-by-app basis.

## Why use Site Recovery for application replication?

Site Recovery contributes to application-level protection and recovery as follows:

- App-agnostic, providing replication for any workloads running on a supported machine.
- Near-synchronous replication, with RPOs as low as 30 seconds to meet the needs of most critical business apps.
- App-consistent snapshots, for single or multi-tier applications.
- Integration with SQL Server AlwaysOn, and partnership with other application-level replication technologies, including AD replication, SQL AlwaysOn, Exchange Database Availability Groups (DAGs).
- Flexible recovery plans, that enable you to recover an entire application stack with a single click, and to include external scripts and manual actions in the plan.
- Advanced network management in Site Recovery and Azure to simplify app network requirements, including the ability to reserve IP addresses, configure load-balancing, and integration with Azure Traffic Manager, for low RTO network switchovers.
- A rich automation library that provides production-ready, application-specific scripts that can be downloaded and integrated with recovery plans.

## Workload summary

Site Recovery can replicate any app running on a supported machine. In addition, we've partnered with product teams to carry out additional testing for the apps specified in the table.

WORKLOAD	REPLICATE AZURE VMS TO AZURE	REPLICATE HYPER-V VMS TO A SECONDARY SITE	REPLICATE HYPER-V VMS TO AZURE	REPLICATE VMWARE VMS TO A SECONDARY SITE	REPLICATE VMWARE VMS TO AZURE
Active Directory, DNS	Y	Y	Y	Y	Y

WORKLOAD	REPLICATE AZURE VMS TO AZURE	REPLICATE HYPER-V VMS TO A SECONDARY SITE	REPLICATE HYPER-V VMS TO AZURE	REPLICATE VMWARE VMS TO A SECONDARY SITE	REPLICATE VMWARE VMS TO AZURE
Web apps (IIS, SQL)	Y	Y	Y	Y	Y
System Center Operations Manager	Y	Y	Y	Y	Y
SharePoint	Y	Y	Y	Y	Y
SAP Replicate SAP site to Azure for non-cluster	Y (tested by Microsoft)	Y (tested by Microsoft)	Y (tested by Microsoft)	Y (tested by Microsoft)	Y (tested by Microsoft)
Exchange (non-DAG)	Y	Y	Y	Y	Y
Remote Desktop/VDI	Y	Y	Y	Y	Y
Linux (operating system and apps)	Y (tested by Microsoft)	Y (tested by Microsoft)	Y (tested by Microsoft)	Y (tested by Microsoft)	Y (tested by Microsoft)
Dynamics AX	Y	Y	Y	Y	Y
Windows File Server	Y	Y	Y	Y	Y
Citrix XenApp and XenDesktop	Y	N/A	Y	N/A	Y

## Replicate Active Directory and DNS

An Active Directory and DNS infrastructure are essential to most enterprise apps. During disaster recovery, you'll need to protect and recover these infrastructure components, before recovering your workloads and apps.

You can use Site Recovery to create a complete automated disaster recovery plan for Active Directory and DNS. For example, if you want to fail over SharePoint and SAP from a primary to a secondary site, you can set up a recovery plan that fails over Active Directory first, and then an additional app-specific recovery plan to fail over the other apps that rely on Active Directory.

[Learn more](#) about protecting Active Directory and DNS.

## Protect SQL Server

SQL Server provides a data services foundation for data services for many business apps in an on-premises data center. Site Recovery can be used together with SQL Server HA/DR technologies, to protect multi-tiered enterprise apps that use SQL Server. Site Recovery provides:

- A simple and cost-effective disaster recovery solution for SQL Server. Replicate multiple versions and editions of SQL Server standalone servers and clusters, to Azure or to a secondary site.

- Integration with SQL AlwaysOn Availability Groups, to manage failover and failback with Azure Site Recovery recovery plans.
- End-to-end recovery plans for the all tiers in an application, including the SQL Server databases.
- Scaling of SQL Server for peak loads with Site Recovery, by “bursting” them into larger IaaS virtual machine sizes in Azure.
- Easy testing of SQL Server disaster recovery. You can run test failovers to analyze data and run compliance checks, without impacting your production environment.

[Learn more](#) about protecting SQL server.

## Protect SharePoint

Azure Site Recovery helps protect SharePoint deployments, as follows:

- Eliminates the need and associated infrastructure costs for a stand-by farm for disaster recovery. Use Site Recovery to replicate an entire farm (Web, app and database tiers) to Azure or to a secondary site.
- Simplifies application deployment and management. Updates deployed to the primary site are automatically replicated, and are thus available after failover and recovery of a farm in a secondary site. Also lowers the management complexity and costs associated with keeping a stand-by farm up-to-date.
- Simplifies SharePoint application development and testing by creating a production-like copy on-demand replica environment for testing and debugging.
- Simplifies transition to the cloud by using Site Recovery to migrate SharePoint deployments to Azure.

[Learn more](#) about protecting SharePoint.

## Protect Dynamics AX

Azure Site Recovery helps protect your Dynamics AX ERP solution, by:

- Orchestrating replication of your entire Dynamics AX environment (Web and AOS tiers, database tiers, SharePoint) to Azure, or to a secondary site.
- Simplifying migration of Dynamics AX deployments to the cloud (Azure).
- Simplifying Dynamics AX application development and testing by creating a production-like copy on-demand, for testing and debugging.

[Learn more](#) about protecting Dynamic AX.

## Protect RDS

Remote Desktop Services (RDS) enables virtual desktop infrastructure (VDI), session-based desktops, and applications, allowing users to work anywhere. With Azure Site Recovery you can:

- Replicate managed or unmanaged pooled virtual desktops to a secondary site, and remote applications and sessions to a secondary site or Azure.
- Here's what you can replicate:

RDS	REPLICATE AZURE VMS TO AZURE	REPLICATE HYPER-V VMs TO A SECONDARY SITE	REPLICATE HYPER-V VMs TO AZURE	REPLICATE VMWARE VMs TO A SECONDARY SITE	REPLICATE VMWARE VMs TO AZURE	REPLICATE PHYSICAL SERVERS TO A SECONDARY SITE	REPLICATE PHYSICAL SERVERS TO AZURE
<b>Pooled Virtual Desktop (unmanaged)</b>	No	Yes	No	Yes	No	Yes	No
<b>Pooled Virtual Desktop (managed and without UPD)</b>	No	Yes	No	Yes	No	Yes	No
<b>Remote applications and Desktop sessions (without UPD)</b>	Yes	Yes	Yes	Yes	Yes	Yes	Yes

[Set up disaster recovery for RDS using Azure Site Recovery.](#)

[Learn more](#) about protecting RDS.

## Protect Exchange

Site Recovery helps protect Exchange, as follows:

- For small Exchange deployments, such as a single or standalone server, Site Recovery can replicate and fail over to Azure or to a secondary site.
- For larger deployments, Site Recovery integrates with Exchange DAGs.
- Exchange DAGs are the recommended solution for Exchange disaster recovery in an enterprise. Site Recovery recovery plans can include DAGs, to orchestrate DAG failover across sites.

[Learn more](#) about protecting Exchange.

## Protect SAP

Use Site Recovery to protect your SAP deployment, as follows:

- Enable protection of SAP NetWeaver and non-NetWeaver Production applications running on-premises, by replicating components to Azure.
- Enable protection of SAP NetWeaver and non-NetWeaver Production applications running Azure, by replicating components to another Azure datacenter.
- Simplify cloud migration, by using Site Recovery to migrate your SAP deployment to Azure.
- Simplify SAP project upgrades, testing, and prototyping, by creating a production clone on-demand for testing SAP applications.

[Learn more](#) about protecting SAP.

## Protect IIS

Use Site Recovery to protect your IIS deployment, as follows:

Azure Site Recovery provides disaster recovery by replicating the critical components in your environment to a cold remote site or a public cloud like Microsoft Azure. Since the virtual machines with the web server and the database are being replicated to the recovery site, there is no requirement to backup configuration files or certificates separately. The application mappings and bindings dependent on environment variables that are changed post failover can be updated through scripts integrated into the disaster recovery plans. Virtual machines are brought up on the recovery site only in the event of a failover. Not only this, Azure Site Recovery also helps you orchestrate the end to end failover by providing you the following capabilities:

- Sequencing the shutdown and startup of virtual machines in the various tiers.
- Adding scripts to allow update of application dependencies and bindings on the virtual machines after they have been started up. The scripts can also be used to update the DNS server to point to the recovery site.
- Allocate IP addresses to virtual machines pre-failover by mapping the primary and recovery networks and hence use scripts that do not need to be updated post failover.
- Ability for a one-click failover for multiple web applications on the web servers, thus eliminating the scope for confusion in the event of a disaster.
- Ability to test the recovery plans in an isolated environment for DR drills.

[Learn more](#) about protecting IIS web farm.

## Protect Citrix XenApp and XenDesktop

Use Site Recovery to protect your Citrix XenApp and XenDesktop deployments, as follows:

- Enable protection of the Citrix XenApp and XenDesktop deployment, by replicating different deployment layers including (AD DNS server, SQL database server, Citrix Delivery Controller, StoreFront server, XenApp Master (VDA), Citrix XenApp License Server) to Azure.
- Simplify cloud migration, by using Site Recovery to migrate your Citrix XenApp and XenDesktop deployment to Azure.
- Simplify Citrix XenApp/XenDesktop testing, by creating a production-like copy on-demand for testing and debugging.
- This solution is only applicable for Windows Server operating system virtual desktops and not client virtual desktops as client virtual desktops are not yet supported for licensing in Azure. [Learn More](#) about licensing for client/server desktops in Azure.

[Learn more](#) about protecting Citrix XenApp and XenDesktop deployments. Alternatively, you can refer the [whitepaper from Citrix](#) detailing the same.

## Next steps

[Get started](#) with Azure VM replication.

# Set up disaster recovery for a multi-tier SAP NetWeaver app deployment

2/12/2020 • 7 minutes to read • [Edit Online](#)

Most large-size and medium-size SAP deployments use 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 like SAP. Azure Site Recovery has been tested and integrated with SAP applications. Site Recovery exceeds the capabilities of most on-premises disaster recovery solutions, and at a lower total cost of ownership than competing solutions.

With Site Recovery, you can:

- Enable protection of SAP NetWeaver and non-NetWeaver production applications that run on-premises by replicating components to Azure.
- Enable protection of SAP NetWeaver and non-NetWeaver production applications that run on Azure by replicating components to another Azure datacenter.
- Simplify cloud migration by using Site Recovery to migrate your SAP deployment to Azure.
- Simplify SAP project upgrades, testing, and prototyping by creating a production clone on-demand for testing SAP applications.

You can protect SAP NetWeaver application deployments by using [Azure Site Recovery](#). This article covers best practices for protecting a three-tier SAP NetWeaver deployment on Azure when you replicate to another Azure datacenter by using Site Recovery. The article describes supported scenarios and configurations, and how to do test failovers (disaster recovery drills) and actual failovers.

## Prerequisites

Before you begin, ensure that you know how to do the following tasks:

- [Replicate a virtual machine to Azure](#)
- [Design a recovery network](#)
- [Do a test failover to Azure](#)
- [Do a failover to Azure](#)
- [Replicate a domain controller](#)
- [Replicate a SQL Server instance](#)

## Supported scenarios

You can use Site Recovery to implement a disaster recovery solution in the following scenarios:

- You have SAP systems running in one Azure datacenter, and you're replicating them to another Azure datacenter (Azure-to-Azure disaster recovery). For more information, see [Azure-to-Azure replication architecture](#).
- You have SAP systems running on VMware (or physical) servers on-premises. You're also replicating the SAP systems to a disaster recovery site in an Azure datacenter (VMware-to-Azure disaster recovery). This scenario requires some additional components. For more information, see [VMware-to-Azure replication architecture](#).
- You have SAP systems running on Hyper-V on-premises. You're also replicating the SAP systems to a disaster recovery site in an Azure datacenter (Hyper-V-to-Azure disaster recovery). This scenario requires some additional components. For more information, see [Hyper-V-to-Azure replication architecture](#).

In this article, we use an **Azure-to-Azure** disaster recovery scenario. The scenario shows you the SAP disaster recovery capabilities of Site Recovery. Because Site Recovery replication isn't application-specific, the process that's described is expected to also apply to other scenarios.

## Required foundation services

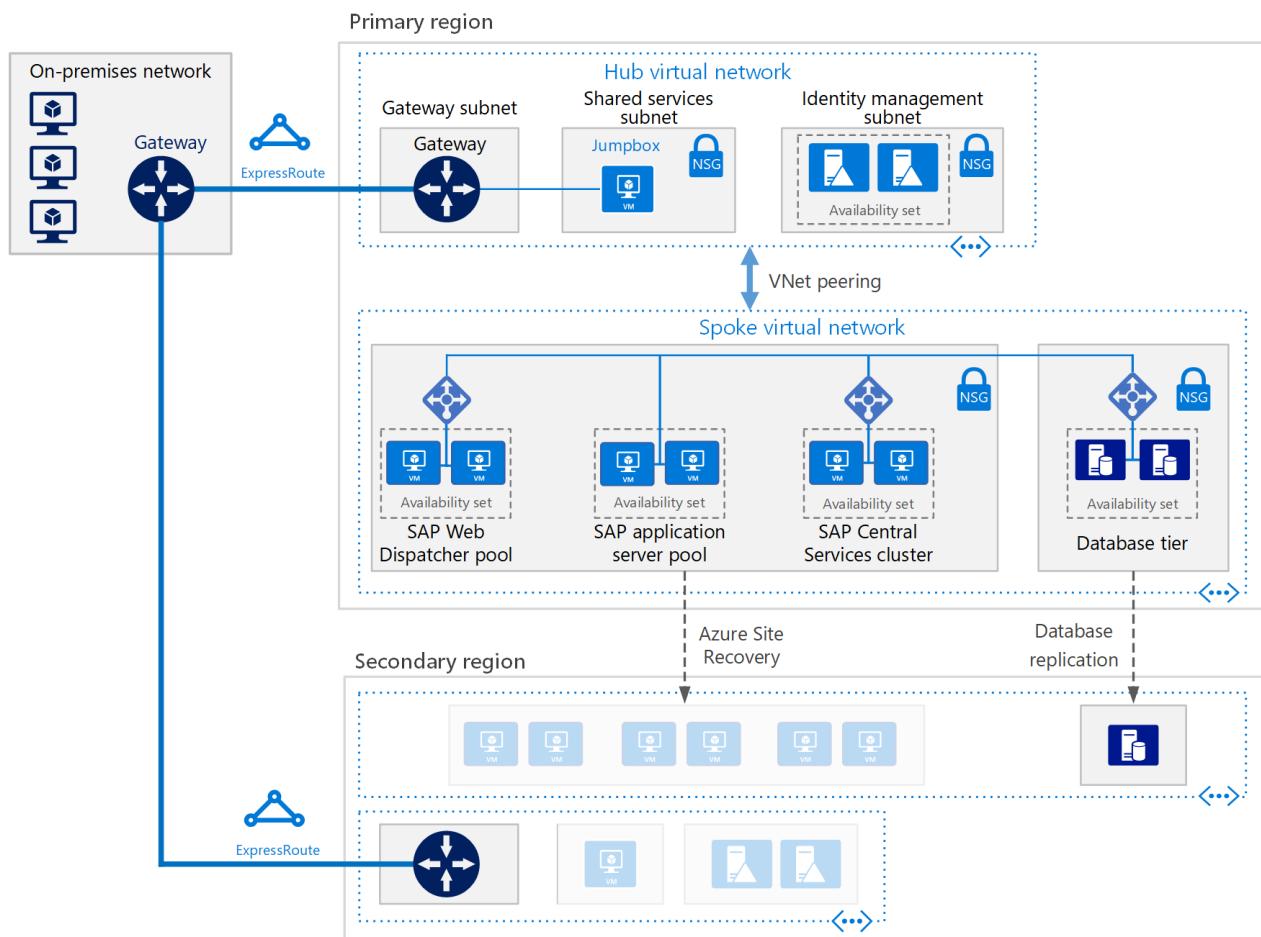
In the scenario we discuss in this article, the following foundation services are deployed:

- Azure ExpressRoute or Azure VPN Gateway
- At least one Azure Active Directory domain controller and DNS server, running in Azure

We recommend that you establish this infrastructure before you deploy Site Recovery.

## Reference SAP application deployment

This reference architecture is running SAP NetWeaver in a Windows environment on Azure with high availability. This architecture is deployed with specific virtual machine (VM) sizes that you can change to accommodate your organization's needs.



## Disaster recovery considerations

For disaster recovery, you must be able to fail over to a secondary region. Each tier uses a different strategy to provide disaster recovery protection.

### VMs running SAP Web Dispatcher pools

The Web Dispatcher component works as a load balancer for SAP traffic among the SAP application servers. To achieve high availability for the Web Dispatcher component, Azure Load Balancer implements the parallel Web Dispatcher setup. Web Dispatcher uses a round-robin configuration for HTTP(S) traffic distribution among the available Web Dispatchers in the balancers pool.

### VMs running application servers pools

The SMLG transaction manages login groups for ABAP application servers. It uses the load-balancing function within the message server of the Central Services to distribute workload among SAP application server pools for SAPGUIs and RFC traffic. You can replicate this management by using Site Recovery.

#### VMs running SAP Central Services clusters

This reference architecture runs Central Services on VMs in the application tier. Central Services is a potential single point of failure when in a single VM. Typical deployment and high availability aren't requirements.

To implement a high availability solution, you can use either a shared disk cluster or a file share cluster. To configure VMs for a shared disk cluster, use Windows Server Failover Cluster. We recommend that you use the cloud witness as a quorum witness.

##### NOTE

Because Site Recovery does not replicate the cloud witness, we recommend that you deploy the cloud witness in the disaster recovery region.

To support the failover cluster environment, [SIOS DataKeeper Cluster Edition](#) does the cluster shared volume function. In the function, SIOS DataKeeper Cluster replicates independent disks owned by the cluster nodes. Because Azure does not natively support shared disks, it requires solutions provided by SIOS.

You can also handle clustering by implementing a file share cluster. SAP recently modified the Central Services deployment pattern to access the /sapmnt global directories via a UNC path. We still recommend you ensure that the /sapmnt UNC share is highly available. You can check your Central Services instance. Use Windows Server Failover Cluster with Scale Out File Server (SOFS) and the Storage Spaces Direct (S2D) feature in Windows Server 2016.

##### NOTE

Site Recovery currently supports only crash-consistent point replication of virtual machines that use storage spaces direct and the passive node of SIOS Datakeeper.

## More disaster recovery considerations

You can use Site Recovery to orchestrate the failover of full SAP deployment across Azure regions. Following are the steps for setting up the disaster recovery:

1. Replicate virtual machines
2. Design a recovery network
3. Replicate a domain controller
4. Replicate data base tier
5. Do a test failover
6. Do a failover

Following is the recommendation for disaster recovery of each tier used in this example.

SAP TIERS	RECOMMENDATION
<b>SAP Web Dispatcher pool</b>	Replicate by using Site Recovery
<b>SAP Application server pool</b>	Replicate by using Site Recovery
<b>SAP Central Services cluster</b>	Replicate by using Site Recovery

SAP TIERS	RECOMMENDATION
<b>Active directory virtual machines</b>	Use Active directory replication
<b>SQL Database servers</b>	Use SQL Server Always On replication

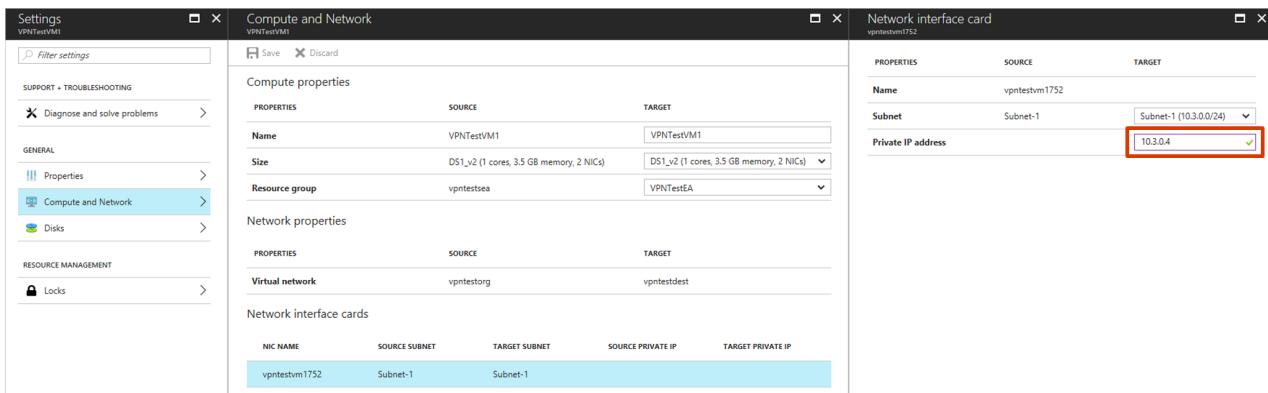
## Replicate virtual machines

To start replicating all the SAP application virtual machines to the Azure disaster recovery datacenter, follow the guidance in [Replicate a virtual machine to Azure](#).

- For guidance on protecting Active Directory and DNS, learn [how to protect Active Directory and DNS](#).
- For guidance on protecting database tier running on SQL Server, learn [how to protect SQL Server](#).

## Networking configuration

If you use a static IP address, you can specify the IP address that you want the virtual machine to take. To set the IP address, go to **Compute and Network settings > Network interface card**.



## Create a recovery plan

A recovery plan supports the sequencing of various tiers in a multi-tier application during a failover. Sequencing helps maintain application consistency. When you create a recovery plan for a multi-tier web application, complete the steps described in [Create a recovery plan by using Site Recovery](#).

### Add virtual machines to failover groups

1. Create a recovery plan by adding the application server, web dispatcher, and SAP Central services VMs.
2. Select **Customize** to group the VMs. By default, all VMs are part of Group 1.

### Add scripts to the recovery plan

For your applications to function correctly, you might need to do some operations on the Azure virtual machines. Do these operations after the failover or during a test failover. You can also automate some post-failover operations. For example, update the DNS entry, and change bindings and connections by adding corresponding scripts to the recovery plan.

You can deploy the most used Site Recovery scripts into your Azure Automation account by selecting **Deploy to Azure**. When you use any published script, follow the guidance in the script.



1. Add a pre-action script to Group 1 to fail over the SQL Server availability group. Use the ASR-SQL-FailoverAG script published in the sample scripts. Follow the guidance in the script and make the required changes in the

script appropriately.

2. Add a post-action script to attach a load balancer onto the failed-over virtual machines of the Web tier (Group 1). Use the ASR-AddSingleLoadBalancer script published in the sample scripts. Follow the guidance in the script and make the required changes in the script as needed.

The screenshot shows the SAP Recovery Plan interface. At the top, there's a header bar with the title 'SAPRecoveryPlan' and a 'Recovery plan' subtitle. Below the header are buttons for '+ Group', 'Save', 'Discard', and 'Change group'. A message box indicates that the recovery plan contains 6 machine(s). The main area is a table with two columns: 'STAGE NAME' and 'DETAILS'. The table lists various recovery stages and their details, such as 'All groups shut down', 'All groups failover', 'Group 1: Pre-steps', 'Group 1: Start', 'Group 1: Post-steps', 'Group 2: Start', 'Group 3: Start', and 'Group 3: Post-steps'. Some rows are expanded to show more details like 'Script: FailoverSQLAG' or 'Machine'. The row for 'sap-appserver2' is highlighted with a blue dashed border.

STAGE NAME	DETAILS
All groups shut down	6 machines in 3 groups. ...
▶ All groups failover	...
▼ Group 1: Pre-steps	1 Step ...
Script: FailoverSQLAG	Script ...
▼ Group 1: Start	2 Machines ...
sap-ascs-02	Machine ...
sap-ascs-01	Machine ...
▼ Group 1: Post-steps	1 Step ...
Script: Add Load balancer	Script ...
▼ Group 2: Start	2 Machines ...
sap-appserver1	Machine ...
sap-appserver2	Machine ...
▼ Group 3: Start	2 Machines ...
sap-dispatcher1	Machine ...
sap-dispatcher2	Machine ...
▼ Group 3: Post-steps	1 Step ...
Script: Add Load balancer	Script ...

## Run a test failover

1. In the Azure portal, select your Recovery Services vault.
2. Select the recovery plan that you created for SAP applications.
3. Select **Test Failover**.
4. To start the test failover process, select the recovery point and the Azure virtual network.
5. When the secondary environment is up, perform validations.
6. When validations are complete, clean the failover environment by selecting **Cleanup test failover**.

For more information, see [Test failover to Azure in Site Recovery](#).

## Run a failover

1. In the Azure portal, select your Recovery Services vault.
2. Select the recovery plan that you created for SAP applications.
3. Select **Failover**.
4. To start the failover process, select the recovery point.

For more information, see [Failover in Site Recovery](#).

## Next steps

- Learn more about building a disaster recovery solution for SAP NetWeaver deployments by using Site Recovery. See the downloadable white paper [SAP NetWeaver: Building a Disaster Recovery Solution with Site Recovery](#). The white paper discusses recommendations for various SAP architectures. You can see supported applications and VM types for SAP on Azure. There are also plan options for testing your disaster recovery solution.
- Learn more about [replicating other workloads](#) by using Site Recovery.

# Protect a file server by using Azure Site Recovery

1/14/2020 • 10 minutes to read • [Edit Online](#)

Azure Site Recovery contributes to your business continuity and disaster recovery (BCDR) strategy by keeping your business apps up and running during planned and unplanned outages. Site Recovery manages and orchestrates disaster recovery of on-premises machines and Azure virtual machines (VMs). Disaster recovery includes replication, failover, and recovery of various workloads.

This article describes how to protect a file server by using Site Recovery and makes other recommendations to suit various environments.

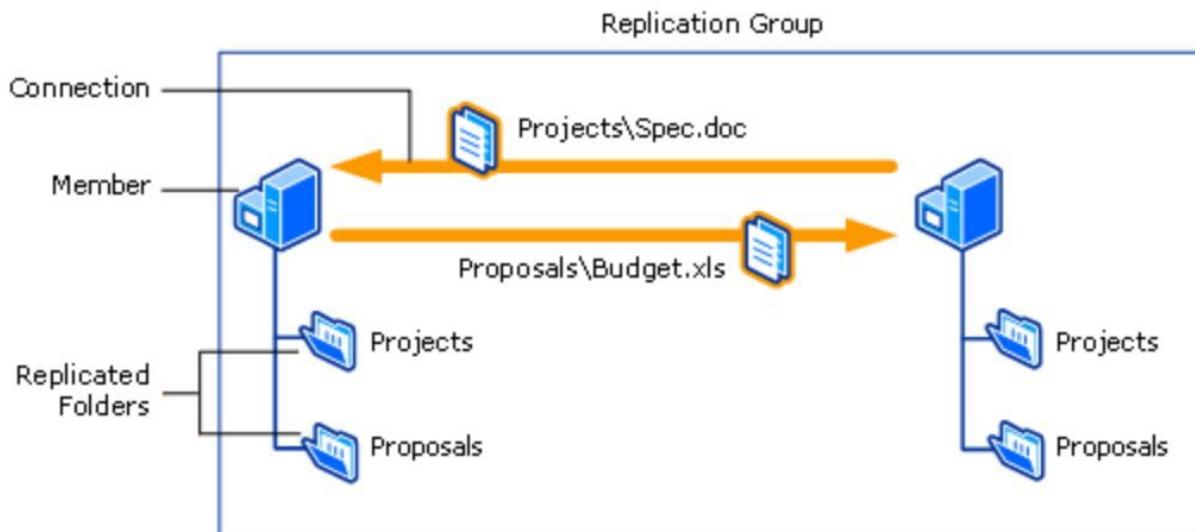
- [Replicate Azure IaaS file server machines](#)
- [Replicate an on-premises file server by using Site Recovery](#)

## File server architecture

The aim of an open distributed file-sharing system is to provide an environment where a group of geographically distributed users can collaborate to work efficiently on files and be guaranteed that their integrity requirements are enforced. A typical on-premises file server ecosystem that supports a high number of concurrent users and a large number of content items uses Distributed File System Replication (DFSR) for replication scheduling and bandwidth throttling.

DFSR uses a compression algorithm known as Remote Differential Compression (RDC) that can be used to efficiently update files over a limited-bandwidth network. It detects insertions, removals, and rearrangements of data in files. DFSR is enabled to replicate only the changed file blocks when files are updated. There are also file server environments, where daily backups are taken in non-peak timings, which cater to disaster needs. DFSR isn't implemented.

The following diagram illustrates the file server environment with DFSR implemented.

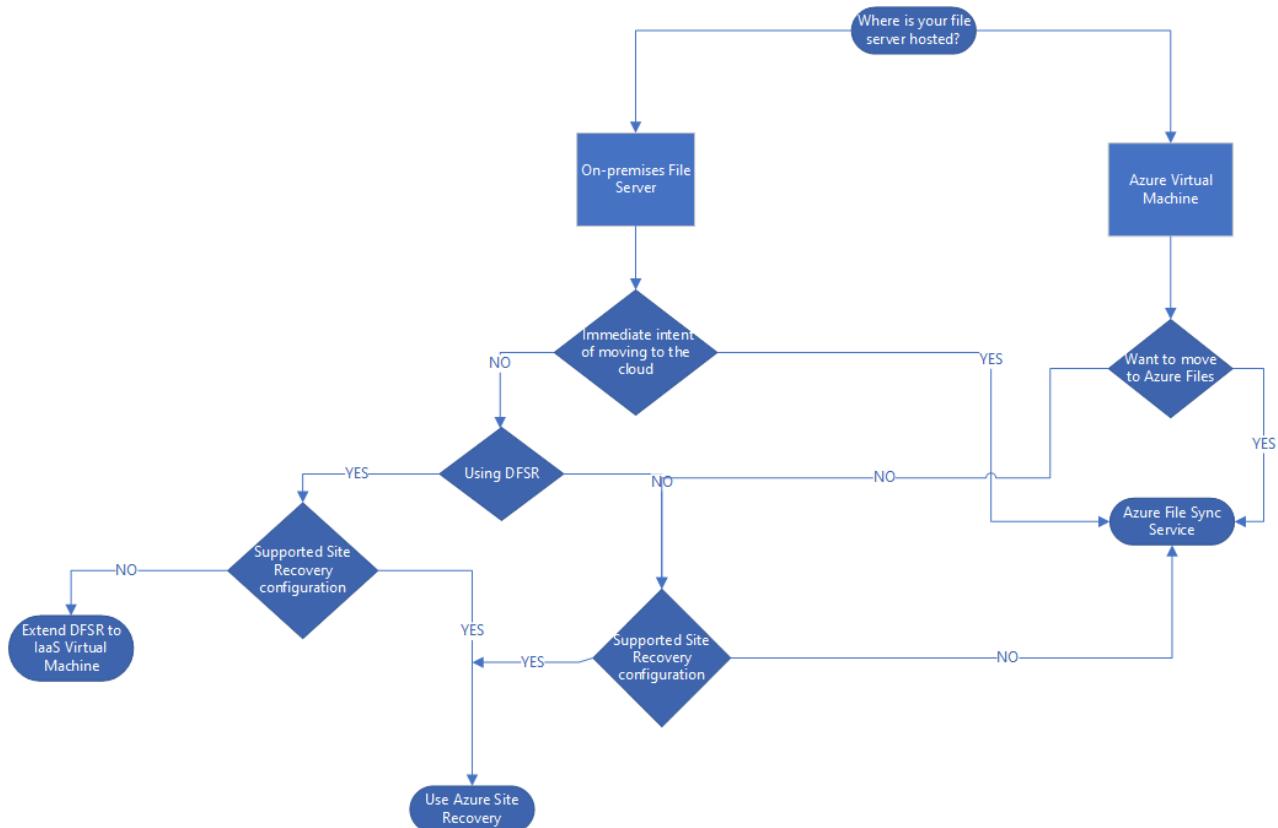


In the previous diagram, multiple file servers called members actively participate in replicating files across a replication group. The contents in the replicated folder are available to all the clients that send requests to either of the members, even if a member goes offline.

## Disaster recovery recommendations for file servers

- **Replicate a file server by using Site Recovery:** File servers can be replicated to Azure by using Site Recovery. When one or more on-premises file servers are inaccessible, the recovery VMs can be brought up in Azure. The VMs can then serve requests from clients, on-premises, provided there is site-to-site VPN connectivity and Active Directory is configured in Azure. You can use this method in the case of a DFSR-configured environment or a simple file server environment with no DFSR.
- **Extend DFSR to an Azure IaaS VM:** In a clustered file server environment with DFSR implemented, you can extend the on-premises DFSR to Azure. An Azure VM is then enabled to perform the file server role.
  - After the dependencies of site-to-site VPN connectivity and Active Directory are handled and DFSR is in place, when one or more on-premises file servers are inaccessible, clients can connect to the Azure VM, which serves the requests.
  - You can use this approach if your VMs have configurations that aren't supported by Site Recovery. An example is a shared cluster disk, which is sometimes commonly used in file server environments. DFSR also works well in low-bandwidth environments with medium churn rate. You need to consider the additional cost of having an Azure VM up and running all the time.
- **Use Azure File Sync to replicate your files:** If you plan to use the cloud or already use an Azure VM, you can use Azure File Sync. Azure File Sync offers syncing of fully managed file shares in the cloud that are accessible via the industry-standard [Server Message Block](#) (SMB) protocol. Azure file shares can then be mounted concurrently by cloud or on-premises deployments of Windows, Linux, and macOS.

The following diagram helps you determine what strategy to use for your file server environment.



#### Factors to consider in your decisions about disaster recovery to Azure

ENVIRONMENT	RECOMMENDATION	POINTS TO CONSIDER
-------------	----------------	--------------------

ENVIRONMENT	RECOMMENDATION	POINTS TO CONSIDER
File server environment with or without DFSR	<a href="#">Use Site Recovery for replication</a>	<p>Site Recovery doesn't support shared disk clusters or network attached storage (NAS). If your environment uses these configurations, use any of the other approaches, as appropriate.</p> <p>Site Recovery doesn't support SMB 3.0. The replicated VM incorporates changes only when changes made to the files are updated in the original location of the files.</p> <p>Site Recovery offers a near-synchronous data replication process, and hence in the event of an unplanned failover scenario, there could be potential data loss, and might create USN mismatch issues.</p>
File server environment with DFSR	<a href="#">Extend DFSR to an Azure IaaS virtual machine</a>	DFSR works well in extremely bandwidth-crunched environments. This approach requires an Azure VM that is up and running all the time. You need to account for the cost of the VM in your planning.
Azure IaaS VM	File Sync	If you use File Sync in a disaster recovery scenario, during failover you must take manual actions to make sure that the file shares are accessible to the client machine in a transparent way. File Sync requires port 445 to be open from the client machine.

## Site Recovery support

Because Site Recovery replication is application agnostic, these recommendations are expected to hold true for the following scenarios.

SOURCE	TO A SECONDARY SITE	TO AZURE
Azure	-	Yes
Hyper-V	Yes	Yes
VMware	Yes	Yes
Physical server	Yes	Yes

### IMPORTANT

Before you continue with any of the following three approaches, make sure that these dependencies are taken care of.

**Site-to-site connectivity:** A direct connection between the on-premises site and the Azure network must be established to allow communication between servers. Use a secure site-to-site VPN connection to an Azure virtual network that is used as the disaster recovery site. For more information, see [Establish a site-to-site VPN connection between an on-premises site and an Azure virtual network](#).

**Active Directory:** DFSR depends on Active Directory. This means that the Active Directory forest with local domain controllers is extended to the disaster recovery site in Azure. Even if you aren't using DFSR, if the intended users need to be granted access or verified for access, you must take these steps. For more information, see [Extend on-premises Active Directory to Azure](#).

## Disaster recovery recommendation for Azure IaaS virtual machines

If you're configuring and managing disaster recovery of file servers hosted on Azure IaaS VMs, you can choose between two options, based on whether you want to move to [Azure Files](#):

- [Use File Sync](#)
- [Use Site Recovery](#)

### Use File Sync to replicate files hosted on an IaaS virtual machine

Azure Files can be used to completely replace or supplement traditional on-premises file servers or NAS devices. Azure file shares also can be replicated with File Sync to Windows servers, either on-premises or in the cloud, for performance and distributed caching of the data where it's used. The following steps describe the disaster recovery recommendation for Azure VMs that perform the same functionality as traditional file servers:

- Protect machines by using Site Recovery. Follow the steps in [Replicate an Azure VM to another Azure region](#).
- Use File Sync to replicate files from the VM that acts as the file server to the cloud.
- Use the Site Recovery [recovery plan](#) feature to add scripts to [mount the Azure file share](#) and access the share in your virtual machine.

The following steps briefly describe how to use File Sync:

1. [Create a storage account in Azure](#). If you chose read-access geo-redundant storage for your storage accounts, you get read access to your data from the secondary region in case of a disaster. For more information, see [Disaster recovery and forced failover \(preview\) in Azure Storage](#).
2. [Create a file share](#).
3. [Start File Sync](#) on your Azure file server.
4. Create a sync group. Endpoints within a sync group are kept in sync with each other. A sync group must contain at least one cloud endpoint, which represents an Azure file share. A sync group also must contain one server endpoint, which represents a path on a Windows server.
5. Your files are now kept in sync across your Azure file share and your on-premises server.
6. In the event of a disaster in your on-premises environment, perform a failover by using a [recovery plan](#). Add the script to [mount the Azure file share](#) and access the share in your virtual machine.

### Replicate an IaaS file server virtual machine by using Site Recovery

If you have on-premises clients that access the IaaS file server virtual machine, take all the following steps. Otherwise, skip to step 3.

1. Establish a site-to-site VPN connection between the on-premises site and the Azure network.
2. Extend on-premises Active Directory.
3. [Set up disaster recovery](#) for the IaaS file server machine to a secondary region.

For more information on disaster recovery to a secondary region, see [this article](#).

### Replicate an on-premises file server by using Site Recovery

The following steps describe replication for a VMware VM. For steps to replicate a Hyper-V VM, see [this tutorial](#).

1. [Prepare Azure resources](#) for replication of on-premises machines.

- Establish a site-to-site VPN connection between the on-premises site and the Azure network.
- Extend on-premises Active Directory.
- [Prepare on-premises VMware servers](#).
- [Set up disaster recovery](#) to Azure for on-premises VMs.

## Extend DFSR to an Azure IaaS virtual machine

- Establish a site-to-site VPN connection between the on-premises site and the Azure network.
- Extend on-premises Active Directory.
- [Create and provision a file server VM](#) on the Azure virtual network. Make sure that the virtual machine is added to the same Azure virtual network, which has cross-connectivity with the on-premises environment.
- Install and [configure DFSR](#) on Windows Server.
- [Implement a DFS namespace](#).
- With the DFS namespace implemented, failover of shared folders from production to disaster recovery sites can be done by updating the DFS namespace folder targets. After these DFS namespace changes replicate via Active Directory, users are connected to the appropriate folder targets transparently.

## Use File Sync to replicate your on-premises files

You can use File Sync to replicate files to the cloud. In the event of a disaster and the unavailability of your on-premises file server, you can mount the desired file locations from the cloud and continue to service requests from client machines. To integrate File Sync with Site Recovery:

- Protect the file server machines by using Site Recovery. Follow the steps in [this tutorial](#).
- Use File Sync to replicate files from the machine that serves as a file server to the cloud.
- Use the recovery plan feature in Site Recovery to add scripts to mount the Azure file share on the failed-over file server VM in Azure.

Follow these steps to use File Sync:

- [Create a storage account in Azure](#). If you chose read-access geo-redundant storage (recommended) for your storage accounts, you have read access to your data from the secondary region in case of a disaster. For more information, see [Disaster recovery and forced failover \(preview\)](#) in Azure Storage..
- [Create a file share](#).
- [Deploy File Sync](#) in your on-premises file server.
- Create a sync group. Endpoints within a sync group are kept in sync with each other. A sync group must contain at least one cloud endpoint, which represents an Azure file share. The sync group also must contain one server endpoint, which represents a path on the on-premises Windows server.
- Your files are now kept in sync across your Azure file share and your on-premises server.
- In the event of a disaster in your on-premises environment, perform a failover by using a [recovery plan](#). Add the script to mount the Azure file share and access the share in your virtual machine.

### NOTE

Make sure that port 445 is open. Azure Files uses the SMB protocol. SMB communicates over TCP port 445. Check to see if your firewall isn't blocking TCP port 445 from a client machine.

## Do a test failover

- Go to the Azure portal, and select your Recovery Service vault.
- Select the recovery plan created for the file server environment.

3. Select **Test Failover**.
4. Select the recovery point and the Azure virtual network to start the test failover process.
5. After the secondary environment is up, perform your validations.
6. After the validations are finished, select **Cleanup test failover** on the recovery plan, and the test failover environment is cleaned.

For more information on how to perform a test failover, see [Test failover to Site Recovery](#).

For guidance on doing test failover for Active Directory and DNS, see [Test failover considerations for Active Directory and DNS](#).

## Do a failover

1. Go to the Azure portal, and select your Recovery Services vault.
2. Select the recovery plan created for the file server environment.
3. Select **Failover**.
4. Select the recovery point to start the failover process.

For more information on how to perform a failover, see [Failover in Site Recovery](#).

# Set up disaster recovery for a multi-tier IIS-based web application

11/12/2019 • 8 minutes to read • [Edit Online](#)

Application software is the engine of business productivity in an organization. Various web applications can serve different purposes in an organization. Some applications, like applications used for payroll processing, financial applications, and customer-facing websites, might be critical to an organization. To prevent loss of productivity, it's important for the organization to have these applications continuously up and running. More importantly, having these applications consistently available can help prevent damage to the brand or image of the organization.

Critical web applications are typically set up as multi-tier applications: the web, database, and application are on different tiers. In addition to being spread across various tiers, the applications might also use multiple servers in each tier to load balance the traffic. Moreover, the mappings between various tiers and on the web server might be based on static IP addresses. On failover, some of these mappings need to be updated, especially if multiple websites are configured on the web server. If web applications use SSL, you must update certificate bindings.

Traditional recovery methods that aren't based on replication involve backing up various configuration files, registry settings, bindings, custom components (COM or .NET), content, and certificates. Files are recovered through a set of manual steps. The traditional recovery methods of backing up and manually recovering files are cumbersome, error-prone, and not scalable. For example, you might easily forget to back up certificates. After failover, you're left with no choice but to buy new certificates for the server.

A good disaster recovery solution supports modeling recovery plans for complex application architectures. You should also be able to add customized steps to the recovery plan to handle application mappings between tiers. If there is a disaster, application mappings provide a single-click, sure-shot solution that helps lead to a lower RTO.

This article describes how to protect a web application that's based on Internet Information Services (IIS) by using [Azure Site Recovery](#). The article covers best practices for replicating a three-tier, IIS-based web application to Azure, how to do a disaster recovery drill, and how to fail over the application to Azure.

## Prerequisites

Before you begin, ensure that you know how to do the following tasks:

- [Replicate a virtual machine to Azure](#)
- [Design a recovery network](#)
- [Do a test failover to Azure](#)
- [Do a failover to Azure](#)
- [Replicate a domain controller](#)
- [Replicate SQL Server](#)

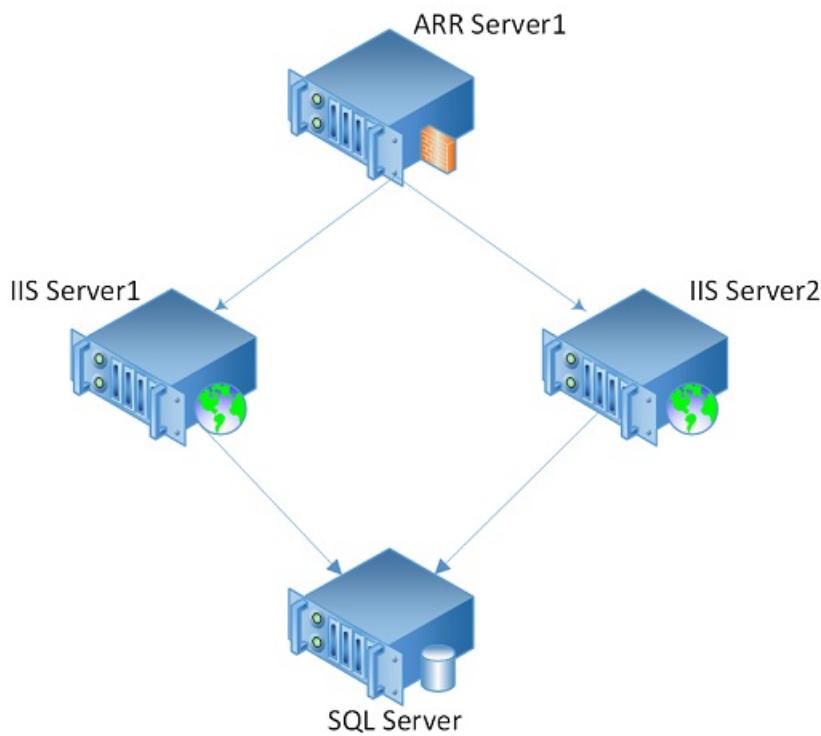
## Deployment patterns

An IIS-based web application typically follows one of the following deployment patterns:

### Deployment pattern 1

An IIS-based web farm with Application Request Routing (ARR), an IIS server, and SQL Server.

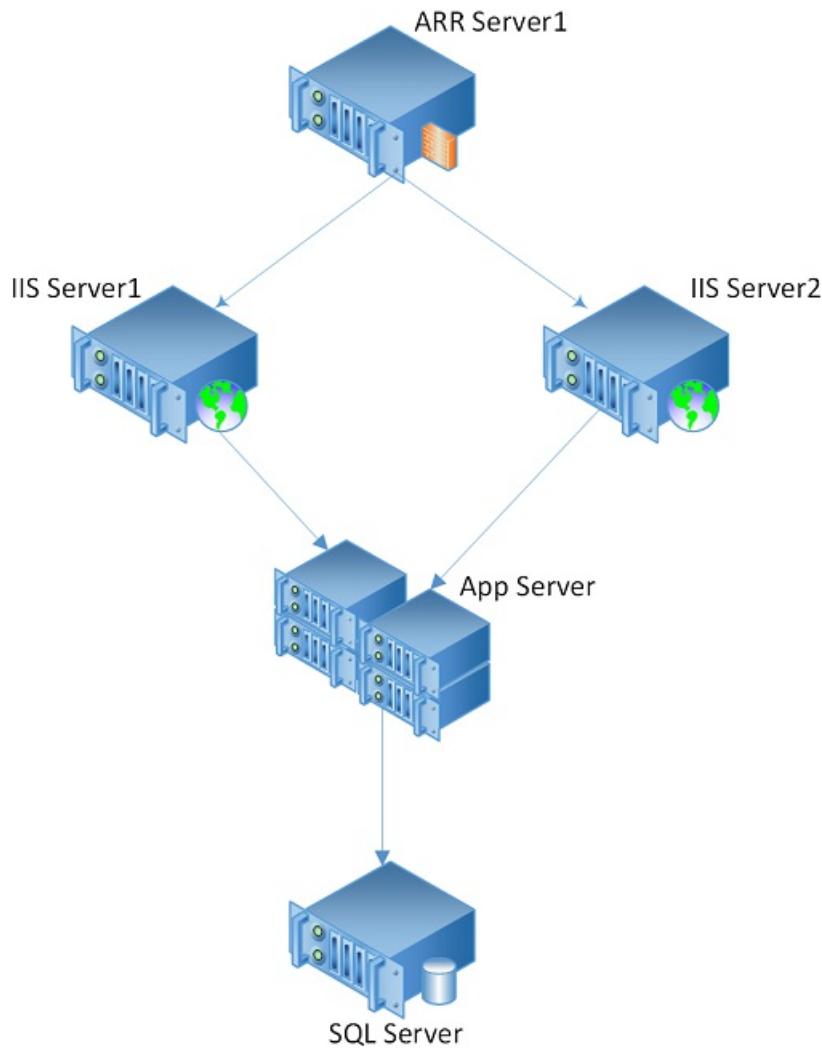
## IIS Web Farm – 3 Tier Deployment



### Deployment pattern 2

An IIS-based web farm with ARR, an IIS server, an application server, and SQL Server.

## IIS Web Farm - 4 Tier Deployment



## Site Recovery support

For the examples in this article, we use VMware virtual machines with IIS 7.5 on Windows Server 2012 R2 Enterprise. Because Site Recovery replication isn't application-specific, the recommendations in this article are expected to apply in the scenarios listed in the following table, and for different versions of IIS.

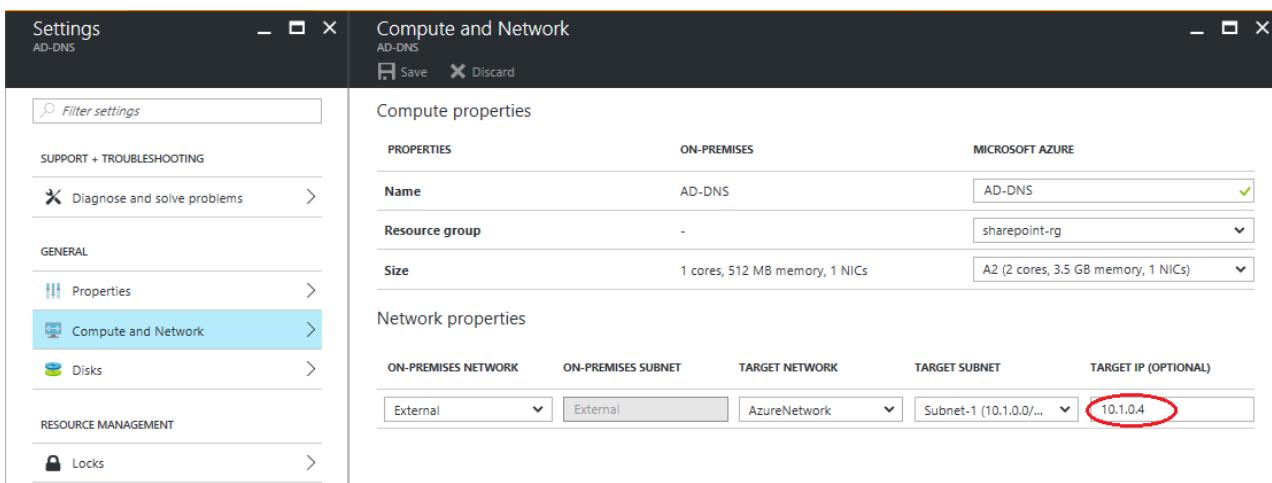
### Source and target

SCENARIO	TO A SECONDARY SITE	TO AZURE
Hyper-V	Yes	Yes
VMware	Yes	Yes
Physical server	No	Yes
Azure	NA	Yes

## Replicate virtual machines

To start replicating all the IIS web farm virtual machines to Azure, follow the guidance in [Test failover to Azure in Site Recovery](#).

If you are using a static IP address, you can specify the IP address that you want the virtual machine to take. To set the IP address, go to **Compute and Network settings** > **TARGET IP**.



## Create a recovery plan

A recovery plan supports the sequencing of various tiers in a multi-tier application during a failover. Sequencing helps maintain application consistency. When you create a recovery plan for a multi-tier web application, complete the steps described in [Create a recovery plan by using Site Recovery](#).

### Add virtual machines to failover groups

A typical multi-tier IIS web application consists of the following components:

- A database tier that has SQL virtual machines.
- The web tier, which consists of an IIS server and an application tier.

Add virtual machines to different groups based on the tier:

1. Create a recovery plan. Add the database tier virtual machines under Group 1. This ensures that database tier virtual machines are shut down last and brought up first.
2. Add the application tier virtual machines under Group 2. This ensures that application tier virtual machines are brought up after the database tier has been brought up.
3. Add the web tier virtual machines in Group 3. This ensures that web tier virtual machines are brought up after the application tier has been brought up.
4. Add load balance virtual machines in Group 4. This ensures that load balance virtual machines are brought up after the web tier has been brought up.

For more information, see [Customize the recovery plan](#).

### Add a script to the recovery plan

For the IIS web farm to function correctly, you might need to do some operations on the Azure virtual machines post-failover or during a test failover. You can automate some post-failover operations. For example, you can update the DNS entry, change a site binding, or change a connection string by adding corresponding scripts to the recovery plan. [Add a VMM script to a recovery plan](#) describes how to set up automated tasks by using a script.

### DNS update

If DNS is configured for dynamic DNS update, virtual machines usually update the DNS with the new IP address when they start. If you want to add an explicit step to update DNS with the new IP addresses of the virtual machines, add a [script to update IP in DNS](#) as a post-failover action on recovery plan groups.

### Connection string in an application's web.config

The connection string specifies the database that the website communicates with. If the connection string carries the name of the database virtual machine, no further steps are needed post-failover. The application can

automatically communicate with the database. Also, if the IP address for the database virtual machine is retained, it doesn't need to update the connection string.

If the connection string refers to the database virtual machine by using an IP address, it needs to be updated post-failover. For example, the following connection string points to the database with the IP address 127.0.1.2:

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
<connectionStrings>
<add name="ConnStringDb1" connectionString="Data Source= 127.0.1.2\SqlExpress; Initial Catalog=TestDB1;Integrated Security=False;" />
</connectionStrings>
</configuration>
```

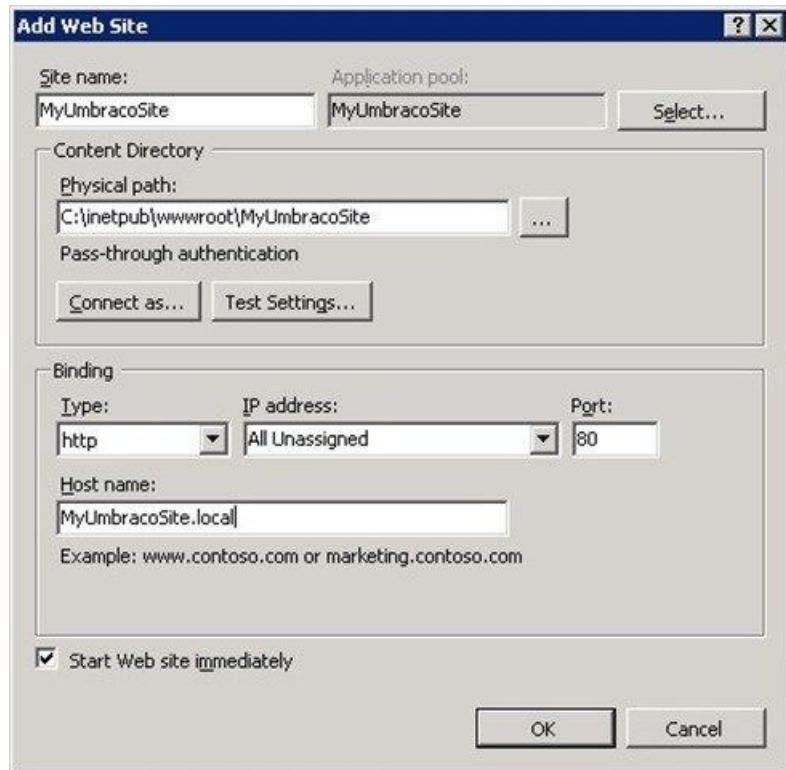
To update the connection string in the web tier, add an [IIS connection update script](#) after Group 3 in the recovery plan.

#### Site bindings for the application

Every site consists of binding information. The binding information includes the type of binding, the IP address at which the IIS server listens to the requests for the site, the port number, and the host names for the site. During the failover, you might need to update these bindings if there's a change in the IP address that's associated with them.

#### NOTE

If you set the site binding to **All unassigned**, you don't need to update this binding post-failover. Also, if the IP address associated with a site isn't changed post-failover, you don't need to update the site binding. (The retention of the IP address depends on the network architecture and subnets assigned to the primary and recovery sites. Updating them might not be feasible for your organization.)



If you associated the IP address with a site, update all site bindings with the new IP address. To change the site bindings, add an [IIS web tier update script](#) after Group 3 in the recovery plan.

#### Update the load balancer IP address

If you have an ARR virtual machine, to update the IP address, add an [IIS ARR failover script](#) after Group 4.

#### **SSL certificate binding for an HTTPS connection**

A website might have an associated SSL certificate that helps ensure a secure communication between the web server and the user's browser. If the website has an HTTPS connection, and also has an associated HTTPS site binding to the IP address of the IIS server with an SSL certificate binding, you must add a new site binding for the certificate with the IP address of the IIS virtual machine post-failover.

The SSL certificate can be issued against these components:

- The fully qualified domain name of the website.
- The name of the server.
- A wildcard certificate for the domain name.
- An IP address. If the SSL certificate is issued against the IP address of the IIS server, another SSL certificate needs to be issued against the IP address of the IIS server on the Azure site. An additional SSL binding for this certificate needs to be created. Because of this, we recommend not using an SSL certificate issued against the IP address. This option is less widely used and will soon be deprecated in accordance with new certificate authority/browser forum changes.

#### **Update the dependency between the web tier and the application tier**

If you have an application-specific dependency that's based on the IP address of the virtual machines, you must update this dependency post-failover.

## Run a test failover

1. In the Azure portal, select your Recovery Services vault.
2. Select the recovery plan that you created for the IIS web farm.
3. Select **Test Failover**.
4. To start the test failover process, select the recovery point and the Azure virtual network.
5. When the secondary environment is up, you can perform validations.
6. When validations are complete, to clean the test failover environment, select **Validations complete**.

For more information, see [Test failover to Azure in Site Recovery](#).

## Run a failover

1. In the Azure portal, select your Recovery Services vault.
2. Select the recovery plan that you created for the IIS web farm.
3. Select **Failover**.
4. To start the failover process, select the recovery point.

For more information, see [Failover in Site Recovery](#).

## Next steps

- Learn more about [replicating other applications](#) by using Site Recovery.

# set up disaster recovery for a multi-tier Citrix XenApp and XenDesktop deployment

11/14/2019 • 7 minutes to read • [Edit Online](#)

Citrix XenDesktop is a desktop virtualization solution that delivers desktops and applications as an ondemand service to any user, anywhere. With FlexCast delivery technology, XenDesktop can quickly and securely deliver applications and desktops to users. Today, Citrix XenApp does not provide any disaster recovery capabilities.

A good disaster recovery solution, should allow modeling of recovery plans around the above complex application architectures and also have the ability to add customized steps to handle application mappings between various tiers hence providing a single-click sure shot solution in the event of a disaster leading to a lower RTO.

This document provides step-by-step guidance for building a disaster recovery solution for your on-premises Citrix XenApp deployments on Hyper-V and VMware vSphere platforms. This document also describes how to perform a test failover(disaster recovery drill) and unplanned failover to Azure using recovery plans, the supported configurations and prerequisites.

## Prerequisites

Before you start, make sure you understand the following:

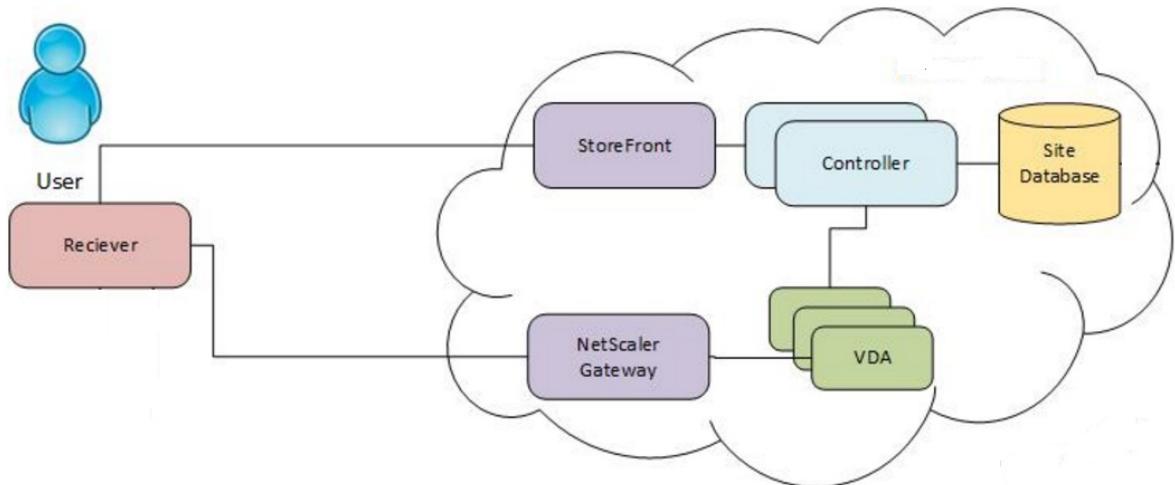
1. [Replicating a virtual machine to Azure](#)
2. How to [design a recovery network](#)
3. [Doing a test failover to Azure](#)
4. [Doing a failover to Azure](#)
5. How to [replicate a domain controller](#)
6. How to [replicate SQL Server](#)

## Deployment patterns

A Citrix XenApp and XenDesktop farm typically have the following deployment pattern:

### **Deployment pattern**

Citrix XenApp and XenDesktop deployment with AD DNS server, SQL database server, Citrix Delivery Controller, StoreFront server, XenApp Master (VDA), Citrix XenApp License Server



## Site Recovery support

For the purpose of this article, Citrix deployments on VMware virtual machines managed by vSphere 6.0 / System Center VMM 2012 R2 were used to setup DR.

### Source and target

SCENARIO	TO A SECONDARY SITE	TO AZURE
<b>Hyper-V</b>	Not in scope	Yes
<b>VMware</b>	Not in scope	Yes
<b>Physical server</b>	Not in scope	Yes

### Versions

Customers can deploy XenApp components as Virtual Machines running on Hyper-V or VMware or as Physical Servers. Azure Site Recovery can protect both physical and virtual deployments to Azure. Since XenApp 7.7 or later is supported in Azure, only deployments with these versions can be failed over to Azure for Disaster Recovery or migration.

### Things to keep in mind

1. Protection and recovery of on-premises deployments using Server OS machines to deliver XenApp published apps and XenApp published desktops is supported.
2. Protection and recovery of on-premises deployments using desktop OS machines to deliver Desktop VDI for client virtual desktops, including Windows 10, is not supported. This is because Site Recovery does not support the recovery of machines with desktop OS'es. Also, some client virtual desktop operating systems (eg. Windows 7) are not yet supported for licensing in Azure. [Learn More](#) about licensing for client/server desktops in Azure.
3. Azure Site Recovery cannot replicate and protect existing on-premises MCS or PVS clones. You need to recreate these clones using Azure RM provisioning from Delivery controller.
4. NetScaler cannot be protected using Azure Site Recovery as NetScaler is based on FreeBSD and Azure Site Recovery does not support protection of FreeBSD OS. You would need to deploy and configure a new NetScaler appliance from Azure Market place after failover to Azure.

## Replicating virtual machines

The following components of the Citrix XenApp deployment need to be protected to enable replication and recovery.

- Protection of AD DNS server
- Protection of SQL database server
- Protection of Citrix Delivery Controller
- Protection of StoreFront server.
- Protection of XenApp Master (VDA)
- Protection of Citrix XenApp License Server

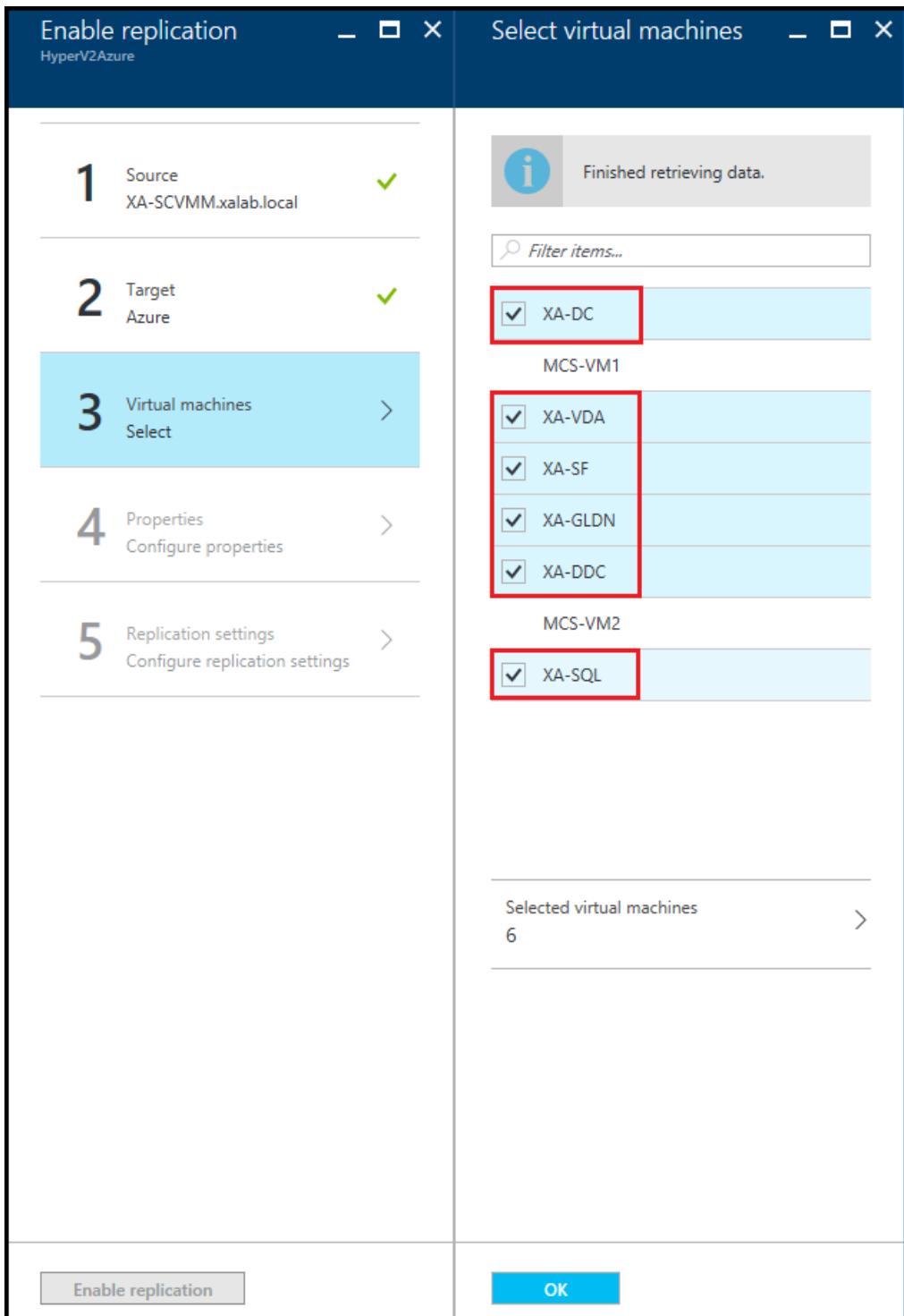
### **AD DNS server replication**

Please refer to [Protect Active Directory and DNS with Azure Site Recovery](#) on guidance for replicating and configuring a domain controller in Azure.

### **SQL database Server replication**

Please refer to [Protect SQL Server with SQL Server disaster recovery and Azure Site Recovery](#) for detailed technical guidance on the recommended options for protecting SQL servers.

Follow [this guidance](#) to start replicating the other component virtual machines to Azure.



## Compute and Network Settings

After the machines are protected (status shows as "Protected" under Replicated Items), the Compute and Network settings need to be configured. In Compute and Network > Compute properties, you can specify the Azure VM name and target size. Modify the name to comply with Azure requirements if you need to. You can also view and add information about the target network, subnet, and IP address that will be assigned to the Azure VM.

Note the following:

- You can set the target IP address. If you don't provide an address, the failed over machine will use DHCP. If you set an address that isn't available at failover, the failover won't work. The same target IP address can be used for test failover if the address is available in the test failover network.
- For the AD/DNS server, retaining the on-premises address lets you specify the same address as the DNS server for the Azure Virtual network.

The number of network adapters is dictated by the size you specify for the target virtual machine, as follows:

- If the number of network adapters on the source machine is less than or equal to the number of adapters allowed for the target machine size, then the target will have the same number of adapters as the source.
- If the number of adapters for the source virtual machine exceeds the number allowed for the target size then the target size maximum will be used.
- For example, if a source machine has two network adapters and the target machine size supports four, the target machine will have two adapters. If the source machine has two adapters but the supported target size only supports one then the target machine will have only one adapter.
- If the virtual machine has multiple network adapters they will all connect to the same network.
- If the virtual machine has multiple network adapters, then the first one shown in the list becomes the Default network adapter in the Azure virtual machine.

## Creating a recovery plan

After replication is enabled for the XenApp component VMs, the next step is to create a recovery plan. A recovery plan groups together virtual machines with similar requirements for failover and recovery.

### Steps to create a recovery plan

1. Add the XenApp component virtual machines in the Recovery Plan.
2. Click Recovery Plans -> + Recovery Plan. Provide an intuitive name for the recovery plan.
3. For VMware virtual machines: Select source as VMware process server, target as Microsoft Azure, and deployment model as Resource Manager and click on Select items.
4. For Hyper-V virtual machines: Select source as VMM server, target as Microsoft Azure, and deployment model as Resource Manager and click on Select items and then select the XenApp deployment VMs.

### Adding virtual machines to failover groups

Recovery plans can be customized to add failover groups for specific startup order, scripts or manual actions. The following groups need to be added to the recovery plan.

1. Failover Group1: AD DNS
2. Failover Group2: SQL Server VMs
3. Failover Group3: VDA Master Image VM
4. Failover Group4: Delivery Controller and StoreFront server VMs

### Adding scripts to the recovery plan

Scripts can be run before or after a specific group in a recovery plan. Manual actions can also be included and performed during failover.

The customized recovery plan looks like the below:

1. Failover Group1: AD DNS
2. Failover Group2: SQL Server VMs
3. Failover Group3: VDA Master Image VM

#### NOTE

Steps 4, 6 and 7 containing manual or script actions are applicable to only an on-premises XenApp > environment with MCS/PVS catalogs.

4. Group 3 Manual or script action: Shut down master VDA VM. The Master VDA VM when failed over to Azure will be in a running state. To create new MCS catalogs using Azure hosting, the master VDA VM is required to be in Stopped (de allocated) state. Shutdown the VM from Azure portal.

5. Failover Group4: Delivery Controller and StoreFront server VMs

6. Group3 manual or script action 1:

#### Add Azure RM host connection

Create Azure host connection in Delivery Controller machine to provision new MCS catalogs in Azure. Follow the steps as explained in this [article](#).

7. Group3 manual or script action 2:

#### Re-create MCS Catalogs in Azure

The existing MCS or PVS clones on the primary site will not be replicated to Azure. You need to recreate these clones using the replicated master VDA and Azure provisioning from Delivery controller. Follow the steps as explained in this [article](#) to create MCS catalogs in Azure.

The screenshot shows the VMWare2Azure Recovery plan interface. At the top, there's a toolbar with 'VMWare2Azure' logo, 'Recovery plan' dropdown, and buttons for '+ Group' (highlighted with a red box), 'Save', 'Discard', and 'Change group'. Below the toolbar, a message box says 'This recovery plan contains 5 machine(s.)' with an info icon. The main area is a table with two columns: 'STAGE NAME' and 'DETAILS'. The stages listed are:

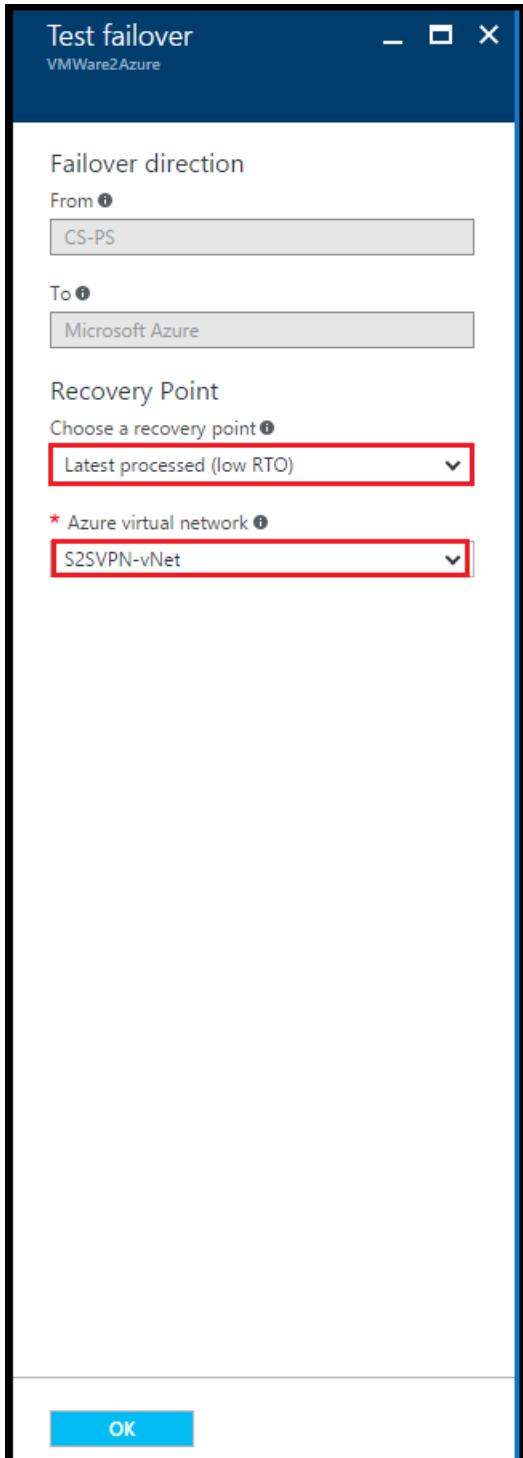
STAGE NAME	DETAILS
All groups shutdown	5 machines in 3 groups.
▶ All groups failover	...
▼ Group 1: Start	2 Machines
CX-DC	Machine
CX-SQL	Machine
▼ Group 2: Start	1 Machine
VDA-TEMP	Machine
▼ Group 2: Post-steps	1 Step
Manual: Turn off the master VDA fr...	Manual action
▼ Group 3: Start	2 Machines
CX-DDC	Machine
CX-SF01	Machine
▼ Group 3: Post-steps	2 Steps
Manual: Add Azure ARM Host conn...	Manual action
Manual: Re-create all MCS Catalogs	Manual action

#### NOTE

You can use scripts at [location](#) to update the DNS with the new IPs of the failed over >virtual machines or to attach a load balancer on the failed over virtual machine, if needed.

## Doing a test failover

Follow [this guidance](#) to do a test failover.



## Doing a failover

Follow [this guidance](#) when you are doing a failover.

## Next steps

You can [learn more](#) about replicating Citrix XenApp and XenDesktop deployments in this white paper. Look at the guidance to [replicate other applications](#) using Site Recovery.

# About disaster recovery for on-premises apps

10/10/2019 • 8 minutes to read • [Edit Online](#)

This article describes on-premises workloads and apps you can protect for disaster recovery with the [Azure Site Recovery](#) service.

## Overview

Organizations need a business continuity and disaster recovery (BCDR) strategy to keep workloads and data safe and available during planned and unplanned downtime, and recover to regular working conditions as soon as possible.

Site Recovery is an Azure service that contributes to your BCDR strategy. Using Site Recovery, you can deploy application-aware replication to the cloud, or to a secondary site. Whether your apps are Windows or Linux-based, running on physical servers, VMware or Hyper-V, you can use Site Recovery to orchestrate replication, perform disaster recovery testing, and run failovers and failback.

Site Recovery integrates with Microsoft applications, including SharePoint, Exchange, Dynamics, SQL Server, and Active Directory. Microsoft also works closely with leading vendors including Oracle, SAP, and Red Hat. You can customize replication solutions on an app-by-app basis.

## Why use Site Recovery for application replication?

Site Recovery contributes to application-level protection and recovery as follows:

- App-agnostic, providing replication for any workloads running on a supported machine.
- Near-synchronous replication, with RPOs as low as 30 seconds to meet the needs of most critical business apps.
- App-consistent snapshots, for single or multi-tier applications.
- Integration with SQL Server AlwaysOn, and partnership with other application-level replication technologies, including AD replication, SQL AlwaysOn, Exchange Database Availability Groups (DAGs).
- Flexible recovery plans, that enable you to recover an entire application stack with a single click, and to include external scripts and manual actions in the plan.
- Advanced network management in Site Recovery and Azure to simplify app network requirements, including the ability to reserve IP addresses, configure load-balancing, and integration with Azure Traffic Manager, for low RTO network switchovers.
- A rich automation library that provides production-ready, application-specific scripts that can be downloaded and integrated with recovery plans.

## Workload summary

Site Recovery can replicate any app running on a supported machine. In addition, we've partnered with product teams to carry out additional testing for the apps specified in the table.

WORKLOAD	REPLICATE AZURE VMS TO AZURE	REPLICATE HYPER-V VMS TO A SECONDARY SITE	REPLICATE HYPER-V VMS TO AZURE	REPLICATE VMWARE VMS TO A SECONDARY SITE	REPLICATE VMWARE VMS TO AZURE
Active Directory, DNS	Y	Y	Y	Y	Y

WORKLOAD	REPLICATE AZURE VMS TO AZURE	REPLICATE HYPER-V VMS TO A SECONDARY SITE	REPLICATE HYPER-V VMS TO AZURE	REPLICATE VMWARE VMS TO A SECONDARY SITE	REPLICATE VMWARE VMS TO AZURE
----------	------------------------------	-------------------------------------------	--------------------------------	------------------------------------------	-------------------------------

Web apps (IIS, SQL)	Y	Y	Y	Y	Y
System Center Operations Manager	Y	Y	Y	Y	Y
SharePoint	Y	Y	Y	Y	Y
SAP Replicate SAP site to Azure for non-cluster	Y (tested by Microsoft)				
Exchange (non-DAG)	Y	Y	Y	Y	Y
Remote Desktop/VDI	Y	Y	Y	Y	Y
Linux (operating system and apps)	Y (tested by Microsoft)				
Dynamics AX	Y	Y	Y	Y	Y
Windows File Server	Y	Y	Y	Y	Y
Citrix XenApp and XenDesktop	Y	N/A	Y	N/A	Y

## Replicate Active Directory and DNS

An Active Directory and DNS infrastructure are essential to most enterprise apps. During disaster recovery, you'll need to protect and recover these infrastructure components, before recovering your workloads and apps.

You can use Site Recovery to create a complete automated disaster recovery plan for Active Directory and DNS. For example, if you want to fail over SharePoint and SAP from a primary to a secondary site, you can set up a recovery plan that fails over Active Directory first, and then an additional app-specific recovery plan to fail over the other apps that rely on Active Directory.

[Learn more](#) about protecting Active Directory and DNS.

## Protect SQL Server

SQL Server provides a data services foundation for data services for many business apps in an on-premises data center. Site Recovery can be used together with SQL Server HA/DR technologies, to protect multi-tiered

enterprise apps that use SQL Server. Site Recovery provides:

- A simple and cost-effective disaster recovery solution for SQL Server. Replicate multiple versions and editions of SQL Server standalone servers and clusters, to Azure or to a secondary site.
- Integration with SQL AlwaysOn Availability Groups, to manage failover and failback with Azure Site Recovery recovery plans.
- End-to-end recovery plans for all tiers in an application, including the SQL Server databases.
- Scaling of SQL Server for peak loads with Site Recovery, by “bursting” them into larger IaaS virtual machine sizes in Azure.
- Easy testing of SQL Server disaster recovery. You can run test failovers to analyze data and run compliance checks, without impacting your production environment.

[Learn more](#) about protecting SQL server.

## Protect SharePoint

Azure Site Recovery helps protect SharePoint deployments, as follows:

- Eliminates the need and associated infrastructure costs for a stand-by farm for disaster recovery. Use Site Recovery to replicate an entire farm (Web, app and database tiers) to Azure or to a secondary site.
- Simplifies application deployment and management. Updates deployed to the primary site are automatically replicated, and are thus available after failover and recovery of a farm in a secondary site. Also lowers the management complexity and costs associated with keeping a stand-by farm up-to-date.
- Simplifies SharePoint application development and testing by creating a production-like copy on-demand replica environment for testing and debugging.
- Simplifies transition to the cloud by using Site Recovery to migrate SharePoint deployments to Azure.

[Learn more](#) about protecting SharePoint.

## Protect Dynamics AX

Azure Site Recovery helps protect your Dynamics AX ERP solution, by:

- Orchestrating replication of your entire Dynamics AX environment (Web and AOS tiers, database tiers, SharePoint) to Azure, or to a secondary site.
- Simplifying migration of Dynamics AX deployments to the cloud (Azure).
- Simplifying Dynamics AX application development and testing by creating a production-like copy on-demand, for testing and debugging.

[Learn more](#) about protecting Dynamic AX.

## Protect RDS

Remote Desktop Services (RDS) enables virtual desktop infrastructure (VDI), session-based desktops, and applications, allowing users to work anywhere. With Azure Site Recovery you can:

- Replicate managed or unmanaged pooled virtual desktops to a secondary site, and remote applications and sessions to a secondary site or Azure.
- Here's what you can replicate:

RDS	REPLICATE AZURE VMs TO AZURE	REPLICATE HYPER-V VMs TO A SECONDARY SITE	REPLICATE HYPER-V VMs TO AZURE	REPLICATE VMWARE VMs TO A SECONDARY SITE	REPLICATE VMWARE VMs TO AZURE	REPLICATE PHYSICAL SERVERS TO A SECONDARY SITE	REPLICATE PHYSICAL SERVERS TO AZURE
<b>Pooled Virtual Desktop (unmanaged)</b>	No	Yes	No	Yes	No	Yes	No
<b>Pooled Virtual Desktop (managed and without UPD)</b>	No	Yes	No	Yes	No	Yes	No
<b>Remote applications and Desktop sessions (without UPD)</b>	Yes	Yes	Yes	Yes	Yes	Yes	Yes

[Set up disaster recovery for RDS using Azure Site Recovery.](#)

[Learn more](#) about protecting RDS.

## Protect Exchange

Site Recovery helps protect Exchange, as follows:

- For small Exchange deployments, such as a single or standalone server, Site Recovery can replicate and fail over to Azure or to a secondary site.
- For larger deployments, Site Recovery integrates with Exchange DAGs.
- Exchange DAGs are the recommended solution for Exchange disaster recovery in an enterprise. Site Recovery recovery plans can include DAGs, to orchestrate DAG failover across sites.

[Learn more](#) about protecting Exchange.

## Protect SAP

Use Site Recovery to protect your SAP deployment, as follows:

- Enable protection of SAP NetWeaver and non-NetWeaver Production applications running on-premises, by replicating components to Azure.
- Enable protection of SAP NetWeaver and non-NetWeaver Production applications running Azure, by replicating components to another Azure datacenter.
- Simplify cloud migration, by using Site Recovery to migrate your SAP deployment to Azure.
- Simplify SAP project upgrades, testing, and prototyping, by creating a production clone on-demand for testing SAP applications.

[Learn more](#) about protecting SAP.

## Protect IIS

Use Site Recovery to protect your IIS deployment, as follows:

Azure Site Recovery provides disaster recovery by replicating the critical components in your environment to a cold remote site or a public cloud like Microsoft Azure. Since the virtual machines with the web server and the database are being replicated to the recovery site, there is no requirement to backup configuration files or certificates separately. The application mappings and bindings dependent on environment variables that are changed post failover can be updated through scripts integrated into the disaster recovery plans. Virtual machines are brought up on the recovery site only in the event of a failover. Not only this, Azure Site Recovery also helps you orchestrate the end to end failover by providing you the following capabilities:

- Sequencing the shutdown and startup of virtual machines in the various tiers.
- Adding scripts to allow update of application dependencies and bindings on the virtual machines after they have been started up. The scripts can also be used to update the DNS server to point to the recovery site.
- Allocate IP addresses to virtual machines pre-failover by mapping the primary and recovery networks and hence use scripts that do not need to be updated post failover.
- Ability for a one-click failover for multiple web applications on the web servers, thus eliminating the scope for confusion in the event of a disaster.
- Ability to test the recovery plans in an isolated environment for DR drills.

[Learn more](#) about protecting IIS web farm.

## Protect Citrix XenApp and XenDesktop

Use Site Recovery to protect your Citrix XenApp and XenDesktop deployments, as follows:

- Enable protection of the Citrix XenApp and XenDesktop deployment, by replicating different deployment layers including (AD DNS server, SQL database server, Citrix Delivery Controller, StoreFront server, XenApp Master (VDA), Citrix XenApp License Server) to Azure.
- Simplify cloud migration, by using Site Recovery to migrate your Citrix XenApp and XenDesktop deployment to Azure.
- Simplify Citrix XenApp/XenDesktop testing, by creating a production-like copy on-demand for testing and debugging.
- This solution is only applicable for Windows Server operating system virtual desktops and not client virtual desktops as client virtual desktops are not yet supported for licensing in Azure. [Learn More](#) about licensing for client/server desktops in Azure.

[Learn more](#) about protecting Citrix XenApp and XenDesktop deployments. Alternatively, you can refer the [whitepaper from Citrix](#) detailing the same.

## Next steps

[Get started](#) with Azure VM replication.

# Set up disaster recovery of on-premises VMware virtual machines or physical servers to a secondary site

11/5/2019 • 17 minutes to read • [Edit Online](#)

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.

## End-of-support announcement

The Azure Site Recovery scenario for replication between on-premises VMware or physical datacenters is reaching end-of-support.

- From August 2018, the scenario can't be configured in the Recovery Services vault, and the InMage Scout software can't be downloaded from the vault. Existing deployments will be supported.
- From December 31 2020, the scenario won't be supported.
- Existing partners can onboard new customers to the scenario until support ends.

During 2018 and 2019, two updates will be released:

- Update 7: Fixes network configuration and compliance issues, and provides TLS 1.2 support.
- Update 8: Adds support for Linux operating systems RHEL/CentOS 7.3/7.4/7.5, and for SUSE 12

After Update 8, no further updates will be released. There will be limited hotfix support for the operating systems added in Update 8, and bug fixes based on best effort.

Azure Site Recovery continues to innovate by providing VMware and Hyper-V customers a seamless and best-in-class DRaaS solution with Azure as a disaster recovery site. Microsoft recommends that existing InMage / ASR Scout customers consider using Azure Site Recovery's VMware to Azure scenario for their business continuity needs. Azure Site Recovery's VMware to Azure scenario is an enterprise-class DR solution for VMware applications, which offers RPO and RTO of minutes, support for multi-VM application replication and recovery, seamless onboarding, comprehensive monitoring, and significant TCO advantage.

## Scenario migration

As an alternative, we recommend setting up disaster recovery for on-premises VMware VMs and physical machines by replicating them to Azure. Do this as follows:

1. Review the quick comparison below. Before you can replicate on-premises machines, you need check that they meet [requirements](#) for replication to Azure. If you're replicating VMware VMs, we recommend that you review [capacity planning guidelines](#), and run the [Deployment Planner tool](#) to identity capacity requirements, and verify compliance.
2. After running the Deployment Planner, you can set up replication:
  - o For VMware VMs, follow these tutorials to [prepare Azure](#), [prepare your on-premises VMware environment](#), and [set up disaster recovery](#).
  - o For physical machines, follow this [tutorial](#).
3. After machines are replicating to Azure, you can run a [disaster recovery drill](#) to make sure everything's working as expected.

## Quick comparison

FEATURE	REPLICATION TO AZURE	REPLICATION BETWEEN VMWARE DATACENTERS
<b>Required components</b>	Mobility service on replicated machines. On-premises configuration server, process server, master target server. Temporary process server in Azure for failback.	Mobility service, Process Server, Configuration Server and Master Target
<b>Configuration and orchestration</b>	Recovery Services vault in the Azure portal	Using vContinuum
<b>Replicated</b>	Disk (Windows and Linux)	Volume-Windows Disk-Linux
<b>Shared disk cluster</b>	Not supported	Supported
<b>Data churn limits (average)</b>	10 MB/s data per disk 25MB/s data per VM <a href="#">Learn more</a>	> 10 MB/s data per disk > 25 MB/s data per VM
<b>Monitoring</b>	From Azure portal	From CX (Configuration Server)
<b>Support Matrix</b>	<a href="#">Click here for details</a>	<a href="#">Download ASR Scout compatible matrix</a>

## Prerequisites

To complete this tutorial:

- [Review](#) the support requirements for all components.
- Make sure that the machines you want to replicate comply with [replicated machine support](#).

## Download and install component updates

Review and install the latest [updates](#). Updates should be installed on servers in the following order:

1. RX server (if applicable)
2. Configuration servers
3. Process servers
4. Master Target servers
5. vContinuum servers
6. Source server (both Windows and Linux Servers)

Install the updates as follows:

### NOTE

All Scout components' file update version may not be the same in the update .zip file. The older version indicate that there is no change in the component since previous update to this update.

Download the [update](#) .zip file and the [MySQL and PHP upgrade](#) configuration files. The update .zip file contains the all the base binaries and cumulative upgrade binaries of the following components:

- InMage\_ScoutCloud\_RX\_8.0.1.0\_RHEL6-64\_GA\_02Mar2015.tar.gz
- RX\_8.0.7.0\_GA\_Update\_7\_2965621\_28Dec18.tar.gz

- InMage\_CX\_8.0.1.0\_Windows\_GA\_26Feb2015\_release.exe
  - InMage\_CX\_TP\_8.0.1.0\_Windows\_GA\_26Feb2015\_release.exe
  - CX\_Windows\_8.0.7.0\_GA\_Update\_7\_2965621\_28Dec18.exe
  - InMage\_PI\_8.0.1.0\_Windows\_GA\_26Feb2015\_release.exe
  - InMage\_Scout\_vContinuum\_MT\_8.0.7.0\_Windows\_GA\_27Dec2018\_release.exe
  - InMage\_UA\_8.0.7.0\_Windows\_GA\_27Dec2018\_release.exe
  - InMage\_UA\_8.0.7.0\_OL5-32\_GA\_03Dec2018\_release.tar.gz
  - InMage\_UA\_8.0.7.0\_OL5-64\_GA\_03Dec2018\_release.tar.gz
  - InMage\_UA\_8.0.7.0\_OL6-32\_GA\_03Dec2018\_release.tar.gz
  - InMage\_UA\_8.0.7.0\_OL6-64\_GA\_03Dec2018\_release.tar.gz
  - InMage\_UA\_8.0.7.0\_RHEL5-32\_GA\_03Dec2018\_release.tar.gz
  - InMage\_UA\_8.0.7.0\_RHEL5-64\_GA\_03Dec2018\_release.tar.gz
  - InMage\_UA\_8.0.7.0\_RHEL6-32\_GA\_03Dec2018\_release.tar.gz
  - InMage\_UA\_8.0.7.0\_RHEL6-64\_GA\_03Dec2018\_release.tar.gz
  - InMage\_UA\_8.0.7.0\_RHEL7-64\_GA\_03Dec2018\_release.tar.gz
  - InMage\_UA\_8.0.7.0\_SLES10-32\_GA\_03Dec2018\_release.tar.gz
  - InMage\_UA\_8.0.7.0\_SLES10-64\_GA\_03Dec2018\_release.tar.gz
  - InMage\_UA\_8.0.7.0\_SLES10-SP1-32\_GA\_03Dec2018\_release.tar.gz
  - InMage\_UA\_8.0.7.0\_SLES10-SP1-64\_GA\_03Dec2018\_release.tar.gz
  - InMage\_UA\_8.0.7.0\_SLES10-SP2-32\_GA\_03Dec2018\_release.tar.gz
  - InMage\_UA\_8.0.7.0\_SLES10-SP2-64\_GA\_03Dec2018\_release.tar.gz
  - InMage\_UA\_8.0.7.0\_SLES10-SP3-32\_GA\_03Dec2018\_release.tar.gz
  - InMage\_UA\_8.0.7.0\_SLES10-SP3-64\_GA\_03Dec2018\_release.tar.gz
  - InMage\_UA\_8.0.7.0\_SLES10-SP4-32\_GA\_03Dec2018\_release.tar.gz
  - InMage\_UA\_8.0.7.0\_SLES10-SP4-64\_GA\_03Dec2018\_release.tar.gz
  - InMage\_UA\_8.0.7.0\_SLES11-32\_GA\_03Dec2018\_release.tar.gz
  - InMage\_UA\_8.0.7.0\_SLES11-64\_GA\_04Dec2018\_release.tar.gz
  - InMage\_UA\_8.0.7.0\_SLES11-SP1-32\_GA\_03Dec2018\_release.tar.gz
  - InMage\_UA\_8.0.7.0\_SLES11-SP1-64\_GA\_04Dec2018\_release.tar.gz
  - InMage\_UA\_8.0.7.0\_SLES11-SP2-32\_GA\_03Dec2018\_release.tar.gz
  - InMage\_UA\_8.0.7.0\_SLES11-SP2-64\_GA\_03Dec2018\_release.tar.gz
  - InMage\_UA\_8.0.7.0\_SLES11-SP3-32\_GA\_03Dec2018\_release.tar.gz
  - InMage\_UA\_8.0.7.0\_SLES11-SP3-64\_GA\_03Dec2018\_release.tar.gz
  - InMage\_UA\_8.0.7.0\_SLES11-SP4-64\_GA\_03Dec2018\_release.tar.gz
1. Extract the .zip files.
  2. **RX server:** Copy **RX\_8.0.7.0\_GA\_Update\_7\_2965621\_28Dec18.tar.gz** to the RX server, and extract it.  
In the extracted folder, run **/Install**.
  3. **Configuration server and process server:** Copy  
**CX\_Windows\_8.0.7.0\_GA\_Update\_7\_2965621\_28Dec18.exe** to the configuration server and process server. Double-click to run it.
  4. **Windows Master Target server:** To update the unified agent, copy  
**InMage\_UA\_8.0.7.0\_Windows\_GA\_27Dec2018\_release.exe** to the server. Double-click it to run it.  
The same file can also be used for fresh installation. The same unified agent update is also applicable for the source server. The update does not need to apply on the Master target prepared with  
**InMage\_Scout\_vContinuum\_MT\_8.0.7.0\_Windows\_GA\_27Dec2018\_release.exe** as this is new GA installer with all the latest changes.
  5. **vContinuum server:** Copy

**InMage\_Scout\_vContinuum\_MT\_8.0.7.0\_Windows\_GA\_27Dec2018\_release.exe** to the server.

Make sure that you've closed the vContinuum wizard. Double-click on the file to run it.

6. **Linux master target server:** To update the unified agent, copy **InMage\_UA\_8.0.7.0\_RHEL6-64\_GA\_03Dec2018\_release.tar.gz** to the Linux Master Target server and extract it. In the extracted folder, run **/Install**.
7. **Windows source server:** To update the unified agent, copy **InMage\_UA\_8.0.7.0\_Windows\_GA\_27Dec2018\_release.exe** to the source server. Double-click on the file to run it.
8. **Linux source server:** To update the unified agent, copy the corresponding version of the unified agent file to the Linux server, and extract it. In the extracted folder, run **/Install**. Example: For RHEL 6.7 64-bit server, copy **InMage\_UA\_8.0.7.0\_RHEL6-64\_GA\_03Dec2018\_release.tar.gz** to the server, and extract it. In the extracted folder, run **/Install**.
9. After upgrading Configuration Server, Process Server and RX server with the above mentioned installers, the PHP and MySQL libraries needs to be upgraded manually with steps mentioned in section 7.4 of the [quick installation guide](#).

## Enable replication

1. Set up replication between the source and target VMware sites.
2. Refer to following documents to learn more about installation, protection, and recovery:
  - [Release notes](#)
  - [Compatibility matrix](#)
  - [User guide](#)
  - [RX user guide](#)
  - [Quick installation guide](#)
  - [Upgrading MYSQL and PHP libraries](#)

## Updates

### Site Recovery Scout 8.0.1 Update 7

Updated: December 31, 2018 Download [Scout update 7](#). Scout Update 7 is a full installer which can be used for fresh installation as well as to upgrade existing agents/MT which are on previous updates (from Update 1 to Update 6). It contains all fixes from Update 1 to Update 6 plus the new fixes and enhancements described below.

#### New features

- PCI compliance
- TLS v1.2 Support

#### Bug and Security Fixes

- Fixed: Windows Cluster/Standalone Machines have incorrect IP configuration upon recovery/DR-Drill.
- Fixed: Sometimes Add disk operation fails for V2V cluster.
- Fixed: vContinuum Wizard gets stuck during recovery phase if the Master Target is Windows Server 2016
- Fixed: MySQL security issues are mitigated by upgrading MySQL to version 5.7.23

#### Manual Upgrade for PHP and MySQL on CS,PS, and RX

The PHP scripting platform should be upgraded to version 7.2.10 on Configuration Server, Process Server and RX Server. The MySQL database management system should be upgraded to version 5.7.23 on Configuration Server, Process Server and RX Server. Please follow the manual steps given in the [Quick installation guide](#) to upgrade PHP and MySQL versions.

### Site Recovery Scout 8.0.1 Update 6

Updated: October 12, 2017

Download [Scout update 6](#).

Scout Update 6 is a cumulative update. It contains all fixes from Update 1 to Update 5 plus the new fixes and enhancements described below.

#### New platform support

- Support has been added for Source Windows Server 2016
- Support has been added for following Linux operating systems:
  - Red Hat Enterprise Linux (RHEL) 6.9
  - CentOS 6.9
  - Oracle Linux 5.11
  - Oracle Linux 6.8
- Support has been added for VMware Center 6.5

Install the updates as follows:

#### NOTE

All Scout components' file update version may not be the same in the update .zip file. The older version indicate that there is no change in the component since previous update to this update.

Download the [update](#) .zip file. The file contains the following components:

- RX\_8.0.4.0\_GA\_Update\_4\_8725872\_16Sep16.tar.gz
- CX\_Windows\_8.0.6.0\_GA\_Update\_6\_13746667\_18Sep17.exe
- UA\_Windows\_8.0.5.0\_GA\_Update\_5\_11525802\_20Apr17.exe
- UA\_RHEL6-64\_8.0.4.0\_GA\_Update\_4\_9035261\_26Sep16.tar.gz
- vCon\_Windows\_8.0.6.0\_GA\_Update\_6\_11525767\_21Sep17.exe
- UA update4 bits for RHEL5, OL5, OL6, SUSE 10, SUSE 11: UA\_<Linux OS>\_8.0.4.0\_GA\_Update\_4\_9035261\_26Sep16.tar.gz
  - 1. Extract the .zip files.
- 2. **RX server:** Copy **RX\_8.0.4.0\_GA\_Update\_4\_8725872\_16Sep16.tar.gz** to the RX server, and extract it. In the extracted folder, run **/Install**.
- 3. **Configuration server and process server:** Copy **CX\_Windows\_8.0.6.0\_GA\_Update\_6\_13746667\_18Sep17.exe** to the configuration server and process server. Double-click to run it.
- 4. **Windows Master Target server:** To update the unified agent, copy **UA\_Windows\_8.0.5.0\_GA\_Update\_5\_11525802\_20Apr17.exe** to the server. Double-click it to run it. The same unified agent update is also applicable for the source server. If source hasn't been updated to Update 4, you should update the unified agent. The update does not need to apply on the Master target prepared with **InMage\_Scout\_vContinuum\_MT\_8.0.1.0\_Windows\_GA\_10Oct2017\_release.exe** as this is new GA installer with all the latest changes.
- 5. **vContinuum server:** Copy **vCon\_Windows\_8.0.6.0\_GA\_Update\_6\_11525767\_21Sep17.exe** to the server. Make sure that you've closed the vContinuum wizard. Double-click on the file to run it. The update does not need to apply on the Master Target prepared with **InMage\_Scout\_vContinuum\_MT\_8.0.1.0\_Windows\_GA\_10Oct2017\_release.exe** as this is new GA installer with all the latest changes.
- 6. **Linux master target server:** To update the unified agent, copy **UA\_RHEL6-64\_8.0.4.0\_GA\_Update\_4\_9035261\_26Sep16.tar.gz** to the master target server and extract it. In the extracted folder, run **/Install**.

7. **Windows source server:** To update the unified agent, copy **UA\_Windows\_8.0.5.0\_GA\_Update\_5\_11525802\_20Apr17.exe** to the source server. Double-click on the file to run it. You don't need to install the Update 5 agent on the source server if it has already been updated to Update 4 or source agent is installed with latest base installer **InMage\_UA\_8.0.1.0\_Windows\_GA\_28Sep2017\_release.exe**.
8. **Linux source server:** To update the unified agent, copy the corresponding version of the unified agent file to the Linux server, and extract it. In the extracted folder, run **/Install**. Example: For RHEL 6.7 64-bit server, copy **UA\_RHEL6-64\_8.0.4.0\_GA\_Update\_4\_9035261\_26Sep16.tar.gz** to the server, and extract it. In the extracted folder, run **/Install**.

#### **NOTE**

- Base Unified Agent(UA) installer for Windows has been refreshed to support Windows Server 2016. The new installer **InMage\_UA\_8.0.1.0\_Windows\_GA\_28Sep2017\_release.exe** is packaged with the base Scout GA package (**InMage\_Scout\_Standard\_8.0.1\_GA-Oct17.zip**). The same installer will be used for all supported Windows version.
- Base Windows vContinuum & Master Target installer has been refreshed to support Windows Server 2016. The new installer **InMage\_Scout\_vContinuum\_MT\_8.0.1.0\_Windows\_GA\_10Oct2017\_release.exe** is packaged with the base Scout GA package (**InMage\_Scout\_Standard\_8.0.1\_GA-Oct17.zip**). The same installer will be used to deploy Windows 2016 Master Target and Windows 2012R2 Master Target.
- Windows server 2016 on physical server is not supported by ASR Scout. It supports only Windows Server 2016 VMware VM.

#### **Bug fixes and enhancements**

- Fallback protection fails for Linux VM with list of disks to be replicated is empty at the end of config.

#### **Site Recovery Scout 8.0.1 Update 5**

Scout Update 5 is a cumulative update. It contains all fixes from Update 1 to Update 4, and the new fixes described below.

- Fixes from Site Recovery Scout Update 4 to Update 5 are specifically for the master target and vContinuum components.
- If source servers, the master target, configuration, process, and RX servers are already running Update 4, then apply it only on the master target server.

#### **New platform support**

- SUSE Linux Enterprise Server 11 Service Pack 4(SP4)
- SLES 11 SP4 64 bit **InMage\_UA\_8.0.1.0\_SLES11-SP4-64\_GA\_13Apr2017\_release.tar.gz** is packaged with the base Scout GA package (**InMage\_Scout\_Standard\_8.0.1\_GA.zip**). Download the GA package from the portal, as described in create a vault.

#### **Bug fixes and enhancements**

- Fixes for increased Windows cluster support reliability:
  - Fixed- Some of the P2V MSCS cluster disks become RAW after recovery.
  - Fixed- P2V MSCS cluster recovery fails due to a disk order mismatch.
  - Fixed- The MSCS cluster operation to add disks fails with a disk size mismatch error.
  - Fixed- The readiness check for the source MSCS cluster with RDM LUNs mapping fails in size verification.
  - Fixed- Single node cluster protection fails because of a SCSI mismatch issue.
  - Fixed- Re-protection of the P2V Windows cluster server fails if target cluster disks are present.
- Fixed: During fallback protection, if the selected master target server isn't on the same ESXi server as the protected source machine (during forward protection), then vContinuum picks up the wrong master target server during fallback recovery, and the recovery operation fails.

#### **NOTE**

- The P2V cluster fixes are applicable only to physical MSCS clusters that are newly protected with Site Recovery Scout Update 5. To install the cluster fixes on protected P2V MSCS clusters with older updates, follow the upgrade steps mentioned in section 12 of the [Site Recovery Scout Release Notes](#).
- if at the time of re-protection, the same set of disks are active on each of the cluster nodes as they were when initially protected, then re-protection of a physical MSCS cluster can only reuse existing target disks. If not, then use the manual steps in section 12 of [Site Recovery Scout Release Notes](#), to move the target side disks to the correct datastore path, for reuse during re-protection. If you reprotect the MSCS cluster in P2V mode without following the upgrade steps, it creates a new disk on the target ESXi server. You will need to manually delete the old disks from the datastore.
- When a source SLES11 or SLES11 (with any service pack) server is rebooted gracefully, then manually mark the **root** disk replication pairs for re-synchronization. There's no notification in the CX interface. If you don't mark the root disk for resynchronization, you might notice data integrity issues.

## **Azure Site Recovery Scout 8.0.1 Update 4**

Scout Update 4 is a cumulative update. It includes all fixes from Update 1 to Update 3, and the new fixes described below.

#### **New platform support**

- Support has been added for vCenter/vSphere 6.0, 6.1 and 6.2
- Support has been added for these Linux operating systems:
  - Red Hat Enterprise Linux (RHEL) 7.0, 7.1 and 7.2
  - CentOS 7.0, 7.1 and 7.2
  - Red Hat Enterprise Linux (RHEL) 6.8
  - CentOS 6.8

#### **NOTE**

RHEL/CentOS 7 64 bit **InMage\_UA\_8.0.1.0\_RHEL7-64\_GA\_06Oct2016\_release.tar.gz** is packaged with the base Scout GA package **InMage\_Scout\_Standard\_8.0.1 GA.zip**. Download the Scout GA package from the portal as described in create a vault.

#### **Bug fixes and enhancements**

- Improved shutdown handling for the following Linux operating systems and clones, to prevent unwanted resynchronization issues:
  - Red Hat Enterprise Linux (RHEL) 6.x
  - Oracle Linux (OL) 6.x
- For Linux, all folder access permissions in the unified agent installation directory are now restricted to the local user only.
- On Windows, a fix for a timing out issue that occurred when issuing common distributed consistency bookmarks, on heavily loaded distributed applications such as SQL Server and Share Point clusters.
- A log related fix in the configuration server base installer.
- A download link to VMware vCLI 6.0 was added to the Windows master target base installer.
- Additional checks and logs were added, for network configuration changes during failover and disaster recovery drills.
- A fix for an issue that caused retention information not to be reported to the configuration server.
- For physical clusters, a fix for an issue that caused volume resizing to fail in the vContinuum wizard, when shrinking the source volume.
- A fix for a cluster protection issue that failed with error: "Failed to find the disk signature", when the cluster disk is a PRDM disk.

- A fix for a cxps transport server crash, caused by an out-of-range exception.
- Server name and IP address columns are now resizable in the **Push Installation** page of the vContinuum wizard.
- RX API enhancements:
  - The five latest available common consistency points now available (only guaranteed tags).
  - Capacity and free space details are displayed for all protected devices.
  - Scout driver state on the source server is available.

#### **NOTE**

- **InMage\_Scout\_Standard\_8.0.1\_GA.zip** base package has:
  - An updated configuration server base installer (**InMage\_CX\_8.0.1.0\_Windows\_GA\_26Feb2015\_release.exe**)
  - A Windows master target base installer (**InMage\_Scout\_vContinuum\_MT\_8.0.1.0\_Windows\_GA\_26Feb2015\_release.exe**).
  - For all new installations, use the new configuration server and Windows master target GA bits.
- Update 4 can be applied directly on 8.0.1 GA.
- The configuration server and RX updates can't be rolled back after they've been applied.

### **Azure Site Recovery Scout 8.0.1 Update 3**

All Site Recovery updates are cumulative. Update 3 contains all fixes from Update 1 and Update 2. Update 3 can be directly applied on 8.0.1 GA. The configuration server and RX updates can't be rolled back after they've been applied.

#### **Bug fixes and enhancements**

Update 3 fixes the following issues:

- The configuration server and RX aren't registered in the vault when they're behind the proxy.
- The number of hours in which the recovery point objective (RPO) wasn't reached is not updated in the health report.
- The configuration server isn't syncing with RX when the ESX hardware details, or network details, contain any UTF-8 characters.
- Windows Server 2008 R2 domain controllers don't start after recovery.
- Offline synchronization isn't working as expected.
- After VM failover, replication-pair deletion doesn't progress in the configuration server console for a long time. Users can't complete the failback or resume operations.
- Overall snapshot operations by the consistency job have been optimized, to help reduce application disconnects such as SQL Server clients.
- Consistency tool (VACP.exe) performance has been improved. Memory usage required for creating snapshots on Windows has been reduced.
- The push install service crashes when the password is larger than 16 characters.
- vContinuum doesn't check and prompt for new vCenter credentials, when credentials are modified.
- On Linux, the master target cache manager (cachemgr) isn't downloading files from the process server. This results in replication pair throttling.
- When the physical failover cluster (MSCS) disk order isn't the same on all nodes, replication isn't set for some of the cluster volumes. The cluster must be reprotected to take advantage of this fix.
- SMTP functionality isn't working as expected, after RX is upgraded from Scout 7.1 to Scout 8.0.1.
- More statistics have been added in the log for the rollback operation, to track the time taken to complete it.
- Support has been added for Linux operating systems on the source server:
  - Red Hat Enterprise Linux (RHEL) 6 update 7
  - CentOS 6 update 7

- The configuration server and RX consoles now show notifications for the pair, which goes into bitmap mode.
- The following security fixes have been added in RX:
  - Authorization bypass via parameter tampering: Restricted access to non-applicable users.
  - Cross-site request forgery: The page-token concept was implemented, and it generates randomly for every page. This means there's only a single sign-in instance for the same user, and page refresh doesn't work. Instead, it redirects to the dashboard.
  - Malicious file upload: Files are restricted to specific extensions: z, aiff, asf, avi, bmp, csv, doc, docx, fla, flv, gif, gz, gzip, jpeg, jpg, log, mid, mov, mp3, mp4, mpc, mpeg, mpg, ods, odt, pdf, png, ppt, ppx, pxd, qt, ram, rar, rm, rmi, rmvb, rtf, sdc, sitd, swf, sxc, sxw, tar, tgz, tif, tiff, txt, vsd, wav, wma, wmv, xls, xlsx, xml, and zip.
  - Persistent cross-site scripting: Input validations were added.

## Azure Site Recovery Scout 8.0.1 Update 2 (Update 03Dec15)

Fixes in Update 2 include:

- **Configuration server:** Issues that prevented the 31-day free metering feature from working as expected, when the configuration server was registered to Azure Site Recovery vault.
- **Unified agent:** Fix for an issue in Update 1 that resulted in the update not being installed on the master target server, during upgrade from version 8.0 to 8.0.1.

## Azure Site Recovery Scout 8.0.1 Update 1

Update 1 includes the following bug fixes and new features:

- 31 days of free protection per server instance. This enables you to test functionality, or set up a proof-of-concept.
- All operations on the server, including failover and failback, are free for the first 31 days. The time starts when a server is first protected with Site Recovery Scout. From the 32nd day, each protected server is charged at the standard instance rate for Site Recovery protection to a customer-owned site.
- At any time, the number of protected servers currently being charged is available on the **Dashboard** in the vault.
- Support was added for vSphere Command-Line Interface (vCLI) 5.5 Update 2.
- Support was added for these Linux operating systems on the source server:
  - RHEL 6 Update 6
  - RHEL 5 Update 11
  - CentOS 6 Update 6
  - CentOS 5 Update 11
- Bug fixes to address the following issues:
  - Vault registration fails for the configuration server, or RX server.
  - Cluster volumes don't appear as expected when clustered VMs are reprotected as they resume.
  - Failback fails when the master target server is hosted on a different ESXi server from the on-premises production VMs.
  - Configuration file permissions are changed when you upgrade to 8.0.1. This change affects protection and operations.
  - The resynchronization threshold isn't enforced as expected, causing inconsistent replication behavior.
  - The RPO settings don't appear correctly in the configuration server console. The uncompressed data value incorrectly shows the compressed value.
  - The Remove operation doesn't delete as expected in the vContinuum wizard, and replication isn't deleted from the configuration server console.
  - In the vContinuum wizard, the disk is automatically unselected when you click **Details** in the disk view, during protection of MSCS VMs.
  - In the physical-to-virtual (P2V) scenario, required HP services (such as CIMnotify and CqMgHost) aren't

moved to manual in VM recovery. This issue results in additional boot time.

- o Linux VM protection fails when there are more than 26 disks on the master target server.

# Deprecation of disaster recovery between customer-managed sites (with VMM) using Azure Site Recovery

2/27/2020 • 2 minutes to read • [Edit Online](#)

This article describes the upcoming deprecation plan, the corresponding implications, and the alternative options available for the customers for the following scenario:

DR between customer owned sites managed by System Center Virtual Machine Manager (SCVMM) using Site Recovery

## IMPORTANT

Customers are advised to take the remediation steps at the earliest to avoid any disruption to their environment.

## What changes should you expect?

- Starting March 2020,you will receive Azure portal notifications & email communications with the upcoming deprecation of site-to-site replication of Hyper-V VMs. The deprecation is planned for March 2023.
- If you have an existing configuration, there will be no impact to the set up.
- Once the scenarios are deprecated unless the customer follows the alternate approaches, the existing replications may get disrupted. Customers won't be able to view, manage, or performs any DR-related operations via the Azure Site Recovery experience in Azure portal.

## Alternatives

Below are the alternatives that the customer can choose from to ensure that their DR strategy is not impacted once the scenario is deprecated.

- Option 1 (Recommended): Choose to [start using Azure as the DR target](#).
- Option 2: Choose to continue with site-to-site replication using the underlying [Hyper-V Replica solution](#), but you will be unable to manage DR configurations using Azure Site Recovery in the Azure portal.

## Remediation steps

If you are choosing to go with Option 1, please execute the following steps:

1. [Disable protection of all the virtual machines associated with the VMMs](#). Use the **Disable replication and remove** option or run the scripts mentioned to ensure the replication settings on-premises are cleaned up.
2. [Unregister all the VMM servers](#) from the site-to-site replication configuration.
3. [Prepare Azure resources](#) for enabling replication of your VMs.
4. [Prepare on-premises Hyper-V servers](#)
5. [Set up replication for the VMs in the VMM cloud](#)
6. Optional but recommended: [Run a DR drill](#)

If you are choosing to go with Option 2 of using Hyper-V replica, execute the following steps:

1. In **Protected Items > Replicated Items**, right-click the machine > **Disable replication**.

2. In **Disable replication**, select **Remove**.

This removes the replicated item from Azure Site Recovery (billing is stopped). Replication configuration on the on-premises virtual machine **will not** be cleaned up.

## Next steps

Plan for the deprecation and choose an alternate option that's best suited for your infrastructure and business. In case you have any queries regarding this, reach out to Microsoft Support

# Set up disaster recovery for Hyper-V VMs to a secondary on-premises site

11/15/2019 • 7 minutes to read • [Edit Online](#)

The [Azure Site Recovery](#) service contributes to your disaster recovery strategy by managing and orchestrating replication, failover, and fallback of on-premises machines, and Azure virtual machines (VMs).

This article shows you how to set up disaster recovery to a secondary site, for on-premises Hyper-V VMs managed in System Center Virtual Machine Manager (VMM) clouds. In this article, you learn how to:

- Prepare on-premises VMM servers and Hyper-V hosts
- Create a Recovery Services vault for Site Recovery
- Set up the source and target replication environments.
- Set up network mapping
- Create a replication policy
- Enable replication for a VM

## Prerequisites

To complete this scenario:

- Review the [scenario architecture and components](#).
- Make sure that VMM servers and Hyper-V hosts comply with [support requirements](#).
- Check that VMs you want to replicate comply with [replicated machine support](#).
- Prepare VMM servers for network mapping.

### Prepare for network mapping

[Network mapping](#) maps between on-premises VMM VM networks in source and target clouds. Mapping does the following:

- Connects VMs to appropriate target VM networks after failover.
- Optimally places replica VMs on target Hyper-V host servers.
- If you don't configure network mapping, replica VMs won't be connected to a VM network after failover.

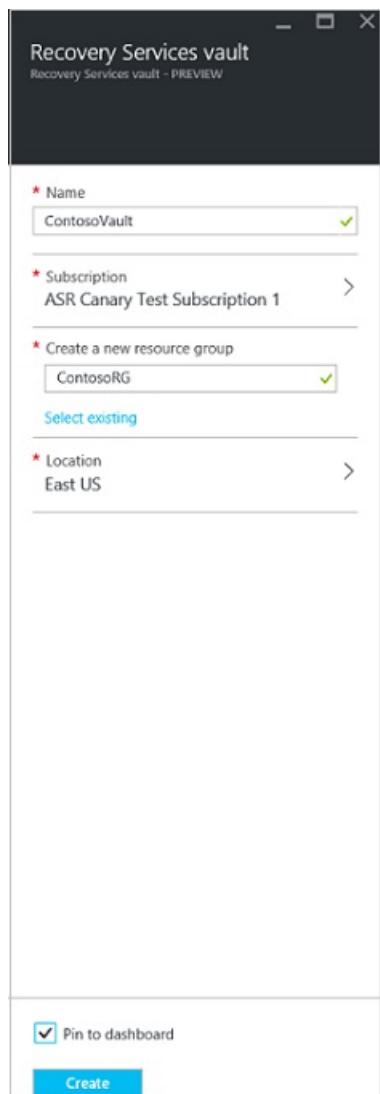
Prepare VMM as follows:

1. Make sure you have [VMM logical networks](#) on the source and target VMM servers.
  - The logical network on the source server should be associated with the source cloud in which Hyper-V hosts are located.
  - The logical network on the target server should be associated with the target cloud.
2. Make sure you have [VM networks](#) on the source and target VMM servers. VM networks should be linked to the logical network in each location.
3. Connect VMs on the source Hyper-V hosts to the source VM network.

## Create a Recovery Services vault

1. Sign in to the [Azure portal](#) > **Recovery Services**.
2. Click **Create a resource** > **Monitoring + Management** > **Backup and Site Recovery**.

3. In **Name**, specify a friendly name to identify the vault. If you have more than one subscription, select the appropriate one.
4. [Create a resource group](#), or select an existing one. Specify an Azure region.
5. To quickly access the vault from the dashboard, click **Pin to dashboard > Create**.



The new vault will appear on the **Dashboard > All resources**, and on the main **Recovery Services vaults** page.

## Choose a protection goal

Select what you want to replicate and where you want to replicate to.

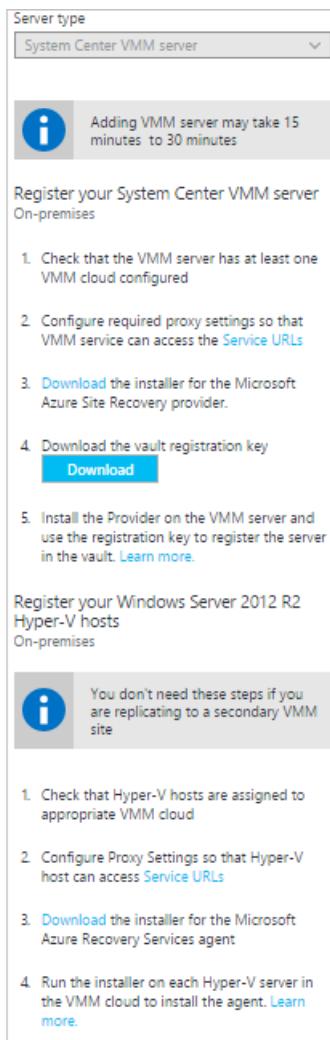
1. Click **Site Recovery > Step 1: Prepare Infrastructure > Protection goal**.
2. Select **To recovery site**, and select **Yes, with Hyper-V**.
3. Select **Yes** to indicate you're using VMM to manage the Hyper-V hosts.
4. Select **Yes** if you have a secondary VMM server. If you're deploying replication between clouds on a single VMM server, click **No**. Then click **OK**.

## Set up the source environment

Install the Azure Site Recovery Provider on VMM servers, and discover and register servers in the vault.

1. Click **Prepare Infrastructure > Source**.
2. In **Prepare source**, click **+ VMM** to add a VMM server.

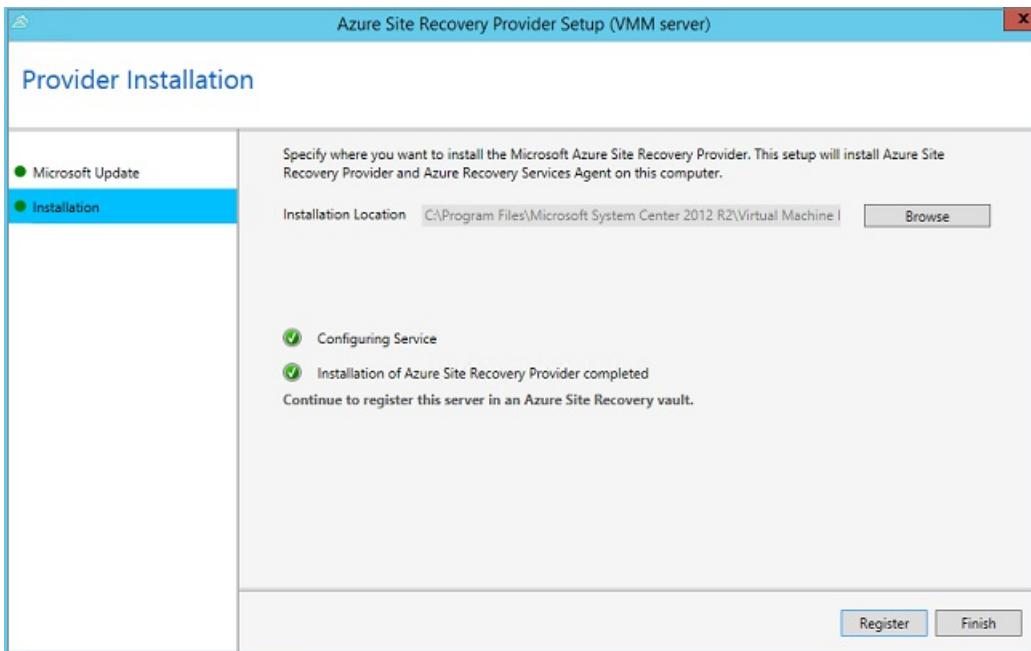
3. In **Add Server**, check that **System Center VMM server** appears in **Server type**.
4. Download the Azure Site Recovery Provider installation file.
5. Download the registration key. You need this when you install the Provider. The key is valid for five days after you generate it.



6. Install the Provider on each VMM server. You don't need to explicitly install anything on Hyper-V hosts.

### Install the Azure Site Recovery Provider

1. Run the Provider setup file on each VMM server. If VMM is deployed in a cluster, install for the first time as follows:
  - Install the Provider on an active node, and finish the installation to register the VMM server in the vault.
  - Then, install the Provider on the other nodes. Cluster nodes should all run the same version of the Provider.
2. Setup runs a few prerequisite checks, and requests permission to stop the VMM service. The VMM service will be restarted automatically when setup finishes. If you install on a VMM cluster, you're prompted to stop the Cluster role.
3. In **Microsoft Update**, you can opt in to specify that provider updates are installed in accordance with your Microsoft Update policy.
4. In **Installation**, accept or modify the default installation location, and click **Install**.
5. After installation is complete, click **Register** to register the server in the vault.

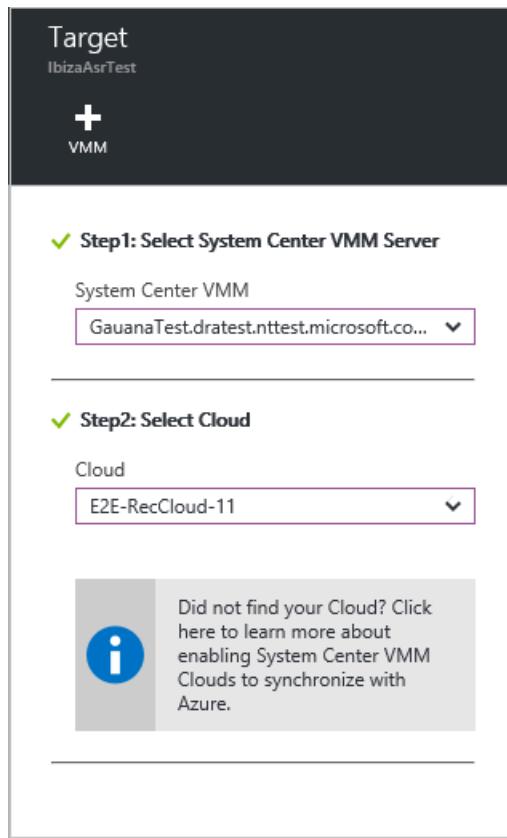


6. In **Vault name**, verify the name of the vault in which the server will be registered. Click **Next**.
7. In **Proxy Connection**, specify how the Provider running on the VMM server connects to Azure.
  - You can specify that the provider should connect directly to the internet, or via a proxy. Specify proxy settings as needed.
  - If you use a proxy, a VMM RunAs account (DRAProxyAccount) is created automatically, using the specified proxy credentials. Configure the proxy server so that this account can authenticate successfully. The RunAs account settings can be modified in the VMM console > **Settings** > **Security** > **Run As Accounts**.
  - Restart the VMM service to update changes.
8. In **Registration Key**, select the key that you downloaded and copied to the VMM server.
9. The encryption setting isn't relevant in this scenario.
10. In **Server name**, specify a friendly name to identify the VMM server in the vault. In a cluster, specify the VMM cluster role name.
11. In **Synchronize cloud metadata**, select whether you want to synchronize metadata for all clouds on the VMM server. This action only needs to happen once on each server. If you don't want to synchronize all clouds, leave this setting unchecked. You can synchronize each cloud individually, in the cloud properties in the VMM console.
12. Click **Next** to complete the process. After registration, Site Recovery retrieves metadata from the VMM server. The server is displayed in **Servers** > **VMM Servers** in the vault.
13. After the server appears in the vault, in **Source** > **Prepare source** select the VMM server, and select the cloud in which the Hyper-V host is located. Then click **OK**.

## Set up the target environment

Select the target VMM server and cloud:

1. Click **Prepare infrastructure** > **Target**, and select the target VMM server.
2. VMM clouds that are synchronized with Site Recovery are displayed. Select the target cloud.



## Set up a replication policy

Before you start, make sure that all hosts using the policy have the same operating system. If hosts are running different versions of Windows Server, you need multiple replication policies.

1. To create a new replication policy, click **Prepare infrastructure > Replication Settings > +Create and associate**.
2. In **Create and associate policy**, specify a policy name. The source and target type should be **Hyper-V**.
3. In **Hyper-V host version**, select which operating system is running on the host.
4. In **Authentication type** and **Authentication port**, specify how traffic is authenticated between the primary and recovery Hyper-V host servers.
  - Select **Certificate** unless you have a working Kerberos environment. Azure Site Recovery will automatically configure certificates for HTTPS authentication. You don't need to do anything manually.
  - By default, port 8083 and 8084 (for certificates) will be opened in the Windows Firewall on the Hyper-V host servers.
  - If you do select **Kerberos**, a Kerberos ticket will be used for mutual authentication of the host servers. Kerberos is only relevant for Hyper-V host servers running on Windows Server 2012 R2 or later.
5. In **Copy frequency**, specify how often you want to replicate delta data after the initial replication (every 30 seconds, 5 or 15 minutes).
6. In **Recovery point retention**, specify how long (in hours) the retention window will be for each recovery point. Replicated machines can be recovered to any point within a window.
7. In **App-consistent snapshot frequency**, specify how frequently (1-12 hours) recovery points containing application-consistent snapshots are created. Hyper-V uses two types of snapshots:
  - **Standard snapshot:** Provides an incremental snapshot of the entire virtual machine.
  - **App-consistent snapshot:** Takes a point-in-time snapshot of the application data inside the VM. Volume Shadow Copy Service (VSS) ensures that apps are in a consistent state when the snapshot is

taken. Enabling application-consistent snapshots, affects app performance on source VMs. Set a value that's less than the number of additional recovery points you configure.

8. In **Data transfer compression**, specify whether transferred replication data should be compressed.
9. Select **Delete replica VM**, to specify that the replica virtual machine should be deleted if you disable protection for the source VM. If you enable this setting, when you disable protection for the source VM it's removed from the Site Recovery console, Site Recovery settings for the VMM are removed from the VMM console, and the replica is deleted.
10. In **Initial replication method**, if you're replicating over the network, specify whether to start the initial replication or schedule it. To save network bandwidth, you might want to schedule it outside your busy hours. Then click **OK**.

The dialog box contains the following configuration:

- Name: Enter policy name
- Source type: Hyper-V
- Target type: Hyper-V
- Hyper-V host version: Hyper-V Server 2012 R2
- Authentication type: Kerberos
- Authentication port: 8083
- Copy frequency: 30 Seconds
- Recovery point retention in hours: 2
- App-consistent snapshot frequency in hours: 1
- Data transfer compression: Disable (selected)
- Delete replica VM: No (selected)
- Initial replication method: Over network (selected)

11. The new policy is automatically associated with the VMM cloud. In **Replication policy**, click **OK**.

## Enable replication

1. Click **Replicate application > Source**.
2. In **Source**, select the VMM server, and the cloud in which the Hyper-V hosts you want to replicate are located. Then click **OK**.
3. In **Target**, verify the secondary VMM server and cloud.
4. In **Virtual machines**, select the VMs you want to protect from the list.

You can track progress of the **Enable Protection** action in **Jobs > Site Recovery jobs**. After the **Finalize Protection** job completes, the initial replication is complete, and the VM is ready for failover.

## Next steps

[Run a disaster recovery drill](#)

# Run a DR drill for Hyper-V VMs to a secondary site

11/15/2019 • 9 minutes to read • [Edit Online](#)

This article describes how to do a disaster recovery (DR) drill for Hyper-V VMs that are managed in System Center Virtual Machine Manager V(MM) clouds, to a secondary on-premises site, using [Azure Site Recovery](#).

You run a test failover to validate your replication strategy, and perform a DR drill without any data loss or downtime. A test failover doesn't have any impact on the ongoing replication, or on your production environment.

## How do test failovers work?

You run a test failover from the primary to the secondary site. If you simply want to check that a VM fails over, you can run a test failover without setting anything up on the secondary site. If you want to verify app failover works as expected, you will need to set up networking and infrastructure in the secondary location.

- You can run a test failover on a single VM, or on a [recovery plan](#).
- You can run a test failover without a network, with an existing network, or with an automatically created network. More details about these options are provided in the table below.
  - You can run a test failover without a network. This option is useful if you simply want to check that a VM was able to fail over, but you won't be able to verify any network configuration.
  - Run the failover with an existing network. We recommend you don't use a production network.
  - Run the failover and let Site Recovery automatically create a test network. In this case Site Recovery will create the network automatically, and clean it up when test failover is complete.
- You need to select a recovery point for the test failover:
  - **Latest processed:** This option fails a VM over to the latest recovery point processed by Site Recovery. This option provides a low RTO (Recovery Time Objective), because no time is spent processing unprocessed data.
  - **Latest app-consistent:** This option fail over a VM to the latest application-consistent recovery point processed by Site Recovery.
  - **Latest:** This option first processes all the data that has been sent to Site Recovery service, to create a recovery point for each VM before failing over to it. This option provides the lowest RPO (Recovery Point Objective), because the VM created after failover will have all the data replicated to Site Recovery when the failover was triggered.
  - **Latest multi-VM processed:** Available for recovery plans that include one or more VMs that have multi-VM consistency enabled. VMs with the setting enabled fail over to the latest common multi-VM consistent recovery point. Other VMs fail over to the latest processed recovery point.
  - **Latest multi-VM app-consistent:** This option is available for recovery plans with one or more VMs that have multi-VM consistency enabled. VMs that are part of a replication group fail over to the latest common multi-VM application-consistent recovery point. Other VMs fail over to their latest application-consistent recovery point.
  - **Custom:** Use this option to fail over a specific VM to a particular recovery point.

## Prepare networking

When you run a test failover, you're asked to select network settings for test replica machines, as summarized in the table.

OPTION	DETAILS	
<b>None</b>	<p>The test VM is created on the host on which the replica VM is located. It isn't added to the cloud, and isn't connected to any network.</p> <p>You can connect the machine to a VM network after it has been created.</p>	
<b>Use existing</b>	<p>The test VM is created on the host on which the replica VM is located. It isn't added to the cloud.</p> <p>Create a VM network that's isolated from your production network.</p> <p>If you're using a VLAN-based network, we recommend that you create a separate logical network (not used in production) in VMM for this purpose. This logical network is used to create VM networks for test failovers.</p> <p>The logical network should be associated with at least one of the network adapters of all the Hyper-V servers that are hosting virtual machines.</p> <p>For VLAN logical networks, the network sites that you add to the logical network should be isolated.</p> <p>If you're using a Windows Network Virtualization-based logical network, Azure Site Recovery automatically creates isolated VM networks.</p>	
<b>Create a network</b>	<p>A temporary test network is created automatically based on the setting that you specify in <b>Logical Network</b> and its related network sites.</p> <p>Failover checks that VMs are created.</p> <p>You should use this option if a recovery plan uses more than one VM network.</p> <p>If you're using Windows Network Virtualization networks, this option can automatically create VM networks with the same settings (subnets and IP address pools) in the network of the replica virtual machine. These VM networks are cleaned up automatically after the test failover is complete.</p> <p>The test VM is created on the host on which the replica virtual machine exists. It isn't added to the cloud.</p>	

## Best practices

- Testing a production network causes downtime for production workloads. Ask your users not to use related apps when the disaster recovery drill is in progress.
- The test network doesn't need to match the VMM logical network type used for test failover. But, some combinations don't work:
  - If the replica uses DHCP and VLAN-based isolation, the VM network for the replica doesn't need a static IP address pool. So using Windows Network Virtualization for the test failover won't work because no address pools are available.
  - Test failover won't work if the replica network uses no isolation, and the test network uses Windows Network Virtualization. This is because the no-isolation network doesn't have the subnets required to create a Windows Network Virtualization network.
- We recommend that you don't use the network you selected for network mapping, for test failover.
- How replica virtual machines are connected to mapped VM networks after failover depends on how the VM network is configured in the VMM console.

### **VM network configured with no isolation or VLAN isolation**

If a VM network is configured in VMM with no isolation, or VLAN isolation, note the following:

- If DHCP is defined for the VM network, the replica virtual machine is connected to the VLAN ID through the settings that are specified for the network site in the associated logical network. The virtual machine receives its IP address from the available DHCP server.
- You don't need to define a static IP address pool for the target VM network. If a static IP address pool is used for the VM network, the replica virtual machine is connected to the VLAN ID through the settings that are specified for the network site in the associated logical network.
- The virtual machine receives its IP address from the pool that's defined for the VM network. If a static IP address pool isn't defined on the target VM network, IP address allocation will fail. Create the IP address pool on both the source and target VMM servers that you will use for protection and recovery.

### **VM network with Windows Network Virtualization**

If a VM network is configured in VMM with Windows Network Virtualization, note the following:

- You should define a static pool for the target VM network, regardless of whether the source VM network is configured to use DHCP or a static IP address pool.
- If you define DHCP, the target VMM server acts as a DHCP server and provides an IP address from the pool that's defined for the target VM network.
- If use of a static IP address pool is defined for the source server, the target VMM server allocates an IP address from the pool. In both cases, IP address allocation will fail if a static IP address pool is not defined.

## **Prepare the infrastructure**

If you simply want to check that a VM can fail over, you can run a test failover without an infrastructure. If you want to do a full DR drill to test app failover, you need to prepare the infrastructure at the secondary site:

- If you run a test failover using an existing network, prepare Active Directory, DHCP, and DNS in that network.
- If you run a test failover with the option to create a VM network automatically, you need to add infrastructure resources to the automatically created network, before you run the test failover. In a recovery plan, you can facilitate this by adding a manual step before Group-1 in the recovery plan that you're going to use for the test failover. Then, add the infrastructure resources to the automatically created network before you run the test failover.

### **Prepare DHCP**

If the virtual machines involved in test failover use DHCP, create a test DHCP server within the isolated network

for the purpose of test failover.

## Prepare Active Directory

To run a test failover for application testing, you need a copy of the production Active Directory environment in your test environment. For more information, review the [test failover considerations for Active Directory](#).

## Prepare DNS

Prepare a DNS server for the test failover as follows:

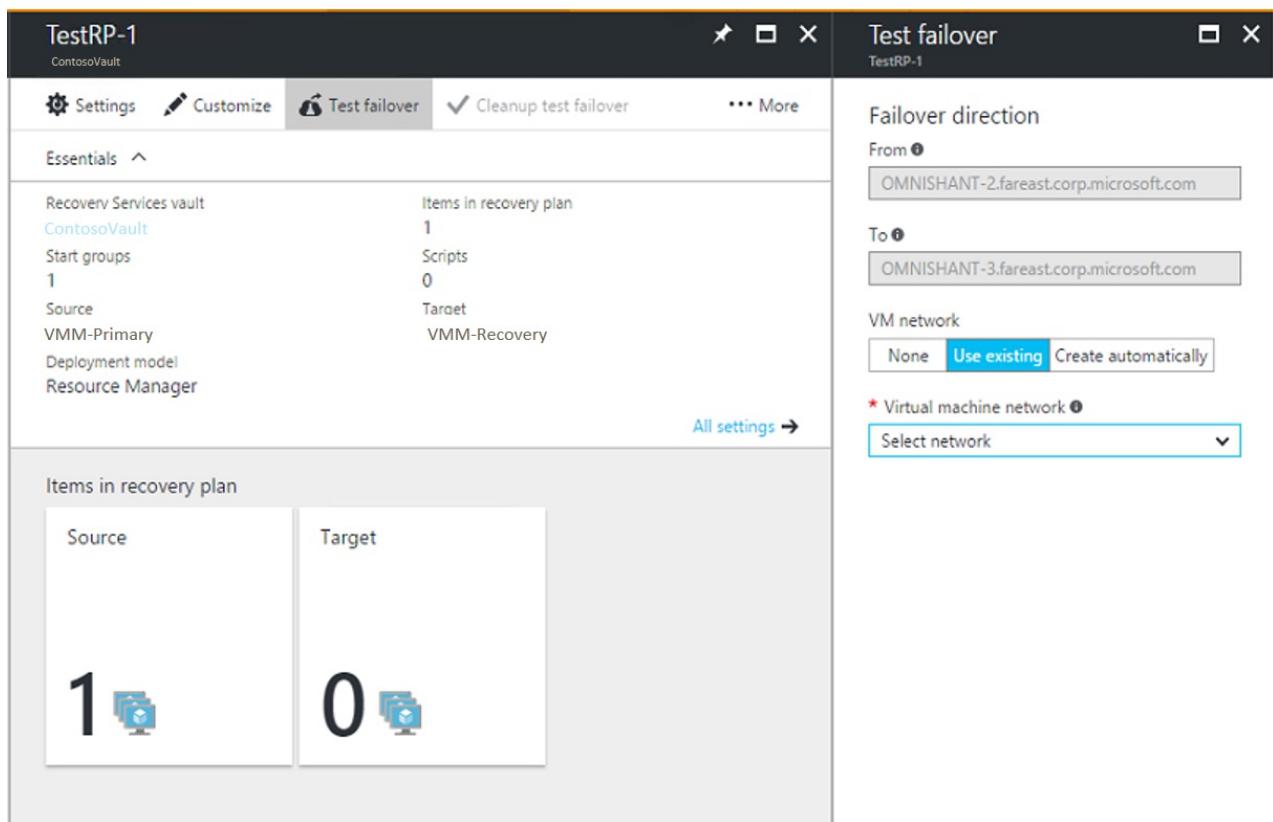
- **DHCP:** If virtual machines use DHCP, the IP address of the test DNS should be updated on the test DHCP server. If you're using a network type of Windows Network Virtualization, the VMM server acts as the DHCP server. Therefore, the IP address of DNS should be updated in the test failover network. In this case, the virtual machines register themselves to the relevant DNS server.
- **Static address:** If virtual machines use a static IP address, the IP address of the test DNS server should be updated in test failover network. You might need to update DNS with the IP address of the test virtual machines. You can use the following sample script for this purpose:

```
Param(
 [string]$Zone,
 [string]$name,
 [string]$IP
)
$Record = Get-DnsServerResourceRecord -ZoneName $zone -Name $name
$newrecord = $record.clone()
$newrecord.RecordData[0].IPv4Address = $IP
Set-DnsServerResourceRecord -zonename $zone -OldInputObject $record -NewInputObject $Newrecord
```

## Run a test failover

This procedure describes how to run a test failover for a recovery plan. Alternatively, you can run the failover for a single virtual machine on the **Virtual Machines** tab.

1. Select **Recovery Plans** > *recoveryplan\_name*. Click **Failover** > **Test Failover**.
2. On the **Test Failover** blade, specify how replica VMs should be connected to networks after the test failover.
3. Track failover progress on the **Jobs** tab.
4. After failover is complete, verify that the VMs start successfully.
5. When you're done, click **Cleanup test failover** on the recovery plan. In **Notes**, record and save any observations associated with the test failover. This step deletes any VMs and networks that were created by Site Recovery during test failover.



#### TIP

The IP address given to a virtual machine during test failover is the same IP address that the virtual machine would receive for a planned or unplanned failover (presuming that the IP address is available in the test failover network). If the same IP address isn't available in the test failover network, the virtual machine receives another IP address that's available in the test failover network.

### Run a test failover to a production network

We recommend that you don't run a test failover to your production recovery site network that you specified during network mapping. But if you do need to validate end-to-end network connectivity in a failed-over VM, note the following points:

- Make sure that the primary VM is shut down when you're doing the test failover. If you don't, two virtual machines with the same identity will be running in the same network at the same time. That situation can lead to undesired consequences.
- Any changes that you make to the test failover VMs are lost when you clean up the test failover virtual machines. These changes are not replicated back to the primary VMs.
- Testing like this leads to downtime for your production application. Ask users of the application not to use the application when the DR drill is in progress.

### Next steps

After you have successfully run a DR drill, you can [run a full failover](#).

# Set up IP addressing to connect to a secondary on-premises site after failover

11/12/2019 • 4 minutes to read • [Edit Online](#)

After you fail over Hyper-V VMs in System Center Virtual Machine Manager (VMM) clouds to a secondary site, you need to be able connect to the replica VMs. This article helps you to do this.

## Connection options

After failover, there are a couple of ways to handle IP addressing for replica VMs:

- **Retain the same IP address after failover:** In this scenario, the replicated VM has the same IP address as the primary VM. This simplifies network related issues after failover, but requires some infrastructure work.
- **Use a different IP address after failover:** In this scenario the VM gets a new IP address after failover.

## Retain the IP address

If you want to retain the IP addresses from the primary site, after failover to the secondary site, you can:

- Deploy a stretched subnet between the primary and the secondary sites.
- Perform a full subnet failover from the primary to secondary site. You need to update routes to indicate the new location of the IP addresses.

### Deploy a stretched subnet

In a stretched configuration, the subnet is available simultaneously in both the primary and secondary sites. In a stretched subnet, when you move a machine and its IP (Layer 3) address configuration to the secondary site, the network automatically routes the traffic to the new location.

- From a Layer 2 (data link layer) perspective, you need networking equipment that can manage a stretched VLAN.
- By stretching the VLAN, the potential fault domain extends to both sites. This becomes a single point of failure. While unlikely, in such a scenario you might not be able to isolate an incident such as a broadcast storm.

### Fail over a subnet

You can fail over the entire subnet to obtain the benefits of the stretched subnet, without actually stretching it. In this solution, a subnet is available in the source or target site, but not in both simultaneously.

- To maintain the IP address space in the event of a failover, you can programmatically arrange for the router infrastructure to move subnets from one site to another.
- When a failover occurs, subnets move with their associated VMs.
- The main drawback of this approach is that in the event of a failure, you have to move the entire subnet.

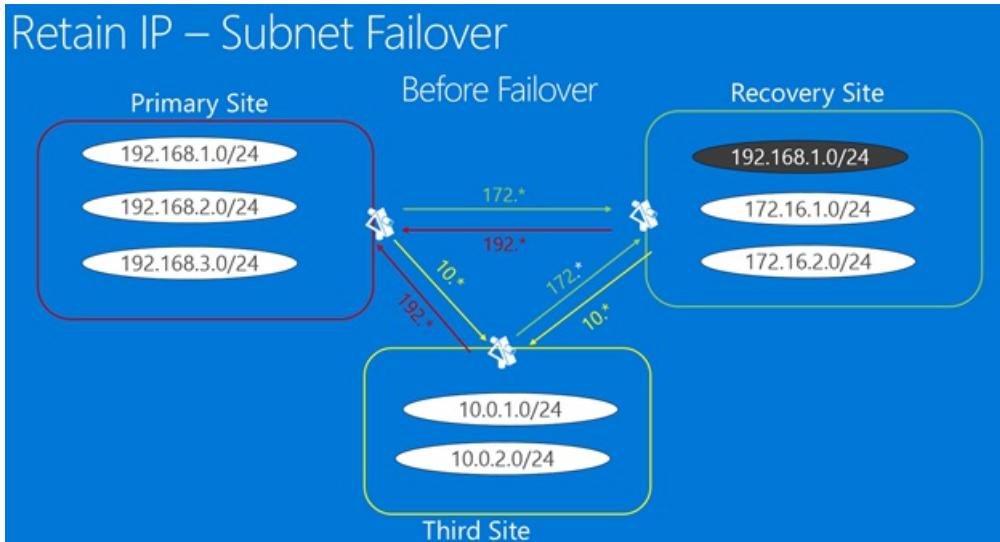
### Example

Here's an example of complete subnet failover.

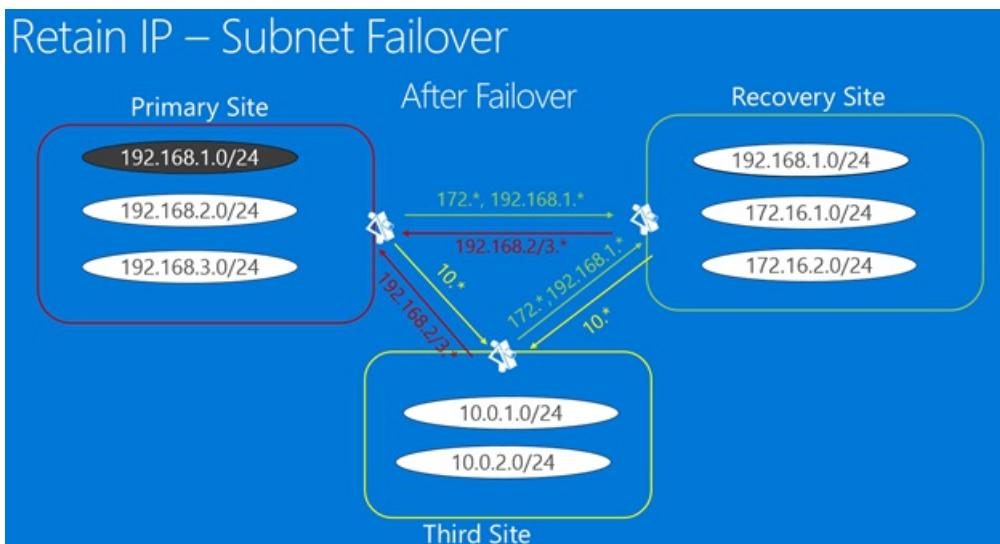
- Before failover, the primary site has applications running in subnet 192.168.1.0/24.
- During failover, all of the VMs in this subnet are failed over to the secondary site, and retain their IP addresses.
- Routes between all sites need to be modified to reflect the fact that all the VMs in subnet 192.168.1.0/24 have now moved to the secondary site.

The following graphics illustrate the subnets before and after failover.

## Before failover



## After failover



After failover, Site Recovery allocates an IP address for each network interface on the VM. The address is allocated from the static IP address pool in the relevant network, for each VM instance.

- If the IP address pool in the secondary site is the same as that on the source site, Site Recovery allocates the same IP address (of the source VM), to the replica VM. The IP address is reserved in VMM, but it isn't set as the failover IP address on the Hyper-V host. The failover IP address on a Hyper-v host is set just before the failover.
- If the same IP address isn't available, Site Recovery allocates another available IP address from the pool.
- If VMs use DHCP, Site Recovery doesn't manage the IP addresses. You need to check that the DHCP server on the secondary site can allocate addresses from the same range as the source site.

## Validate the IP address

After you enable protection for a VM, you can use following sample script to verify the address assigned to the VM. This IP address is set as the failover IP address, and assigned to the VM at the time of failover:

```
...
$vm = Get-SCVirtualMachine -Name <VM_NAME>
$na = $vm[0].VirtualNetworkAdapters>
$ip = Get-SCIPAddress -GrantToObjectID $na[0].id
$ip.address
...
```

# Use a different IP address

In this scenario, the IP addresses of VMs that fail over are changed. The drawback of this solution is the maintenance required. DNS and cache entries might need to be updated. This can result in downtime, which can be mitigated as follows:

- Use low TTL values for intranet applications.
- Use the following script in a Site Recovery recovery plan, for a timely update of the DNS server. You don't need the script if you use dynamic DNS registration.

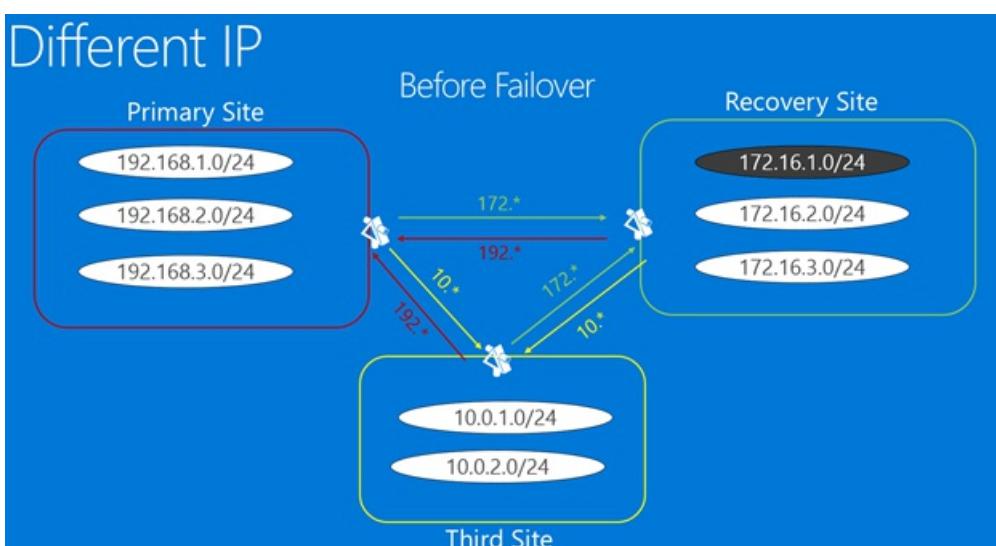
```
param(
[string]$Zone,
[string]$name,
[string]$IP
)
$Record = Get-DnsServerResourceRecord -ZoneName $zone -Name $name
$newrecord = $record.clone()
$newrecord.RecordData[0].IPv4Address = $IP
Set-DnsServerResourceRecord -zonename $zone -OldInputObject $record -NewInputObject $Newrecord
```

## Example

In this example we have different IP addresses across primary and secondary sites, and there's a third site from which applications hosted on the primary or recovery site can be accessed.

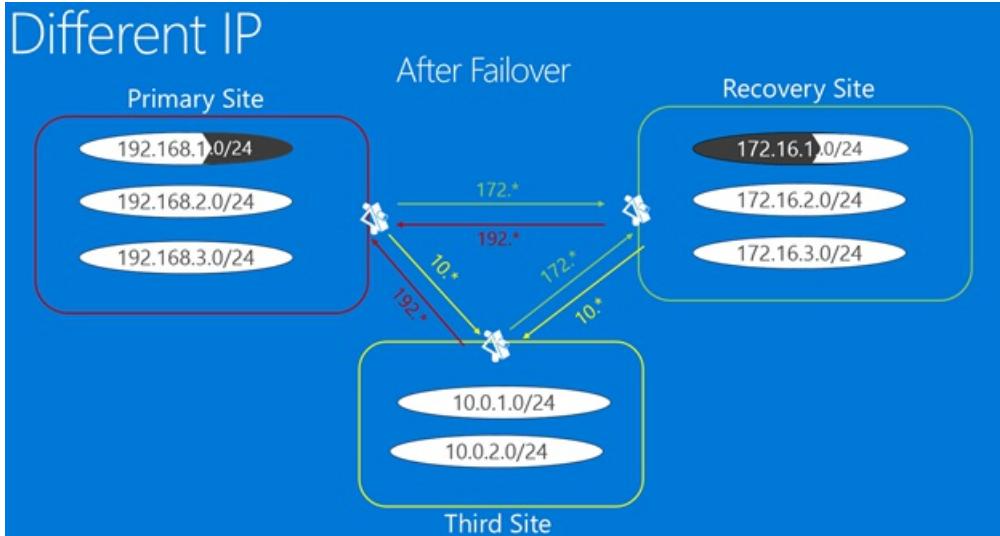
- Before failover, apps are hosted subnet 192.168.1.0/24 on the primary site.
- After failover, apps are configured in subnet 172.16.1.0/24 in the secondary site.
- All three sites can access each other.
- After failover, apps will be restored in the recovery subnet.
- In this scenario there's no need to fail over the entire subnet, and no changes are needed to reconfigure VPN or network routes. The failover, and some DNS updates, ensure that applications remain accessible.
- If DNS is configured to allow dynamic updates, then the VMs will register themselves using the new IP address, when they start after failover.

## Before failover



## After failover

# Different IP



## Next steps

[Run a failover](#)

# Add a VMM script to a recovery plan

11/14/2019 • 4 minutes to read • [Edit Online](#)

This article describes how to create a System Center Virtual Machine Manager (VMM) script and add it to a recovery plan in [Azure Site Recovery](#).

Post any comments or questions at the bottom of this article, or on the [Azure Recovery Services forum](#).

## Prerequisites

You can use PowerShell scripts in your recovery plans. To be accessible from the recovery plan, you must author the script and place the script in the VMM library. Keep the following considerations in mind while you write the script:

- Ensure that scripts use try-catch blocks, so that exceptions are handled gracefully.
  - If an exception occurs in the script, the script stops running, and the task shows as failed.
  - If an error occurs, the remainder of the script doesn't run.
  - If an error occurs when you run an unplanned failover, the recovery plan continues.
  - If an error occurs when you run a planned failover, the recovery plan stops. Fix the script, check that it runs as expected, and then run the recovery plan again.
  - The `Write-Host` command doesn't work in a recovery plan script. If you use the `Write-Host` command in a script, the script fails. To create output, create a proxy script that in turn runs your main script. To ensure that all output is piped out, use the `>>` command.
  - The script times out if it doesn't return within 600 seconds.
  - If anything is written to `STDERR`, the script is classified as failed. This information is displayed in the script execution details.
- Scripts in a recovery plan run in the context of the VMM service account. Ensure that this account has read permissions for the remote share on which the script is located. Test the script to run with the same level of user rights as the VMM service account.
- VMM cmdlets are delivered in a Windows PowerShell module. The module is installed when you install the VMM console. To load the module into your script, use the following command in the script:

```
Import-Module -Name virtualmachinemanager
```

For more information, see [Get started with Windows PowerShell and VMM](#).

- Ensure that you have at least one library server in your VMM deployment. By default, the library share path for a VMM server is located locally on the VMM server. The folder name is `MSCVMMLibrary`.

If your library share path is remote (or if it's local but not shared with `MSCVMMLibrary`), configure the share as follows, using `\libserver2.contoso.com\share\` as an example:

1. Open the Registry Editor, and then go to  
**`HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\Azure Site Recovery\Registration`**.
2. Change the value for **`ScriptLibraryPath`** to `\\\libserver2.contoso.com\share\`. Specify the full FQDN. Provide permissions to the share location. This is the root node of the share. To check for the root node, in VMM, go to the root node in the library. The path that opens is the root of the path. This is the path that you must use in the variable.

3. Test the script by using a user account that has the same level of user rights as the VMM service account. Using these user rights verifies that standalone, tested scripts run the same way that they run in recovery plans. On the VMM server, set the execution policy to bypass, as follows:

- a. Open the **64-bit Windows PowerShell** console as an administrator.
- b. Enter **Set-executionpolicy bypass**. For more information, see [Using the Set-ExecutionPolicy cmdlet](#).

**IMPORTANT**

Set **Set-executionpolicy bypass** only in the 64-bit PowerShell console. If you set it for the 32-bit PowerShell console, the scripts don't run.

## Add the script to the VMM library

If you have a VMM source site, you can create a script on the VMM server. Then, include the script in your recovery plan.

1. In the library share, create a new folder. For example, <VMM server name>\MSSCVMMLibrary\RPScripts. Place the folder on the source and target VMM servers.
2. Create the script. For example, name the script RPScript. Verify that the script works as expected.
3. Place the script in the <VMM server name>\MSSCVMMLibrary folder on the source and target VMM servers.

## Add the script to a recovery plan

After you've added VMs or replication groups to a recovery plan and created the plan, you can add the script to the group.

1. Open the recovery plan.
2. In the **Step** list, select an item. Then, select either **Script** or **Manual Action**.
3. Specify whether to add the script or action before or after the selected item. To move the position of the script up or down, select the **Move Up** and **Move Down** buttons.
4. If you add a VMM script, select **Failover to VMM script**. In **Script Path**, enter the relative path to the share. For example, enter **\RPScripts\RPScript.PS1**.
5. If you add an Azure Automation runbook, specify the Automation account in which the runbook is located. Then, select the Azure runbook script that you want to use.
6. To ensure that the script works as expected, do a test failover of the recovery plan.

## Next steps

- Learn more about [running failovers](#).

# Fail over and fail back Hyper-V VMs replicated to your secondary on-premises site

11/14/2019 • 2 minutes to read • [Edit Online](#)

The [Azure Site Recovery](#) service manages and orchestrates replication, failover, and failback of on-premises machines, and Azure virtual machines (VMs).

This article describes how to fail over a Hyper-V VM managed in a System Center Virtual Machine Manager (VMM) cloud, to a secondary VMM site. After you've failed over, you fail back to your on-premises site when it's available. In this article, you learn how to:

- Fail over a Hyper-V VM from a primary VMM cloud to a secondary VMM cloud
- Reprotect from the secondary site to the primary, and fail back
- Optionally start replicating from primary to secondary again

## Failover and failback

Failover and failback has three stages:

1. **Fail over to secondary site:** Fail machines over from the primary site to the secondary.
2. **Fail back from the secondary site:** Replicate VMs from secondary to primary, and run a planned failover to fail back.
3. After the planned failover, optionally start replicating from the primary site to the secondary again.

## Prerequisites

- Make sure you've completed a [disaster recovery drill](#) to check that everything's working as expected.
- To complete failback, make sure that the primary and secondary VMM servers are connected to Site Recovery.

## Run a failover from primary to secondary

You can run a regular or planned failover for Hyper-V VMs.

- Use a regular failover for unexpected outages. When you run this failover, Site Recovery creates a VM in the secondary site, and powers it up. Data loss can occur depending on pending data that hasn't been synchronized.
- A planned failover can be used for maintenance, or during expected outage. This option provides zero data loss. When a planned failover is triggered, the source VMs are shut down. Unsynchronized data is synchronized, and the failover is triggered.
- This procedure describes how to run a regular failover.

1. In **Settings > Replicated items** click the VM > **Failover**.
2. Select **Shutdown machine before beginning failover** if you want Site Recovery to attempt to do a shutdown of source VMs before triggering the failover. Site Recovery will also try to synchronize on-premises data that hasn't yet been sent to the secondary site, before triggering the failover. Note that failover continues even if shutdown fails. You can follow the failover progress on the **Jobs** page.
3. You should now be able to see the VM in the secondary VMM cloud.
4. After you verify the VM, **Commit** the failover. This deletes all the available recovery points.

#### **WARNING**

**Don't cancel a failover in progress:** Before failover is started, VM replication is stopped. If you cancel a failover in progress, failover stops, but the VM won't replicate again.

## Reverse replicate and failover

Start replicating from the secondary site to the primary, and fail back to the primary site. After VMs are running in the primary site again, you can replicate them to the secondary site.

1. Click the VM > click on **Reverse Replicate**.
2. Once the job is complete, click the VM > In **Failover**, verify the failover direction (from secondary VMM cloud), and select the source and target locations.
3. Initiate the failover. You can follow the failover progress on the **Jobs** tab.
4. In the primary VMM cloud, check that the VM is available.
5. If you want to start replicating the primary VM back to the secondary site again, click on **Reverse Replicate**.

## Next steps

[Review the step](#) for replicating Hyper-V VMs to a secondary site.

# Test results for Hyper-V replication to a secondary site

11/6/2019 • 6 minutes to read • [Edit Online](#)

This article provides the results of performance testing when replicating Hyper-V VMs in System Center Virtual Machine Manager (VMM) clouds, to a secondary datacenter.

## Test goals

The goal of testing was to examine how Site Recovery performs during steady state replication.

- Steady state replication occurs when VMs have completed initial replication, and are synchronizing delta changes.
- It's important to measure performance using steady state, because it's the state in which most VMs remain, unless unexpected outages occur.
- The test deployment consisted of two on-premises sites, with a VMM server in each site. This test deployment is typical of a head office/branch office deployment, with head office acting as the primary site, and the branch office as the secondary or recovery site.

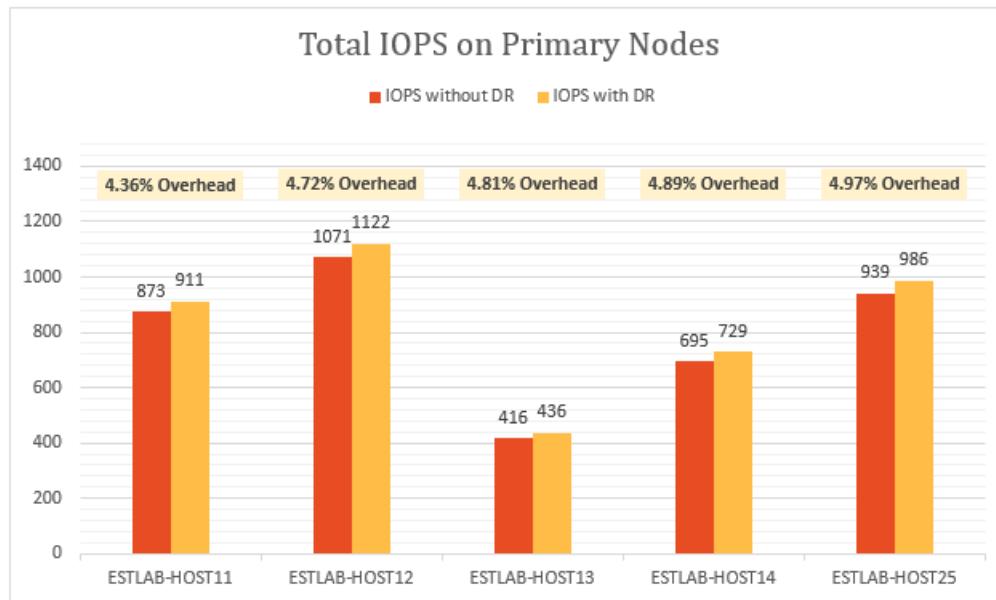
## What we did

Here's what we did in the test pass:

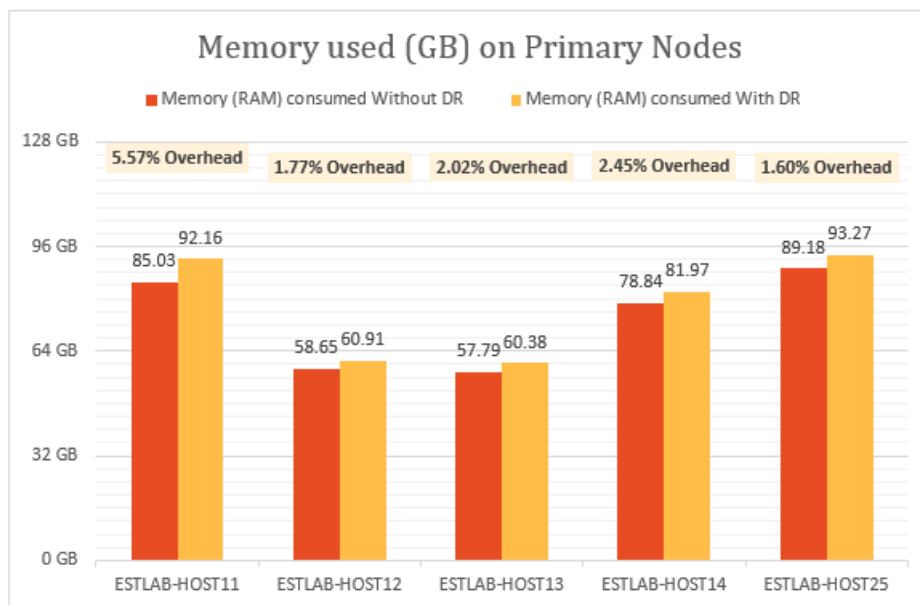
1. Created VMs using VMM templates.
2. Started VMs, and captured baseline performance metrics over 12 hours.
3. Created clouds on the primary and recovery VMM servers.
4. Configured replication in Site Recovery, including mapping between source and recovery clouds.
5. Enabled protection for VMs, and allowed them to complete initial replication.
6. Waited a couple of hours for system stabilization.
7. Captured performance metrics over 12 hours, where all VMs remained in an expected replication state for those 12 hours.
8. Measured the delta between the baseline performance metrics, and the replication performance metrics.

## Primary server performance

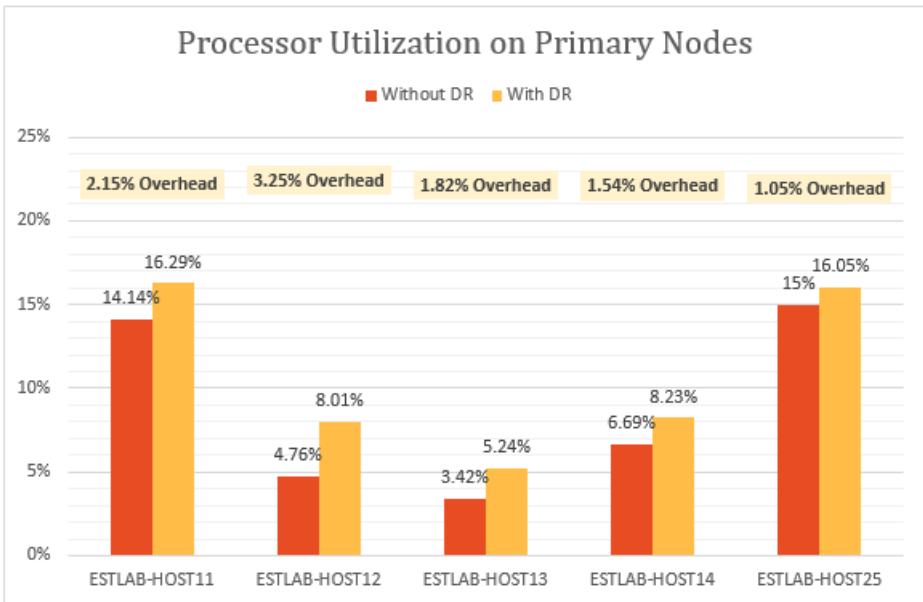
- Hyper-V Replica (used by Site Recovery) asynchronously tracks changes to a log file, with minimum storage overhead on the primary server.
- Hyper-V Replica utilizes self-maintained memory cache to minimize IOPS overhead for tracking. It stores writes to the VHDX in memory, and flushes them into the log file before the time that the log is sent to the recovery site. A disk flush also happens if the writes hit a predetermined limit.
- The graph below shows the steady state IOPS overhead for replication. We can see that the IOPS overhead due to replication is around 5%, which is quite low.



Hyper-V Replica uses memory on the primary server, to optimize disk performance. As shown in the following graph, memory overhead on all servers in the primary cluster is marginal. The memory overhead shown is the percentage of memory used by replication, compared to the total installed memory on the Hyper-V server.

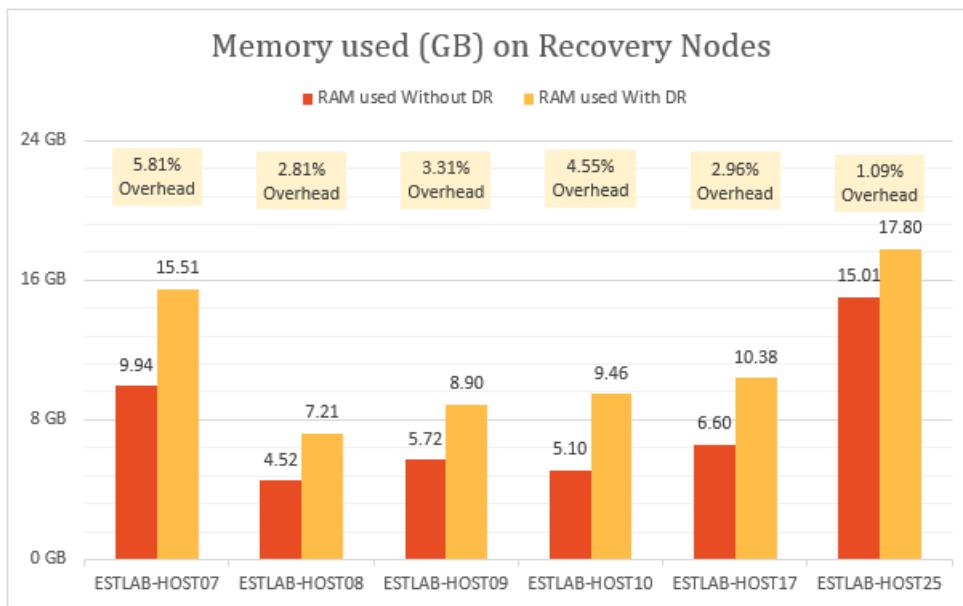


Hyper-V Replica has minimum CPU overhead. As shown in the graph, replication overhead is in the range of 2-3%.



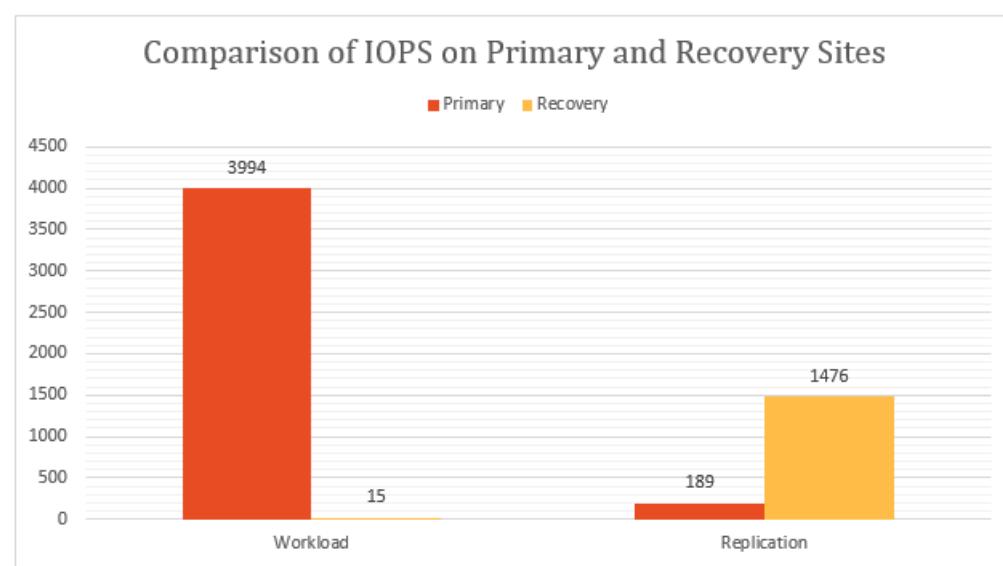
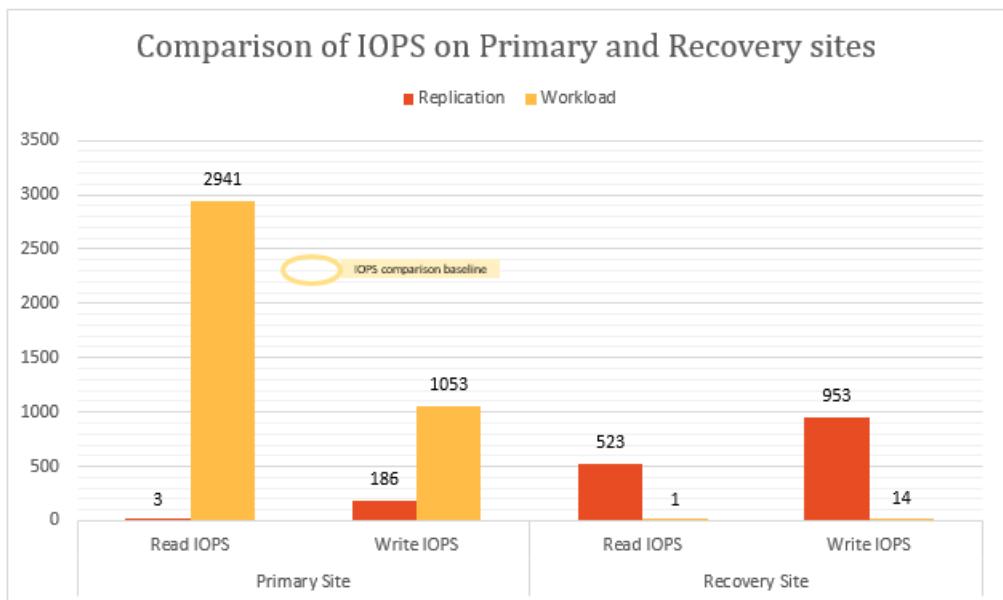
## Secondary server performance

Hyper-V Replica uses a small amount of memory on the recovery server, to optimize the number of storage operations. The graph summarizes the memory usage on the recovery server. The memory overhead shown is the percentage of memory used by replication, compared to the total installed memory on the Hyper-V server.



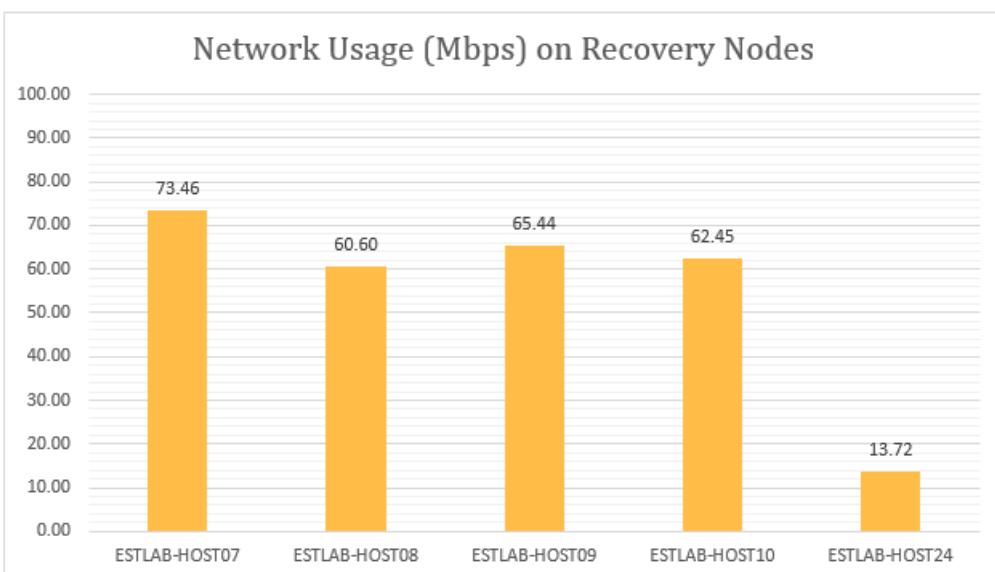
The amount of I/O operations on the recovery site is a function of the number of write operations on the primary site. Let's look at the total I/O operations on the recovery site in comparison with the total I/O operations and write operations on the primary site. The graphs show that the total IOPS on the recovery site is

- Around 1.5 times the write IOPS on the primary.
- Around 37% of the total IOPS on the primary site.



## Effect on network utilization

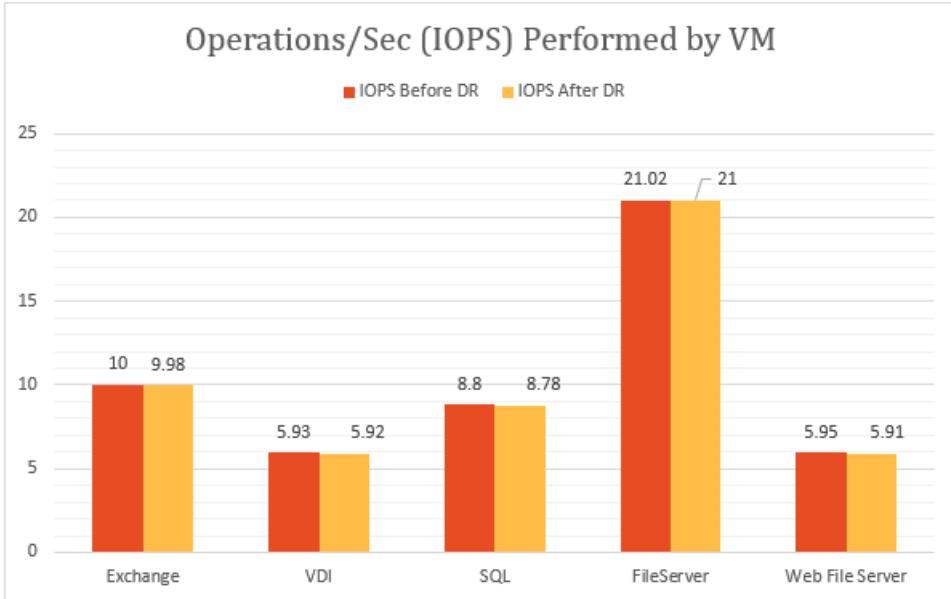
An average of 275 Mb per second of network bandwidth was used between the primary and recovery nodes (with compression enabled), against an existing bandwidth of 5 Gb per second.



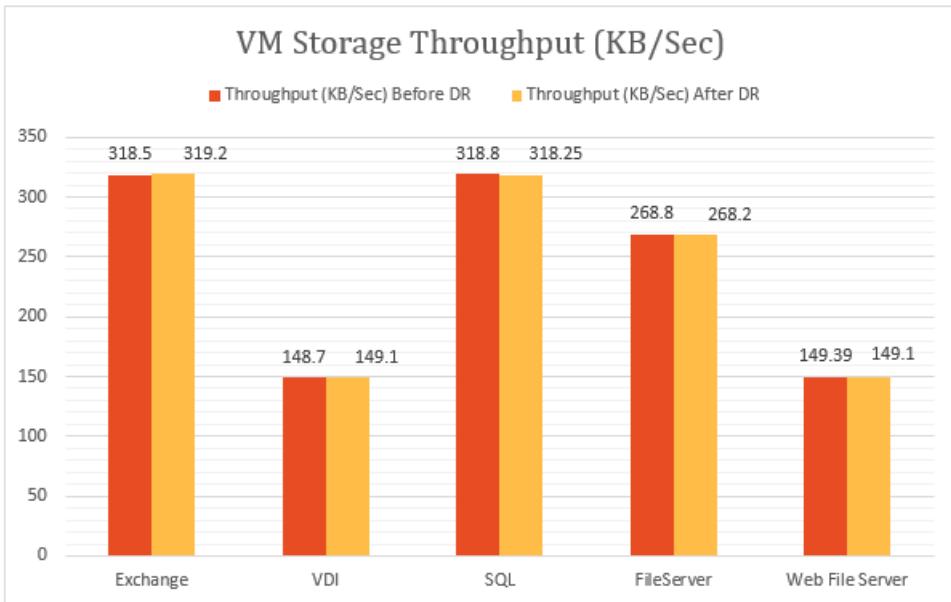
## Effect on VM performance

An important consideration is the impact of replication on production workloads running on the virtual machines. If the primary site is adequately provisioned for replication, there shouldn't be any impact on the workloads. Hyper-V Replica's lightweight tracking mechanism ensures that workloads running in the virtual machines are not impacted during steady-state replication. This is illustrated in the following graphs.

This graph shows IOPS performed by virtual machines running different workloads, before and after replication was enabled. You can observe that there is no difference between the two.



The following graph shows the throughput of virtual machines running different workloads, before and after replication was enabled. You can observe that replication has no significant impact.



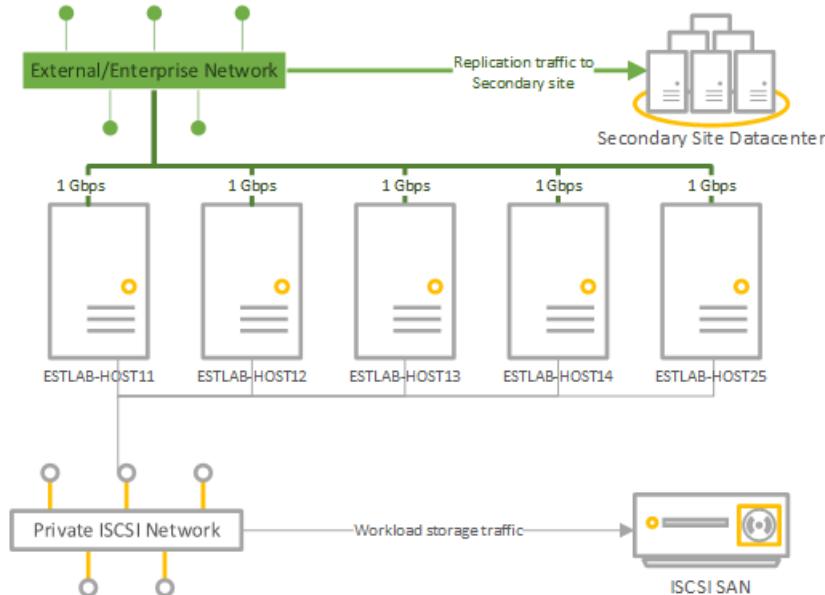
## Conclusion

The results clearly show that Site Recovery, coupled with Hyper-V Replica, scales well with minimum overhead for a large cluster. Site Recovery provides simple deployment, replication, management and monitoring. Hyper-V Replica provides the necessary infrastructure for successful replication scaling.

## Test environment details

## Primary site

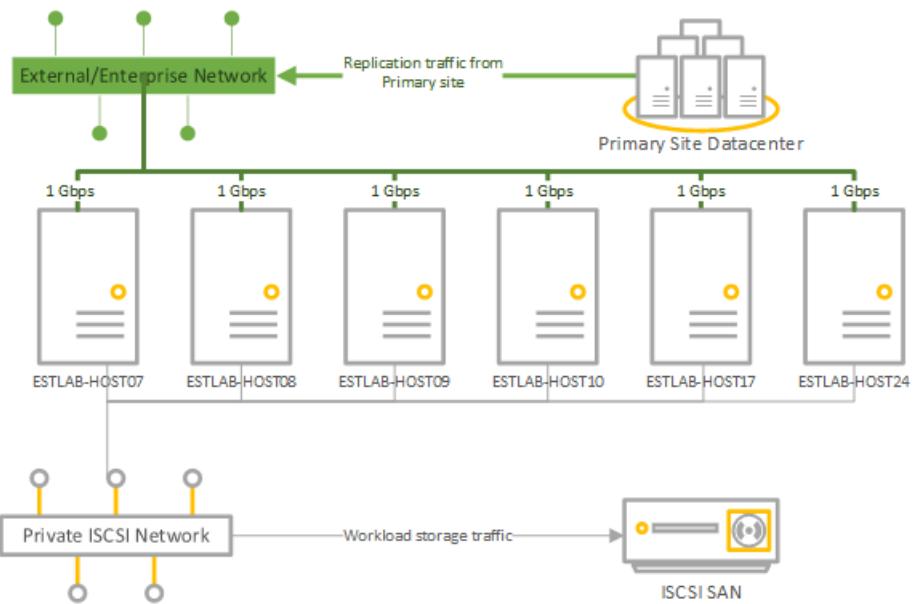
- The primary site has a cluster containing five Hyper-V servers, running 470 virtual machines.
- The VMs run different workloads, and all have Site Recovery protection enabled.
- Storage for the cluster node is provided by an iSCSI SAN. Model – Hitachi HUS130.
- Each cluster server has four network cards (NICs) of one Gbps each.
- Two of the network cards are connected to an iSCSI private network, and two are connected to an external enterprise network. One of the external networks is reserved for cluster communications only.



SERVER	RAM	MODEL	PROCESSOR	NUMBER OF PROCESSORS	NIC	SOFTWARE
Hyper-V servers in cluster: ESTLAB-HOST11 ESTLAB-HOST12 ESTLAB-HOST13 ESTLAB-HOST14 ESTLAB-HOST25	128 ESTLAB-HOST25 has 256	Dell™ PowerEdge™ R820	Intel(R) Xeon(R) CPU E5-4620 0 @ 2.20GHz	4	1 Gbps x 4	Windows Server Datacenter 2012 R2 (x64) + Hyper-V role
VMM Server	2			2	1 Gbps	Windows Server Database 2012 R2 (x64) + VMM 2012 R2

## Secondary site

- The secondary site has a six-node failover cluster.
- Storage for the cluster node is provided by an iSCSI SAN. Model – Hitachi HUS130.



SERVER	RAM	MODEL	PROCESSOR	NUMBER OF PROCESSORS	NIC	SOFTWARE
Hyper-V servers in cluster: ESTLAB-HOST07 ESTLAB-HOST08 ESTLAB-HOST09 ESTLAB-HOST10	96	Dell™ PowerEdge™ R720	Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz	2	1 Gbps x 4	Windows Server Datacenter 2012 R2 (x64) + Hyper-V role
ESTLAB-HOST17	128	Dell™ PowerEdge™ R820	Intel(R) Xeon(R) CPU E5-4620 0 @ 2.20GHz	4		Windows Server Datacenter 2012 R2 (x64) + Hyper-V role
ESTLAB-HOST24	256	Dell™ PowerEdge™ R820	Intel(R) Xeon(R) CPU E5-4620 0 @ 2.20GHz	2		Windows Server Datacenter 2012 R2 (x64) + Hyper-V role
VMM Server	2			2	1 Gbps	Windows Server Database 2012 R2 (x64) + VMM 2012 R2

### Server workloads

- For test purposes we picked workloads commonly used in enterprise customer scenarios.
- We use [IOmeter](#) with the workload characteristic summarized in the table for simulation.

- All IOMeter profiles are set to write random bytes to simulate worst-case write patterns for workloads.

WORKLOAD	I/O SIZE (KB)	% ACCESS	%READ	OUTSTANDING I/O/S	I/O PATTERN
File Server	4	60%	80%	8	All 100% random
	8	20%	80%	8	
	16	5%	80%	8	
	32	5%	80%	8	
	64	10%	80%	8	
SQL Server (volume 1)	8	100%	70%	8	100% random
	64	100%	0%	8	100% sequential
SQL Server (volume 2)					
Exchange	32	100%	67%	8	100% random
Workstation/VDI	4	66%	70%	1	Both 100% random
	64	34%	95%	1	
Web File Server	4	33%	95%	8	All 75% random
	8	34%	95%	8	
	64	33%	95%	8	

### VM configuration

- 470 VMs on the primary cluster.
- All VMs with VHDX disk.
- VMs running workloads summarized in the table. All were created with VMM templates.

WORKLOAD	# VMS	MINIMUM RAM (GB)	MAXIMUM RAM (GB)	LOGICAL DISK SIZE (GB) PER VM	MAXIMUM IOPS
SQL Server	51	1	4	167	10
Exchange Server	71	1	4	552	10
File Server	50	1	2	552	22
VDI	149	.5	1	80	6
Web server	149	.5	1	80	6
TOTAL	470			96.83 TB	4108

### Site Recovery settings

- Site Recovery was configured for on-premises to on-premises protection
- The VMM server has four clouds configured, containing the Hyper-V cluster servers and their VMs.

PRIMARY VMM CLOUD	PROTECTED VMS	REPLICATION FREQUENCY	ADDITIONAL RECOVERY POINTS
PrimaryCloudRpo15m	142	15 mins	None

PRIMARY VMM CLOUD	PROTECTED VMs	REPLICATION FREQUENCY	ADDITIONAL RECOVERY POINTS
PrimaryCloudRpo30s	47	30 secs	None
PrimaryCloudRpo30sArp1	47	30 secs	1
PrimaryCloudRpo5m	235	5 mins	None

## Performance metrics

The table summarizes the performance metrics and counters that were measured in the deployment.

METRIC	COUNTER
CPU	\Processor(_Total)% Processor Time
Available memory	\Memory\Available MBytes
IOPS	\PhysicalDisk(_Total)\Disk Transfers/sec
VM read (IOPS) operations/sec	\Hyper-V Virtual Storage Device(<VHD>)\Read Operations/Sec
VM write (IOPS) operations/sec	\Hyper-V Virtual Storage Device(<VHD>)\Write Operations/S
VM read throughput	\Hyper-V Virtual Storage Device(<VHD>)\Read Bytes/sec
VM write throughput	\Hyper-V Virtual Storage Device(<VHD>)\Write Bytes/sec

## Next steps

[Set up replication](#)

# Set up disaster recovery for Azure virtual machines using Azure PowerShell

2/14/2020 • 16 minutes to read • [Edit Online](#)

In this article, you see how to set up and test disaster recovery for Azure virtual machines using Azure PowerShell.

You learn how to:

- Create a Recovery Services vault.
- Set the vault context for the PowerShell session.
- Prepare the vault to start replicating Azure virtual machines.
- Create network mappings.
- Create storage accounts to replicate virtual machines to.
- Replicate Azure virtual machines to a recovery region for disaster recovery.
- Perform a test failover, validate, and cleanup test failover.
- Fail over to the recovery region.

## NOTE

Not all scenario capabilities available through the portal may be available through Azure PowerShell. Some of the scenario capabilities not currently supported through Azure PowerShell are:

- The ability to specify that all disks in a virtual machine should be replicated without having to explicitly specify each disk of the virtual machine.

## NOTE

This article has been updated to use the new Azure PowerShell Az module. You can still use the AzureRM module, which will continue to receive bug fixes until at least December 2020. To learn more about the new Az module and AzureRM compatibility, see [Introducing the new Azure PowerShell Az module](#). For Az module installation instructions, see [Install Azure PowerShell](#).

## Prerequisites

Before you start:

- Make sure that you understand the [scenario architecture and components](#).
- Review the [support requirements](#) for all components.
- You have the Azure PowerShell `Az` module. If you need to install or upgrade Azure PowerShell, follow this [Guide to install and configure Azure PowerShell](#).

## Sign in to your Microsoft Azure subscription

Sign in to your Azure subscription with the `Connect-AzAccount` cmdlet.

`Connect-AzAccount`

Select your Azure subscription. Use the `Get-AzSubscription` cmdlet to get the list of Azure subscriptions you have access to. Select the Azure subscription to work with using the `Set-AzContext` cmdlet.

```
Set-AzContext -SubscriptionId "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
```

## Get details of the virtual machine to be replicated

In this article, a virtual machine in the East US region is replicated to and recovered in the West US 2 region. The virtual machine being replicated has an OS disk and a single data disk. The name of the virtual machine used in the example is `AzureDemoVM`.

```
Get details of the virtual machine
$VM = Get-AzVM -ResourceGroupName "A2AdemoRG" -Name "AzureDemoVM"

Write-Output $VM
```

```
ResourceGroupName : A2AdemoRG
Id : /subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx/resourceGroups/A2AdemoRG/providers/Microsoft.Compute/virtualMachines/AzureDemoVM
VmId : 1b864902-c7ea-499a-ad0f-65da2930b81b
Name : AzureDemoVM
Type : Microsoft.Compute/virtualMachines
Location : eastus
Tags : {}
DiagnosticsProfile : {BootDiagnostics}
HardwareProfile : {VmSize}
NetworkProfile : {NetworkInterfaces}
OSProfile : {ComputerName, AdminUsername, WindowsConfiguration, Secrets}
ProvisioningState : Succeeded
StorageProfile : {ImageReference, OsDisk, DataDisks}
```

Get disk details for the virtual machine's disks. Disk details will be used later when starting replication for the virtual machine.

```
$OSDiskVhdURI = $VM.StorageProfile.OsDisk.Vhd
$dataDisk1VhdURI = $VM.StorageProfile.DataDisks[0].Vhd
```

## Create a Recovery Services vault

Create a resource group in which to create the Recovery Services vault.

### IMPORTANT

- The Recovery services vault and the virtual machines being protected, must be in different Azure locations.
- The resource group of the Recovery services vault, and the virtual machines being protected, must be in different Azure locations.
- The Recovery services vault, and the resource group to which it belongs, can be in the same Azure location.

In the example in this article, the virtual machine being protected is in the East US region. The recovery region selected for disaster recovery is the West US 2 region. The recovery services vault, and the resource group of the vault, are both in the recovery region, West US 2.

```
#Create a resource group for the recovery services vault in the recovery Azure region
New-AzResourceGroup -Name "a2ademorecoveryrg" -Location "West US 2"
```

```
ResourceGroupName : a2ademorecoveryrg
Location : westus2
ProvisioningState : Succeeded
Tags :
ResourceId : /subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx/resourceGroups/a2ademorecoveryrg
```

Create a Recovery services vault. In this example, a Recovery Services vault named `a2aDemoRecoveryVault` is created in the West US 2 region.

```
#Create a new Recovery services vault in the recovery region
$vault = New-AzRecoveryServicesVault -Name "a2aDemoRecoveryVault" -ResourceGroupName "a2ademorecoveryrg" -
Location "West US 2"

Write-Output $vault
```

```
Name : a2aDemoRecoveryVault
ID : /subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx/resourceGroups/a2ademorecoveryrg/providers/Microsoft.RecoveryServices/vaults/a2aDemoRecoveryVault
Type : Microsoft.RecoveryServices/vaults
Location : westus2
ResourceGroupName : a2ademorecoveryrg
SubscriptionId : xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
Properties : Microsoft.Azure.Commands.RecoveryServices.ARSVaultProperties
```

## Set the vault context

Set the vault context for use in the PowerShell session. After the vault context is set, Azure Site Recovery operations in the PowerShell session are performed in the context of the selected vault.

```
#Setting the vault context.
Set-AzRecoveryServicesAsrVaultContext -Vault $vault
```

ResourceName	ResourceGroupName	ResourceNamespace	ResourceType
a2aDemoRecoveryVault	a2ademorecoveryrg	Microsoft.RecoveryServices	Vaults

```
#Delete the downloaded vault settings file
Remove-Item -Path $Vaultsettingsfile.FilePath
```

For an Azure-to-Azure migration, you can set the vault context to the newly created vault:

```
#Set the vault context for the PowerShell session.
Set-AzRecoveryServicesAsrVaultContext -Vault $vault
```

## Prepare the vault to start replicating Azure virtual machines

### Create a Site Recovery fabric object to represent the primary (source) region

The fabric object in the vault represents an Azure region. The primary fabric object is created to represent the Azure region that virtual machines being protected to the vault belong to. In the example in this article, the virtual machine being protected is in the East US region.

- Only one fabric object can be created per region.
- If you've previously enabled Site Recovery replication for a VM in the Azure portal, Site Recovery creates a fabric object automatically. If a fabric object exists for a region, you can't create a new one.

Before you start, understand that Site Recovery operations are executed asynchronously. When you initiate an operation, an Azure Site Recovery job is submitted and a job tracking object is returned. Use the job tracking object to get the latest status for the job (`Get-AzRecoveryServicesAsrJob`), and to monitor the status of the operation.

```
#Create Primary ASR fabric
$tempASRJob = New-AzRecoveryServicesAsrFabric -Azure -Location 'East US' -Name "A2Ademo-EastUS"

Track Job status to check for completion
while (($tempASRJob.State -eq "InProgress") -or ($tempASRJob.State -eq "NotStarted")){
 #If the job hasn't completed, sleep for 10 seconds before checking the job status again
 sleep 10;
 $tempASRJob = Get-AzRecoveryServicesAsrJob -Job $tempASRJob
}

#Check if the Job completed successfully. The updated job state of a successfully completed job should be
#"Succeeded"
Write-Output $tempASRJob.State

$PrimaryFabric = Get-AzRecoveryServicesAsrFabric -Name "A2Ademo-EastUS"
```

If virtual machines from multiple Azure regions are being protected to the same vault, create one fabric object for each source Azure region.

### Create a Site Recovery fabric object to represent the recovery region

The recovery fabric object represents the recovery Azure location. If there's a failover, virtual machines are replicated and recovered to the recovery region represented by the recovery fabric. The recovery Azure region used in this example is West US 2.

```
#Create Recovery ASR fabric
$tempASRJob = New-AzRecoveryServicesAsrFabric -Azure -Location 'West US 2' -Name "A2Ademo-WestUS"

Track Job status to check for completion
while (($tempASRJob.State -eq "InProgress") -or ($tempASRJob.State -eq "NotStarted")){
 sleep 10;
 $tempASRJob = Get-AzRecoveryServicesAsrJob -Job $tempASRJob
}

#Check if the Job completed successfully. The updated job state of a successfully completed job should be
#"Succeeded"
Write-Output $tempASRJob.State

$RecoveryFabric = Get-AzRecoveryServicesAsrFabric -Name "A2Ademo-WestUS"
```

### Create a Site Recovery protection container in the primary fabric

The protection container is a container used to group replicated items within a fabric.

```

#Create a Protection container in the primary Azure region (within the Primary fabric)
$TempASRJob = New-AzRecoveryServicesAsrProtectionContainer -InputObject $PrimaryFabric -Name
"A2AEastUSProtectionContainer"

#Track Job status to check for completion
while (($TempASRJob.State -eq "InProgress") -or ($TempASRJob.State -eq "NotStarted")){
 sleep 10;
 $TempASRJob = Get-AzRecoveryServicesAsrJob -Job $TempASRJob
}

Write-Output $TempASRJob.State

$PrimaryProtContainer = Get-AzRecoveryServicesAsrProtectionContainer -Fabric $PrimaryFabric -Name
"A2AEastUSProtectionContainer"

```

## Create a Site Recovery protection container in the recovery fabric

```

#Create a Protection container in the recovery Azure region (within the Recovery fabric)
$TempASRJob = New-AzRecoveryServicesAsrProtectionContainer -InputObject $RecoveryFabric -Name
"A2AWestUSProtectionContainer"

#Track Job status to check for completion
while (($TempASRJob.State -eq "InProgress") -or ($TempASRJob.State -eq "NotStarted")){
 sleep 10;
 $TempASRJob = Get-AzRecoveryServicesAsrJob -Job $TempASRJob
}

#Check if the Job completed successfully. The updated job state of a successfully completed job should be
"Succeeded"

Write-Output $TempASRJob.State

$RecoveryProtContainer = Get-AzRecoveryServicesAsrProtectionContainer -Fabric $RecoveryFabric -Name
"A2AWestUSProtectionContainer"

```

## Create a replication policy

```

#Create replication policy
$TempASRJob = New-AzRecoveryServicesAsrPolicy -AzureToAzure -Name "A2APolicy" -RecoveryPointRetentionInHours
24 -ApplicationConsistentSnapshotFrequencyInHours 4

#Track Job status to check for completion
while (($TempASRJob.State -eq "InProgress") -or ($TempASRJob.State -eq "NotStarted")){
 sleep 10;
 $TempASRJob = Get-AzRecoveryServicesAsrJob -Job $TempASRJob
}

#Check if the Job completed successfully. The updated job state of a successfully completed job should be
"Succeeded"
Write-Output $TempASRJob.State

$ReplicationPolicy = Get-AzRecoveryServicesAsrPolicy -Name "A2APolicy"

```

## Create a protection container mapping between the primary and recovery protection container

A protection container mapping maps the primary protection container with a recovery protection container and a replication policy. Create one mapping for each replication policy that you'll use to replicate virtual machines between a protection container pair.

```

#Create Protection container mapping between the Primary and Recovery Protection Containers with the
Replication policy
$tempASRJob = New-AzRecoveryServicesAsrProtectionContainerMapping -Name "A2APrimaryToRecovery" -Policy
$ReplicationPolicy -PrimaryProtectionContainer $PrimaryProtContainer -RecoveryProtectionContainer
$RecoveryProtContainer

#Track Job status to check for completion
while (($tempASRJob.State -eq "InProgress") -or ($tempASRJob.State -eq "NotStarted")){
 sleep 10;
 $tempASRJob = Get-AzRecoveryServicesAsrJob -Job $tempASRJob
}

#Check if the Job completed successfully. The updated job state of a successfully completed job should be
"Succeeded"
Write-Output $tempASRJob.State

$eusToWusPCMapping = Get-AzRecoveryServicesAsrProtectionContainerMapping -ProtectionContainer
$PrimaryProtContainer -Name "A2APrimaryToRecovery"

```

### Create a protection container mapping for failback (reverse replication after a failover)

After a failover, when you're ready to bring the failed over virtual machine back to the original Azure region, you do a failback. To fail back, the failed over virtual machine is reverse replicated from the failed over region to the original region. For reverse replication the roles of the original region and the recovery region switch. The original region now becomes the new recovery region, and what was originally the recovery region now becomes the primary region. The protection container mapping for reverse replication represents the switched roles of the original and recovery regions.

```

#Create Protection container mapping (for fail back) between the Recovery and Primary Protection Containers
with the Replication policy
$tempASRJob = New-AzRecoveryServicesAsrProtectionContainerMapping -Name "A2ARecoveryToPrimary" -Policy
$ReplicationPolicy -PrimaryProtectionContainer $RecoveryProtContainer -RecoveryProtectionContainer
$PrimaryProtContainer

#Track Job status to check for completion
while (($tempASRJob.State -eq "InProgress") -or ($tempASRJob.State -eq "NotStarted")){
 sleep 10;
 $tempASRJob = Get-AzRecoveryServicesAsrJob -Job $tempASRJob
}

#Check if the Job completed successfully. The updated job state of a successfully completed job should be
"Succeeded"
Write-Output $tempASRJob.State

$wusToEusPCMapping = Get-AzRecoveryServicesAsrProtectionContainerMapping -ProtectionContainer
$RecoveryProtContainer -Name "A2ARecoveryToPrimary"

```

## Create cache storage account and target storage account

A cache storage account is a standard storage account in the same Azure region as the virtual machine being replicated. The cache storage account is used to hold replication changes temporarily, before the changes are moved to the recovery Azure region. You can choose to, but it's not necessary, to specify different cache storage accounts for the different disks of a virtual machine.

```

#create Cache storage account for replication logs in the primary region
$eastUSCacheStorageAccount = New-AzStorageAccount -Name "a2acachestorage" -ResourceGroupName "A2AdemoRG" -
Location 'East US' -SkuName Standard_LRS -Kind Storage

```

For virtual machines **not using managed disks**, the target storage account is the storage account in the recovery

region to which disks of the virtual machine are replicated. The target storage account can be either a standard storage account or a premium storage account. Select the kind of storage account required based on the data change rate (IO write rate) for the disks and the Azure Site Recovery supported churn limits for the storage type.

```
#Create Target storage account in the recovery region. In this case a Standard Storage account
$WestUSTargetStorageAccount = New-AzStorageAccount -Name "a2atargetstorage" -ResourceGroupName
"a2ademorecoveryrg" -Location 'West US 2' -SkuName Standard_LRS -Kind Storage
```

## Create network mappings

A network mapping maps virtual networks in the primary region to virtual networks in the recovery region. The network mapping specifies the Azure virtual network in the recovery region, that a virtual machine in the primary virtual network should fail over to. One Azure virtual network can be mapped to only a single Azure virtual network in a recovery region.

- Create an Azure virtual network in the recovery region to fail over to:

```
#Create a Recovery Network in the recovery region
$WestUSRecoveryVnet = New-AzVirtualNetwork -Name "a2arecoveryvnet" -ResourceGroupName
"a2ademorecoveryrg" -Location 'West US 2' -AddressPrefix "10.0.0.0/16"

Add-AzVirtualNetworkSubnetConfig -Name "default" -VirtualNetwork $WestUSRecoveryVnet -AddressPrefix
"10.0.0.0/20" | Set-AzVirtualNetwork

$WestUSRecoveryNetwork = $WestUSRecoveryVnet.Id
```

- Retrieve the primary virtual network. The VNet that the virtual machine is connected to:

```
#Retrieve the virtual network that the virtual machine is connected to

#Get first network interface card(nic) of the virtual machine
$SplitNicArmId = $VM.NetworkProfile.NetworkInterfaces[0].Id.split("/")

#Extract resource group name from the ResourceId of the nic
$NICRG = $SplitNicArmId[4]

#Extract resource name from the ResourceId of the nic
$NICname = $SplitNicArmId[-1]

#Get network interface details using the extracted resource group name and resource name
$NIC = Get-AzNetworkInterface -ResourceGroupName $NICRG -Name $NICname

#Get the subnet ID of the subnet that the nic is connected to
$PrimarySubnet = $NIC.IpConfigurations[0].Subnet

Extract the resource ID of the Azure virtual network the nic is connected to from the subnet ID
$EastUSPrimaryNetwork = (Split-Path(Split-Path($PrimarySubnet.Id))).Replace("\","/")
```

- Create network mapping between the primary virtual network and the recovery virtual network:

```

#Create an ASR network mapping between the primary Azure virtual network and the recovery Azure
virtual network
$TempASRJob = New-AzRecoveryServicesAsrNetworkMapping -AzureToAzure -Name "A2AEusToWusNwMapping" -
PrimaryFabric $PrimaryFabric -PrimaryAzureNetworkId $EastUSPrimaryNetwork -RecoveryFabric
$RecoveryFabric -RecoveryAzureNetworkId $WestUSRecoveryNetwork

#Track Job status to check for completion
while (($TempASRJob.State -eq "InProgress") -or ($TempASRJob.State -eq "NotStarted")){
 sleep 10;
 $TempASRJob = Get-AzRecoveryServicesAsrJob -Job $TempASRJob
}

#Check if the Job completed successfully. The updated job state of a successfully completed job
should be "Succeeded"
Write-Output $TempASRJob.State

```

- Create network mapping for the reverse direction (fail back):

```

#Create an ASR network mapping for fail back between the recovery Azure virtual network and the primary
Azure virtual network
$TempASRJob = New-AzRecoveryServicesAsrNetworkMapping -AzureToAzure -Name "A2AwusToEusNwMapping" -
PrimaryFabric $RecoveryFabric -PrimaryAzureNetworkId $WestUSRecoveryNetwork -RecoveryFabric
$PrimaryFabric -RecoveryAzureNetworkId $EastUSPrimaryNetwork

#Track Job status to check for completion
while (($TempASRJob.State -eq "InProgress") -or ($TempASRJob.State -eq "NotStarted")){
 sleep 10;
 $TempASRJob = Get-AzRecoveryServicesAsrJob -Job $TempASRJob
}

#Check if the Job completed successfully. The updated job state of a successfully completed job should
be "Succeeded"
Write-Output $TempASRJob.State

```

## Replicate Azure virtual machine

Replicate the Azure virtual machine with **managed disks**.

```

#Get the resource group that the virtual machine must be created in when failed over.
$RecoveryRG = Get-AzResourceGroup -Name "a2adomorecoveryrg" -Location "West US 2"

#Specify replication properties for each disk of the VM that is to be replicated (create disk replication configuration)

#OsDisk
$OSdiskId = $vm.StorageProfile.OsDisk.ManagedDisk.Id
$RecoveryOSDiskAccountType = $vm.StorageProfile.OsDisk.ManagedDisk.StorageAccountType
$RecoveryReplicaDiskAccountType = $vm.StorageProfile.OsDisk.ManagedDisk.StorageAccountType

$OSDiskReplicationConfig = New-AzRecoveryServicesAsrAzureToAzureDiskReplicationConfig -ManagedDisk -
LogStorageAccountId $EastUSCacheStorageAccount.Id `
 -DiskId $OSdiskId -RecoveryResourceGroupId $RecoveryRG.ResourceId -RecoveryReplicaDiskAccountType
$RecoveryReplicaDiskAccountType `
 -RecoveryTargetDiskAccountType $RecoveryOSDiskAccountType

Data disk
$datadiskId1 = $vm.StorageProfile.DataDisks[0].ManagedDisk.Id
$RecoveryReplicaDiskAccountType = $vm.StorageProfile.DataDisks[0].ManagedDisk.StorageAccountType
$RecoveryTargetDiskAccountType = $vm.StorageProfile.DataDisks[0].ManagedDisk.StorageAccountType

>DataDisk1ReplicationConfig = New-AzRecoveryServicesAsrAzureToAzureDiskReplicationConfig -ManagedDisk -
LogStorageAccountId $CacheStorageAccount.Id `
 -DiskId $datadiskId1 -RecoveryResourceGroupId $RecoveryRG.ResourceId -RecoveryReplicaDiskAccountType
$RecoveryReplicaDiskAccountType `
 -RecoveryTargetDiskAccountType $RecoveryTargetDiskAccountType

#Create a list of disk replication configuration objects for the disks of the virtual machine that are to be replicated.
$diskconfigs = @()
$diskconfigs += $OSDiskReplicationConfig, $DataDisk1ReplicationConfig

#Start replication by creating replication protected item. Using a GUID for the name of the replication protected item to ensure uniqueness of name.
$tempASRJob = New-AzRecoveryServicesAsrReplicationProtectedItem -AzureToAzure -AzureVmId $VM.Id -Name (New-Guid).Guid -ProtectionContainerMapping $EusToWusPCMapping -AzureToAzureDiskReplicationConfiguration
$diskconfigs -RecoveryResourceGroupId $RecoveryRG.ResourceId

```

Replicate the Azure virtual machine with **unmanaged disks**.

```

#Specify replication properties for each disk of the VM that is to be replicated (create disk replication configuration)

#Disk replication configuration for the OS disk
$OSDiskReplicationConfig = New-AzRecoveryServicesAsrAzureToAzureDiskReplicationConfig -VhdUri
$OSDiskVhdURI.Uri -LogStorageAccountId $EastUSCacheStorageAccount.Id -RecoveryAzureStorageAccountId
$WestUSTargetStorageAccount.Id

#Disk replication configuration for data disk
$dataDisk1ReplicationConfig = New-AzRecoveryServicesAsrAzureToAzureDiskReplicationConfig -VhdUri
$dataDisk1VhdURI.Uri -LogStorageAccountId $EastUSCacheStorageAccount.Id -RecoveryAzureStorageAccountId
$WestUSTargetStorageAccount.Id

#create a list of disk replication configuration objects for the disks of the virtual machine that are to be replicated.
$diskconfigs = @()
$diskconfigs += $OSDiskReplicationConfig, $dataDisk1ReplicationConfig

#get the resource group that the virtual machine must be created in when failed over.
$RecoveryRG = Get-AzResourceGroup -Name "a2ademozure" -Location "West US 2"

#Start replication by creating replication protected item. Using a GUID for the name of the replication protected item to ensure uniqueness of name.
$tempASRJob = New-AzRecoveryServicesAsrReplicationProtectedItem -AzureToAzure -AzureVmId $VM.Id -Name (New-Guid).Guid -ProtectionContainerMapping $EusToWusPCMapping -AzureToAzureDiskReplicationConfiguration
$diskconfigs -RecoveryResourceGroupId $RecoveryRG.ResourceId

#Track Job status to check for completion
while (($tempASRJob.State -eq "InProgress") -or ($tempASRJob.State -eq "NotStarted")){
 sleep 10;
 $tempASRJob = Get-AzRecoveryServicesAsrJob -Job $tempASRJob
}

#Check if the Job completed successfully. The updated job state of a successfully completed job should be "Succeeded"
Write-Output $tempASRJob.State

```

Once the start replication operation succeeds, virtual machine data is replicated to the recovery region.

The replication process starts by initially seeding a copy of the replicating disks of the virtual machine in the recovery region. This phase is called the initial replication phase.

After initial replication completes, replication moves to the differential synchronization phase. At this point, the virtual machine is protected and a test failover operation can be performed on it. The replication state of the replicated item representing the virtual machine goes to the **Protected** state after initial replication completes.

Monitor the replication state and replication health for the virtual machine by getting details of the replication protected item corresponding to it.

```
Get-AzRecoveryServicesAsrReplicationProtectedItem -ProtectionContainer $PrimaryProtContainer | Select FriendlyName, ProtectionState, ReplicationHealth
```

FriendlyName	ProtectionState	ReplicationHealth
AzureDemoVM	Protected	Normal

## Do a test failover, validate, and cleanup test failover

After replication for the virtual machine has reached a protected state, a test failover operation can be performed on the virtual machine (on the replication protected item of the virtual machine).

```
#Create a separate network for test failover (not connected to my DR network)
$TFOVnet = New-AzVirtualNetwork -Name "a2aTFOVnet" -ResourceGroupName "a2ademorecoveryrg" -Location 'West US 2' -AddressPrefix "10.3.0.0/16"

Add-AzVirtualNetworkSubnetConfig -Name "default" -VirtualNetwork $TFOVnet -AddressPrefix "10.3.0.0/20" | Set-AzVirtualNetwork

$TFONetwork= $TFOVnet.Id
```

Do a test failover.

```
$ReplicationProtectedItem = Get-AzRecoveryServicesAsrReplicationProtectedItem -FriendlyName "AzureDemoVM" -ProtectionContainer $PrimaryProtContainer

$TFOJob = Start-AzRecoveryServicesAsrTestFailoverJob -ReplicationProtectedItem $ReplicationProtectedItem -AzureVMNetworkId $TFONetwork -Direction PrimaryToRecovery
```

Wait for the test failover operation to complete.

```
Get-AzRecoveryServicesAsrJob -Job $TFOJob
```

```
Name : 3dcb043e-3c6d-4e0e-a42e-8d4245668547
ID : /Subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx/resourceGroups/a2ademorecoveryrg/providers/Microsoft.RecoveryServices/vaults/a2aDemoR
ecoverVault/replicationJobs/3dcb043e-3c6d-4e0e-a42e-8d4245668547
Type : Microsoft.RecoveryServices/vaults/replicationJobs
JobType : TestFailover
DisplayName : Test failover
ClientRequestId : 1ef8515b-b130-4452-a44d-91aa0f071931c ActivityId: 907bb2bc-ebe6-4732-8b66-77d0546eaba8
State : Succeeded
StateDescription : Completed
StartTime : 4/25/2018 4:29:43 AM
EndTime : 4/25/2018 4:33:06 AM
TargetObjectId : ce86206c-bd78-53b4-b004-39b722c1ac3a
TargetObjectType : ProtectionEntity
TargetObjectName : azuredemovm
AllowedActions :
Tasks : {Prerequisites check for test failover, Create test virtual machine, Preparing the virtual machine, Start the virtual machine}
Errors : {}
```

After the test failover job completes successfully, you can connect to the test failed over virtual machine, and validate the test failover.

Once testing is complete on the test failed over virtual machine, clean up the test copy by starting the cleanup test failover operation. This operation deletes the test copy of the virtual machine that was created by the test failover.

```
$Job_TFOCleanup = Start-AzRecoveryServicesAsrTestFailoverCleanupJob -ReplicationProtectedItem $ReplicationProtectedItem

Get-AzRecoveryServicesAsrJob -Job $Job_TFOCleanup | Select State
```

```
State

Succeeded
```

## Fail over to Azure

Fail over the virtual machine to a specific recovery point.

```
$RecoveryPoints = Get-AzRecoveryServicesAsrRecoveryPoint -ReplicationProtectedItem $ReplicationProtectedItem

#The list of recovery points returned may not be sorted chronologically and will need to be sorted first, in
order to be able to find the oldest or the latest recovery points for the virtual machine.
"{0} {1}" -f $RecoveryPoints[0].RecoveryPointType, $RecoveryPoints[-1].RecoveryPointTime
```

```
CrashConsistent 4/24/2018 11:10:25 PM
```

```
#Start the fail over job
$Job_Failover = Start-AzRecoveryServicesAsrUnplannedFailoverJob -ReplicationProtectedItem
$ReplicationProtectedItem -Direction PrimaryToRecovery -RecoveryPoint $RecoveryPoints[-1]

do {
 $Job_Failover = Get-AzRecoveryServicesAsrJob -Job $Job_Failover;
 sleep 30;
} while (($Job_Failover.State -eq "InProgress") -or ($JobFailover.State -eq "NotStarted"))

$Job_Failover.State
```

```
Succeeded
```

When the failover job is successful, you can commit the failover operation.

```
$CommitFailoverJob = Start-AzRecoveryServicesAsrCommitFailoverJob -ReplicationProtectedItem
$ReplicationProtectedItem

Get-AzRecoveryServicesAsrJob -Job $CommitFailoverJob
```

```
Name : 58afc2b7-5cfe-4da9-83b2-6df358c6e4ff
ID : /Subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx/resourceGroups/a2ademozurecoveryrg/providers/Microsoft.RecoveryServices/vaults/a2aDemoR
 ecoveryVault/replicationJobs/58afc2b7-5cfe-4da9-83b2-6df358c6e4ff
Type : Microsoft.RecoveryServices/vaults/replicationJobs
JobType : CommitFailover
DisplayName: Commit
ClientRequestId : 10a95d6c-359e-4603-b7d9-b7ee3317ce94 ActivityId: 8751ada4-fc42-4238-8de6-a82618408fcf
State : Succeeded
StateDescription : Completed
StartTime : 4/25/2018 4:50:58 AM
EndTime : 4/25/2018 4:51:01 AM
TargetObjectId : ce86206c-bd78-53b4-b004-39b722c1ac3a
TargetObjectType : ProtectionEntity
TargetObjectName : azuredemovm
AllowedActions :
Tasks : {Prerequisite check, Commit}
Errors : {}
```

## Reprotect and fail back to the source region

After a failover, when you're ready to go back to the original region, start reverse replication for the replication protected item using the `Update-AzRecoveryServicesAsrProtectionDirection` cmdlet.

```
#Create Cache storage account for replication logs in the primary region
$WestUSCacheStorageAccount = New-AzStorageAccount -Name "a2acachestoragewestus" -ResourceGroupName
"A2AdemoRG" -Location 'West US' -SkuName Standard_LRS -Kind Storage
```

```
#Use the recovery protection container, new cache storage account in West US and the source region VM
resource group
Update-AzRecoveryServicesAsrProtectionDirection -ReplicationProtectedItem $ReplicationProtectedItem -
AzureToAzure
-ProtectionContainerMapping $WusToEusPCMapping -LogStorageAccountId $WestUSCacheStorageAccount.Id -
RecoveryResourceGroupID $sourceVMResourcegroup.ResourceId
```

After reprotection is complete, you can fail over in the reverse direction, West US to East US, and fail back to source region.

## Disable replication

You can disable replication with the `Remove-AzRecoveryServicesAsrReplicationProtectedItem` cmdlet.

```
Remove-AzRecoveryServicesAsrReplicationProtectedItem -ReplicationProtectedItem $ReplicatedItem
```

## Next steps

View the [Azure Site Recovery PowerShell reference](#) to learn how you can do other tasks such as creating recovery plans and testing failover of recovery plans with PowerShell.

# Set up disaster recovery of VMware VMs to Azure with PowerShell

1/10/2020 • 13 minutes to read • [Edit Online](#)

In this article, you see how to replicate and failover VMware virtual machines to Azure using Azure PowerShell.

You learn how to:

- Create a Recovery Services vault and set the vault context.
- Validate server registration in the vault.
- Set up replication, including a replication policy. Add your vCenter server and discover VMs.
- Add a vCenter server and discover
- Create storage accounts to hold replication logs or data, and replicate the VMs.
- Perform a failover. Configure failover settings, perform a settings for replicating virtual machines.

## NOTE

This article has been updated to use the new Azure PowerShell Az module. You can still use the AzureRM module, which will continue to receive bug fixes until at least December 2020. To learn more about the new Az module and AzureRM compatibility, see [Introducing the new Azure PowerShell Az module](#). For Az module installation instructions, see [Install Azure PowerShell](#).

## Prerequisites

Before you start:

- Make sure that you understand the [scenario architecture and components](#).
- Review the [support requirements](#) for all components.
- You have the Azure PowerShell `Az` module. If you need to install or upgrade Azure PowerShell, follow this [Guide to install and configure Azure PowerShell](#).

## Log into Azure

Log into your Azure subscription using the `Connect-AzAccount` cmdlet:

```
Connect-AzAccount
```

Select the Azure subscription you want to replicate your VMware virtual machines to. Use the `Get-AzSubscription` cmdlet to get the list of Azure subscriptions you have access to. Select the Azure subscription to work with using the `Select-AzSubscription` cmdlet.

```
Select-AzSubscription -SubscriptionName "ASR Test Subscription"
```

## Set up a Recovery Services vault

1. Create a resource group in which to create the Recovery Services vault. In the example below, the resource group is named `VMwareDRtoAzurePS` and is created in the East Asia region.

```
New-AzResourceGroup -Name "VMwareDRtoAzurePS" -Location "East Asia"
```

```
ResourceGroupName : VMwareDRtoAzurePS
Location : eastasia
ProvisioningState : Succeeded
Tags :
ResourceId : /subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx/resourceGroups/VMwareDRtoAzurePS
```

2. Create a Recovery services vault. In the example below, the Recovery services vault is named VMwareDRTToAzurePs, and is created in the East Asia region and in the resource group created in the previous step.

```
New-AzRecoveryServicesVault -Name "VMwareDRTToAzurePs" -Location "East Asia" -ResourceGroupName "VMwareDRTToAzurePs"
```

```
Name : VMwareDRTToAzurePs
ID : /subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx/resourceGroups/VMwareDRTToAzurePs/providers/Microsoft.RecoveryServices/vaults/VMwareDRTToAzu
rePs
Type : Microsoft.RecoveryServices/vaults
Location : eastasia
ResourceGroupName : VMwareDRTToAzurePs
SubscriptionId : xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
Properties : Microsoft.Azure.Commands.RecoveryServices.ARSVaultProperties
```

3. Download the vault registration key for the vault. The vault registration key is used to register the on-premises Configuration Server to this vault. Registration is part of the Configuration Server software installation process.

```
#Get the vault object by name and resource group and save it to the $vault PowerShell variable
$vault = Get-AzRecoveryServicesVault -Name "VMwareDRTToAzurePS" -ResourceGroupName "VMwareDRTToAzurePS"

#Download vault registration key to the path C:\Work
Get-AzRecoveryServicesVaultSettingsFile -SiteRecovery -Vault $Vault -Path "C:\Work\"
```

```
FilePath

C:\Work\VMwareDRTToAzurePs_2017-11-23T19-52-34.VaultCredentials
```

4. Use the downloaded vault registration key and follow the steps in the articles given below to complete installation and registration of the Configuration Server.

- [Choose your protection goals](#)
- [Set up the source environment](#)

### Set the vault context

Set the vault context using the Set-ASRVaultContext cmdlet. Once set, subsequent Azure Site Recovery operations in the PowerShell session are performed in the context of the selected vault.

## TIP

The Azure Site Recovery PowerShell module (Az.RecoveryServices module) comes with easy to use aliases for most cmdlets. The cmdlets in the module take the form <Operation>-**AzRecoveryServicesAsr**<Object> and have equivalent aliases that take the form <Operation>-**ASR**<Object>. You can replace the cmdlet aliases for ease of use.

In the example below, the vault details from the \$vault variable is used to specify the vault context for the PowerShell session.

```
Set-ASRVaultContext -Vault $vault
```

ResourceName	ResourceGroupName	ResourceNamespace	ResourceType
VMwareDRToAzurePs	VMwareDRToAzurePs	Microsoft.RecoveryServices	vaults

As an alternative to the Set-ASRVaultContext cmdlet, one can also use the Import-AzRecoveryServicesAsrVaultSettingsFile cmdlet to set the vault context. Specify the path at which the vault registration key file is located as the -path parameter to the Import-AzRecoveryServicesAsrVaultSettingsFile cmdlet. For example:

```
Get-AzRecoveryServicesVaultSettingsFile -SiteRecovery -Vault $Vault -Path "C:\Work\"
Import-AzRecoveryServicesAsrVaultSettingsFile -Path "C:\Work\VMwareDRToAzurePs_2017-11-23T19-52-
34.VaultCredentials"
```

Subsequent sections of this article assume that the vault context for Azure Site Recovery operations has been set.

## Validate vault registration

For this example, we have the following:

- A configuration server (**ConfigurationServer**) has been registered to this vault.
  - An additional process server (**ScaleOut-ProcessServer**) has been registered to *ConfigurationServer*
  - Accounts (**vCenter\_account**, **WindowsAccount**, **LinuxAccount**) have been set up on the Configuration server. These accounts are used to add the vCenter server, to discover virtual machines, and to push-install the mobility service software on Windows and Linux servers that are to be replicated.
1. Registered configuration servers are represented by a fabric object in Site Recovery. Get the list of fabric objects in the vault and identify the configuration server.

```
Verify that the Configuration server is successfully registered to the vault
$ASRFabrics = Get-AzRecoveryServicesAsrFabric
$ASRFabrics.count
```

1

```
#Print details of the Configuration Server
$ASRFabrics[0]
```

```

Name : 2c33d710a5ee6af753413e97f01e314fc75938ea4e9ac7bafbf4a31f6804460d
FriendlyName : ConfigurationServer
ID : /Subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxx/resourceGroups/VMwareDRToAzurePs/providers/Microsoft.RecoveryServices/vaults/VMwareDRToAzurePs/replicationFabrics
 /2c33d710a5ee6af753413e97f01e314fc75938ea4e9ac7bafbf4a31f6804460d
Type : Microsoft.RecoveryServices/vaults/replicationFabrics
FabricType : VMware
SiteIdentifier : ef7a1580-f356-4a00-aa30-7bf80f952510
FabricSpecificDetails : Microsoft.Azure.Commands.RecoveryServices.SiteRecovery.ASRVMWareSpecificDetails

```

- Identify the process servers that can be used to replicate machines.

```

$ProcessServers = $ASRFabrics[0].FabricSpecificDetails.ProcessServers
for($i=0; $i -lt $ProcessServers.count; $i++) {
 "{0,-5} {1}" -f $i, $ProcessServers[$i].FriendlyName
}

```

```

0 ScaleOut-ProcessServer
1 ConfigurationServer

```

From the output above **\$ProcessServers[0]** corresponds to *ScaleOut-ProcessServer* and **\$ProcessServers[1]** corresponds to the Process Server role on *ConfigurationServer*

- Identify accounts that have been set up on the Configuration Server.

```

$AccountHandles = $ASRFabrics[0].FabricSpecificDetails.RunAsAccounts
#Print the account details
$AccountHandles

```

AccountId	AccountName
1	vCenter_account
2	WindowsAccount
3	LinuxAccount

From the output above **\$AccountHandles[0]** corresponds to the account *vCenter\_account*, **\$AccountHandles[1]** to account *WindowsAccount*, and **\$AccountHandles[2]** to account *LinuxAccount*

## Create a replication policy

In this step, two replication policies are created. One policy to replicate VMware virtual machines to Azure, and the other to replicate failed over virtual machines running in Azure back to the on-premises VMware site.

### NOTE

Most Azure Site Recovery operations are executed asynchronously. When you initiate an operation, an Azure Site Recovery job is submitted and a job tracking object is returned. This job tracking object can be used to monitor the status of the operation.

- Create a replication policy named *ReplicationPolicy* to replicate VMware virtual machines to Azure with the specified properties.

```

$Job_PolicyCreate = New-AzRecoveryServicesAsrPolicy -VmwareToAzure -Name "ReplicationPolicy" -
RecoveryPointRetentionInHours 24 -ApplicationConsistentSnapshotFrequencyInHours 4 -
RPOWarningThresholdInMinutes 60

Track Job status to check for completion
while (($Job_PolicyCreate.State -eq "InProgress") -or ($Job_PolicyCreate.State -eq "NotStarted")){
 sleep 10;
 $Job_PolicyCreate = Get-ASRJob -Job $Job_PolicyCreate
}

#Display job status
$Job_PolicyCreate

```

```

Name : 8d18e2d9-479f-430d-b76b-6bc7eb2d0b3e
ID : /Subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxx/resourceGroups/VMwareDRToAzurePs/providers/Microsoft.RecoveryServices/vaults/VMwareDRToAzurePs/replicationJobs/8d18e2d9-479f-430d-b76b-6bc7eb2d0b3e
Type :
JobType : AddProtectionProfile
DisplayName : Create replication policy
ClientRequestId : a162b233-55d7-4852-abac-3d595a1faac2 ActivityId: 9895234a-90ea-4c1a-83b5-1f2c6586252a
State : Succeeded
StateDescription : Completed
StartTime : 11/24/2017 2:49:24 AM
EndTime : 11/24/2017 2:49:23 AM
TargetObjectId : ab31026e-4866-5440-969a-8ebcb13a372f
TargetObjectType : ProtectionProfile
TargetObjectName : ReplicationPolicy
AllowedActions :
Tasks : {Prerequisites check for creating the replication policy, Creating the replication policy}
Errors : {}

```

## 2. Create a replication policy to use for failback from Azure to the on-premises VMware site.

```

$Job_FailbackPolicyCreate = New-AzRecoveryServicesAsrPolicy -AzureToVmware -Name "ReplicationPolicy-Failback" -RecoveryPointRetentionInHours 24 -ApplicationConsistentSnapshotFrequencyInHours 4 -RPOWarningThresholdInMinutes 60

```

Use the job details in `$Job_FailbackPolicyCreate` to track the operation to completion.

- Create a protection container mapping to map replication policies with the Configuration Server.

```

#Get the protection container corresponding to the Configuration Server
$ProtectionContainer = Get-AzRecoveryServicesAsrProtectionContainer -Fabric $ASRFabrics[0]

#Get the replication policies to map by name.
$ReplicationPolicy = Get-AzRecoveryServicesAsrPolicy -Name "ReplicationPolicy"
$FallbackReplicationPolicy = Get-AzRecoveryServicesAsrPolicy -Name "ReplicationPolicy-Failback"

Associate the replication policies to the protection container corresponding to the Configuration
Server.

$Job_AssociatePolicy = New-AzRecoveryServicesAsrProtectionContainerMapping -Name "PolicyAssociation1" -
PrimaryProtectionContainer $ProtectionContainer -Policy $ReplicationPolicy

Check the job status
while (($Job_AssociatePolicy.State -eq "InProgress") -or ($Job_AssociatePolicy.State -eq "NotStarted"))
{
 sleep 10;
 $Job_AssociatePolicy = Get-ASRJob -Job $Job_AssociatePolicy
}
$Job_AssociatePolicy.State

<# In the protection container mapping used for failback (replicating failed over virtual machines
running in Azure, to the primary VMware site.) the protection container corresponding to the
Configuration server acts as both the Primary protection container and the recovery protection
container
#>
$Job_AssociateFallbackPolicy = New-AzRecoveryServicesAsrProtectionContainerMapping -Name
"FailbackPolicyAssociation" -PrimaryProtectionContainer $ProtectionContainer -
RecoveryProtectionContainer $ProtectionContainer -Policy $FallbackReplicationPolicy

Check the job status
while (($Job_AssociateFallbackPolicy.State -eq "InProgress") -or ($Job_AssociateFallbackPolicy.State -
eq "NotStarted")){
 sleep 10;
 $Job_AssociateFallbackPolicy = Get-ASRJob -Job $Job_AssociateFallbackPolicy
}
$Job_AssociateFallbackPolicy.State

```

## Add a vCenter server and discover VMs

Add a vCenter Server by IP address or hostname. The **-port** parameter specifies the port on the vCenter server to connect to, **-Name** parameter specifies a friendly name to use for the vCenter server, and the **-Account** parameter specifies the account handle on the Configuration server to use to discover virtual machines managed by the vCenter server.

```

The $AccountHandles[0] variable holds details of vCenter_account

$Job_AddvCenterServer = New-AzRecoveryServicesAsrvCenter -Fabric $ASRFabrics[0] -Name "MyvCenterServer" -
IpOrHostName "10.150.24.63" -Account $AccountHandles[0] -Port 443

#Wait for the job to complete and ensure it completed successfully

while (($Job_AddvCenterServer.State -eq "InProgress") -or ($Job_AddvCenterServer.State -eq "NotStarted")) {
 sleep 30;
 $Job_AddvCenterServer = Get-ASRJob -Job $Job_AddvCenterServer
}
$Job_AddvCenterServer

```

```

Name : 0f76f937-f9cf-4e0e-bf27-10c9d1c252a4
ID : /Subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx/resourceGroups/VMwareDRToAzurePs/providers/Microsoft.RecoveryServices/vaults/VMwareDRToAzurePs/r
eplicationJobs/0f76f93
 7-f9cf-4e0e-bf27-10c9d1c252a4
Type :
JobType : DiscoverVCenter
DisplayName : Add vCenter server
ClientRequestId : a2af8892-5686-4d64-a528-10445bc2f698 ActivityId: 7ec05aad-002e-4da0-991f-95d0de7a9f3a
State : Succeeded
StateDescription : Completed
StartTime : 11/24/2017 2:41:47 AM
EndTime : 11/24/2017 2:44:37 AM
TargetObjectId : 10.150.24.63
TargetObjectType : VCenter
TargetObjectName : MyvCenterServer
AllowedActions :
Tasks : {Adding vCenter server}
Errors : {}

```

## Create storage accounts for replication

**To write to managed disk, use [Powershell Az.RecoveryServices module 2.0.0 onwards](#).** It only requires creation of a log storage account. It is recommended to use a standard account type and LRS redundancy since it is used to store only temporary logs. Ensure that the storage account is created in the same Azure region as the vault.

If you are using a version of Az.RecoveryServices module older than 2.0.0, use the following steps to create storage accounts. These storage accounts are used later to replicate virtual machines. Ensure that the storage accounts are created in the same Azure region as the vault. You can skip this step if you plan to use an existing storage account for replication.

### NOTE

While replicating on-premises virtual machines to a premium storage account, you need to specify an additional standard storage account (log storage account). The log storage account holds replication logs as an intermediate store until the logs can be applied on the premium storage target.

```

$PremiumStorageAccount = New-AzStorageAccount -ResourceGroupName "VMwareDRToAzurePs" -Name
"premiumstorageaccount1" -Location "East Asia" -SkuName Premium_LRS

$LogStorageAccount = New-AzStorageAccount -ResourceGroupName "VMwareDRToAzurePs" -Name "logstorageaccount1" -
Location "East Asia" -SkuName Standard_LRS

$ReplicationStdStorageAccount= New-AzStorageAccount -ResourceGroupName "VMwareDRToAzurePs" -Name
"replicationstdstorageaccount1" -Location "East Asia" -SkuName Standard_LRS

```

## Replicate VMware VMs

It takes about 15-20 minutes for virtual machines to be discovered from the vCenter server. Once discovered, a protectable item object is created in Azure Site Recovery for each discovered virtual machine. In this step, three of the discovered virtual machines are replicated to the Azure Storage accounts created in the previous step.

You will need the following details to protect a discovered virtual machine:

- The protectable item to be replicated.

- The storage account to replicate the virtual machine to (only if you are replicating to storage account).
- A log storage is needed to protect virtual machines to a premium storage account or to a managed disk.
- The Process Server to be used for replication. The list of available process servers has been retrieved and saved in the **\$ProcessServers[0]** (*ScaleOut-ProcessServer*) and **\$ProcessServers[1]** (*ConfigurationServer*) variables.
- The account to use to push-install the Mobility service software onto the machines. The list of available accounts has been retrieved and stored in the **\$AccountHandles** variable.
- The protection container mapping for the replication policy to be used for replication.
- The resource group in which virtual machines must be created on failover.
- Optionally, the Azure virtual network and subnet to which the failed over virtual machine should be connected.

Now replicate the following virtual machines using the settings specified in this table

VIRTUAL MACHINE	PROCESS SERVER	STORAGE ACCOUNT	LOG STORAGE ACCOUNT	POLICY	ACCOUNT FOR MOBILITY SERVICE INSTALLATION	TARGET RESOURCE GROUP	TARGET VIRTUAL NETWORK	TARGET SUBNET
CentOSV M1	Configura tionServer	N/A	logstorag eaccount 1	Replicatio nPolicy	LinuxAcco unt	VMwareD RToAzure Ps	ASR-vnet	Subnet-1
Win2K12 VM1	ScaleOut- ProcessSe rver	premiums torageacc ount1	logstorag eaccount 1	Replicatio nPolicy	Windows Account	VMwareD RToAzure Ps	ASR-vnet	Subnet-1
CentOSV M2	Configura tionServer	replicatio nstdstora geaccoun t1	N/A	Replicatio nPolicy	LinuxAcco unt	VMwareD RToAzure Ps	ASR-vnet	Subnet-1

```

#Get the target resource group to be used
$ResourceGroup = Get-AzResourceGroup -Name "VMwareToAzureDrPs"

#Get the target virtual network to be used
$RecoveryVnet = Get-AzVirtualNetwork -Name "ASR-vnet" -ResourceGroupName "asrrg"

#Get the protection container mapping for replication policy named ReplicationPolicy
$PolicyMap = Get-AzRecoveryServicesAsrProtectionContainerMapping -ProtectionContainer $ProtectionContainer | where PolicyFriendlyName -eq "ReplicationPolicy"

#Get the protectable item corresponding to the virtual machine CentOSVM1
$VM1 = Get-AzRecoveryServicesAsrProtectableItem -ProtectionContainer $ProtectionContainer -FriendlyName "CentOSVM1"

Enable replication for virtual machine CentOSVM1 using the Az.RecoveryServices module 2.0.0 onwards to replicate to managed disks
The name specified for the replicated item needs to be unique within the protection container. Using a random GUID to ensure uniqueness
$Job_EnableReplication1 = New-AzRecoveryServicesAsrReplicationProtectedItem -VmwareToAzure -ProtectableItem $VM1 -Name (New-Guid).Guid -ProtectionContainerMapping $PolicyMap -ProcessServer $ProcessServers[1] -Account $AccountHandles[2] -RecoveryResourceGroupId $ResourceGroup.ResourceId -logStorageAccountId $LogStorageAccount.Id -RecoveryAzureNetworkId $RecoveryVnet.Id -RecoveryAzureSubnetName "Subnet-1"

Alternatively, if the virtual machine CentOSVM1 has CMK enabled disks, enable replication using Az module 3.3.0 onwards as below
$diskID is the Disk Encryption Set ID to be used for all replica managed disks and target managed disks in the target region
$Job_EnableReplication1 = New-AzRecoveryServicesAsrReplicationProtectedItem -VmwareToAzure -ProtectableItem $VM1 -Name (New-Guid).Guid -ProtectionContainerMapping $PolicyMap -ProcessServer $ProcessServers[1] -Account $AccountHandles[2] -RecoveryResourceGroupId $ResourceGroup.ResourceId -logStorageAccountId -DiskEncryptionSetId $diskId $LogStorageAccount.Id -RecoveryAzureNetworkId $RecoveryVnet.Id -RecoveryAzureSubnetName "Subnet-1"

#Get the protectable item corresponding to the virtual machine Win2K12VM1
$VM2 = Get-AzRecoveryServicesAsrProtectableItem -ProtectionContainer $ProtectionContainer -FriendlyName "Win2K12VM1"

Enable replication for virtual machine Win2K12VM1
$Job_EnableReplication2 = New-AzRecoveryServicesAsrReplicationProtectedItem -VmwareToAzure -ProtectableItem $VM2 -Name (New-Guid).Guid -ProtectionContainerMapping $PolicyMap -RecoveryAzureStorageAccountId $PremiumStorageAccount.Id -LogStorageAccountId $LogStorageAccount.Id -ProcessServer $ProcessServers[0] -Account $AccountHandles[1] -RecoveryResourceGroupId $ResourceGroup.ResourceId -RecoveryAzureNetworkId $RecoveryVnet.Id -RecoveryAzureSubnetName "Subnet-1"

#Get the protectable item corresponding to the virtual machine CentOSVM2
$VM3 = Get-AzRecoveryServicesAsrProtectableItem -ProtectionContainer $ProtectionContainer -FriendlyName "CentOSVM2"

Enable replication for virtual machine CentOSVM2
$Job_EnableReplication3 = New-AzRecoveryServicesAsrReplicationProtectedItem -VmwareToAzure -ProtectableItem $VM3 -Name (New-Guid).Guid -ProtectionContainerMapping $PolicyMap -RecoveryAzureStorageAccountId $ReplicationStdStorageAccount.Id -ProcessServer $ProcessServers[1] -Account $AccountHandles[2] -RecoveryResourceGroupId $ResourceGroup.ResourceId -RecoveryAzureNetworkId $RecoveryVnet.Id -RecoveryAzureSubnetName "Subnet-1"

```

Once the enable replication job completes successfully, initial replication is started for the virtual machines. Initial replication may take a while depending on the amount of data to be replicated and the bandwidth available for replication. After initial replication completes, the virtual machine moves to a protected state. Once the virtual machine reaches a protected state you can perform a test failover for the virtual machine, add it to recovery plans etc.

You can check the replication state and replication health of the virtual machine with the Get-ASRReplicationProtectedItem cmdlet.

```
Get-AzRecoveryServicesAsrReplicationProtectedItem -ProtectionContainer $ProtectionContainer | Select
FriendlyName, ProtectionState, ReplicationHealth
```

FriendlyName	ProtectionState	ReplicationHealth
CentOSVM1	Protected	Normal
CentOSVM2	InitialReplicationInProgress	Normal
Win2K12VM1	Protected	Normal

## Configure failover settings

Failover settings for protected machines can be updated using the Set-ASRReplicationProtectedItem cmdlet. Some of the settings that can be updated through this cmdlet are:

- Name of the virtual machine to be created on failover
- VM size of the virtual machine to be created on failover
- Azure virtual network and subnet that the NICs of the virtual machine should be connected to on failover
- Failover to managed disks
- Apply Azure Hybrid Use Benefit
- Assign a static IP address from the target virtual network to be assigned to the virtual machine on failover.

In this example, we update the VM size of the virtual machine to be created on failover for the virtual machine *Win2K12VM1* and specify that the virtual machine use managed disks on failover.

```
$ReplicatedVM1 = Get-AzRecoveryServicesAsrReplicationProtectedItem -FriendlyName "Win2K12VM1" -
ProtectionContainer $ProtectionContainer

Set-AzRecoveryServicesAsrReplicationProtectedItem -InputObject $ReplicatedVM1 -Size "Standard_DS11" -
UseManagedDisk True
```

```
Name : cafa459c-44a7-45b0-9de9-3d925b0e7db9
ID : /Subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxx/resourceGroups/VMwareDRToAzurePs/providers/Microsoft.RecoveryServices/vaults/VMwareDRToAzurePs/r
eplicationJobs/cafa459
 c-44a7-45b0-9de9-3d925b0e7db9
Type :
JobType : UpdateVmProperties
DisplayName : Update the virtual machine
ClientRequestId : b0b51b2a-f151-4e9a-a98e-064a5b5131f3 ActivityId: ac2ba316-be7b-4c94-a053-5363f683d38f
State : InProgress
StateDescription : InProgress
StartTime : 11/24/2017 2:04:26 PM
EndTime :
TargetObjectId : 88bc391e-d091-11e7-9484-000c2955bb50
TargetObjectType : ProtectionEntity
TargetObjectName : Win2K12VM1
AllowedActions :
Tasks : {Update the virtual machine properties}
Errors : {}
```

## Run a test failover

1. Run a DR drill (test failover) as follows:

```

#Test failover of Win2K12VM1 to the test virtual network "V2TestNetwork"

#Get details of the test failover virtual network to be used
$TestFailovervnet = Get-AzVirtualNetwork -Name "V2TestNetwork" -ResourceGroupName "asrrg"

#Start the test failover operation
$TFOJob = Start-AzRecoveryServicesAsrTestFailoverJob -ReplicationProtectedItem $ReplicatedVM1 -
AzureVMNetworkId $TestFailovervnet.Id -Direction PrimaryToRecovery

```

2. Once the test failover job completes successfully, you will notice that a virtual machine suffixed with "-Test" (Win2K12VM1-Test in this case) to its name is created in Azure.
3. You can now connect to the test failed over virtual machine, and validate the test failover.
4. Clean up the test failover using the Start-ASRTTestFailoverCleanupJob cmdlet. This operation deletes the virtual machine created as part of the test failover operation.

```

$Job_TFOCleanup = Start-AzRecoveryServicesAsrTestFailoverCleanupJob -ReplicationProtectedItem
$ReplicatedVM1

```

## Fail over to Azure

In this step, we fail over the virtual machine Win2K12VM1 to a specific recovery point.

1. Get a list of available recovery points to use for the failover:

```

Get the list of available recovery points for Win2K12VM1
$RecoveryPoints = Get-AzRecoveryServicesAsrRecoveryPoint -ReplicationProtectedItem $ReplicatedVM1
"{0} {1}" -f $RecoveryPoints[0].RecoveryPointType, $RecoveryPoints[0].RecoveryPointTime

```

```
CrashConsistent 11/24/2017 5:28:25 PM
```

```

#Start the failover job
$Job_Failover = Start-AzRecoveryServicesAsrUnplannedFailoverJob -ReplicationProtectedItem
$ReplicatedVM1 -Direction PrimaryToRecovery -RecoveryPoint $RecoveryPoints[0]
do {
 $Job_Failover = Get-ASRJob -Job $Job_Failover;
 sleep 60;
} while (($Job_Failover.State -eq "InProgress") -or ($JobFailover.State -eq "NotStarted"))
$Job_Failover.State

```

```
Succeeded
```

2. Once failed over successfully, you can commit the failover operation, and set up reverse replication from Azure back to the on-premises VMware site.

## Next steps

Learn how to automate more tasks using the [Azure Site Recovery PowerShell reference](#).

# Set up disaster recovery to Azure for Hyper-V VMs using PowerShell and Azure Resource Manager

1/28/2020 • 7 minutes to read • [Edit Online](#)

Azure Site Recovery contributes to your business continuity and disaster recovery (BCDR) strategy by orchestrating replication, failover, and recovery of Azure virtual machines (VMs), and on-premises VMs and physical servers.

This article describes how to use Windows PowerShell, together with Azure Resource Manager, to replicate Hyper-V VMs to Azure. The example used in this article shows you how to replicate a single VM running on a Hyper-V host, to Azure.

## NOTE

This article has been updated to use the new Azure PowerShell Az module. You can still use the AzureRM module, which will continue to receive bug fixes until at least December 2020. To learn more about the new Az module and AzureRM compatibility, see [Introducing the new Azure PowerShell Az module](#). For Az module installation instructions, see [Install Azure PowerShell](#).

## Azure PowerShell

Azure PowerShell provides cmdlets to manage Azure using Windows PowerShell. Site Recovery PowerShell cmdlets, available with Azure PowerShell for Azure Resource Manager, help you protect and recover your servers in Azure.

You don't need to be a PowerShell expert to use this article, but you do need to understand basic concepts, such as modules, cmdlets, and sessions. For more information, see the [PowerShell Documentation](#) and [Using Azure PowerShell with Azure Resource Manager](#).

## NOTE

Microsoft partners in the Cloud Solution Provider (CSP) program can configure and manage protection of customer servers to their respective CSP subscriptions (tenant subscriptions).

## Before you start

Make sure you have these prerequisites in place:

- A Microsoft Azure account. You can start with a [free trial](#). In addition, you can read about [Azure Site Recovery Manager pricing](#).
- Azure PowerShell. For information about this release and how to install it, see [Install Azure PowerShell](#).

In addition, the specific example described in this article has the following prerequisites:

- A Hyper-V host running Windows Server 2012 R2 or Microsoft Hyper-V Server 2012 R2 containing one or more VMs. Hyper-V servers should be connected to the Internet, either directly or through a proxy.
- The VMs you want to replicate should conform with [these prerequisites](#).

## Step 1: Sign in to your Azure account

1. Open a PowerShell console and run this command to sign in to your Azure account. The cmdlet brings up a web page prompts you for your account credentials: `Connect-AzAccount`.

- Alternately, you can include your account credentials as a parameter in the `Connect-AzAccount` cmdlet, using the **Credential** parameter.
- If you're a CSP partner working on behalf of a tenant, specify the customer as a tenant, by using their tenantID or tenant primary domain name. For example: `Connect-AzAccount -Tenant "fabrikam.com"`

2. Associate the subscription you want to use with the account, since an account can have several subscriptions:

```
Set-AzContext -Subscription $SubscriptionName
```

3. Verify that your subscription is registered to use the Azure providers for Recovery Services and Site Recovery, using these commands:

```
Get-AzResourceProvider -ProviderNamespace Microsoft.RecoveryServices
```

4. Verify that in the command output, the **RegistrationState** is set to **Registered**, you can proceed to Step 2. If not, you should register the missing provider in your subscription, by running these commands:

```
Register-AzResourceProvider -ProviderNamespace Microsoft.RecoveryServices
```

5. Verify that the Providers registered successfully, using the following commands:

```
Get-AzResourceProvider -ProviderNamespace Microsoft.RecoveryServices
```

## Step 2: Set up the vault

1. Create an Azure Resource Manager resource group in which to create the vault, or use an existing resource group. Create a new resource group as follows. The `$ResourceGroupName` variable contains the name of the resource group you want to create, and the `$Geo` variable contains the Azure region in which to create the resource group (for example, "Brazil South").

```
New-AzResourceGroup -Name $ResourceGroupName -Location $Geo
```

2. To obtain a list of resource groups in your subscription, run the `Get-AzResourceGroup` cmdlet.

3. Create a new Azure Recovery Services vault as follows:

```
$vault = New-AzRecoveryServicesVault -Name <string> -ResourceGroupName <string> -Location <string>
```

You can retrieve a list of existing vaults with the `Get-AzRecoveryServicesVault` cmdlet.

## Step 3: Set the Recovery Services vault context

Set the vault context as follows:

```
Set-AzRecoveryServicesAsrVaultContext -Vault $vault
```

## Step 4: Create a Hyper-V site

1. Create a new Hyper-V site as follows:

```
$sitename = "MySite" #Specify site friendly name
New-AzRecoveryServicesAsrFabric -Type HyperVSite -Name $sitename
```

2. This cmdlet starts a Site Recovery job to create the site, and returns a Site Recovery job object. Wait for the job to complete and verify that the job completed successfully.
3. Use the `Get-AzRecoveryServicesAsrJob` cmdlet to retrieve the job object, and check the current status of the job.
4. Generate and download a registration key for the site, as follows:

```
$SiteIdentifier = Get-AzRecoveryServicesAsrFabric -Name $sitename | Select-Object -ExpandProperty
SiteIdentifier
$path = Get-AzRecoveryServicesVaultSettingsFile -Vault $vault -SiteIdentifier $SiteIdentifier -
SiteFriendlyName $sitename
```

5. Copy the downloaded key to the Hyper-V host. You need the key to register the Hyper-V host to the site.

## Step 5: Install the Provider and agent

1. Download the installer for the latest version of the Provider from [Microsoft](#).
2. Run the installer on the Hyper-V host.
3. At the end of the installation continue to the registration step.
4. When prompted, provide the downloaded key, and complete registration of the Hyper-V host.
5. Verify that the Hyper-V host is registered to the site as follows:

```
$server = Get-AzRecoveryServicesAsrFabric -Name $siteName | Get-AzRecoveryServicesAsrServiceProvider -
FriendlyName $server-friendlyname
```

If you're running a Hyper-V core server, download the setup file and follow these steps:

1. Extract the files from `AzureSiteRecoveryProvider.exe` to a local directory by running this command:

```
AzureSiteRecoveryProvider.exe /x:. /q
```

2. Run the following command:

```
.\setupdr.exe /i
```

Results are logged to `%ProgramData%\ASRLogs\DRASetupWizard.log`.

3. Register the server by running this command:

```
cd C:\Program Files\Microsoft Azure Site Recovery Provider\DRConfigurator.exe" /r /Friendlyname
"FriendlyName of the Server" /Credentials "path to where the credential file is saved"
```

## Step 6: Create a replication policy

Before you start, the storage account specified should be in the same Azure region as the vault, and should have geo-replication enabled.

1. Create a replication policy as follows:

```
$ReplicationFrequencyInSeconds = "300"; #options are 30,300,900
$PolicyName = "replicapolicy"
$Recoverypoints = 6 #specify the number of recovery points
$storageaccountID = Get-AzStorageAccount -Name "mystorea" -ResourceGroupName "MyRG" | Select-Object -
ExpandProperty Id

$PolicyResult = New-AzRecoveryServicesAsrPolicy -Name $PolicyName -ReplicationProvider
"HyperVReplicaAzure" -ReplicationFrequencyInSeconds $ReplicationFrequencyInSeconds -
NumberOfRecoveryPointsToRetain $Recoverypoints -ApplicationConsistentSnapshotFrequencyInHours 1 -
RecoveryAzureStorageAccountId $storageaccountID
```

2. Check the returned job to ensure that the replication policy creation succeeds.

3. Retrieve the protection container that corresponds to the site, as follows:

```
$protectionContainer = Get-AzRecoveryServicesAsrProtectionContainer
```

4. Associate the protection container with the replication policy, as follows:

```
$Policy = Get-AzRecoveryServicesAsrPolicy -FriendlyName $PolicyName
$associationJob = New-AzRecoveryServicesAsrProtectionContainerMapping -Name $mappingName -Policy
$Policy -PrimaryProtectionContainer $protectionContainer[0]
```

5. Wait for the association job to complete successfully.

6. Retrieve the protection container mapping.

```
$ProtectionContainerMapping = Get-AzRecoveryServicesAsrProtectionContainerMapping -ProtectionContainer
$protectionContainer
```

## Step 7: Enable VM protection

1. Retrieve the protectable item that corresponds to the VM you want to protect, as follows:

```
$VMFriendlyName = "Fabrikam-app" #Name of the VM
$ProtectableItem = Get-AzRecoveryServicesAsrProtectableItem -ProtectionContainer $protectionContainer -
FriendlyName $VMFriendlyName
```

2. Protect the VM. If the VM you're protecting has more than one disk attached to it, specify the operating system disk by using the **OSDiskName** parameter.

```
$OSType = "Windows" # "Windows" or "Linux"
$DRjob = New-AzRecoveryServicesAsrReplicationProtectedItem -ProtectableItem $VM -Name $VM.Name -
ProtectionContainerMapping $ProtectionContainerMapping -RecoveryAzureStorageAccountId $StorageAccountID
-OSDiskName $OSDiskNameList[$i] -OS $OSType -RecoveryResourceGroupId $ResourceGroupId
```

3. Wait for the VMs to reach a protected state after the initial replication. This can take a while, depending on factors such as the amount of data to be replicated, and the available upstream bandwidth to Azure. When a

protected state is in place, the job State and StateDescription are updated as follows:

```
PS C:\> $DRjob = Get-AzRecoveryServicesAsrJob -Job $DRjob

PS C:\> $DRjob | Select-Object -ExpandProperty State
Succeeded

PS C:\> $DRjob | Select-Object -ExpandProperty StateDescription
Completed
```

4. Update recovery properties (such as the VM role size) and the Azure network to which to attach the VM NIC after failover.

```
PS C:\> $nw1 = Get-AzVirtualNetwork -Name "FailoverNw" -ResourceGroupName "MyRG"

PS C:\> $VMFriendlyName = "Fabrikam-App"

PS C:\> $rpi = Get-AzRecoveryServicesAsrReplicationProtectedItem -ProtectionContainer
$protectionContainer -FriendlyName $VMFriendlyName

PS C:\> $UpdateJob = Set-AzRecoveryServicesAsrReplicationProtectedItem -InputObject $rpi -PrimaryNic
$VM.NicDetailsList[0].NicId -RecoveryNetworkId $nw1.Id -RecoveryNicSubnetName $nw1.Subnets[0].Name

PS C:\> $UpdateJob = Get-AzRecoveryServicesAsrJob -Job $UpdateJob

PS C:\> $UpdateJob | Select-Object -ExpandProperty state

PS C:\> Get-AzRecoveryServicesAsrJob -Job $job | Select-Object -ExpandProperty state

Succeeded
```

#### NOTE

If you wish to replicate to CMK enabled managed disks in Azure, do the following steps using Az PowerShell 3.3.0 onwards:

1. Enable failover to managed disks by updating VM properties
2. Use the `Get-AzRecoveryServicesAsrReplicationProtectedItem` cmdlet to fetch the disk ID for each disk of the protected item
3. Create a dictionary object using  
`New-Object "System.Collections.Generic.Dictionary`2[System.String,System.String]"` cmdlet to contain the mapping of disk ID to disk encryption set. These disk encryption sets are to be pre-created by you in the target region.
4. Update the VM properties using `Set-AzRecoveryServicesAsrReplicationProtectedItem` cmdlet by passing the dictionary object in `DiskIdToDiskEncryptionSetMap` parameter.

## Step 8: Run a test failover

1. Run a test failover as follows:

```
$nw = Get-AzVirtualNetwork -Name "TestFailoverNw" -ResourceGroupName "MyRG" #Specify Azure vnet name
and resource group

$rpi = Get-AzRecoveryServicesAsrReplicationProtectedItem -ProtectionContainer $protectionContainer -
FriendlyName $VMFriendlyName

$TFjob = Start-AzRecoveryServicesAsrTestFailoverJob -ReplicationProtectedItem $VM -Direction
PrimaryToRecovery -AzureVMNetworkId $nw.Id
```

2. Verify that the test VM is created in Azure. The test failover job is suspended after creating the test VM in

Azure.

3. To clean up and complete the test failover, run:

```
$TFjob = Start-AzRecoveryServicesAsrTestFailoverCleanupJob -ReplicationProtectedItem $rpi -Comment "TFO done"
```

## Next steps

[Learn more](#) about Azure Site Recovery with Azure Resource Manager PowerShell cmdlets.

# Set up disaster recovery of Hyper-V VMs to a secondary site by using PowerShell (Resource Manager)

2/5/2020 • 7 minutes to read • [Edit Online](#)

This article shows how to automate the steps for replication of Hyper-V VMs in System Center Virtual Machine Manager clouds to a Virtual Machine Manager cloud in a secondary on-premises site by using [Azure Site Recovery](#).

## NOTE

This article has been updated to use the new Azure PowerShell Az module. You can still use the AzureRM module, which will continue to receive bug fixes until at least December 2020. To learn more about the new Az module and AzureRM compatibility, see [Introducing the new Azure PowerShell Az module](#). For Az module installation instructions, see [Install Azure PowerShell](#).

## Prerequisites

- Review the [scenario architecture and components](#).
- Review the [support requirements](#) for all components.
- Make sure that Virtual Machine Manager servers and Hyper-V hosts comply with [support requirements](#).
- Check that the VMs you want to replicate comply with [replicated machine support](#).

## Prepare for network mapping

[Network mapping](#) maps between on-premises Virtual Machine Manager VM networks in source and target clouds. Mapping does the following:

- Connects VMs to appropriate target VM networks after failover.
- Optimally places replica VMs on target Hyper-V host servers.
- If you don't configure network mapping, replica VMs won't be connected to a VM network after failover.

Prepare Virtual Machine Manager as follows:

- Make sure you have [Virtual Machine Manager logical networks](#) on the source and target Virtual Machine Manager servers:
  - The logical network on the source server should be associated with the source cloud in which Hyper-V hosts are located.
  - The logical network on the target server should be associated with the target cloud.
- Make sure you have [VM networks](#) on the source and target Virtual Machine Manager servers. VM networks should be linked to the logical network in each location.
- Connect VMs on the source Hyper-V hosts to the source VM network.

## Prepare for PowerShell

Make sure you have Azure PowerShell ready to go:

- If you already use PowerShell, upgrade to version 0.8.10 or later. [Learn more](#) about how to set up PowerShell.

- After you set up and configure PowerShell, review the [service cmdlets](#).
- To learn more about how to use parameter values, inputs, and outputs in PowerShell, read the [Get started](#) guide.

## Set up a subscription

1. From PowerShell, sign in to your Azure account.

```
$UserName = "<user@live.com>"
$Password = "<password>"
$SecurePassword = ConvertTo-SecureString -AsPlainText $Password -Force
$Cred = New-Object System.Management.Automation.PSCredential -ArgumentList $UserName, $SecurePassword
Connect-AzAccount #-Credential $Cred
```

2. Retrieve a list of your subscriptions, with the subscription IDs. Note the ID of the subscription in which you want to create the Recovery Services vault.

```
Get-AzSubscription
```

3. Set the subscription for the vault.

```
Set-AzContext -SubscriptionID <subscriptionId>
```

## Create a Recovery Services vault

1. Create an Azure Resource Manager resource group if you don't have one.

```
New-AzResourceGroup -Name #ResourceGroupName -Location #location
```

2. Create a new Recovery Services vault. Save the vault object in a variable to be used later.

```
$vault = New-AzRecoveryServicesVault -Name #vaultname -ResourceGroupName #ResourceGroupName -Location #location
```

You can retrieve the vault object after you create it by using the `Get-AzRecoveryServicesVault` cmdlet.

## Set the vault context

1. Retrieve an existing vault.

```
$vault = Get-AzRecoveryServicesVault -Name #vaultname
```

2. Set the vault context.

```
Set-AzRecoveryServicesAsrVaultContext -Vault $vault
```

## Install the Site Recovery provider

1. On the Virtual Machine Manager machine, create a directory by running the following command:

```
New-Item -Path C:\ASR -ItemType Directory
```

2. Extract the files by using the downloaded provider setup file.

```
pushd C:\ASR\
.\\AzureSiteRecoveryProvider.exe /x:. /q
```

3. Install the provider, and wait for installation to finish.

```
.\\SetupDr.exe /i
$installationRegPath = "HKLM:\\Software\\Microsoft\\Microsoft System Center Virtual Machine Manager
Server\\DRAdapter"
do
{
 $isNotInstalled = $true;
 if(Test-Path $installationRegPath)
 {
 $isNotInstalled = $false;
 }
}While($isNotInstalled)
```

4. Register the server in the vault.

```
$BinPath = $env:SystemDrive+"\\Program Files\\Microsoft System Center 2012 R2\\Virtual Machine
Manager\\bin"
pushd $BinPath
$encryptionFilePath = "C:\\temp\\\".\\DRConfigurator.exe /r /Credentials $VaultSettingFilePath
/vmmfriendlyname $env:COMPUTERNAME /dataencryptionenabled $encryptionFilePath /startvmmservice
```

## Create and associate a replication policy

1. Create a replication policy, in this case for Hyper-V 2012 R2, as follows:

```
$ReplicationFrequencyInSeconds = "300"; #options are 30,300,900
$PolicyName = "replicapolicy"
$RepProvider = HyperVReplica2012R2
$Recoverypoints = 24 #specify the number of hours to retain recovery points
$AppConsistentSnapshotFrequency = 4 #specify the frequency (in hours) at which app consistent snapshots
are taken
$AuthMode = "Kerberos" #options are "Kerberos" or "Certificate"
$AuthPort = "8083" #specify the port number that will be used for replication traffic on Hyper-V hosts
$InitialRepMethod = "Online" #options are "Online" or "Offline"

$policyresult = New-AzRecoveryServicesAsrPolicy -Name $policyname -ReplicationProvider $RepProvider -
ReplicationFrequencyInSeconds $Replicationfrequencyinseconds -NumberOfRecoveryPointsToRetain
$recoverypoints -ApplicationConsistentSnapshotFrequencyInHours $AppConsistentSnapshotFrequency -
Authentication $AuthMode -ReplicationPort $AuthPort -ReplicationMethod $InitialRepMethod
```

### NOTE

The Virtual Machine Manager cloud can contain Hyper-V hosts running different versions of Windows Server, but the replication policy is for a specific version of an operating system. If you have different hosts running on different operating systems, create separate replication policies for each system. For example, if you have five hosts running on Windows Server 2012 and three hosts running on Windows Server 2012 R2, create two replication policies. You create one for each type of operating system.

2. Retrieve the primary protection container (primary Virtual Machine Manager cloud) and recovery protection container (recovery Virtual Machine Manager cloud).

```
$PrimaryCloud = "testprimarycloud"
$primaryprotectionContainer = Get-AzRecoveryServicesAsrProtectionContainer -FriendlyName $PrimaryCloud;

$RecoveryCloud = "testrecoverycloud"
$recoveryprotectionContainer = Get-AzRecoveryServicesAsrProtectionContainer -FriendlyName
$RecoveryCloud;
```

3. Retrieve the replication policy you created by using the friendly name.

```
$policy = Get-AzRecoveryServicesAsrPolicy -FriendlyName $policyname
```

4. Start the association of the protection container (Virtual Machine Manager cloud) with the replication policy.

```
$associationJob = New-AzRecoveryServicesAsrProtectionContainerMapping -Policy $Policy -
PrimaryProtectionContainer $primaryprotectionContainer -RecoveryProtectionContainer
$recoveryprotectionContainer
```

5. Wait for the policy association job to finish. To check if the job is finished, use the following PowerShell snippet:

```
$job = Get-AzRecoveryServicesAsrJob -Job $associationJob

if($job -eq $null -or $job.StateDescription -ne "Completed")
{
 $isJobLeftForProcessing = $true;
}
```

6. After the job finishes processing, run the following command:

```
if($isJobLeftForProcessing)
{
 Start-Sleep -Seconds 60
}
While($isJobLeftForProcessing)
```

To check the completion of the operation, follow the steps in [Monitor activity](#).

## Configure network mapping

1. Use this command to retrieve servers for the current vault. The command stores the Site Recovery servers in the `$Servers` array variable.

```
$Servers = Get-AzRecoveryServicesAsrFabric
```

2. Run this command to retrieve the networks for the source Virtual Machine Manager server and the target Virtual Machine Manager server.

```
$PrimaryNetworks = Get-AzRecoveryServicesAsrNetwork -Fabric $Servers[0]

$RecoveryNetworks = Get-AzRecoveryServicesAsrNetwork -Fabric $Servers[1]
```

#### NOTE

The source Virtual Machine Manager server can be the first or second one in the server array. Check Virtual Machine Manager server names, and retrieve the networks appropriately.

3. This cmdlet creates a mapping between the primary network and the recovery network. It specifies the primary network as the first element of `$PrimaryNetworks`. It specifies the recovery network as the first element of `$RecoveryNetworks`.

```
New-AzRecoveryServicesAsrNetworkMapping -PrimaryNetwork $PrimaryNetworks[0] -RecoveryNetwork
$RecoveryNetworks[0]
```

## Enable protection for VMs

After the servers, clouds, and networks are configured correctly, enable protection for VMs in the cloud.

1. To enable protection, run the following command to retrieve the protection container:

```
$PrimaryProtectionContainer = Get-AzRecoveryServicesAsrProtectionContainer -FriendlyName
$PrimaryCloudName
```

2. Get the protection entity (VM), as follows:

```
$protectionEntity = Get-AzRecoveryServicesAsrProtectableItem -FriendlyName $VMName -ProtectionContainer
$PrimaryProtectionContainer
```

3. Enable replication for the VM.

```
$jobResult = New-AzRecoveryServicesAsrReplicationProtectedItem -ProtectableItem $protectionentity -
ProtectionContainerMapping $policy -VmToVm
```

#### NOTE

If you wish to replicate to CMK enabled managed disks in Azure, do the following steps using Az PowerShell 3.3.0 onwards:

1. Enable failover to managed disks by updating VM properties
2. Use the `Get-AzRecoveryServicesAsrReplicationProtectedItem` cmdlet to fetch the disk ID for each disk of the protected item
3. Create a dictionary object using  
`New-Object "System.Collections.Generic.Dictionary`2[System.String,System.String]"` cmdlet to contain the mapping of disk ID to disk encryption set. These disk encryption sets are to be pre-created by you in the target region.
4. Update the VM properties using `Set-AzRecoveryServicesAsrReplicationProtectedItem` cmdlet by passing the dictionary object in **DiskIdToDiskEncryptionSetMap** parameter.

## Run a test failover

To test your deployment, run a test failover for a single virtual machine. You also can create a recovery plan that contains multiple VMs and run a test failover for the plan. Test failover simulates your failover and recovery mechanism in an isolated network.

1. Retrieve the VM into which VMs will fail over.

```
$Servers = Get-AzRecoveryServicesASRFabric
$RecoveryNetworks = Get-AzRecoveryServicesAsrNetwork -Name $Servers[1]
```

## 2. Perform a test failover.

For a single VM:

```
$protectionEntity = Get-AzRecoveryServicesAsrProtectableItem -FriendlyName $VMName -ProtectionContainer
$PrimaryprotectionContainer

$jobIDResult = Start-AzRecoveryServicesAsrTestFailoverJob -Direction PrimaryToRecovery -
ReplicationProtectedItem $protectionEntity -VMNetwork $RecoveryNetworks[1]
```

For a recovery plan:

```
$recoveryplanname = "test-recovery-plan"

$recoveryplan = Get-AzRecoveryServicesAsrRecoveryPlan -FriendlyName $recoveryplanname

$jobIDResult = Start-AzRecoveryServicesAsrTestFailoverJob -Direction PrimaryToRecovery -RecoveryPlan
$recoveryplan -VMNetwork $RecoveryNetworks[1]
```

To check the completion of the operation, follow the steps in [Monitor activity](#).

## Run planned and unplanned failovers

### 1. Perform a planned failover.

For a single VM:

```
$protectionEntity = Get-AzRecoveryServicesAsrProtectableItem -Name $VMName -ProtectionContainer
$PrimaryprotectionContainer

$jobIDResult = Start-AzRecoveryServicesAsrPlannedFailoverJob -Direction PrimaryToRecovery -
ReplicationProtectedItem $protectionEntity
```

For a recovery plan:

```
$recoveryplanname = "test-recovery-plan"

$recoveryplan = Get-AzRecoveryServicesAsrRecoveryPlan -FriendlyName $recoveryplanname

$jobIDResult = Start-AzRecoveryServicesAsrPlannedFailoverJob -Direction PrimaryToRecovery -RecoveryPlan
$recoveryplan
```

### 2. Perform an unplanned failover.

For a single VM:

```
$protectionEntity = Get-AzRecoveryServicesAsrProtectableItem -Name $VMName -ProtectionContainer
$PrimaryprotectionContainer

$jobIDResult = Start-AzRecoveryServicesAsrUnplannedFailoverJob -Direction PrimaryToRecovery -
ReplicationProtectedItem $protectionEntity
```

For a recovery plan:

```
$recoveryplanname = "test-recovery-plan"

$recoveryplan = Get-AzRecoveryServicesAsrRecoveryPlan -FriendlyName $recoveryplanname

$jobIDResult = Start-AzRecoveryServicesAsrUnplannedFailoverJob -Direction PrimaryToRecovery - RecoveryPlan $recoveryplan
```

## Monitor activity

Use the following commands to monitor failover activity. Wait for the processing to finish in between jobs.

```
Do
{
 $job = Get-AzRecoveryServicesAsrJob -TargetObjectId $associationJob.JobId;
 Write-Host "Job State:{0}, StateDescription:{1}" -f Job.State, $job.StateDescription;
 if($job -eq $null -or $job.StateDescription -ne "Completed")
 {
 $isJobLeftForProcessing = $true;
 }

 if($isJobLeftForProcessing)
 {
 Start-Sleep -Seconds 60
 }
}While($isJobLeftForProcessing)
```

## Next steps

[Learn more](#) about Site Recovery with Resource Manager PowerShell cmdlets.

# Add Azure Automation runbooks to recovery plans

10/9/2019 • 7 minutes to read • [Edit Online](#)

This article describes how to integrate Azure Automation runbooks, to extend [Azure Site Recovery](#) recovery plans. We show you how to automate basic tasks that would otherwise need manual intervention, and how to convert a multi-step recovery into a single-click action.

## Recovery plans

You can use recovery plans when you fail over on-premises machines, or Azure VMs. Recovery plans help you to define a systematic recovery process that defines how machines fail over, and how they start and recover after failover.

Recovering large apps can be complex. Recovery plans help impose order so that recovery is consistently accurate, repeatable, and automated. You can automate tasks within a recovery plan using scripts, as well as Azure Automation runbooks. Typical examples might be configuring settings on an Azure VM after failover, or reconfiguring an app that's running on the VM.

- [Learn more about recovery plans.](#)
- [Learn more about Azure Automation runbooks.](#)

## Runbooks in recovery plans

You add an Azure Automation account and runbooks to a recovery plan. The runbook is invoked when the recovery plan runs.

- The Automation account can be in any Azure region, and must be in the same subscription as the Site Recovery vault.
- A runbook can run in a recovery plan during failover from a primary location to secondary, or during failback from the secondary location to the primary.
- Runbooks in a recovery plan run serially, one after another, in the set order.
- If runbooks in a recovery plan configure VMs to start in different groups, the recovery plan will continue only when Azure reports all VMs as running.
- Recovery plans continue to run, even if a script fails.

### Recovery plan context

When a script runs, it injects a recovery plan context to the runbook. The context contains the variables summarized in the table.

VARIABLE NAME	DESCRIPTION
RecoveryPlanName	Recovery plan name. Used in actions based on the name.
FailoverType	Specifies whether it's a test or production failover.
FailoverDirection	Specifies whether recovery is to a primary or secondary location.
GroupID	Identifies the group number in the recovery plan when the plan is running.

VARIABLE NAME	DESCRIPTION
VmMap	An array of all VMs in the group.
VMMMap key	A unique key (GUID) for each VM.
SubscriptionId	The Azure subscription ID in which the VM was created.
ResourceGroupName	Name of the resource group in which the VM is located.
CloudServiceName	The Azure cloud service name under which the VM was created.
RoleName	The name of the Azure VM.
RecoveryPointId	The timestamp for the VM recovery.

The following example shows a context variable:

```
{
 "RecoveryPlanName": "hrweb-recovery",
 "FailoverType": "Test",
 "FailoverDirection": "PrimaryToSecondary",
 "GroupId": "1",
 "VmMap": {
 "7a1069c6-c1d6-49c5-8c5d-33bfce8dd183": {
 "SubscriptionId": "7a111111-c1d6-49c5-8c5d-111ce8dd183",
 "ResourceGroupName": "ContosoRG",
 "CloudServiceName": "pod02hrweb-Chicago-test",
 "RoleName": "Fabrikam-Hrweb-frontend-test",
 "RecoveryPointId": "TimeStamp"
 }
 }
}
```

If you want to access all VMs in VMMMap in a loop, you can use the following code:

```
$VMinfo = $RecoveryPlanContext.VmMap | Get-Member | Where-Object MemberType -EQ NoteProperty | select -ExpandProperty Name
$vmMap = $RecoveryPlanContext.VmMap
foreach($VMID in $VMinfo)
{
 $VM = $vmMap.$VMID
 if(!($VM -eq $Null) -Or ($VM.ResourceGroupName -eq $Null) -Or ($VM.RoleName -eq $Null)) {
 #this check is to ensure that we skip when some data is not available else it will fail
 Write-output "Resource group name ", $VM.ResourceGroupName
 Write-output "Rolename " = $VM.RoleName
 }
}
```

Aman Sharma's blog over at [Harvesting Clouds](#) has a useful example of a [recovery plan context script](#).

## Before you start

- If you're new to Azure Automation, you can [sign up](#) and [download sample scripts](#).
- Ensure that the Automation account has the following modules:
  - AzureRM.profile
  - AzureRM.Resources

- o AzureRM.Automation
- o AzureRM.Network
- o AzureRM.Compute

All modules should be of compatible versions. The simplest way is to always use the latest versions of all modules.

## Customize the recovery plan

1. In the vault, select **Recovery Plans (Site Recovery)**
2. To create a recovery plan, click **+Recovery Plan**. [Learn more](#). If you already have a recovery plan, then select to open it.
3. In the recovery plan page, click **Customize**.

The screenshot shows the 'Sharepoint Recovery' recovery plan in the Azure Recovery Services vault. The top navigation bar includes 'Settings', 'Customize', 'Test failover', 'Cleanup test failover', and 'More'. Below the navigation is a section titled 'Essentials' with a collapse arrow. It displays the following details:

Recovery Services vault	Items in recovery plan
<a href="#">maygvault</a>	2
Start groups	Scripts
2	0
Source	Target
North Central US	Central US
Deployment model	
Resource Manager	

A blue button labeled 'All settings →' is located at the bottom right of this section. Below this is a summary box titled 'Items in recovery plan' containing two columns: 'Source' (with a value of 2) and 'Target' (with a value of 0). Each column has a large number and a small icon representing the count.

4. Click the ellipses (...) next to **Group 1: Start > Add post action**.
5. In **Insert action**, verify that **Script** is selected, and specify a name for the script (**Hello World**).
6. Specify an automation account and select a runbook. To save the script, click **OK**. The script is added to **Group 1: Post-steps**.

## Reuse a runbook script

You can use a single runbook script in multiple recovery plans, by using external variables.

- You use [Azure Automation variables](#) to store parameters for running a recovery plan.
- By adding the recovery plan name as a prefix to the variable, you can create individual variables for each recovery plan. Then, use the variables as parameters.
- You can change a parameter without changing the script, but still change the way the script works.

### Use a simple string variable in a runbook script

In this example, a script takes the input of a Network Security Group (NSG) and applies it to the VMs in a recovery plan.

1. So that the script can detect which recovery plan is running, use this recovery plan context:

```
workflow AddPublicIPAndNSG {
 param (
 [parameter(Mandatory=$false)]
 [Object]$RecoveryPlanContext
)

 $RPName = $RecoveryPlanContext.RecoveryPlanName
```

2. Note the NSG name and resource group. You use these variables as inputs for recovery plan scripts.
3. In the Automation account assets, create a variable to store the NSG name. Add a prefix to the variable name with the name of the recovery plan.



## RPscripttest-NSG

Variable



Save



Discard



Delete

### Name

RPscripttest-NSG

### Last modified

1/24/2017, 4:25 PM

### Description

Store the name of the NSG that needs to be applied to all VMs

### Encrypted

No

### Type

String



### Value

RPtestnsg

4. Create a variable to store the resource group name for the NSG resource. Add a prefix to the variable name with the name of the recovery plan.



## RPscripttest-NSGRG



Save



Discard



Delete

### Name

RPscripttest-NSGRG

### Last modified

1/24/2017, 7:33 PM

### Description

Resource group of the NSG you want to apply.



### Encrypted

No

### Type

String



### Value

ContosoRG



5. In the script, use this reference code to get the variable values:

```
$NSGValue = $RecoveryPlanContext.RecoveryPlanName + "-NSG"
$NSGRGValue = $RecoveryPlanContext.RecoveryPlanName + "-NSGRG"

$NSGnameVar = Get-AutomationVariable -Name $NSGValue
$RGnameVar = Get-AutomationVariable -Name $NSGRGValue
```

6. Use the variables in the runbook to apply the NSG to the network interface of the failed-over VM:

```

InlineScript {
if (($Using:NSGname -ne $Null) -And ($Using:NSGRGname -ne $Null)) {
 $NSG = Get-AzureRmNetworkSecurityGroup -Name $Using:NSGname -ResourceGroupName $Using:NSGRGname
 Write-output $NSG.Id
 #Apply the NSG to a network interface
 #$vnet = Get-AzureRmVirtualNetwork -ResourceGroupName TestRG -Name TestVNet
 #Set-AzureRmVirtualNetworkSubnetConfig -VirtualNetwork $vnet -Name FrontEnd `
 # -AddressPrefix 192.168.1.0/24 -NetworkSecurityGroup $NSG
}
}

```

For each recovery plan, create independent variables so that you can reuse the script. Add a prefix by using the recovery plan name.

For a complete, end-to-end script for this scenario, review [this script](#).

### Use a complex variable to store more information

In some scenarios you might not be able to create separate variables for each recovery plan. Consider a scenario in which you want a single script to assign a public IP address on specific VMs. In another scenario, you might want to apply different NSGs on different VMs (not on all VMs). Note that:

- You can make a script that's reusable for any recovery plan.
- Each recovery plan can have a variable number of VMs.
- For example, a SharePoint recovery has two front ends. A basic line-of-business (LOB) application has only one front end.
- In this scenario you can't create separate variables for each recovery plan.

In the following example, we create a [complex variable](#) in the Azure Automation account.

We do this by specifying multiple values, using Azure PowerShell.

1. In PowerShell, sign in to your Azure subscription:

```

Connect-AzureRmAccount
$sub = Get-AzureRmSubscription -Name <SubscriptionName>
$sub | Select-AzureRmSubscription

```

2. To store the parameters, create the complex variable using the name of the recovery plan:

```

$VMDetails =
@{ "VMGUID"=@{ "ResourceGroupName"="RGNameOfNSG" ; "NSGName"="NameOfNSG" } ; "VMGUID2"=@{ "ResourceGroupName"="RGNameOfNSG" ; "NSGName"="NameOfNSG" } }
New-AzureRmAutomationVariable -ResourceGroupName <RG of Automation Account> -AutomationAccountName <AA Name> -Name <RecoveryPlanName> -Value $VMDetails -Encrypted $false

```

3. In this complex variable, **VMDetails** is the VM ID for the protected VM. To get the VM ID, in the Azure portal, view the VM properties. The following screenshot shows a variable that stores the details of two VMs:



4. Use this variable in your runbook. If the indicated VM GUID is found in the recovery plan context, apply the NSG on the VM:

```
$VMDetailsObj = (Get-AutomationVariable -Name
$RecoveryPlanContext.RecoveryPlanName).ToObject([hashtable])
```

5. In your runbook, loop through the VMs of the recovery plan context. Check whether the VM exists in **\$VMDetailsObj**. If it exists, access the properties of the variable to apply the NSG:

```
$VMInfo = $RecoveryPlanContext.VmMap | Get-Member | Where-Object MemberType -EQ NoteProperty |
select -ExpandProperty Name
$vmMap = $RecoveryPlanContext.VmMap

foreach($VMID in $VMInfo) {
 $VMDetails = $VMDetailsObj[$VMID].ToObject([hashtable]);
 Write-output $VMDetails
 if ($VMDetails -ne $Null) { #If the VM exists in the context, this will not be Null
 $VM = $vmMap.$VMID
 # Access the properties of the variable
 $NSGname = $VMDetails.NSGName
 $NSGRGname = $VMDetails.NSGResourceGroupName

 # Add code to apply the NSG properties to the VM
 }
}
```

You can use the same script for different recovery plans. Enter different parameters by storing the value that corresponds to a recovery plan in different variables.

## Sample scripts

To deploy sample scripts to your Automation account, click the **Deploy to Azure** button.



This video provides another example. It demonstrates how to recover a two-tier WordPress application to Azure:

## Next steps

- Learn about an [Azure Automation Run As account](#)
- Review [Azure Automation sample scripts](#).
- [Learn more](#) about running failovers.

# Common questions about Site Recovery monitoring

8/1/2019 • 2 minutes to read • [Edit Online](#)

This article answers common questions about monitoring Azure [Site Recovery](#), using inbuilt Site Recovery monitoring, and Azure Monitor (Log Analytics).

## General

### **How is the RPO value logged different from the latest available recovery point?**

Site Recovery uses a multi-step, asynchronous process to replicate machines to Azure.

- In the penultimate step of replication, recent changes on the machine, along with metadata, are copied into a log/cache storage account.
- These changes, along with the tag that identifies a recoverable point, are written to the storage account/managed disk in the target region.
- Site Recovery can now generate a recoverable point for the machine.
- At this point, the RPO has been met for the changes uploaded to the storage account so far. In other words, the machine RPO at this point is equal to amount of time that's elapsed from the timestamp corresponding to the recoverable point.
- Now, Site Recovery picks the uploaded data from the storage account, and applies it to the replica disks created for the machine.
- Site Recovery then generates a recovery point, and makes this point available for recovery at failover.
- Thus, the latest available recovery point indicates the timestamp corresponding to the latest recovery point that has already been processed, and applied to the replica disks.

An incorrect system time on the replicating source machine, or on on-premises infrastructure servers, will skew the computed RPO value. For accurate RPO reporting, make sure that the system clock is accurate on all servers and machines.

## Inbuilt Site Recovery logging

### **Why is the VM count in the vault infrastructure view different from the total count shown in Replicated Items?**

The vault infrastructure view is scoped by replication scenarios. Only machines in the currently selected replication scenario are included in the count for the view. In addition, we only count VMs that are configured to replicate to Azure. Failed over machines, or machines replicating back to an on-premises site, aren't counted in the view.

### **Why is the count of replicated items in Essentials different from the total count of replicated items on the dashboard?**

Only machines for which initial replication has completed are included in the count shown in Essentials. The replicated items total includes all the machines in the vault, including those for which initial replication is currently in progress.

## Azure Monitor logging

### **How often does Site Recovery send diagnostic logs to Azure Monitor Log?**

- AzureSiteRecoveryReplicationStats and AzureSiteRecoveryRecoveryPoints are sent every 15 minutes.
- AzureSiteRecoveryReplicationDataUploadRate and AzureSiteRecoveryProtectedDiskDataChurn are sent every five minutes.

- AzureSiteRecoveryJobs is sent at the trigger and completion of a job.
- AzureSiteRecoveryEvents is sent whenever an event is generated.
- AzureSiteRecoveryReplicatedItems is sent whenever there is any environment change. Typically, the data refresh time is 15 minutes after a change.

### How long is data kept in Azure Monitor logs?

By default, retention is for 31 days. You can increase the period in the **Usage and Estimated Cost** section in the Log Analytics workspace. Click on **Data Retention**, and choose the range.

### What's the size of the diagnostic logs?

Typically the size of a log is 15-20 KB.

## Next steps

Learn how to monitor with [Site Recovery inbuilt monitoring](#), or [Azure Monitor](#).

# Monitor Site Recovery

8/1/2019 • 7 minutes to read • [Edit Online](#)

In this article, learn how to monitor Azure [Site Recovery](#), using Site Recovery inbuilt monitoring. You can monitor:

- The health and status of machines replicated by Site Recovery
- Test failover status of machines.
- Issues and errors affecting configuration and replication.
- Infrastructure components such as on-premises servers.

## Before you start

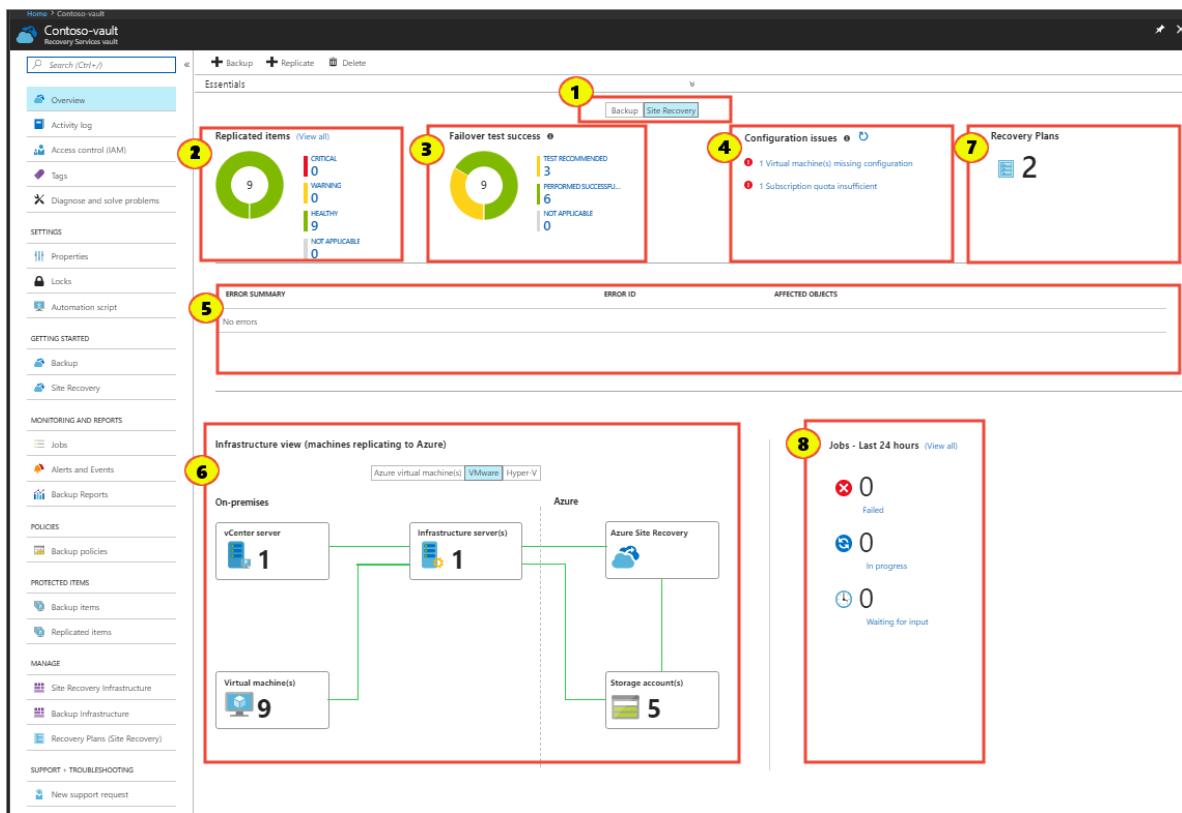
You might want to review [common monitoring questions](#) before you start.

## Monitor in the dashboard

1. In the vault, click **Overview**. The Recovery Services dashboard consolidates all monitoring information for the vault in a single location. There are pages for both Site Recovery and the Azure Backup service, and you can switch between them.

The screenshot shows the Azure Recovery Services Overview dashboard for the 'RayneTestVault' recovery services vault. The left sidebar contains navigation links for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Properties, Locks, Automation script, Backup, and Site Recovery. The main area is divided into several sections: 'Replicated items' (0 items, with categories: CRITICAL, HEALTHY, WARNING, NOT APPLICABLE), 'Failover test success' (0 tests, with categories: TEST RECOMMENDED, PERFORMED SUCCESSFUL, NOT APPLICABLE), 'Configuration issues' (0 issues, with status: No errors), and 'Recovery Plans' (0 plans). Below these are sections for 'ERROR SUMMARY' (No errors), 'INFRASTRUCTURE view (machines replicating to Azure)' (Azure virtual machines, VMware, Hyper-V), and 'Jobs - Last 24 hours' (0 failed, 0 in progress, 0 waiting for input). A feedback survey banner at the top right asks, 'Do you use Azure Site Recovery to migrate servers to Azure? We'd love to hear your feedback.'

2. From the dashboard, drill down into different areas.



3. In **Replicated items**, click **View All** to see all the servers in the vault.
4. Click the status details in each section to drill down.
5. In **Infrastructure view**, sort monitoring information by the type of machines you're replicating.

## Monitor replicated items

In **Replicated items**, monitor the health of all machines in the vault that have replication enabled.

STATE	DETAILS
Healthy	Replication is progressing normally. No error or warning symptoms are detected.
Warning	One or more warning symptoms that might impact replication are detected.
Critical	<p>One or more critical replication error symptoms have been detected.</p> <p>These error symptoms are typically indicators that replication stuck, or not progressing as fast as the data change rate.</p>
Not applicable	Servers that aren't currently expected to be replicating. This might include machines that have been failed over.

## Monitor test failovers

In **Failover test success**, monitor the failover status for machines in the vault.

- We recommend that you run a test failover on replicated machines at least once every six months. It's a way to check that failover is working as expected, without disrupting your production environment.

- A test failover is considered successful only after the failover and post-failover cleanup have completed successfully.

STATE	DETAILS
Test recommended	Machines that haven't had a test failover since protection was enabled.
Performed successfully	Machines with or more successful test failovers.
Not applicable	Machines that aren't currently eligible for a test failover. For example, machines that are failed over, have initial replication/test failover/failover in progress.

## Monitor configuration issues

In **Configuration issues**, monitor any issues that might impact your ability to fail over successfully.

- Configuration issues (except for software update availability), are detected by a periodic validator operation that runs every 12 hours by default. You can force the validator operation to run immediately by clicking the refresh icon next to the **Configuration issues** section heading.
- Click the links to get more details. For issues impacting specific machines, click **needs attention** in the **Target configurations** column. Details include remediation recommendations.

STATE	DETAILS
Missing configurations	A necessary setting is missing, such as a recovery network or a resource group.
Missing resources	A specified resource can't be found or isn't available in the subscription. For example, the resource was deleted or migrated. Monitored resources included the target resource group, target VNet/subnet, log/target storage account, target availability set, target IP address.
Subscription quota	The available subscription resource quota balance is compared against the balance needed to fail over all of the machines in the vault.  If there aren't enough resources, an insufficient quota balance is reported.  Quotas are monitoring for VM core count, VM family core count, network interface card (NIC) count.
Software updates	The availability of new software updates, and information about expiring software versions.

## Monitor errors

In **Error summary**, monitor currently active error symptoms that might impact replication of servers in the vault, and monitor the number of impacted machines.

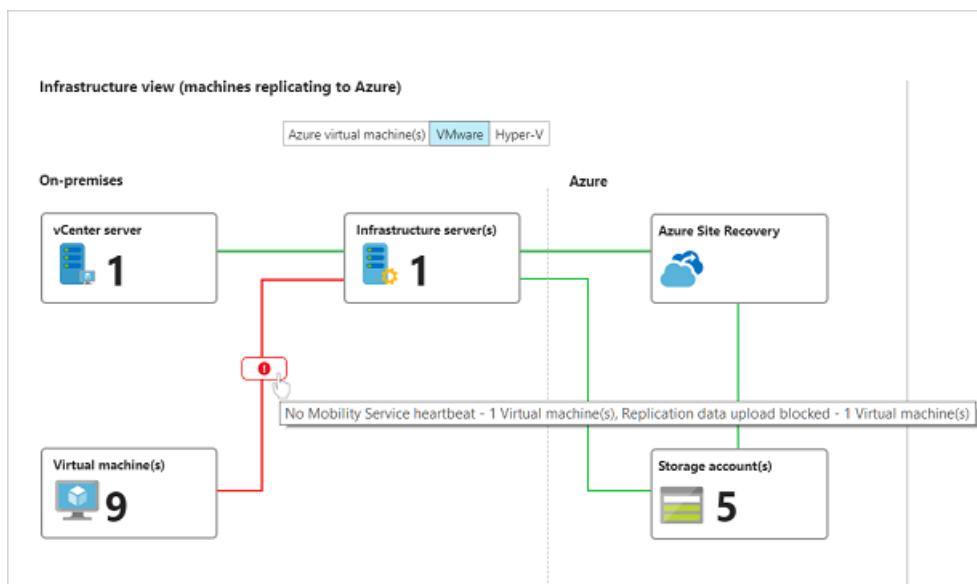
- Errors impacting on-premises infrastructure components are shown at the beginning of the section. For example, non-receipt of a heartbeat from the Azure Site Recovery Provider on the on-premises configuration server, or Hyper-V host.

- Next, replication error symptoms impacting replicated servers are shown.
- The table entries are sorted by decreasing order of the error severity, and then by decreasing count order of the impacted machines.
- The impacted server count is a useful way to understand whether a single underlying issue might impact multiple machines. For example, a network glitch could potentially impact all machines that replicate to Azure.
- Multiple replication errors can occur on a single server. In this case, each error symptom counts that server in the list of its impacted servers. After the issue is fixed, replication parameters improve, and the error is cleared from the machine.

## Monitor the infrastructure.

In **Infrastructure view**, monitor the infrastructure components involved in replication, and connectivity health between servers and the Azure services.

- A green line indicates that connection is healthy.
- A red line with the overlaid error icon indicates the existence of one or more error symptoms that impact connectivity.
- Hover the mouse pointer over the error icon to show the error and the number of impacted entities. Click the icon for a filtered list of impacted entities.



### Tips for monitoring the infrastructure

- Make sure that the on-premises infrastructure components (configuration server, process servers, VMM servers, Hyper-V hosts, VMware machines) are running the latest versions of the Site Recovery Provider and/or agents.
- To use all the features in the infrastructure view, you should be running [Update rollup 22](#) for these components.
- To use the infrastructure view, select the appropriate replication scenario in your environment. You can drill down in the view for more details. The following table shows which scenarios are represented.

SCENARIO	STATE	VIEW AVAILABLE?
Replication between on-premises sites	All states	No

SCENARIO	STATE	VIEW AVAILABLE?
<b>Azure VM replication between Azure regions</b>	Replication enabled/initial replication in progress	Yes
<b>Azure VM replication between Azure regions</b>	Failed over/fail back	No
<b>VMware replication to Azure</b>	Replication enabled/initial replication in progress	Yes
<b>VMware replication to Azure</b>	Failed over/failed back	No
<b>Hyper-V replication to Azure</b>	Failed over/failed back	No

- To see the infrastructure view for a single replicating machine, in the vault menu, click **Replicated items**, and select a server.

## Monitor recovery plans

In **Recovery plans**, monitor the number of plans, create new plans, and modify existing ones.

## Monitor jobs

In **Jobs**, monitor the status of Site Recovery operations.

- Most operations in Azure Site Recovery are executed asynchronously, with a tracking job being created and used to track progress of the operation.
- The job object has all the information you need to track the state and the progress of the operation.

Monitor jobs as follows:

- In the dashboard > **Jobs** section, you can see a summary of jobs that have completed, are in progress, or waiting for input, in the last 24 hours. You can click on any state to get more information about the relevant jobs.
- Click **View all** to see all jobs in the last 24 hours.

### NOTE

You can also access job information from the vault menu > **Site Recovery Jobs**.

- In the **Site Recovery Jobs** list, a list of jobs is displayed. On the top menu you can get error details for a specific jobs, filter the jobs list based on specific criteria, and export selected job details to Excel.
- You can drill into a job by clicking it.

## Monitor virtual machines

In **Replicated items**, get a list of replicated machines.

NAME	REPLICATION HEALTH	STATUS	RPO	TARGET CONFIGURATIONS
ContosoVM9	<span>Healthy</span>	Protected	5 minutes	<span>OK</span>
ContosoVM7	<span>Healthy</span>	Protected	1 minute	<span>Needs attention</span>
ContosoVM1	<span>Healthy</span>	Protected	3 minutes	<span>OK</span>
ContosoVM2	<span>Critical</span>	Protected	32 minutes	<span>OK</span>
ContosoVM3	<span>Healthy</span>	Protected	4 minutes	<span>OK</span>
ContosoVM4	<span>Healthy</span>	Protected	3 minutes	<span>OK</span>
ContosoVM5	<span>Healthy</span>	Protected	2 minutes	<span>OK</span>
ContosoVM6	<span>Healthy</span>	Protected	6 minutes	<span>OK</span>
ContosoVM8	<span>Healthy</span>	Protected	4 minutes	<span>OK</span>

2. You can view and filter information. On the action menu at the top, you can perform actions for a particular machine, including running a test failover, or viewing specific errors.
3. Click **Columns** to show additional columns. For example to show RPO, target configuration issues, and replication errors.
4. Click **Filter** to view information based on specific parameters such as replication health, or a particular replication policy.
5. Right-click a machine to initiate operations such as test failover for it, or to view specific error details associated with it.
6. Click a machine to drill into more details for it. Details include:
  - **Replication information:** Current status and health of the machine.
  - **RPO** (recovery point objective): Current RPO for the virtual machine and the time at which the RPO was last computed.
  - **Recovery points:** Latest available recovery points for the machine.
  - **Failover readiness:** Indicates whether a test failover was run for the machine, the agent version running on the machine (for machines running the Mobility service), and any configuration issues.
  - **Errors:** List of replication error symptoms currently observed on the machine, and possible causes/actions.
  - **Events:** A chronological list of recent events impacting the machine. Error details shows the currently observable error symptoms, while events is a historical record of issues that have impacted the machine.
  - **Infrastructure view:** Shows state of infrastructure for the scenario when machines are replicating to Azure.

## Subscribe to email notifications

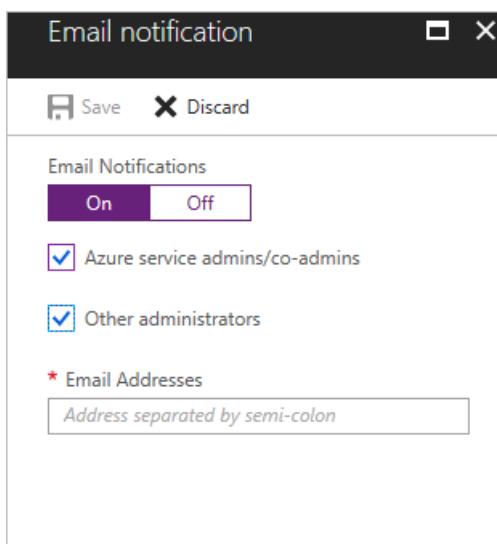
You can subscribe to receive email notifications for these critical events:

- Critical state for replicated machine.
- No connectivity between the on-premises infrastructure components and Site Recovery service. Connectivity between Site Recovery and on-premises servers registered in a vault is detected using a heartbeat mechanism.
- Failover failures.

Subscribe as follows:

In the vault > **Monitoring** section, click **Site Recovery Events**.

1. Click **Email notifications**.
2. In **Email notification**, turn on notifications and specify who to send to. You can send to all subscription admins be sent notifications, and optionally specific email addresses.



## Next steps

[Learn about](#) monitoring Site Recovery with Azure Monitor.

# Monitor Site Recovery with Azure Monitor Logs

11/15/2019 • 7 minutes to read • [Edit Online](#)

This article describes how to monitor machines replicated by Azure [Site Recovery](#), using [Azure Monitor Logs](#), and [Log Analytics](#).

Azure Monitor Logs provide a log data platform that collects activity and diagnostic logs, along with other monitoring data. Within Azure Monitor Logs, you use Log Analytics to write and test log queries, and to interactively analyze log data. You can visualize and query log results, and configure alerts to take actions based on monitored data.

For Site Recovery, you can use Azure Monitor Logs to help you do the following:

- **Monitor Site Recovery health and status.** For example, you can monitor replication health, test failover status, Site Recovery events, recovery point objectives (RPOs) for protected machines, and disk/data change rates.
- **Set up alerts for Site Recovery.** For example, you can configure alerts for machine health, test failover status, or Site Recovery job status.

Using Azure Monitor Logs with Site Recovery is supported for **Azure to Azure** replication, and **VMware VM/physical server to Azure** replication.

## NOTE

To get the churn data logs and upload rate logs for VMware and physical machines, you need to install a Microsoft monitoring agent on the Process Server. This agent sends the logs of the replicating machines to the workspace. This capability is available only for 9.30 mobility agent version onwards.

## Before you start

Here's what you need:

- At least one machine protected in a Recovery Services vault.
- A Log Analytics workspace to store Site Recovery logs. [Learn about](#) setting up a workspace.
- A basic understanding of how to write, run, and analyze log queries in Log Analytics. [Learn more](#).

We recommend that you review [common monitoring questions](#) before you start.

## Configure Site Recovery to send logs

1. In the vault, click **Diagnostic settings > Add diagnostic setting**.

Subscription: Azure Migrate Program Management Team  
Resource group: maygrg  
Resource type: Recovery Services vaults  
Resource: maygvault

NAME	STORAGE ACCOUNT	EVENT HUB	LOG ANALYTIC	EDIT SETTING
hsainidiagnostics	-	-	saliniv2workspace	Edit setting
maygvaultAdiag	-	-	maygl	Edit setting

+ Add diagnostic setting

Click 'Add Diagnostic setting' above to configure the collection of the following data:

- AzureBackupReport
- AzureSiteRecoveryJobs
- AzureSiteRecoveryEvents
- AzureSiteRecoveryReplicatedItems
- AzureSiteRecoveryReplicationStats
- AzureSiteRecoveryRecoveryPoints
- AzureSiteRecoveryReplicationDataUploadRate
- AzureSiteRecoveryProtectedDiskDataChurn

2. In **Diagnostic settings**, specify a name, and check the box **Send to Log Analytics**.
3. Select the Azure Monitor Logs subscription, and the Log Analytics workspace.
4. Select **Azure Diagnostics** in the toggle.
5. From the log list, select all the logs with the prefix **AzureSiteRecovery**. Then click **OK**.

**Diagnostics settings**

\* Name  
DiagnosticSetting1

Archive to a storage account

Stream to an event hub

Send to Log Analytics

Subscription

Log Analytics Workspace

Destination table i  
 Azure diagnostics  Resource specific

LOG

AzureBackupReport

AzureSiteRecoveryJobs

AzureSiteRecoveryEvents

AzureSiteRecoveryReplicatedItems

AzureSiteRecoveryReplicationStats

AzureSiteRecoveryRecoveryPoints

AzureSiteRecoveryReplicationDataUploadRate

AzureSiteRecoveryProtectedDiskDataChurn

The Site Recovery logs start to feed into a table (**AzureDiagnostics**) in the selected workspace.

## Configure Microsoft monitoring agent on the Process Server to send churn and upload rate logs

You can capture the data churn rate information and source data upload rate information for your VMware/physical machines at on-premises. To enable this, a Microsoft monitoring agent is required to be installed on the Process Server.

1. Go to the Log Analytics workspace and click on **Advanced Settings**.
2. Click on **Connected Sources** page and further select **Windows Servers**.
3. Download the Windows Agent (64 bit) on the Process Server.
4. [Obtain the workspace ID and key](#)
5. [Configure agent to use TLS 1.2](#)
6. [Complete the agent installation](#) by providing the obtained workspace ID and key.

- Once the installation is complete, go to Log Analytics workspace and click on **Advanced Settings**. Go to the **Data** page and further click on **Windows Performance Counters**.
- Click on '+' to add the following two counters with sample interval of 300 seconds:

```
ASRAalytics(*)\SourceVmChurnRate
ASRAalytics(*)\SourceVmThrpRate
```

The churn and upload rate data will start feeding into the workspace.

## Query the logs - examples

You retrieve data from logs using log queries written with the [Kusto query language](#). This section provides a few examples of common queries you might use for Site Recovery monitoring.

### NOTE

Some of the examples use **replicationProviderName\_s** set to **A2A**. This retrieves Azure VMs that are replicated to a secondary Azure region using Site Recovery. In these examples, you can replace **A2A** with **InMageAzureV2**, if you want to retrieve on-premises VMware VMs or physical servers that are replicated to Azure using Site Recovery.

### Query replication health

This query plots a pie chart for the current replication health of all protected Azure VMs, broken down into three states: Normal, Warning, or Critical.

```
AzureDiagnostics
|wherereplicationProviderName_s=="A2A"
|whereisnotempty(name_s)andisnotnull(name_s)
|summarizehint.strategy=partitionedarg_max(TimeGenerated, *)byname_s
|projectname_s,replicationHealth_s
|summarizecount()byreplicationHealth_s
|renderpiechart
```

### Query Mobility service version

This query plots a pie chart for Azure VMs replicated with Site Recovery, broken down by the version of the Mobility agent that they're running.

```
AzureDiagnostics
|wherereplicationProviderName_s=="A2A"
|whereisnotempty(name_s)andisnotnull(name_s)
|summarizehint.strategy=partitionedarg_max(TimeGenerated, *)byname_s
|projectname_s,agentVersion_s
|summarizecount()byagentVersion_s
|renderpiechart
```

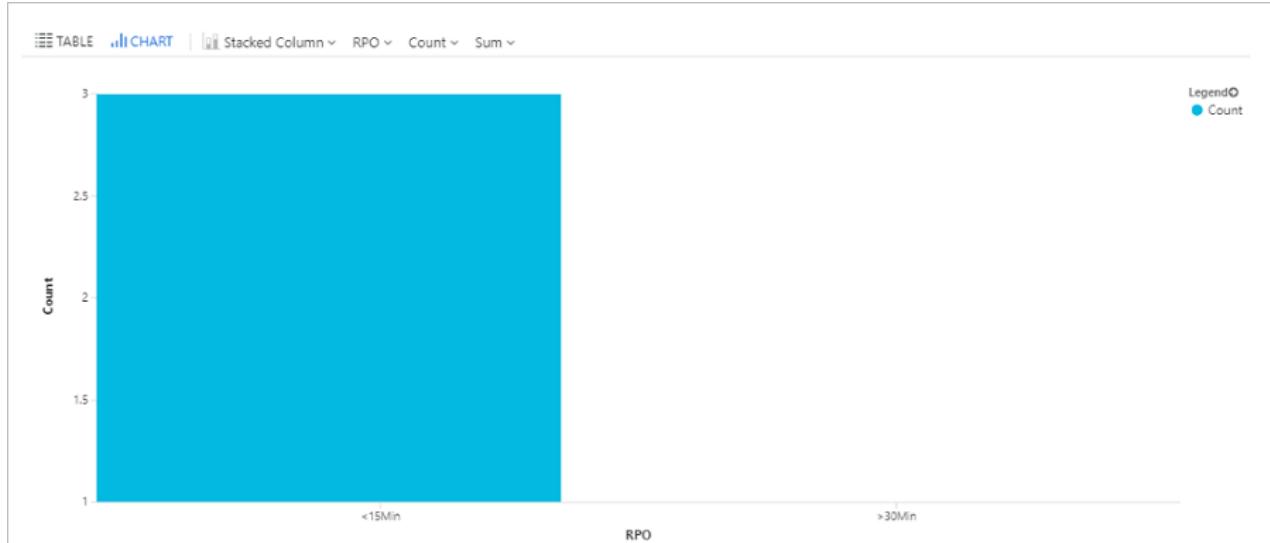
### Query RPO time

This query plots a bar chart of Azure VMs replicated with Site Recovery, broken down by recovery point objective (RPO): Less than 15 minutes, between 15-30 minutes, more than 30 minutes.

```

AzureDiagnostics
|wherereplicationProviderName_s=="A2A"
|whereisnotempty(name_s)andisnotnull(name_s)
|extendRPO = case(rpoInSeconds_d<=900,"<15Min",
rpoInSeconds_d<=1800,"15-30Min",>30Min")
|summarizehint.strategy=partitionedarg_max(TimeGenerated, *)byname_s
|projectname_s, RPO
|summarizeCount =count()byRPO
|renderbarchart

```



## Query Site Recovery jobs

This query retrieves all Site Recovery jobs (for all disaster recovery scenarios), triggered in the last 72 hours, and their completion state.

```

AzureDiagnostics
|whereCategory == "AzureSiteRecoveryJobs"
|whereTimeGenerated >= ago(72h)
|projectJobName=OperationName,VaultName= Resource ,TargetName=affectedResourceName_s, State =ResultType

```

## Query Site Recovery events

This query retrieves all Site Recovery events (for all disaster recovery scenarios) raised in the last 72 hours, along with their severity.

```

AzureDiagnostics
|whereCategory == "AzureSiteRecoveryEvents"
|whereTimeGenerated >= ago(72h)
|projectAffectedObject=affectedResourceName_s,VaultName= Resource,Description_s=healthErrors_s, Severity =
Level

```

## Query test failover state (pie chart)

This query plots a pie chart for the test failover status of Azure VMs replicated with Site Recovery.

```

AzureDiagnostics
|wherereplicationProviderName_s=="A2A"
|whereisnotempty(name_s)andisnotnull(name_s)
|whereisnotempty(failoverHealth_s)andisnotnull(failoverHealth_s)
|summarizehint.strategy=partitionedarg_max(TimeGenerated, *)byname_s
|projectname_s, Resource,failoverHealth_s
|summarizecount()byfailoverHealth_s
|renderpiechart

```

## Query test failover state (table)

This query plots a table for the test failover status of Azure VMs replicated with Site Recovery.

```

AzureDiagnostics
|wherereplicationProviderName_s=="A2A"
|whereisnotempty(name_s)andisnotnull(name_s)
|whereisnotempty(failoverHealth_s)andisnotnull(failoverHealth_s)
|summarizehint.strategy=partitionedarg_max(TimeGenerated, *)byname_s
|projectVirtualMachine=name_s,VaultName=Resource ,TestFailoverStatus=failoverHealth_s

```

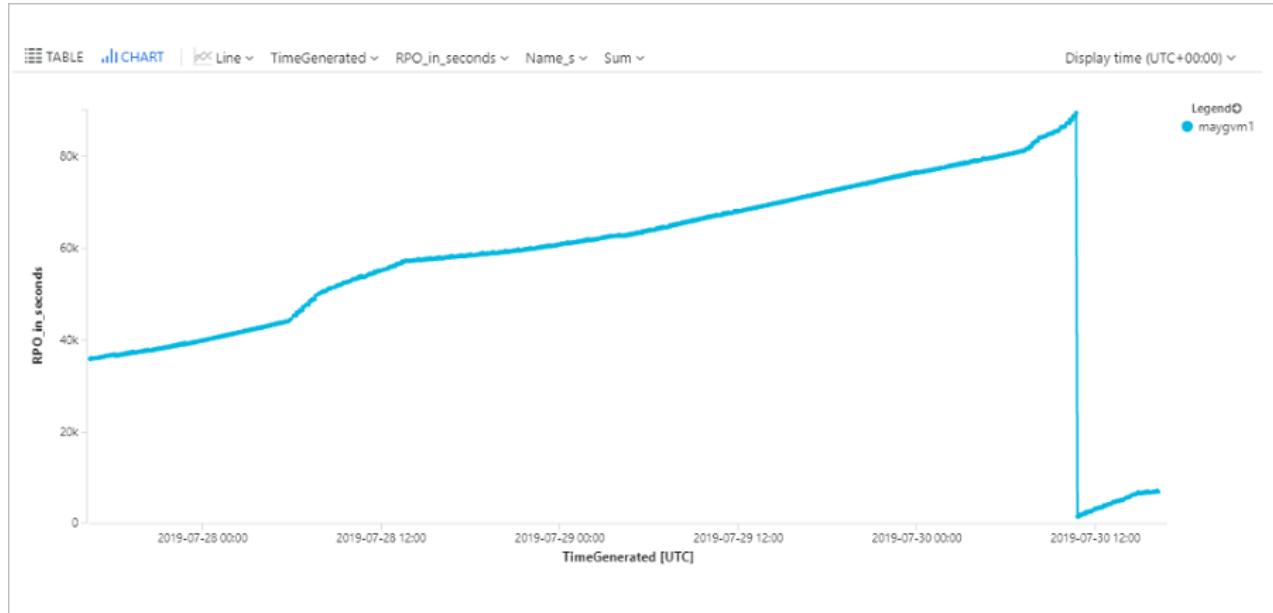
## Query machine RPO

This query plots a trend graph that tracks the RPO of a specific Azure VM (ContosoVM123) for the last 72 hours.

```

AzureDiagnostics
|wherereplicationProviderName_s=="A2A"
|whereTimeGenerated > ago(72h)
|whereisnotempty(name_s)andisnotnull(name_s)
|wherename_s=="ContosoVM123"
|projectTimeGenerated,name_s,RPO_in_seconds=rpoInSeconds_d
|rendertimechart

```



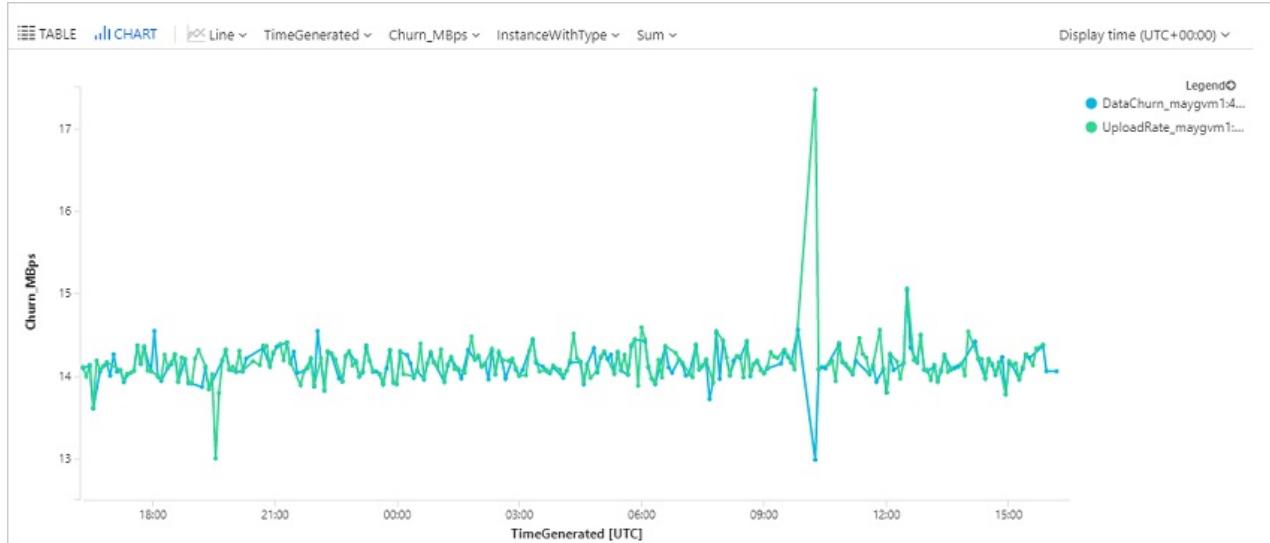
## Query data change rate (churn) and upload rate for an Azure VM

This query plots a trend graph for a specific Azure VM (ContosoVM123), that represents the data change rate (Write Bytes per Second), and data upload rate.

```

AzureDiagnostics
|whereCategory in ("AzureSiteRecoveryProtectedDiskDataChurn", "AzureSiteRecoveryReplicationDataUploadRate")
|extendCategoryS=case(Categorycontains"Churn", "DataChurn",
Categorycontains"Upload", "UploadRate", "none")
|extendInstanceWithType=strcat(CategoryS, "_", InstanceName_s)
|whereTimeGenerated > ago(24h)
|whereInstanceName_sstartswith"ContosoVM123"
|projectTimeGenerated, InstanceWithType, Churn_MBps=todouble(Value_s)/1048576
|rendertimechart

```



## Query data change rate (churn) and upload rate for a VMware or physical machine

### NOTE

Ensure you set up the monitoring agent on the Process Server to fetch these logs. Refer [steps to configure monitoring agent](#).

This query plots a trend graph for a specific disk **disk0** of a replicated item **win-9r7sfh9qlru**, that represents the data change rate (Write Bytes per Second), and data upload rate. You can find the disk name on **Disk**s blade of the replicated item in the recovery services vault. Instance name to be used in the query is DNS name of the machine followed by \_ and disk name as in this example.

```

Perf
| where ObjectName == "ASRAalytics"
| where InstanceName contains "win-9r7sfh9qlru_disk0"
| where TimeGenerated >= ago(4h)
| project TimeGenerated ,CounterName, Churn_MBps = todouble(CounterValue)/5242880
| render timechart

```

Process Server pushes this data every 5 minutes to the Log Analytics workspace. These data points represent the average computed for 5 minutes.

## Query disaster recovery summary (Azure to Azure)

This query plots a summary table for Azure VMs replicated to a secondary Azure region. It shows VM name, replication and protection status, RPO, test failover status, Mobility agent version, any active replication errors, and the source location.

```
AzureDiagnostics
|wherereplicationProviderName_s=="A2A"
|whereisnotempty(name_s)andisnotnull(name_s)
|summarizehint.strategy=partitionedarg_max(TimeGenerated, *)byname_s
|projectVirtualMachine=name_s, Vault = Resource ,ReplicationHealth=replicationHealth_s, Status
=protectionState_s,RPO_in_seconds=rpoInSeconds_d,TestFailoverStatus=failoverHealth_s,AgentVersion=agentVersion
_s,ReplicationError=replicationHealthErrors_s,SourceLocation=primaryFabricName_s
```

## Query disaster recovery summary (VMware/physical servers)

This query plots a summary table for VMware VMs and physical servers replicated to Azure. It shows machine name, replication and protection status, RPO, test failover status, Mobility agent version, any active replication errors, and the relevant process server.

```
AzureDiagnostics
|wherereplicationProviderName_s=="InMageAzureV2"
|whereisnotempty(name_s)andisnotnull(name_s)
|summarizehint.strategy=partitionedarg_max(TimeGenerated, *)byname_s
|projectVirtualMachine=name_s, Vault = Resource ,ReplicationHealth=replicationHealth_s, Status
=protectionState_s,RPO_in_seconds=rpoInSeconds_d,TestFailoverStatus=failoverHealth_s,AgentVersion=agentVersion
_s,ReplicationError=replicationHealthErrors_s,ProcessServer=processServerName_g
```

## Set up alerts - examples

You can set up Site Recovery alerts based on Azure Monitor data. [Learn more](#) about setting up log alerts.

### NOTE

Some of the examples use **replicationProviderName\_s** set to **A2A**. This sets alerts for Azure VMs that are replicated to a secondary Azure region. In these examples, you can replace **A2A** with **InMageAzureV2** if you want to set alerts for on-premises VMware VMs or physical servers replicated to Azure.

### Multiple machines in a critical state

Set up an alert if more than 20 replicated Azure VMs go into a Critical state.

```
AzureDiagnostics
|wherereplicationProviderName_s=="A2A"
|wherereplicationHealth_s=="Critical"
|whereisnotempty(name_s)andisnotnull(name_s)
|summarizehint.strategy=partitionedarg_max(TimeGenerated, *)byname_s
|summarizecount()
```

For the alert, set **Threshold value** to 20.

### Single machine in a critical state

Set up an alert if a specific replicated Azure VM goes into a Critical state.

```
AzureDiagnostics
|wherereplicationProviderName_s=="A2A"
|wherereplicationHealth_s=="Critical"
|wherename_s=="ContosoVM123"
|whereisnotempty(name_s)andisnotnull(name_s)
|summarizehint.strategy=partitionedarg_max(TimeGenerated, *)byname_s
|summarizecount()
```

For the alert, set **Threshold value** to 1.

## Multiple machines exceed RPO

Set up an alert if the RPO for more than 20 Azure VMs exceeds 30 minutes.

```
AzureDiagnostics
|wherereplicationProviderName_s=="A2A"
|whereisnotempty(name_s)andisnotnull(name_s)
|whererpoInSeconds_d> 1800
|summarizehint.strategy=partitionedarg_max(TimeGenerated, *)byname_s
|projectname_s,rpoInSeconds_d
|summarizecount()
```

For the alert, set **Threshold value** to 20.

## Single machine exceeds RPO

Set up an alert if the RPO for a single Azure VM exceeds 30 minutes.

```
AzureDiagnostics
|wherereplicationProviderName_s=="A2A"
|whereisnotempty(name_s)andisnotnull(name_s)
|wherename_s=="ContosoVM123"
|whererpoInSeconds_d> 1800
|summarizehint.strategy=partitionedarg_max(TimeGenerated, *)byname_s
|projectname_s,rpoInSeconds_d
|summarizecount()
```

For the alert, set **Threshold value** to 1.

## Test failover for multiple machines exceeds 90 days

Set up an alert if the last successful test failover was more than 90 days, for more than 20 VMs.

```
AzureDiagnostics
|wherereplicationProviderName_s=="A2A"
|whereCategory == "AzureSiteRecoveryReplicatedItems"
|whereisnotempty(name_s)andisnotnull(name_s)
|wherelastSuccessfulTestFailoverTime_t<= ago(90d)
|summarizehint.strategy=partitionedarg_max(TimeGenerated, *)byname_s
|summarizecount()
```

For the alert, set **Threshold value** to 20.

## Test failover for single machine exceeds 90 days

Set up an alert if the last successful test failover for a specific VM was more than 90 days ago.

```
AzureDiagnostics
|wherereplicationProviderName_s=="A2A"
|whereCategory == "AzureSiteRecoveryReplicatedItems"
|whereisnotempty(name_s)andisnotnull(name_s)
|wherelastSuccessfulTestFailoverTime_t<= ago(90d)
|wherename_s=="ContosoVM123"
|summarizehint.strategy=partitionedarg_max(TimeGenerated, *)byname_s
|summarizecount()
```

For the alert, set **Threshold value** to 1.

## Site Recovery job fails

Set up an alert if a Site Recovery job (in this case the Reprotect job) fails for any Site Recovery scenario, during the last day.

```
AzureDiagnostics
|whereCategory == "AzureSiteRecoveryJobs"
|whereOperationName=="Reprotect"
|whereResultType=="Failed"
|summarizecount()
```

For the alert, set **Threshold value** to 1, and **Period** to 1440 minutes, to check failures in the last day.

## Next steps

[Learn about](#) inbuilt Site Recovery monitoring.

# Monitor the process server

11/14/2019 • 3 minutes to read • [Edit Online](#)

This article describes how to monitor the [Site Recovery](#) process server.

- The process server is used when you set up disaster recovery of on-premises VMware VMs and physical servers to Azure.
- By default the process server runs on the configuration server. It's installed by default when you deploy the configuration server.
- Optionally, to scale and handle larger numbers of replicated machines and higher volumes of replication traffic, you can deploy additional, scale-out process servers.

[Learn more](#) about the role and deployment of process servers.

## Monitoring overview

Since the process server has so many roles, particularly in replicated data caching, compression, and transfer to Azure, it's important to monitor process server health on an ongoing basis.

There are a number of situations that commonly affect process server performance. Issues affecting performance will have a cascading effect on VM health, eventually pushing both the process server and its replicated machines into a critical state. Situations include:

- High numbers of VMs use a process server, approaching or exceeding recommended limitations.
- VMs using the process server have a high churn rate.
- Network throughput between VMs and the process server isn't enough to upload replication data to the process server.
- Network throughput between the process server and Azure isn't sufficient to upload replication data from the process server to Azure.

All of these issues can affect the recovery point objective (RPO) of VMs.

**Why?** Because generating a recovery point for a VM requires all disks on the VM to have a common point. If one disk has a high churn rate, replication is slow, or the process server isn't optimal, it impacts how efficiently recovery points are created.

## Monitor proactively

To avoid issues with the process server, it's important to:

- Understand specific requirements for process servers using [capacity and sizing guidance](#), and make sure process servers are deployed and running according to recommendations.
- Monitor alerts, and troubleshoot issues as they occur, to keep process servers running efficiently.

## Process server alerts

The process server generates a number of health alerts, summarized in the following table.

ALERT TYPE	DETAILS
	Process server is connected and healthy.
	CPU utilization > 80% for the last 15 minutes
	Memory usage > 80% for the last 15 minutes
	Cache folder free space < 30% for the last 15 minutes
	Site Recovery monitors pending/outgoing data every five minutes, and estimates that data in the process server cache can't be uploaded to Azure within 30 minutes.
	Process server services aren't running for the last 15 minutes
	CPU utilization > 95% for the last 15 minutes
	Memory usage > 95% for the last 15 minutes
	Cache folder free space < 25% for the last 15 minutes
	Site Recovery monitors pending/outgoing data every five minutes, and estimates that data in the process server cache can't be uploaded to Azure within 45 minutes.
	No heartbeat from the process server for 15 minutes.



Healthy



Warning



Critical

#### NOTE

The overall health status of the process server is based on the worst alert generated.

## Monitor process server health

You can monitor the health state of your process servers as follows:

1. To monitor the replication health and status of a replicated machine, and of its process server, in vault > **Replicated items**, click the machine you want to monitor.
2. In **Replication Health**, you can monitor the VM health status. Click the status to drill down for error

details.

Home > VishalMachine2

VishalMachine2

Overview

General Properties Compute and Network Disks

F failover T test failover C cleanup test failover K commit R synchronize P change recovery point M complete migration A re-protect D disable replication E error details

Essentials

Health and status

Replication Health: Critical (Protected)

Latest available recovery points

Crash-consistent: 11/28/2016, 4:05:51 PM

App-consistent: 11/28/2016, 4:05:38 PM

F failover readiness

Last successful Test Failover: Never performed successfully

Configuration issues: 1 issue(s)

Agent version: 3.3.00

Process Server Health: Warning

Errors(2)

Error ID: 70144

Error Message: No application consistent recovery point available for the VM in the last 240 minutes.

Possible causes:

- App consistent recovery point threshold exceeded.
- Issues in the volume shadow copy service (Windows) are causing application consistent snapshot failures.
- Replication is progressing slowly or is not progressing as expected.
- The target storage account is not provisioned with sufficient throughput or IOPs to handle the volume of replication data.

Events - Last 72 hours(2)

TIME	EVENT NAME	SEVERITY
12/17/2018, 7:41:10 AM	App-consistent recovery p...	Information
12/15/2018, 7:35:32 PM	App-consistent recovery p...	Information

Infrastructure view

On-premises

```
graph LR; vCenter[vCenter server
vCenter] --- CS[Configuration Server
VISHALCONTROL]; VM[Virtual machine
vishalmachine2] --- CS; CS --- ASR[Azure Site Recovery]; ASR --- SA[Storage account(s)
HGSTORAGE]
```

Azure

Table view

3. In **Process Server Health**, you can monitor the status of the process server. Drill down for details.

Home > v2atest2v2 - Replicated items > v2a-test-1 > CS1921

## CS1921

Process Server

Load balance Switch Error Details

Essentials

Recovery Services vault	v2atest2v2	Server ID	108febbb-c7b6-47fe-9085-c7fd8af05760
FQDN	CS1921	IP address	10.150.208.92
Process Server version	9.21.0.0	Protected items	4
Last heartbeat at	3/14/2019, 11:03:57 AM		

### Process Server health

Processor queue	0
CPU utilization	2% used
Memory usage	UnKnown
Free space	99.27% (615.47 GB free of 620 GB)
Process server services	Running
Certificate Expires On	2/21/2022, 5:01:41 AM

4. Health can also be monitored using the graphical representation on the VM page.

- A scale-out process server will be highlighted in orange if there are warnings associated with it, and red if it has any critical issues.
- If the process server is running in the default deployment on the configuration server, then the configuration server will be highlighted accordingly.
- To drill down, click on the configuration server or process server. Note any issues, and any remediation recommendations.

You can also monitor process servers in the vault under **Site Recovery Infrastructure**. In **Manage your Site Recovery infrastructure**, click **Configuration Servers**. Select the configuration server associated with the process server, and drill down into process server details.

## Next steps

- If you have any process servers issues, follow our [troubleshooting guidance](#)
- If you need more help, post your question in the [Azure Site Recovery forum](#).

# Troubleshoot Azure-to-Azure VM replication errors

1/11/2020 • 17 minutes to read • [Edit Online](#)

This article describes how to troubleshoot common errors in Azure Site Recovery during replication and recovery of Azure virtual machines (VMs) from one region to another. For more information about supported configurations, see the [support matrix for replicating Azure VMs](#).

## Azure resource quota issues (error code 150097)

Make sure your subscription is enabled to create Azure VMs in the target region that you plan to use as your disaster-recovery region. Also make sure your subscription has sufficient quota to create VMs of the necessary sizes. By default, Site Recovery chooses a target VM size that's the same as the source VM size. If the matching size isn't available, Site Recovery automatically chooses the closest available size.

If there's no size that supports the source VM configuration, the following message appears:

"Replication couldn't be enabled for the virtual machine *VmName*."

### Possible causes

- Your subscription ID isn't enabled to create any VMs in the target region location.
- Your subscription ID isn't enabled, or doesn't have sufficient quota, to create specific VM sizes in the target region location.
- No suitable target VM size is found to match the source VM's network interface card (NIC) count (2), for the subscription ID in the target region location.

### Fix the problem

Contact [Azure billing support](#) to enable your subscription to create VMs of the required sizes in the target location. Then, retry the failed operation.

If the target location has a capacity constraint, disable replication to it. Then, enable replication to a different location where your subscription has sufficient quota to create VMs of the required sizes.

## Trusted root certificates (error code 151066)

If not all the latest trusted root certificates are present on the VM, your "Enable replication" Site Recovery job might fail. Authentication and authorization of Site Recovery service calls from the VM fail without these certificates.

If the "Enable replication" job fails, the following message appears:

"Site Recovery configuration failed."

### Possible cause

The trusted root certificates required for authorization and authentication aren't present on the virtual machine.

### Fix the problem

#### Windows

For a VM running the Windows operating system, install the latest Windows updates on the VM so that all the trusted root certificates are present on the machine. Follow the typical Windows update-management or certificate update-management process in your organization to get the latest root certificates and the updated certificate-

revocation list on the VMs.

If you're in a disconnected environment, follow the standard Windows update process in your organization to get the certificates. If the required certificates aren't present on the VM, the calls to the Site Recovery service fail for security reasons.

To verify that the issue is resolved, go to [login.microsoftonline.com](https://login.microsoftonline.com) from a browser in your VM.

For more information, see [Configure trusted roots and disallowed certificates](#).

#### Linux

Follow the guidance provided by the distributor of your Linux operating system version to get the latest trusted root certificates and the latest certificate-revocation list on the VM.

Because SUSE Linux uses symbolic links (or *symlinks*) to maintain a certificate list, follow these steps:

1. Sign in as a root user.
2. Run this command to change the directory:

```
cd /etc/ssl/certs
```

3. Check whether the Symantec root CA certificate is present:

```
ls VeriSign_Class_3_Public_Primary_Certification_Authority_G5.pem
```

4. If the Symantec root CA certificate is not found, run the following command to download the file. Check for any errors and follow recommended actions for network failures.

```
wget https://www.symantec.com/content/dam/symantec/docs/other-resources/verisign-class-3-public-primary-certification-authority-g5-en.pem -O
VeriSign_Class_3_Public_Primary_Certification_Authority_G5.pem
```

5. Check whether the Baltimore root CA certificate is present:

```
ls Baltimore_CyberTrust_Root.pem
```

6. If the Baltimore root CA certificate is not found, run this command to download the certificate:

```
wget https://www.digicert.com/CACerts/BaltimoreCyberTrustRoot.crt.pem -O
Baltimore_CyberTrust_Root.pem
```

7. Check whether the DigiCert\_Global\_Root\_CA certificate is present:

```
ls DigiCert_Global_Root_CA.pem
```

8. If the DigiCert\_Global\_Root\_CA is not found, run the following commands to download the certificate:

```
wget http://www.digicert.com/CACerts/DigiCertGlobalRootCA.crt

openssl x509 -in DigiCertGlobalRootCA.crt -inform der -outform pem -out
DigiCert_Global_Root_CA.pem
```

9. Run the rehash script to update the certificate subject hashes for the newly downloaded certificates:

```
c_rehash
```

10. Run these commands to check whether the subject hashes as symlinks have been created for the certificates:

- Command:

```
ls -l | grep Baltimore
```

- Output:

```
1rwxrwxrwx 1 root root 29 Jan 8 09:48 3ad48a91.0 -> Baltimore_CyberTrust_Root.pem
```

```
-rw-r--r-- 1 root root 1303 Jun 5 2014 Baltimore_CyberTrust_Root.pem
```

- Command:

```
ls -l | grep VeriSign_Class_3_Public_Primary_Certification_Authority_G5
```

- Output:

```
-rw-r--r-- 1 root root 1774 Jun 5 2014
VeriSign_Class_3_Public_Primary_Certification_Authority_G5.pem
```

```
1rwxrwxrwx 1 root root 62 Jan 8 09:48 facacbc6.0 ->
VeriSign_Class_3_Public_Primary_Certification_Authority_G5.pem
```

- Command:

```
ls -l | grep DigiCert_Global_Root
```

- Output:

```
1rwxrwxrwx 1 root root 27 Jan 8 09:48 399e7759.0 -> DigiCert_Global_Root_CA.pem
```

```
-rw-r--r-- 1 root root 1380 Jun 5 2014 DigiCert_Global_Root_CA.pem
```

- Create a copy of the file VeriSign\_Class\_3\_Public\_Primary\_Certification\_Authority\_G5.pem with filename b204d74a.0:

```
cp VeriSign_Class_3_Public_Primary_Certification_Authority_G5.pem b204d74a.0
```

- Create a copy of the file Baltimore\_CyberTrust\_Root.pem with filename 653b494a.0:

```
cp Baltimore_CyberTrust_Root.pem 653b494a.0
```

- Create a copy of the file DigiCert\_Global\_Root\_CA.pem with filename 3513523f.0:

```
cp DigiCert_Global_Root_CA.pem 3513523f.0
```

- Check whether the files are present:

- Command:

```
ls -l 653b494a.0 b204d74a.0 3513523f.0
```

- Output

```
-rw-r--r-- 1 root root 1774 Jan 8 09:52 3513523f.0
```

```
-rw-r--r-- 1 root root 1303 Jan 8 09:52 653b494a.0
```

```
-rw-r--r-- 1 root root 1774 Jan 8 09:52 b204d74a.0
```

## Outbound connectivity for Site Recovery URLs or IP ranges (error code 151037 or 151072)

For Site Recovery replication to work, outbound connectivity is required from the VM to specific URLs or IP ranges. If your VM is behind a firewall or uses network security group (NSG) rules to control outbound connectivity, you might face one of these issues.

### **Issue 1: Failed to register the Azure virtual machine with Site Recovery (error code 151195)**

#### **Possible cause**

The connection to Site Recovery endpoints can't be established because of a DNS resolution failure.

This problem happens most frequently during reprottection, when you have failed over the virtual machine but the DNS server is not reachable from the disaster-recovery (DR) region.

#### Fix the problem

If you're using a custom DNS, make sure that the DNS server is accessible from the disaster-recovery region. To find out whether you have a custom DNS, on the VM, go to *disaster recovery network > DNS servers*.

The screenshot shows the Azure portal interface for managing a virtual network. The left sidebar lists various network-related settings like Address space, Connected devices, Subnets, DDoS protection, Firewall, and DNS servers. The 'DNS servers' section is currently selected. On the right, under 'Custom' DNS, the IP address '10.1.4.6' is listed. There is also a 'Save' and 'Discard' button at the top right.

Try accessing the DNS server from the virtual machine. If the server is not accessible, make it accessible either by failing over the DNS server or by creating the line of site between the DR network and the DNS.

#### Issue 2: Site Recovery configuration failed (error code 151196)

##### Possible cause

The connection to Office 365 authentication and identity IP4 endpoints can't be established.

#### Fix the problem

Site Recovery requires access to Office 365 IP ranges for authentication. If you're using Azure NSG rules or firewall proxy to control outbound network connectivity on the VM, be sure you allow communication to Office 365 IP ranges. Create an NSG rule based on an [Azure Active Directory \(Azure AD\) service tag](#), allowing access to all IP addresses corresponding to Azure AD. If new addresses are added to Azure AD in the future, you must create new NSG rules.

##### NOTE

If VMs are behind a *Standard* internal load balancer, the load balancer by default does not have access to Office 365 IP ranges (that is, login.microsoftonline.com). Either change the internal load balancer type to *Basic* or create outbound access as described in the article [Configure load balancing and outbound rules](#).

#### Issue 3: Site Recovery configuration failed (error code 151197)

##### Possible cause

The connection can't be established to Site Recovery service endpoints.

#### Fix the problem

Site Recovery requires access to [Site Recovery IP ranges](#), depending on the region. Make sure that the required IP ranges are accessible from the virtual machine.

#### **Issue 4: Azure-to-Azure replication failed when the network traffic goes through an on-premises proxy server (error code 151072)**

##### **Possible cause**

The custom proxy settings are invalid, and the Site Recovery Mobility Service agent did not auto-detect the proxy settings from Internet Explorer.

##### **Fix the problem**

The Mobility Service agent detects the proxy settings from Internet Explorer on Windows and from /etc/environment on Linux.

If you prefer to set the proxy only for the Mobility Service, you can provide the proxy details in the ProxyInfo.conf file in these locations:

- **Linux:** /usr/local/InMage/config/
- **Windows:** C:\ProgramData\Microsoft Azure Site Recovery\Config

In ProxyInfo.conf, provide the proxy settings in the following initialization-file format:

[proxy]

Address=<http://1.2.3.4>

Port=567

##### **NOTE**

The Site Recovery Mobility Service agent supports only *un-authenticated proxies*.

#### **More information**

To specify [required URLs](#) or required IP ranges, follow the guidance in [About networking in Azure to Azure replication](#).

## Disk not found in the machine (error code 150039)

A new disk attached to the VM must be initialized. If the disk is not found, the following message appears:

"Azure data disk *DiskName DiskURI* with logical unit number *LUN LUNValue* was not mapped to a corresponding disk being reported from within the VM that has the same LUN value.

##### **Possible causes**

- A new data disk was attached to the VM but wasn't initialized.
- The data disk inside the VM is not correctly reporting the logical unit number (LUN) value at which the disk was attached to the VM.

##### **Fix the problem**

Make sure that the data disks are initialized, and then retry the operation.

- **Windows:** [Attach and initialize a new disk](#).
- **Linux:** [Initialize a new data disk in Linux](#).

If the problem persists, contact support.

## One or more disks are available for protection (error code 153039)

### Possible causes

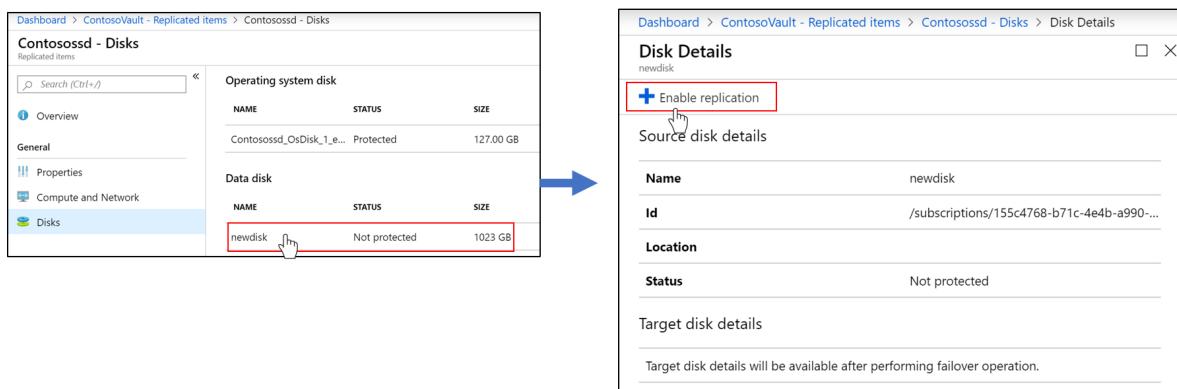
- One or more disks were recently added to the virtual machine after protection.
- One or more disks were initialized after protection of the virtual machine.

### Fix the problem

To make the replication status of the VM healthy again, you can choose either to protect the disks or to dismiss the warning.

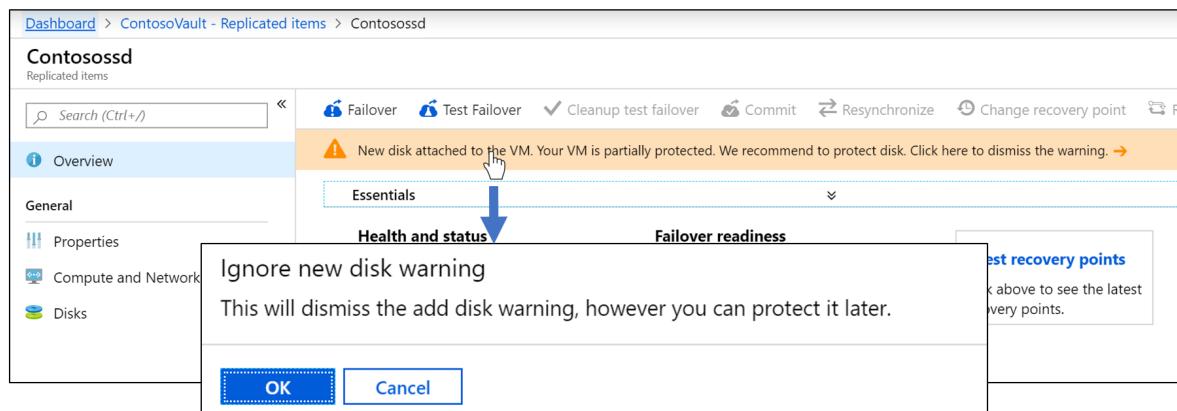
#### To protect the disks

1. Go to **Replicated Items > VM name > Disks**.
2. Select the unprotected disk, and then select **Enable replication**:



#### To dismiss the warning

1. Go to **Replicated items > VM name**.
2. Select the warning in the **Overview** section, and then select **OK**.



## Remove the virtual machine from the vault completed with information (error code 150225)

When it protects the virtual machine, Site Recovery creates some links on the source virtual machine. When you remove the protection or disable replication, Site Recovery removes these links as a part of the cleanup job. If the virtual machine has a resource lock, the cleanup job gets completed with the information. The information says that the virtual machine has been removed from the Recovery Services vault, but that some of the stale links couldn't be cleaned up on the source machine.

You can ignore this warning if you never intend to protect this virtual machine again. But if you have to protect this

virtual machine later, follow the steps under "Fix the problem" to clean up the links.

#### WARNING

If you don't do the cleanup:

- When you enable replication by means of the Recovery Services vault, the virtual machine won't be listed.
- If you try to protect the VM by using **Virtual machine > Settings > Disaster Recovery**, the operation will fail with the message "Replication cannot be enabled because of the existing stale resource links on the VM."

#### Fix the problem

#### NOTE

Site Recovery doesn't delete the source virtual machine or affect it in any way while you perform these steps.

1. Remove the lock from the VM or VM resource group. For example, in the following image, the resource lock on the VM named "MoveDemo" must be deleted:

LOCK NAME	LOCK TYPE	SCOPE	NOTES
cannotdelete	Read-only	This resource	mylock to test behaviour

2. Download the script to [remove a stale Site Recovery configuration](#).
3. Run the script, which is called Cleanup-stale-asr-config-Azure-VM.ps1. Supply the subscription ID, VM Resource Group, and VM name as parameters.
4. If you're asked for Azure credentials, provide them. Then verify that the script runs without any failures.

## Replication can't be enabled because of stale resource links on the VM (error code 150226)

#### Possible cause

The virtual machine has a stale configuration from previous Site Recovery protection.

A stale configuration can occur on an Azure VM if you enabled replication for the Azure VM by using Site Recovery, and then:

- You disabled replication, but the source VM had a resource lock.
- You deleted the Site Recovery vault without explicitly disabling replication on the VM.
- You deleted the resource group containing the Site Recovery vault without explicitly disabling replication on the VM.

#### Fix the problem

#### NOTE

Site Recovery doesn't delete the source virtual machine or affect it in any way while you perform these steps.

1. Remove the lock from the VM or VM resource group. For example, in the following image, the resource lock on the VM named "MoveDemo" must be deleted:

The screenshot shows the 'MoveDemo - Locks' page in the Azure portal. On the left, there's a sidebar with options: Configuration, Identity, Properties, Locks (which is selected and highlighted in blue), and Export template. The main area has a search bar and buttons for Add, Resource group, Subscription, and Refresh. A table lists locks with columns: LOCK NAME, LOCK TYPE, SCOPE, and NOTES. One row is highlighted with a red box: 'cannotdelete' (LOCK NAME), 'Read-only' (LOCK TYPE), 'This resource' (SCOPE), and 'mylock to test behaviour' (NOTES).

2. Download the script to [remove a stale Site Recovery configuration](#).
3. Run the script, which is called Cleanup-stale-asr-config-Azure-VM.ps1. Supply the subscription ID, VM Resource Group, and VM name as parameters.
4. If you're asked for Azure credentials, provide them. Then verify that the script runs without any failures.

## Unable to see the Azure VM or resource group for the selection in the "Enable replication" job

### Cause 1: The resource group and source virtual machine are in different locations

Site Recovery currently requires the source region resource group and virtual machines to be in the same location. If they are not, you won't be able to find the virtual machine or resource group when you try to apply protection.

As a workaround, you can enable replication from the VM instead of the Recovery Services vault. Go to **Source VM > Properties > Disaster Recovery** and enable the replication.

### Cause 2: The resource group is not part of the selected subscription

You might not be able to find the resource group at the time of protection if the resource group is not part of the selected subscription. Make sure that the resource group belongs to the subscription that you're using.

### Cause 3: Stale configuration

You might not see the VM that you want to enable for replication if a stale Site Recovery configuration has been left on the Azure VM. This condition could occur if you enabled replication for the Azure VM by using Site Recovery, and then:

- You deleted the Site Recovery vault without explicitly disabling replication on the VM.
- You deleted the resource group containing the Site Recovery vault without explicitly disabling replication on the VM.
- You disabled replication, but the source VM had a resource lock.

### Fix the problem

#### NOTE

Make sure to update the "AzureRM.Resources" module before using the script mentioned in this section. Site Recovery doesn't delete the source virtual machine or affect it in any way while you perform these steps.

1. Remove the lock, if any, from the VM or VM resource group. For example, in the following image, the resource lock on the VM named "MoveDemo" must be deleted:

The screenshot shows the Azure portal interface for managing locks on a virtual machine named 'MoveDemo'. On the left, there's a sidebar with options like Configuration, Identity, Properties, Locks (which is selected), and Export template. The main area is titled 'MoveDemo - Locks' and shows a table with columns: LOCK NAME, LOCK TYPE, SCOPE, and NOTES. One row in the table is highlighted with a red border. The row contains the following data:

LOCK NAME	LOCK TYPE	SCOPE	NOTES
cannotdelete	Read-only	This resource	mylock to test behaaviour

2. Download the script to [remove a stale Site Recovery configuration](#).
3. Run the script, which is called Cleanup-stale-asr-config-Azure-VM.ps1. Supply the subscription ID, VM Resource Group, and VM name as parameters.
4. If you're asked for Azure credentials, provide them. Then verify that the script runs without any failures.

## Unable to select a virtual machine for protection

### Cause 1: The virtual machine has an extension installed in a failed or unresponsive state

Go to **Virtual machines** > **Settings** > **Extensions** and check for any extensions in a failed state. Uninstall any failed extension, and then try again to protect the virtual machine.

### Cause 2: The VM's provisioning state is not valid

See the troubleshooting steps in [The VM's provisioning state is not valid](#), later in this article.

## The VM's provisioning state is not valid (error code 150019)

To enable replication on the VM, its provisioning state must be **Succeeded**. Follow these steps to check the provisioning state:

1. In the Azure portal, select the **Resource Explorer** from **All Services**.
2. Expand the **Subscriptions** list and select your subscription.
3. Expand the **ResourceGroups** list and select the resource group of the VM.
4. Expand the **Resources** list and select your VM.
5. Check the **provisioningState** field in Instance view on the right side.

### Fix the problem

- If **provisioningState** is **Failed**, contact support with details to troubleshoot.
- If **provisioningState** is **Updating**, another extension might be being deployed. Check whether there are any ongoing operations on the VM, wait for them to finish, and then retry the failed Site Recovery "Enable replication" job.

## Unable to select target VM (network selection tab is unavailable)

## Cause 1: Your VM is attached to a network that's already mapped to a target network

If the source VM is part of a virtual network, and another VM from the same virtual network is already mapped with a network in the target resource group, the network-selection drop-down list box is unavailable (appears dimmed) by default.

The screenshot shows the 'Configure disaster recovery' page. Under 'Target settings', there is a table with three rows:

	SOURCE	TARGET
VM resource group	[redacted]	[redacted] <input type="button" value="▼"/>
Availability set	[redacted]-ASR	[redacted] <input type="button" value="▼"/>
Virtual network	[redacted] vnet-asr	[redacted] vnet-asr-asr <input type="button" value="▼"/>

## Cause 2: You previously protected the VM by using Site Recovery, and then you disabled the replication

Disabling replication of a VM doesn't delete the network mapping. The mapping must be deleted from the Recovery Services vault where the VM was protected. Go to *Recovery Services vault > Site Recovery Infrastructure > Network Mapping*.

### Infrastructure > Network Mapping

The screenshot shows the 'Network mappings' blade. It displays a table of network mappings:

SOURCE NETWORK	SOURCE	TARGET NETWORK	TARGET
[redacted]-vnet	South India	[redacted]-vnet-asr	Central India
[redacted]-vnet-asr	Central India	[redacted]-vnet	[redacted]

A context menu is open over the second row, showing options: 'Pin to dashboard' and 'Delete'.

The target network that was configured during the disaster-recovery setup can be changed after the initial setup, after the VM is protected:

Note that changing network mapping affects all protected VMs that use that same network mapping.

## COM+ or Volume Shadow Copy service error (error code 151025)

When this error occurs, the following message appears:

"Site Recovery extension failed to install"

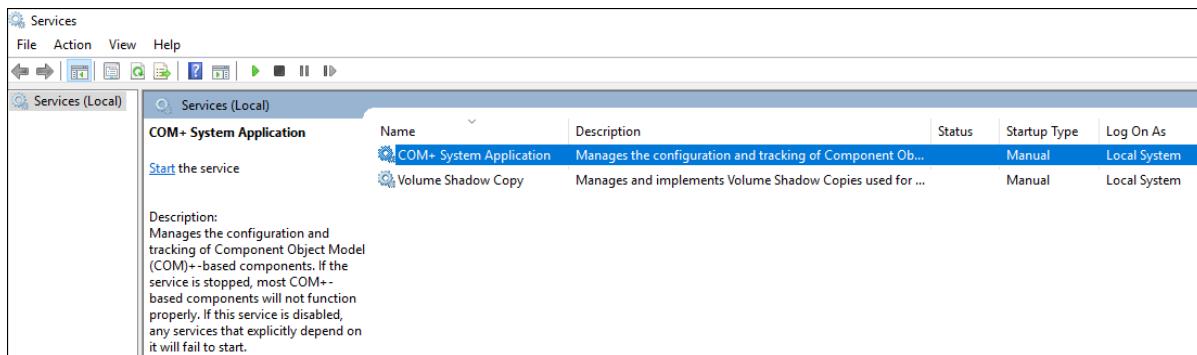
### Possible causes

- The COM+ System Application service is disabled.
- The Volume Shadow Copy service is disabled.

### Fix the problem

Set the COM+ System Application and Volume Shadow Copy services to automatic or manual startup mode.

- Open the Services console in Windows.
- Make sure the COM+ System Application and Volume Shadow Copy services are not set to **Disabled** as their **Startup Type**.



## Unsupported managed-disk size (error code 150172)

When this error occurs, the following message appears:

"Protection couldn't be enabled for the virtual machine as it has *DiskName* with size *DiskSize*\* that is lesser than the minimum supported size 1024 MB."

### Possible cause

The disk is smaller than the supported size of 1024 MB.

### Fix the problem

Make sure that the disk size is within the supported size range, and then retry the operation.

## Protection was not enabled because the GRUB configuration includes

## the device name instead of the UUID (error code 151126)

### Possible cause

The Linux GRUB configuration files (`/boot/grub/menu.lst`, `/boot/grub/grub.cfg`, `/boot/grub2/grub.cfg`, or `/etc/default/grub`) might specify the actual device names instead of UUID values for the `root` and `resume` parameters. Site Recovery requires UUIDs because device names can change. Upon restart, a VM might not come up with the same name on failover, resulting in problems.

The following examples are lines from GRUB files where device names (shown in bold) appear instead of the required UUIDs:

- File `/boot/grub2/grub.cfg`

```
linux /boot/vmlinuz-3.12.49-11-default root=/dev/sda2 ${extra_cmdline} resume=/dev/sda1
splash=silent quiet showopts
```

- File: `/boot/grub/menu.lst`

```
kernel /boot/vmlinuz-3.0.101-63-default root=/dev/sda2 resume=/dev/sda1 splash=silent
crashkernel=256M:128M showopts vga=0x314
```

### Fix the problem

Replace each device name with the corresponding UUID:

1. Find the UUID of the device by executing the command **`blkid device name`**. For example:

```
blkid /dev/sda1
/dev/sda1: UUID="6f614b44-433b-431b-9ca1-4dd2f6f74f6b" TYPE="swap"
blkid /dev/sda2
/dev/sda2: UUID="62927e85-f7ba-40bc-9993-cc1feeb191e4" TYPE="ext3"
```

2. Replace the device name with its UUID, in the formats **`root=UUID=UUID`** and **`resume=UUID=UUID`**. For example, after replacement, the line from `/boot/grub/menu.lst` (discussed earlier) would look like this:

```
kernel /boot/vmlinuz-3.0.101-63-default root=UUID=62927e85-f7ba-40bc-9993-cc1feeb191e4
resume=UUID=6f614b44-433b-431b-9ca1-4dd2f6f74f6b splash=silent crashkernel=256M:128M
showopts vga=0x314
```

3. Retry the protection.

## Enable protection failed because the device mentioned in the GRUB configuration doesn't exist (error code 151124)

### Possible cause

The GRUB configuration files (`/boot/grub/menu.lst`, `/boot/grub/grub.cfg`, `/boot/grub2/grub.cfg`, or `/etc/default/grub`) might contain the parameters `rd.lvm.lv` or `rd_LVM_LV`. These parameters identify the Logical Volume Manager (LVM) devices that are to be discovered at boot time. If these LVM devices don't exist, the protected system itself won't boot and will be stuck in the boot process. The same problem will also be seen with the failover VM. Here are few examples:

- File: `/boot/grub2/grub.cfg` on RHEL7:

```
linux16 /vmlinuz-3.10.0-957.el7.x86_64 root=/dev/mapper/rhel_mup--rhel7u6-root ro
```

```
crashkernel=128M@64M rd.lvm.lv=rootvg/root rd.lvm.lv=rootvg/swap rhgb quiet
LANG=en_US.UTF-8
```

- File: /etc/default/grub on RHEL7:

```
GRUB_CMDLINE_LINUX="crashkernel=auto rd.lvm.lv=rootvg/root rd.lvm.lv=rootvg/swap rhgb
quiet"
```

- File: /boot/grub/menu.lst on RHEL6:

```
kernel /vmlinuz-2.6.32-754.el6.x86_64 ro root=UUID=36dd8b45-e90d-40d6-81ac-ad0d0725d69e
rd_NO_LUKS LANG=en_US.UTF-8 rd_NO_MD SYSFONT=latarcyrheb-sun16 crashkernel=auto
rd_LVM_LV=rootvg/lv_root KEYBOARDTYPE=pc KEYTABLE=us rd_LVM_LV=rootvg/lv_swap
rd_NO_DM rhgb quiet
```

In each example, the portion in bold shows that the GRUB has to detect two LVM devices with the names "root" and "swap" from the volume group "rootvg."

### Fix the problem

If the LVM device doesn't exist, either create it or remove the corresponding parameters from the GRUB configuration files. Then, try again to enable protection.

## A Site Recovery Mobility Service update finished with warnings (error code 151083)

The Site Recovery Mobility Service has many components, one of which is called the filter driver. The filter driver is loaded into system memory only during system restart. Whenever a Mobility Service update includes filter driver changes, the machine is updated but you still see a warning that some fixes require a restart. The warning appears because the filter driver fixes can take effect only when the new filter driver is loaded, which happens only during a restart.

#### NOTE

This is only a warning. Existing replication continues to work even after the new agent update. You can choose to restart whenever you want the benefits of the new filter driver, but the old filter driver keeps working if you don't restart.

Apart from the filter driver, the benefits of any other enhancements and fixes in the Mobility Service update take effect without requiring a restart.

## Protection couldn't be enabled because the replica managed disk already exists, without expected tags, in the target resource group (error code 150161)

### Possible cause

This problem can occur if the virtual machine was previously protected, and when replication was disabled, the replica disk was not cleaned.

### Fix the problem

Delete the replica disk identified in the error message and retry the failed protection job.

## Next steps

[Replicate Azure virtual machines](#)

# Troubleshoot Azure-to-Azure VM network connectivity issues

1/14/2020 • 4 minutes to read • [Edit Online](#)

This article describes the common issues related to network connectivity when you replicate and recover Azure virtual machines from one region to another region. For more information about networking requirements, see the [connectivity requirements for replicating Azure VMs](#).

For Site Recovery replication to work, outbound connectivity to specific URLs or IP ranges is required from the VM. If your VM is behind a firewall or uses network security group (NSG) rules to control outbound connectivity, you might face one of these issues.

URL	DETAILS
*.blob.core.windows.net	Required so that data can be written to the cache storage account in the source region from the VM. If you know all the cache storage accounts for your VMs, you can allow-list the specific storage account URLs (for example, cache1.blob.core.windows.net and cache2.blob.core.windows.net) instead of *.blob.core.windows.net
login.microsoftonline.com	Required for authorization and authentication to the Site Recovery service URLs.
*.hypervrecoverymanager.windowsazure.com	Required so that the Site Recovery service communication can occur from the VM. You can use the corresponding 'Site Recovery IP' if your firewall proxy supports IPs.
*.servicebus.windows.net	Required so that the Site Recovery monitoring and diagnostics data can be written from the VM. You can use the corresponding 'Site Recovery Monitoring IP' if your firewall proxy supports IPs.

## Outbound connectivity for Site Recovery URLs or IP ranges (error code 151037 or 151072)

### Issue 1: Failed to register Azure virtual machine with Site Recovery (151195)

#### • Possible cause

- Connection cannot be established to Site Recovery endpoints due to DNS resolution failure.
- This is more frequently seen during re-protection when you have failed over the virtual machine but the DNS server is not reachable from the DR region.

#### • Resolution

- If you're using custom DNS, make sure that the DNS server is accessible from the Disaster Recovery region. To check if you have a custom DNS go to the VM > Disaster Recovery network > DNS servers. Try accessing the DNS server from the virtual machine. If it is not accessible, make it accessible by

either failing over the DNS server or creating the line of site between DR network and DNS.

The screenshot shows the Azure portal interface for managing a virtual machine named 'sap-ad'. The 'Networking' section is selected. Under 'DNS servers', the 'Custom' option is chosen, and the IP address '10.1.4.6' is listed. There is a 'Save' button at the top right and an 'Add DNS server' button at the bottom.

## Issue 2: Site Recovery configuration failed (151196)

### NOTE

If the virtual machines are behind **Standard** internal load balancer, it would not have access to O365 IPs (that is, login.microsoftonline.com) by default. Either change it to **Basic** internal load balancer type or create outbound access as mentioned in the [article](#).

### • Possible cause

- Connection cannot be established to Office 365 authentication and identity IP4 endpoints.

### • Resolution

- Azure Site Recovery required access to Office 365 IPs ranges for authentication. If you are using Azure Network security group (NSG) rules/firewall proxy to control outbound network connectivity on the VM, ensure you allow communication to O365 IP ranges. Create an [Azure Active Directory \(Azure AD\) service tag](#) based NSG rule for allowing access to all IP addresses corresponding to Azure AD
  - If new addresses are added to Azure AD in the future, you need to create new NSG rules.

### Example NSG configuration

This example shows how to configure NSG rules for a VM to replicate.

- If you're using NSG rules to control outbound connectivity, use "Allow HTTPS outbound" rules to port:443 for all the required IP address ranges.
- The example presumes that the VM source location is "East US" and the target location is "Central US".

### NSG rules - East US

1. Create an outbound HTTPS (443) security rule for "Storage.EastUS" on the NSG as shown in the screenshot below.

Add outbound security rule  
A2ANSG-nsg

Basic

\* Source VirtualNetwork

\* Source port ranges \*

\* Destination Service Tag

Destination service tag Storage.EastUS

\* Destination port ranges 443

\* Protocol Any TCP UDP

\* Action Allow Deny

\* priority 2500

\* Name Allow-Storage-account-access

Description  
Allow outbound to Storage accounts

OK

This screenshot shows the configuration of an outbound security rule in Azure. The rule is named 'Allow-Storage-account-access' and is set to allow TCP port 443 from the virtual network to the 'Storage.EastUS' service tag. The priority is 2500, and the action is 'Allow'. The description indicates it allows outbound access to Storage accounts.

2. Create an outbound HTTPS (443) security rule for "AzureActiveDirectory" on the NSG as shown in the screenshot below.

Add outbound security rule

AZANSG-nsg

**Basic**

\* Source: VirtualNetwork

\* Source port ranges: \*

\* Destination: Service Tag

Destination service tag: AzureActiveDirectory

\* Destination port range: 443

\* Protocol: TCP

\* Action: Allow

\* Priority: 2600

\* Name: Allow-Azure-Active-Directory

Description: Allow outbound to Azure Active Directory

**Add**

3. Create outbound HTTPS (443) rules for the Site Recovery IPs that correspond to the target location:

LOCATION	SITE RECOVERY IP ADDRESS	SITE RECOVERY MONITORING IP ADDRESS
Central US	40.69.144.231	52.165.34.144

#### NSG rules - Central US

These rules are required so that replication can be enabled from the target region to the source region post-failover:

1. Create an outbound HTTPS (443) security rule for "Storage.CentralUS" on the NSG.
2. Create an outbound HTTPS (443) security rule for "AzureActiveDirectory" on the NSG.
3. Create outbound HTTPS (443) rules for the Site Recovery IPs that correspond to the source location:

LOCATION	SITE RECOVERY IP ADDRESS	SITE RECOVERY MONITORING IP ADDRESS
Central US	13.82.88.226	104.45.147.24

## Issue 3: Site Recovery configuration failed (151197)

- **Possible cause**
  - Connection cannot be established to Azure Site Recovery service endpoints.
- **Resolution**

- Azure Site Recovery required access to [Site Recovery IP ranges](#) depending on the region. Make sure that required ip ranges are accessible from the virtual machine.

## Issue 4: A2A replication failed when the network traffic goes through on-premises proxy server (151072)

- **Possible cause**

- The custom proxy settings are invalid, and Azure Site Recovery Mobility Service agent did not auto-detect the proxy settings from IE

- **Resolution**

1. Mobility Service agent detects the proxy settings from IE on Windows and /etc/environment on Linux.
2. If you prefer to set proxy only for Azure Site Recovery Mobility Service, you can provide the proxy details in ProxyInfo.conf located at:
  - `/usr/local/InMage/config/` on **Linux**
  - `C:\ProgramData\Microsoft Azure Site Recovery\Config` on **Windows**
3. The ProxyInfo.conf should have the proxy settings in the following INI format.

```
[proxy]
Address=http://1.2.3.4
Port=567
```
4. Azure Site Recovery Mobility Service agent supports only ***un-authenticated proxies***.

### Fix the problem

To allow [the required URLs](#) or the [required IP ranges](#), follow the steps in the [networking guidance document](#).

## Next steps

[Replicate Azure virtual machines](#)

# Troubleshoot replication in Azure VM disaster recovery

2/12/2020 • 7 minutes to read • [Edit Online](#)

This article describes common problems in Azure Site Recovery when you're replicating and recovering Azure virtual machines from one region to another region. It also explains how to troubleshoot the common problems. For more information about supported configurations, see the [support matrix for replicating Azure VMs](#).

Azure Site Recovery consistently replicates data from the source region to the disaster recovery region. It also creates a crash-consistent recovery point every 5 minutes. If Site Recovery can't create recovery points for 60 minutes, it alerts you with this information:

Error message: "No crash consistent recovery point available for the VM in the last 60 minutes."

Error ID: 153007

The following sections describe causes and solutions.

## High data change rate on the source virtual machine

Azure Site Recovery creates an event if the data change rate on the source virtual machine is higher than the supported limits. To see whether the problem is because of high churn, go to **Replicated items > VM > Events - last 72 hours**. You should see the event "Data change rate beyond supported limits":

Filter items...						
NAME	SOURCE	TYPE	\$...	SEVERITY	TIME	
Virtual machine health is in Warning state.	ContosoWin2016	Virtual machine status	as...	<span style="color: orange;">⚠</span> Warning	10/24/2018, 4:25:35 PM	
Data change rate beyond supported limits.	ContosoWin2016	Virtual machine status	as...	<span style="color: orange;">⚠</span> Warning	10/24/2018, 4:25:34 PM	
Virtual machine health is in OK state.	ContosoWin2016	Virtual machine status	as...	<span style="color: blue;">ℹ</span> Information	10/24/2018, 3:17:44 PM	
Virtual machine health is in Critical state.	ContosoWin2016	Virtual machine status	as...	<span style="color: red;">✖</span> Critical	10/24/2018, 2:05:55 PM	
Recent crash consistent recovery point not available.	ContosoWin2016	Virtual machine status	as...	<span style="color: red;">✖</span> Critical	10/24/2018, 2:05:55 PM	
Virtual machine health is in Warning state.	ContosoWin2016	Virtual machine status	as...	<span style="color: orange;">⚠</span> Warning	10/24/2018, 1:05:18 PM	
Data change rate beyond supported limits.	ContosoWin2016	Virtual machine status	as...	<span style="color: orange;">⚠</span> Warning	10/24/2018, 1:05:18 PM	

If you select the event, you should see the exact disk information:

## Event Details

□ X

EVENT NAME	Data change rate beyond supported limits.
EVENT TYPE	VmHealth
SOURCE	ContosoWin2016
ASSOCIATED SERVERS	asr-a2a-default-centralus
TIME	2018-10-24T07:35:18.539329Z
ERROR ID	153018

ERROR MESSAGE	The data change rate(churn) for one or more replicating disks(ContosoWin2016_OsDisk_1_6fb798fbbf5f410bac0d234ad4511666) has exceeded the Azure Site Recovery supported limits: <a href="https://aka.ms/asr-a2a-target-limits">https://aka.ms/asr-a2a-target-limits</a> .
---------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

## Azure Site Recovery limits

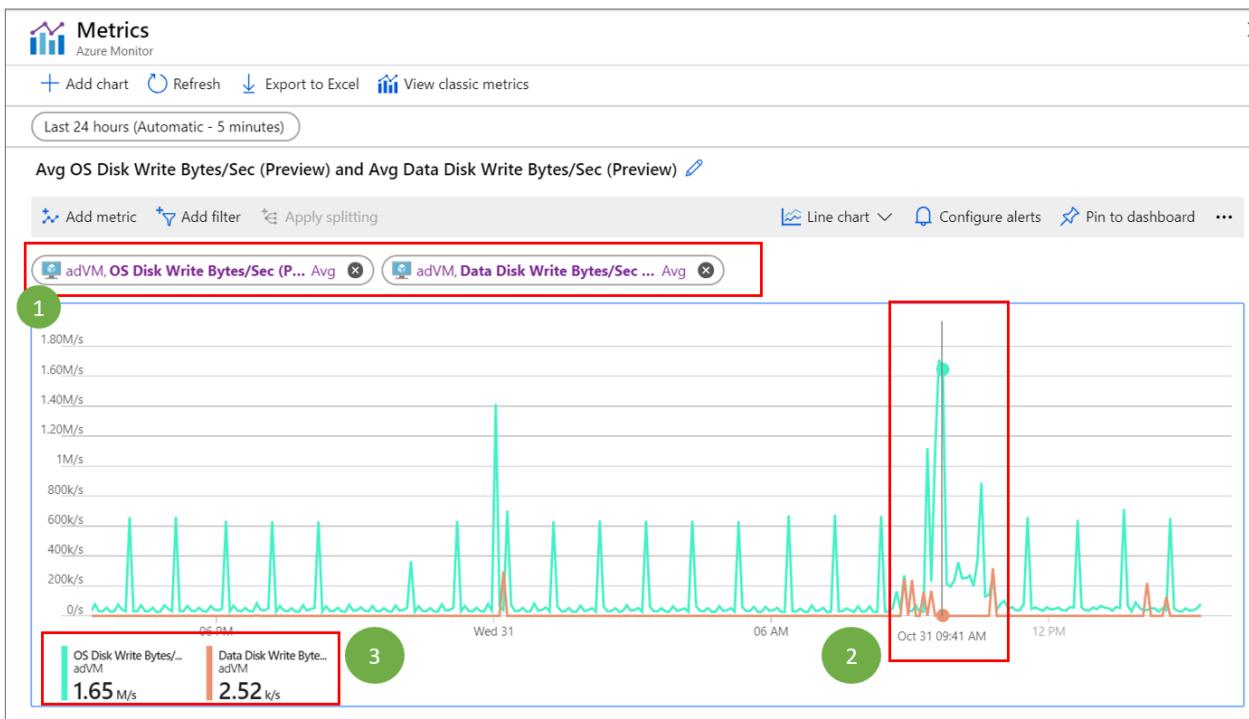
The following table provides the Azure Site Recovery limits. These limits are based on our tests, but they can't cover all possible application input-output (I/O) combinations. Actual results can vary based on your application I/O mix.

There are two limits to consider: data churn per disk and data churn per virtual machine. Let's look at the Premium P20 disk in the following table for an example. For a single VM, Site Recovery can handle 5 MB/s of churn per disk with a maximum of five such disks. Site Recovery has a limit of 25 MB/s of total churn per VM.

REPLICATION STORAGE TARGET	AVERAGE I/O SIZE FOR SOURCE DISK	AVERAGE DATA CHURN FOR SOURCE DISK	TOTAL DATA CHURN PER DAY FOR SOURCE DATA DISK
Standard storage	8 KB	2 MB/s	168 GB per disk
Premium P10 or P15 disk	8 KB	2 MB/s	168 GB per disk
Premium P10 or P15 disk	16 KB	4 MB/s	336 GB per disk
Premium P10 or P15 disk	32 KB or greater	8 MB/s	672 GB per disk
Premium P20 or P30 or P40 or P50 disk	8 KB	5 MB/s	421 GB per disk
Premium P20 or P30 or P40 or P50 disk	16 KB or greater	10 MB/s	842 GB per disk

## Solution

Azure Site Recovery has limits on data change rates, depending on the type of disk. To see if this problem is recurring or temporary, find the data change rate of the affected virtual machine. Go to the source virtual machine, find the metrics under **Monitoring**, and add the metrics as shown in this screenshot:



1. Select **Add metric**, and add **OS Disk Write Bytes/Sec** and **Data Disk Write Bytes/Sec**.
2. Monitor the spike as shown in the screenshot.
3. View the total write operations happening across OS disks and all data disks combined. These metrics might not give you information at the per-disk level, but they indicate the total pattern of data churn.

A spike in data change rate might come from an occasional data burst. If the data change rate is greater than 10 MB/s (for Premium) or 2 MB/s (for Standard) and comes down, replication will catch up. If the churn is consistently well beyond the supported limit, consider one of these options:

- Exclude the disk that's causing a high data-change rate: First, disable the replication. Then you can exclude the disk by using [PowerShell](#).
- Change the tier of the disaster recovery storage disk: This option is possible only if the disk data churn is less than 20 MB/s. Let's say a VM with a P10 disk has a data churn of greater than 8 MB/s but less than 10 MB/s. If the customer can use a P30 disk for target storage during protection, the problem can be solved. This solution is only possible for machines that are using Premium-Managed Disks. Follow these steps:

1. Go to **Disks** of the affected replicated machine and copy the replica disk name.
2. Go to this replica of the managed disk.
3. You might see a banner in **Overview** that says an SAS URL has been generated. Select this banner and cancel the export. Ignore this step if you don't see the banner.
4. As soon as the SAS URL is revoked, go to **Configuration** for the managed disk. Increase the size so that Site Recovery supports the observed churn rate on the source disk.

## Network connectivity problems

### Network latency to a cache storage account

Site Recovery sends replicated data to the cache storage account. You might experience network latency if uploading the data from a virtual machine to the cache storage account is slower than 4 MB in 3 seconds.

To check for a problem related to latency, use [AzCopy](#). You can use this command-line utility to upload data from the virtual machine to the cache storage account. If the latency is high, check whether you're using a network virtual appliance (NVA) to control outbound network traffic from VMs. The appliance might get throttled if all the replication traffic passes through the NVA.

We recommend creating a network service endpoint in your virtual network for "Storage" so that the replication traffic doesn't go to the NVA. For more information, see [Network virtual appliance configuration](#).

## Network connectivity

For Site Recovery replication to work, it needs the VM to provide outbound connectivity to specific URLs or IP ranges. You might have your VM behind a firewall or use network security group (NSG) rules to control outbound connectivity. If so, you might experience issues. To make sure all the URLs are connected, see [Outbound connectivity for Site Recovery URLs](#).

# Error ID 153006 - No app-consistent recovery point available for the VM in the past "X" minutes

Following are some of the most common issues.

### Known issue in SQL server 2008/2008 R2

**How to fix:** There's a known issue with SQL server 2008/2008 R2. Refer to the article [Azure Site Recovery Agent or other non-component VSS backup fails for a server hosting SQL Server 2008 R2](#).

### Azure Site Recovery jobs fail on servers hosting any version of SQL Server instances with AUTO\_CLOSE DBs

**How to fix:** Refer to the article [Non-component VSS backups such as Azure Site Recovery jobs fail on servers hosting SQL Server instances with AUTO\\_CLOSE DBs](#).

### Known issue in SQL Server 2016 and 2017

**How to fix:** Refer to the article [Error occurs when you back up a virtual machine with non-component based backup in SQL Server 2016 and 2017](#).

### You're using Azure Storage Spaces Direct Configuration

**How to fix:** Azure Site Recovery can't create application consistent recovery point for Storage Spaces Direct Configuration. [Configure the replication policy](#).

### More causes because of VSS-related issues:

To troubleshoot further, check the files on the source machine to get the exact error code for failure:

```
C:\Program Files (x86)\Microsoft Azure Site Recovery\agent\Application Data\ApplicationPolicyLogs\vacp.log
```

To locate the errors in the file, search for the string "vacpError" by opening the vacp.log file in an editor.

```
Ex: vacpError:220#Following disks are in FilteringStopped state [\\.\\PHYSICALDRIVE1=5,]#220|^|224#FAILED:
CheckWriterStatus().#2147754994|^|226#FAILED to revoke tags.FAILED: CheckWriterStatus().#2147754994|^|
```

In the preceding example, **2147754994** is the error code that tells you about the failure following this sentence.

### VSS writer is not installed - Error 2147221164

**How to fix:** To generate application consistency tag, Azure Site Recovery uses Volume Shadow Copy Service (VSS). Site Recovery installs a VSS Provider for its operation to take app consistency snapshots. Azure Site Recovery installs this VSS Provider as a service. If VSS Provider isn't installed, the application consistency snapshot creation fails. It shows the error ID 0x80040154 "Class not registered." Refer to the article for [VSS writer installation troubleshooting](#).

### VSS writer is disabled - Error 2147943458

**How to fix:** To generate the application consistency tag, Azure Site Recovery uses VSS. Site Recovery installs a VSS Provider for its operation to take app consistency snapshots. This VSS Provider is installed as a service. If you don't have the VSS Provider service enabled, the application consistency snapshot creation fails. It shows the error "The specified service is disabled and cannot be started (0x80070422)."

If VSS is disabled:

- Verify that the startup type of the VSS Provider service is set to **Automatic**.
- Restart the following services:
  - VSS service
  - Azure Site Recovery VSS Provider
  - VDS service

#### VSS PROVIDER NOT\_REGISTERED - Error 2147754756

**How to fix:** To generate the application consistency tag, Azure Site Recovery uses VSS. Check whether the Azure Site Recovery VSS Provider service is installed.

Use the following commands to reinstall VSS Provider:

1. Uninstall existing provider: C:\Program Files (x86)\Microsoft Azure Site Recovery\agent\InMageVSSProvider\_Uninstall.cmd
2. Reinstall VSS Provider: C:\Program Files (x86)\Microsoft Azure Site Recovery\agent\InMageVSSProvider\_Install.cmd

Verify that the startup type of the VSS Provider service is set to **Automatic**.

Restart the following services:

- VSS service
- Azure Site Recovery VSS Provider
- VDS service

# Troubleshoot Azure VM extension issues

2/12/2020 • 3 minutes to read • [Edit Online](#)

This article provides troubleshooting steps that can help you resolve Azure Site Recovery errors related to the VM agent and extension.

## Azure Site Recovery extension time-out

Error message: "Task execution has timed out while tracking for extension operation to be started"

Error code: "151076"

Azure Site Recovery installed an extension on the virtual machine as a part of an enable protection job. Any of the following conditions might prevent the protection from being triggered and cause the job to fail. Complete the following troubleshooting steps, and then retry your operation:

- [The agent is installed in the VM, but it's unresponsive \(for Windows VMs\)](#)
- [The agent installed in the VM is out of date \(for Linux VMs\)](#)
- [The Site Recovery extension fails to update or load](#)

Error message: "Previous Site Recovery extension operation is taking more time than expected."

Error code: "150066"

- [The agent is installed in the VM, but it's unresponsive \(for Windows VMs\)](#)
- [The agent installed in the VM is out of date \(for Linux VMs\)](#)
- [The Site Recovery extension status is incorrect](#)

## Protection fails because the VM agent is unresponsive

Error message: "Task execution has timed out while tracking for extension operation to be started."

Error code: "151099"

This error can happen if the Azure guest agent in the virtual machine isn't in the ready state.

You can check the status of Azure guest agent in the [Azure portal](#). Go to the virtual machine you're trying to protect and check the status in **VM > Settings > Properties > Agent status**. Most of the time, the status of the agent is ready after rebooting the virtual machine. However, if you can't reboot or you're still facing the issue, then complete the following troubleshooting steps:

- [The agent is installed in the VM, but it's unresponsive \(for Windows VMs\)](#)
- [The agent installed in the VM is out of date \(for Linux VMs\)](#)

Error message: "Task execution has timed out while tracking for extension operation to be started."

Error code: "151095"

This error occurs when the agent version on the Linux machine is out of date. Complete the following troubleshooting step:

- [The agent installed in the VM is out of date \(for Linux VMs\)](#)

## Causes and solutions

### The agent is installed in the VM, but it's unresponsive (for Windows VMs)

#### Solution

The VM agent might have been corrupted, or the service might have been stopped. Reinstalling the VM agent helps get the latest version. It also helps restart communication with the service.

1. Determine whether the Windows Azure Guest Agent service is running in the VM services (`services.msc`).  
Restart the Windows Azure Guest Agent service.
2. If the Windows Azure Guest Agent service isn't visible in services, open the Control Panel. Go to **Programs and Features** to see whether the Windows Guest Agent service is installed.
3. If the Windows Azure Guest Agent appears in **Programs and Features**, uninstall the Windows Azure Guest Agent.
4. Download and install the [latest version of the agent MSI](#). You need administrator rights to complete the installation.
5. Verify that the Windows Azure Guest Agent service appears in services.
6. Restart the protection job.

Also, verify that [Microsoft .NET 4.5 is installed](#) in the VM. You need .NET 4.5 for the VM agent to communicate with the service.

### The agent installed in the VM is out of date (for Linux VMs)

#### Solution

Most agent-related or extension-related failures for Linux VMs are caused by issues that affect an outdated VM agent. To troubleshoot this issue, follow these general guidelines:

1. Follow the instructions for [updating the Linux VM agent](#).

#### NOTE

We strongly recommend that you update the agent only through a distribution repository. We don't recommend downloading the agent code directly from GitHub and updating it. If the latest agent for your distribution isn't available, contact distribution support for instructions on how to install it. To check for the most recent agent, go to the [Windows Azure Linux agent](#) page in the GitHub repository.

2. Ensure that the Azure agent is running on the VM by running the following command: `ps -e`

If the process isn't running, restart it by using the following commands:

- For Ubuntu: `service walinuxagent start`
- For other distributions: `service waagent start`

3. [Configure the automatic restart agent](#).

4. Enable protection of the virtual machine.

### The Site Recovery extension fails to update or load

The extension status shows as "Empty," "NotReady," or "Transitioning."

#### Solution

Uninstall the extension and restart the operation again.

To uninstall the extension:

1. In the [Azure portal](#), go to the VM that is experiencing Backup failure.
2. Select **Settings**.
3. Select **Extensions**.
4. Select **Site Recovery Extension**.
5. Select **Uninstall**.

For Linux VM, if the VMSnapshot extension does not show in the Azure portal, [update the Azure Linux Agent](#). Then run the protection.

When you complete these steps, it causes the extension to be reinstalled during the protection.

# Troubleshoot replication issues for VMware VMs and physical servers

11/22/2019 • 9 minutes to read • [Edit Online](#)

This article describes some common issues and specific errors you might encounter when you replicate on-premises VMware VMs and physical servers to Azure using [Site Recovery](#).

## Step 1: Monitor process server health

Site Recovery uses the [process server](#) to receive and optimize replicated data, and send it to Azure.

We recommend that you monitor the health of process servers in portal, to ensure that they are connected and working properly, and that replication is progressing for the source machines associated with the process server.

- [Learn about](#) monitoring process servers.
- [Review best practices](#)
- [Troubleshoot](#) process server health.

## Step 2: Troubleshoot connectivity and replication issues

Initial and ongoing replication failures often are caused by connectivity issues between the source server and the process server or between the process server and Azure.

To solve these issues, [troubleshoot connectivity and replication](#).

## Step 3: Troubleshoot source machines that aren't available for replication

When you try to select the source machine to enable replication by using Site Recovery, the machine might not be available for one of the following reasons:

- **Two virtual machines with same instance UUID:** If two virtual machines under the vCenter have the same instance UUID, the first virtual machine discovered by the configuration server is shown in the Azure portal. To resolve this issue, ensure that no two virtual machines have the same instance UUID. This scenario is commonly seen in instances where a backup VM becomes active and is logged into our discovery records. Refer to [Azure Site Recovery VMware-to-Azure: How to clean up duplicate or stale entries](#) to resolve.
- **Incorrect vCenter user credentials:** Ensure that you added the correct vCenter credentials when you set up the configuration server by using the OVF template or unified setup. To verify the credentials that you added during setup, see [Modify credentials for automatic discovery](#).
- **vCenter insufficient privileges:** If the permissions provided to access vCenter don't have the required permissions, failure to discover virtual machines might occur. Ensure that the permissions described in [Prepare an account for automatic discovery](#) are added to the vCenter user account.
- **Azure Site Recovery management servers:** If the virtual machine is used as management server under one or more of the following roles - Configuration server /scale-out process server / Master target server, then you will not be able to choose the virtual machine from portal. Managements servers cannot be replicated.
- **Already protected/failed over through Azure Site Recovery services:** If the virtual machine is already protected or failed over through Site Recovery, the virtual machine isn't available to select for protection in the portal. Ensure that the virtual machine you're looking for in the portal isn't already protected by any other user or under a different subscription.

- **vCenter not connected:** Check if vCenter is in connected state. To verify, go to Recovery Services vault > Site Recovery Infrastructure > Configuration Servers > Click on respective configuration server > a blade opens on your right with details of associated servers. Check if vCenter is connected. If it's in a "Not Connected" state, resolve the issue and then [refresh the configuration server](#) on the portal. After this, virtual machine will be listed on the portal.
- **ESXi powered off:** If ESXi host under which the virtual machine resides is in powered off state, then virtual machine will not be listed or will not be selectable on the Azure portal. Power on the ESXi host, [refresh the configuration server](#) on the portal. After this, virtual machine will be listed on the portal.
- **Pending reboot:** If there is a pending reboot on the virtual machine, then you will not be able to select the machine on Azure portal. Ensure to complete the pending reboot activities, [refresh the configuration server](#). After this, virtual machine will be listed on the portal.
- **IP not found:** If the virtual machine doesn't have a valid IP address associated with it, then you will not be able to select the machine on Azure portal. Ensure to assign a valid IP address to the virtual machine, [refresh the configuration server](#). After this, virtual machine will be listed on the portal.

#### **Troubleshoot protected virtual machines greyed out in the portal**

Virtual machines that are replicated under Site Recovery aren't available in the Azure portal if there are duplicate entries in the system. To learn how to delete stale entries and resolve the issue, refer to [Azure Site Recovery VMware-to-Azure: How to clean up duplicate or stale entries](#).

## No crash consistent recovery point available for the VM in the last 'XXX' minutes

Some of the most common issues are listed below

#### **Initial replication issues [error 78169]**

Over an above ensuring that there are no connectivity, bandwidth or time sync related issues, ensure that:

- No anti-virus software is blocking Azure Site Recovery. Learn [more](#) on folder exclusions required for Azure Site Recovery.

#### **Source machines with high churn [error 78188]**

Possible Causes:

- The data change rate (write bytes/sec) on the listed disks of the virtual machine is more than the [Azure Site Recovery supported limits](#) for the replication target storage account type.
- There is a sudden spike in the churn rate due to which high amount of data is pending for upload.

To resolve the issue:

- Ensure that the target storage account type (Standard or Premium) is provisioned as per the churn rate requirement at source.
- If you are already replicating to a Premium managed disk (asrseeddisk type), ensure that the size of the disk supports the observed churn rate as per Site Recovery limits. You can increase the size of the asrseeddisk if required. Follow the below steps:
  - Navigate to the Disks blade of the impacted replicated machine and copy the replica disk name
  - Navigate to this replica managed disk
  - You may see a banner on the Overview blade saying that a SAS URL has been generated. Click on this banner and cancel the export. Ignore this step if you do not see the banner.
  - As soon as the SAS URL is revoked, go to Configuration blade of the Managed Disk and increase the size so that ASR supports the observed churn rate on source disk
- If the observed churn is temporary, wait for a few hours for the pending data upload to catch up and to create recovery points.

- If the disk contains non-critical data like temporary logs, test data etc., consider moving this data elsewhere or completely exclude this disk from replication
- If the problem continues to persist, use the Site Recovery [deployment planner](#) to help plan replication.

### **Source machines with no heartbeat [error 78174]**

This happens when Azure Site Recovery Mobility agent on the Source Machine is not communicating with the Configuration Server (CS).

To resolve the issue, use the following steps to verify the network connectivity from the source VM to the Config Server:

1. Verify that the Source Machine is running.
2. Sign in to the Source Machine using an account that has administrator privileges.
3. Verify that the following services are running and if not restart the services:
  - Svagents (InMage Scout VX Agent)
  - InMage Scout Application Service
4. On the Source Machine, examine the logs at the location for error details:

```
C:\Program Files (X86)\Microsoft Azure Site Recovery\agent\svagents*log
```

### **Process server with no heartbeat [error 806]**

In case there is no heartbeat from the Process Server (PS), check that:

1. PS VM is up and running
2. Check following logs on the PS for error details:

```
C:\ProgramData\ASR\home\svsystems\eventmanager*.log
and
C:\ProgramData\ASR\home\svsystems\monitor_protection*.log
```

### **Master target server with no heartbeat [error 78022]**

This happens when Azure Site Recovery Mobility agent on the Master Target is not communicating with the Configuration Server.

To resolve the issue, use the following steps to verify the service status:

1. Verify that the Master Target VM is running.
2. Sign in to the Master Target VM using an account that has administrator privileges.
  - Verify that the svagents service is running. If it is running, restart the service
  - Check the logs at the location for error details:

```
C:\Program Files (X86)\Microsoft Azure Site Recovery\agent\svagents*log
```

3. To register master target with configuration server, navigate to folder **%PROGRAMDATA%\ASR\Agent**, and run the following on command prompt:

```
cmd
cdpcli.exe --registermt

net stop obengine

net start obengine

exit
```

## Error ID 78144 - No app-consistent recovery point available for the VM in the last 'XXX' minutes

Enhancements have been made in mobility agent [9.23](#) & [9.27](#) versions to handle VSS installation failure behaviors. Ensure that you are on the latest versions for best guidance on troubleshooting VSS failures.

Some of the most common issues are listed below

### Cause 1: Known issue in SQL server 2008/2008 R2

**How to fix :** There is a known issue with SQL server 2008/2008 R2. Please refer this KB article [Azure Site Recovery Agent or other non-component VSS backup fails for a server hosting SQL Server 2008 R2](#)

### Cause 2: Azure Site Recovery jobs fail on servers hosting any version of SQL Server instances with AUTO\_CLOSE DBs

**How to fix :** Refer Kb [article](#)

### Cause 3: Known issue in SQL Server 2016 and 2017

**How to fix :** Refer Kb [article](#)

### More causes due to VSS related issues:

To troubleshoot further, Check the files on the source machine to get the exact error code for failure:

```
C:\Program Files (x86)\Microsoft Azure Site Recovery\agent\Application Data\ApplicationPolicyLogs\vacp.log
```

How to locate the errors in the file? Search for the string "vacpError" by opening the vacp.log file in an editor

```
Ex: vacpError:220#Following disks are in FilteringStopped state [\\.\PHYSICALDRIVE1=5,]#220|^|224#FAILED:
CheckWriterStatus().#2147754994|^|226#FAILED to revoke tags.FAILED: CheckWriterStatus().#2147754994|^|
```

In the above example **2147754994** is the error code that tells you about the failure as shown below

#### VSS writer is not installed - Error 2147221164

**How to fix:** To generate application consistency tag, Azure Site Recovery uses Microsoft Volume Shadow copy Service (VSS). It installs a VSS Provider for its operation to take app consistency snapshots. This VSS Provider is installed as a service. In case the VSS Provider service is not installed, the application consistency snapshot creation fails with the error id 0x80040154 "Class not registered".

Refer [article for VSS writer installation troubleshooting](#)

#### VSS writer is disabled - Error 2147943458

**How to fix:** To generate application consistency tag, Azure Site Recovery uses Microsoft Volume Shadow copy Service (VSS). It installs a VSS Provider for its operation to take app consistency snapshots. This VSS Provider is installed as a service. In case the VSS Provider service is disabled, the application consistency snapshot creation fails with the error id "The specified service is disabled and cannot be started(0x80070422)".

- If VSS is disabled,
  - Verify that the startup type of the VSS Provider service is set to **Automatic**.
  - Restart the following services:

- VSS service
- Azure Site Recovery VSS Provider
- VDS service

#### **VSS PROVIDER NOT\_REGISTERED - Error 2147754756**

**How to fix:** To generate application consistency tag, Azure Site Recovery uses Microsoft Volume Shadow copy Service (VSS). Check if the Azure Site Recovery VSS Provider service is installed or not.

- Retry the Provider installation using the following commands:
- Uninstall existing provider: C:\Program Files (x86)\Microsoft Azure Site Recovery\agent\InMageVSSProvider\_Uninstall.cmd
- Reinstall: C:\Program Files (x86)\Microsoft Azure Site Recovery\agent\InMageVSSProvider\_Install.cmd

Verify that the startup type of the VSS Provider service is set to **Automatic**. - Restart the following services: - VSS service - Azure Site Recovery VSS Provider - VDS service

## Next steps

If you need more help, post your question in the [Azure Site Recovery forum](#). We have an active community, and one of our engineers can assist you.

# Troubleshoot configuration server issues

11/7/2019 • 11 minutes to read • [Edit Online](#)

This article helps you troubleshoot issues when you deploy and manage the [Azure Site Recovery](#) configuration server. The configuration server acts as a management server. Use the configuration server to set up disaster recovery of on-premises VMware VMs and physical servers to Azure by using Site Recovery. The following sections discuss the most common failures you might experience when you add a new configuration server and when you manage a configuration server.

## Registration failures

The source machine registers with the configuration server when you install the mobility agent. You can debug any failures during this step by following these guidelines:

1. Open the C:\ProgramData\ASR\home\svsystems\var\configurator\_register\_host\_static\_info.log file. (The ProgramData folder might be a hidden folder. If you don't see the ProgramData folder, in File Explorer, on the **View** tab, in the **Show/hide** section, select the **Hidden items** check box.) Failures might be caused by multiple issues.
2. Search for the string **No Valid IP Address found**. If the string is found:
  - a. Verify that the requested host ID is the same as the host ID of the source machine.
  - b. Verify that the source machine has at least one IP address assigned to the physical NIC. For agent registration with the configuration server to succeed, the source machine must have at least one valid IP v4 address assigned to the physical NIC.
  - c. Run one of the following commands on the source machine to get all the IP addresses of the source machine:
    - For Windows: > ipconfig /all
    - For Linux: # ifconfig -a
3. If the string **No Valid IP Address found** isn't found, search for the string **Reason=>NULL**. This error occurs if the source machine uses an empty host to register with the configuration server. If the string is found:
  - After you resolve the issues, follow guidelines in [Register the source machine with the configuration server](#) to retry the registration manually.
4. If the string **Reason=>NULL** isn't found, on the source machine, open the C:\ProgramData\ASRSetupLogs\UploadedLogs\ASRUnifiedAgentInstaller.log file. (The ProgramData folder might be a hidden folder. If you don't see the ProgramData folder, in File Explorer, on the **View** tab, in the **Show/hide** section, select the **Hidden items** check box.) Failures might be caused by multiple issues.
5. Search for the string **post request: (7) - Couldn't connect to server**. If the string is found:
  - a. Resolve the network issues between the source machine and the configuration server. Verify that the configuration server is reachable from the source machine by using network tools like ping, traceroute, or a web browser. Ensure that the source machine can reach the configuration server through port 443.
  - b. Check whether any firewall rules on the source machine block the connection between the source machine and the configuration server. Work with your network admins to unblock any connection issues.
  - c. Ensure that the folders listed in [Site Recovery folder exclusions from antivirus programs](#) are excluded from the antivirus software.
  - d. When network issues are resolved, retry the registration by following the guidelines in [Register the source machine with the configuration server](#).

source machine with the configuration server.

6. If the string **post request: (7) - Couldn't connect to server** isn't found, in the same log file, look for the string **request: (60) - Peer certificate cannot be authenticated with given CA certificates**. This error might occur because the configuration server certificate has expired or the source machine doesn't support TLS 1.0 or later SSL protocols. It also might occur if a firewall blocks SSL communication between the source machine and the configuration server. If the string is found:
  - a. To resolve, connect to the configuration server IP address by using a web browser on the source machine. Use the URI `https://<configuration server IP address>:443/`. Ensure that the source machine can reach the configuration server through port 443.
  - b. Check whether any firewall rules on the source machine need to be added or removed for the source machine to talk to the configuration server. Because of the variety of firewall software that might be in use, we can't list all required firewall configurations. Work with your network admins to unblock any connection issues.
  - c. Ensure that the folders listed in [Site Recovery folder exclusions from antivirus programs](#) are excluded from the antivirus software.
  - d. After you resolve the issues, retry the registration by following guidelines in [Register the source machine with the configuration server](#).
7. On Linux, if the value of the platform in <INSTALLATION\_DIR>/etc/drscout.conf is corrupted, registration fails. To identify this issue, open the /var/log/ua\_install.log file. Search for the string **Aborting configuration as VM\_PLATFORM value is either null or it is not VmWare/Azure**. The platform should be set to either **VmWare** or **Azure**. If the drscout.conf file is corrupted, we recommend that you [uninstall the mobility agent](#) and then reinstall the mobility agent. If uninstallation fails, complete the following steps: a. Open the Installation\_Directory/uninstall.sh file and comment out the call to the **StopServices** function. b. Open the Installation\_Directory/Vx/bin/uninstall.sh file and comment out the call to the **stop\_services** function. c. Open the Installation\_Directory/Fx/uninstall.sh file and comment out the entire section that's trying to stop the Fx service. d. [Uninstall](#) the mobility agent. After successful uninstallation, reboot the system, and then try to reinstall the mobility agent.

## Installation failure: Failed to load accounts

This error occurs when the service can't read data from the transport connection when it's installing the mobility agent and registering with the configuration server. To resolve the issue, ensure that TLS 1.0 is enabled on your source machine.

## vCenter discovery failures

To resolve vCenter discovery failures, add the vCenter server to the byPass list proxy settings.

- Download PsExec tool from [here](#) to access System user content.
- Open Internet Explorer in system user content by running the following command line `psexec -s - "%programfiles%\Internet Explorer\iexplore.exe"`
- Add proxy settings in IE and restart tmanssvc service.
- To configure DRA proxy settings, run `cd C:\Program Files\Microsoft Azure Site Recovery Provider`
- Next, execute `DRCONFIGULATOR.EXE /configure /AddBypassUrls [add IP Address/FQDN of vCenter Server provided during Configure vCenter Server/vSphere ESXi server step of Configuration Server deployment]`

## Change the IP address of the configuration server

We strongly recommend that you don't change the IP address of a configuration server. Ensure that all IP addresses that are assigned to the configuration server are static IP addresses. Don't use DHCP IP addresses.

## ACS50008: SAML token is invalid

To avoid this error, ensure that the time on your system clock isn't different from the local time by more than 15 minutes. Rerun the installer to complete the registration.

## Failed to create a certificate

A certificate that's required to authenticate Site Recovery can't be created. Rerun setup after you ensure that you're running setup as a local administrator.

## Failure to activate Windows License from Server Standard EVALUATION to Server Standard

1. As part of Configuration server deployment through OVF, an evaluation license is used, which is valid for 180 days. You need to activate this License before this gets expired. Else, this can result in frequent shutdown of configuration server and thus cause hindrance to replication activities.
2. If you are unable to activate Windows license, reach out to [Windows support team](#) to resolve the issue.

## Register source machine with configuration server

### If the source machine runs Windows

Run the following command on the source machine:

```
cd C:\Program Files (x86)\Microsoft Azure Site Recovery\agent
UnifiedAgentConfigurator.exe /CSEndPoint <configuration server IP address> /PassphraseFilePath <passphrase file path>
```

SETTING	DETAILS
Usage	UnifiedAgentConfigurator.exe /CSEndPoint <configuration server IP address> /PassphraseFilePath <passphrase file path>
Agent configuration logs	Located under %ProgramData%\ASRSetupLogs\ASRUnifiedAgentConfigurator.log.
/CSEndPoint	Mandatory parameter. Specifies the IP address of the configuration server. Use any valid IP address.
/PassphraseFilePath	Mandatory. The location of the passphrase. Use any valid UNC or local file path.

### If the source machine runs Linux

Run the following command on the source machine:

```
/usr/local/ASR/Vx/bin/UnifiedAgentConfigurator.sh -i <configuration server IP address> -P
/var/passphrase.txt
```

SETTING	DETAILS

SETTING	DETAILS
Usage	cd /usr/local/ASR/Vx/bin UnifiedAgentConfigurator.sh -i <configuration server IP address> -P <passphrase file path>
-i	Mandatory parameter. Specifies the IP address of the configuration server. Use any valid IP address.
-P	Mandatory. The full file path of the file in which the passphrase is saved. Use any valid folder.

## Unable to configure the configuration server

If you install applications other than the configuration server on the virtual machine, you might be unable to configure the master target.

The configuration server must be a single purpose server and using it as a shared server is unsupported.

For more information, see the configuration FAQ in [Deploy a configuration server](#).

## Remove the stale entries for protected items from the configuration server database

To remove stale protected machine on the configuration server, use the following steps.

1. To determine the source machine and IP address of the stale entry:
  - a. Open the MYSQL cmdline in administrator mode.
  - b. Execute the following commands.

```
mysql> use svldb1;
mysql> select id as hostid, name, ipaddress, ostype as operatingystem,
from_unixtime(lasthostupdatetime) as heartbeat from hosts where name != 'InMageProfiler'\G;
```

This returns the list of registered machines along with their IP addresses and last heart beat. Find the host that has stale replication pairs.

2. Open an elevated command prompt and navigate to C:\ProgramData\ASR\home\svsystems\bin.
3. To remove the registered hosts details and the stale entry information from the configuration server, run the following command using the source machine and the IP address of the stale entry.

```
Syntax: Unregister-ASRComponent.pl -IPAddress <IP_ADDRESS_OF_MACHINE_TO_UNREGISTER> -Component <Source/PS / MT>
```

If you have a source server entry of "OnPrem-VM01" with an ip-address of 10.0.0.4 then use the following command instead.

```
perl Unregister-ASRComponent.pl -IPAddress 10.0.0.4 -Component Source
```

4. Restart the following services on source machine to reregister with the configuration server.
  - InMage Scout Application Service
  - InMage Scout VX Agent - Sentinel/Outpost

## Upgrade fails when the services fail to stop

The configuration server upgrade fails when certain services do not stop.

To identify the issue, navigate to C:\ProgramData\ASRSetupLogs\CX\_TP\_InstallLogFile on the configuration server. If you find following errors, use the steps below to resolve the issue:

```
2018-06-28 14:28:12.943 Successfully copied php.ini to C:\Temp from C:\thirdparty\php5nts
2018-06-28 14:28:12.943 svagents service status - SERVICE_RUNNING
2018-06-28 14:28:12.944 Stopping svagents service.
2018-06-28 14:31:32.949 Unable to stop svagents service.
2018-06-28 14:31:32.949 Stopping svagents service.
2018-06-28 14:34:52.960 Unable to stop svagents service.
2018-06-28 14:34:52.960 Stopping svagents service.
2018-06-28 14:38:12.971 Unable to stop svagents service.
2018-06-28 14:38:12.971 Rolling back the install changes.
2018-06-28 14:38:12.971 Upgrade has failed.
```

To resolve the issue:

Manually stop the following services:

- cxprocessserver
- InMage Scout VX Agent – Sentinel/Outpost,
- Microsoft Azure Recovery Services Agent,
- Microsoft Azure Site Recovery Service,
- tmansvc

To update the configuration server, run the [unified setup](#) again.

## Azure Active Directory application creation failure

You have insufficient permissions to create an application in Azure Active Directory (AAD) using the [Open Virtualization Application \(OVA\)](#) template.

To resolve the issue, sign in to the Azure portal and do one of the following:

- Request the Application Developer role in AAD. For more information on the Application Developer role, see [Administrator role permissions in Azure Active Directory](#).
- Verify that the **User can create application** flag is set to *true* in AAD. For more information, see [How to: Use the portal to create an Azure AD application and service principal that can access resources](#).

## Process server/Master Target are unable to communicate with the configuration server

The process server (PS) and Master Target (MT) modules are unable to communicate with the configuration server (CS) and their status is shown as not connected on Azure portal.

Typically, this is due to an error with port 443. Use the following steps to unblock the port and re-enable communication with the CS.

### **Verify that the MARS agent is being invoked by the Master Target agent**

To verify that the Master Target Agent can create a TCP session for the Configuration server IP, look for a trace similar to the following in the Master Target agent logs:

TCP <Replace IP with CS IP here>:52739 <Replace IP with CS IP here>:443 SYN\_SENT

TCP 192.168.1.40:52739 192.168.1.40:443 SYN\_SENT // Replace IP with CS IP here

If you find traces similar to the following in the MT agent logs, the MT Agent is reporting errors on port 443:

```
#~> (11-20-2018 20:31:51): ERROR 2508 8408 313 FAILED : PostToSVServer with error [at curlwrapper.cpp:CurlWrapper::processCurlResponse:212] failed to post request: (7) - Couldn't connect to server
#~> (11-20-2018 20:31:54): ERROR 2508 8408 314 FAILED : PostToSVServer with error [at curlwrapper.cpp:CurlWrapper::processCurlResponse:212] failed to post request: (7) - Couldn't connect to server
```

This error can be encountered when other applications are also using port 443 or due to a firewall setting blocking the port.

To resolve the issue:

- Verify that port 443 is not blocked by your firewall.
- If the port is unreachable due to another application using that port, stop and uninstall the app.
  - If stopping the app is not feasible, setup a new clean CS.
- Restart the configuration server.
- Restart the IIS service.

#### Configuration server is not connected due to incorrect UUID entries

This error can occur when there are multiple configuration server (CS) instance UUID entries in the database. The issue often occurs when you clone the configuration server VM.

To resolve the issue:

1. Remove stale/old CS VM from vCenter. For more information, see [Remove servers and disable protection](#).
2. Sign in to the configuration server VM and connect to the MySQL svsdb1 database.
3. Execute the following query:

##### IMPORTANT

Verify that you are entering the UUID details of the cloned configuration server or the stale entry of the configuration server that is no longer used to protect virtual machines. Entering an incorrect UUID will result in losing the information for all existing protected items.

```
MySQL> use svsdb1;
MySQL> delete from infrastructurevms where infrastructurevmid='<Stale CS VM UUID>';
MySQL> commit;
```

4. Refresh the portal page.

#### An infinite sign in loop occurs when entering your credentials

After entering the correct username and password on the configuration server OVF, Azure sign in continues to prompt for the correct credentials.

This issue can occur when the system time is incorrect.

To resolve the issue:

Set the correct time on the computer and retry the sign in.

# Troubleshoot the process server

9/9/2019 • 10 minutes to read • [Edit Online](#)

The [Site Recovery](#) process server is used when you set up disaster recovery to Azure for on-premises VMware VMs and physical servers. This article describes how to troubleshoot issues with the process server, including replication and connectivity issues.

[Learn more](#) about the process server.

## Before you start

Before you start troubleshooting:

1. Make sure you understand how to [monitor process servers](#).
2. Review the best practices below.
3. Make sure you follow [capacity considerations](#), and use sizing guidance for the [configuration server](#) or [standalone process servers](#).

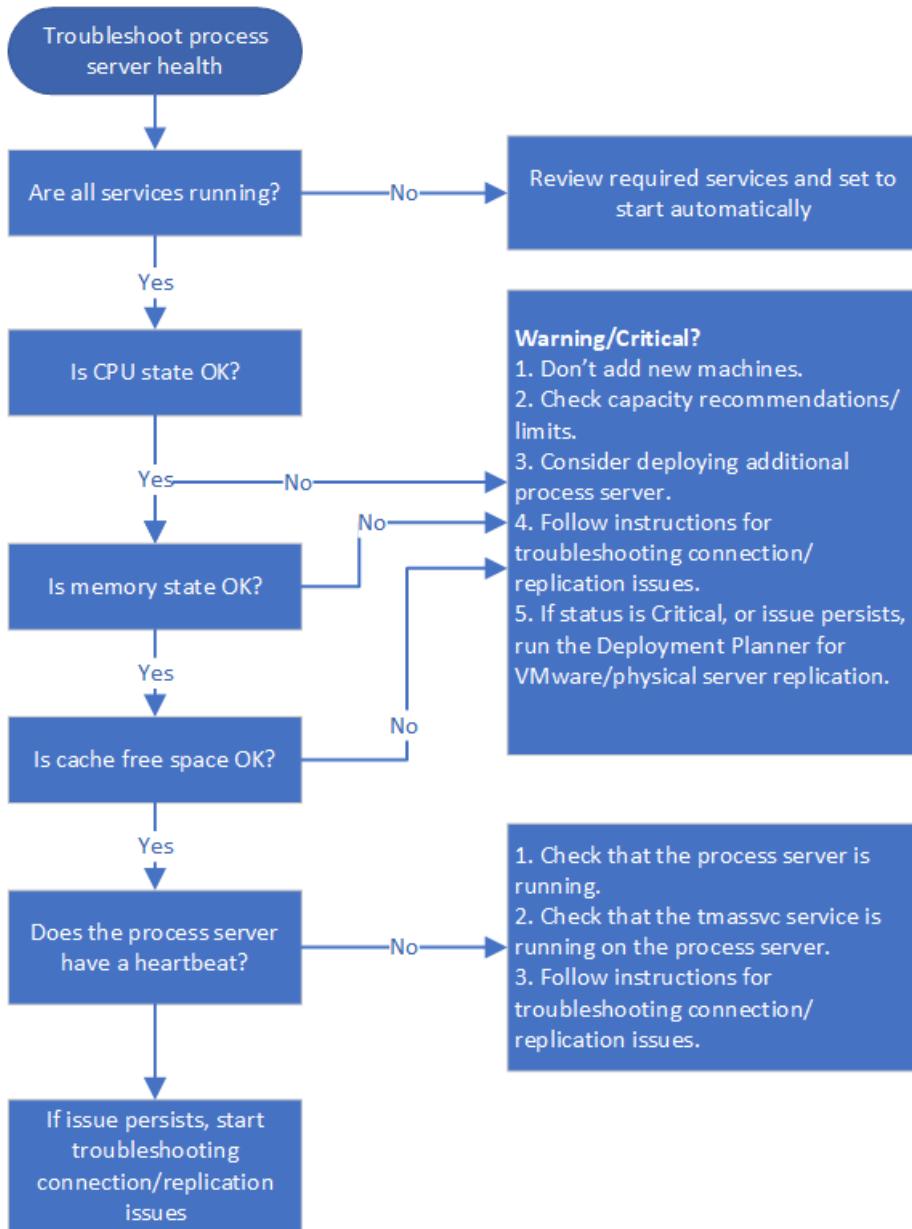
## Best practices for process server deployment

For optimum performance of process servers, we've summarized a number of general best practices.

BEST PRACTICE	DETAILS
<b>Usage</b>	Make sure the configuration server/standalone process server are only used for the intended purpose. Don't run anything else on the machine.
<b>IP address</b>	Make sure that the process server has a static IPv4 address, and doesn't have NAT configured.
<b>Control memory/CPU usage</b>	Keep CPU and memory usage under 70%.
<b>Ensure free space</b>	Free space refers to the cache disk space on the process server. Replication data is stored in the cache before it's uploaded to Azure.  Keep free space above 25%. If it goes below 20%, replication is throttled for replicated machines that are associated with the process server.

## Check process server health

The first step in troubleshooting is to check the health and status of the process server. To do this, review all alerts, check that required services are running, and verify that there's a heartbeat from the process server. These steps are summarized in the following graphic, followed by procedures to help you perform the steps.



## Step 1: Troubleshoot process server health alerts

The process server generates a number of health alerts. These alerts, and recommended actions, are summarized in the following table.

ALERT TYPE	ERROR	TROUBLESHOOT
	None	Process server is connected and healthy.
	Specified services aren't running.	<ol style="list-style-type: none"> <li>Check that services are running.</li> <li>If services are running as expected, follow the instructions below to <a href="#">troubleshoot connectivity and replication issues</a>.</li> </ol>

ALERT TYPE	ERROR	TROUBLESHOOT
	CPU utilization > 80% for the last 15 minutes.	<ol style="list-style-type: none"> <li>1. Don't add new machines.</li> <li>2. Check that the number of VMs using the process server aligns to <a href="#">defined limits</a>, and consider setting up an <a href="#">additional process server</a>.</li> <li>3. Follow the instructions below to <a href="#">troubleshoot connectivity and replication issues</a>.</li> </ol>
	CPU utilization > 95% for the last 15 minutes.	<ol style="list-style-type: none"> <li>1. Don't add new machines.</li> <li>2. Check that the number of VMs using the process server aligns to <a href="#">defined limits</a>, and consider setting up an <a href="#">additional process server</a>.</li> <li>3. Follow the instructions below to <a href="#">troubleshoot connectivity and replication issues</a>.</li> <li>4. If the issue persists, run the <a href="#">Deployment Planner</a> for VMware/physical server replication.</li> </ol>
	Memory usage > 80% for the last 15 minutes.	<ol style="list-style-type: none"> <li>1. Don't add new machines.</li> <li>2. Check that the number of VMs using the process server aligns to <a href="#">defined limits</a>, and consider setting up an <a href="#">additional process server</a>.</li> <li>3. Follow any instructions associated with the warning.</li> <li>4. If the issue persists, follow the instructions below to <a href="#">troubleshoot connectivity and replication issues</a>.</li> </ol>
	Memory usage > 95% for the last 15 minutes.	<ol style="list-style-type: none"> <li>1. Don't add new machines, and considering setting up an <a href="#">additional process server</a>.</li> <li>2. Follow any instructions associated with the warning.</li> <li>3. 4. If the issue continues, follow the instructions below to <a href="#">troubleshoot connectivity and replication issues</a>.</li> <li>4. If the issue persists, run the <a href="#">Deployment Planner</a> for VMware/physical server replication issues.</li> </ol>
	Cache folder free space < 30% for the last 15 minutes.	<ol style="list-style-type: none"> <li>1. Don't add new machines, and consider setting up an <a href="#">additional process server</a>.</li> <li>2. Check that the number of VMs using the process server aligns to <a href="#">guidelines</a>.</li> <li>3. Follow the instructions below to <a href="#">troubleshoot connectivity and replication issues</a>.</li> </ol>

ALERT TYPE	ERROR	TROUBLESHOOT
	Free space < 25% for last 15 minutes	<ol style="list-style-type: none"> <li>Follow the instructions associated with the warning for this issue.</li> <li>Follow the instructions below to <a href="#">troubleshoot connectivity and replication issues</a>.</li> <li>If the issue persists, run the <a href="#">Deployment Planner</a> for VMware/physical server replication.</li> </ol>
	No heartbeat from the process server for 15 minutes or more. The tmansvs service isn't communicating with the configuration server.	<ol style="list-style-type: none"> <li>Check that the process server is up and running.</li> <li>Check that the tmassvc is running on the process server.</li> <li>Follow the instructions below to <a href="#">troubleshoot connectivity and replication issues</a>.</li> </ol>



Healthy



Warning



Critical

## Step 2: Check process server services

Services that should be running on the process server are summarized in the following table. There are slight differences in services, depending on how the process server is deployed.

For all services except the Microsoft Azure Recovery Services Agent (obengine), check that the StartType is set to **Automatic** or **Automatic (Delayed Start)**.

DEPLOYMENT	RUNNING SERVICES
<b>Process server on the configuration server</b>	ProcessServer; ProcessServerMonitor; cxprocessserver; InMage PushInstall; Log Upload Service (LogUpload); InMage Scout Application Service; Microsoft Azure Recovery Services Agent (obengine); InMage Scout VX Agent-Sentinel/Outpost (svagents); tmansvc; World Wide Web Publishing Service (W3SVC); MySQL; Microsoft Azure Site Recovery Service (dra)
<b>Process server running as a standalone server</b>	ProcessServer; ProcessServerMonitor; cxprocessserver; InMage PushInstall; Log Upload Service (LogUpload); InMage Scout Application Service; Microsoft Azure Recovery Services Agent (obengine); InMage Scout VX Agent-Sentinel/Outpost (svagents); tmansvc.
<b>Process server deployed in Azure for failback</b>	ProcessServer; ProcessServerMonitor; cxprocessserver; InMage PushInstall; Log Upload Service (LogUpload)

## Step 3: Check the process server heartbeat

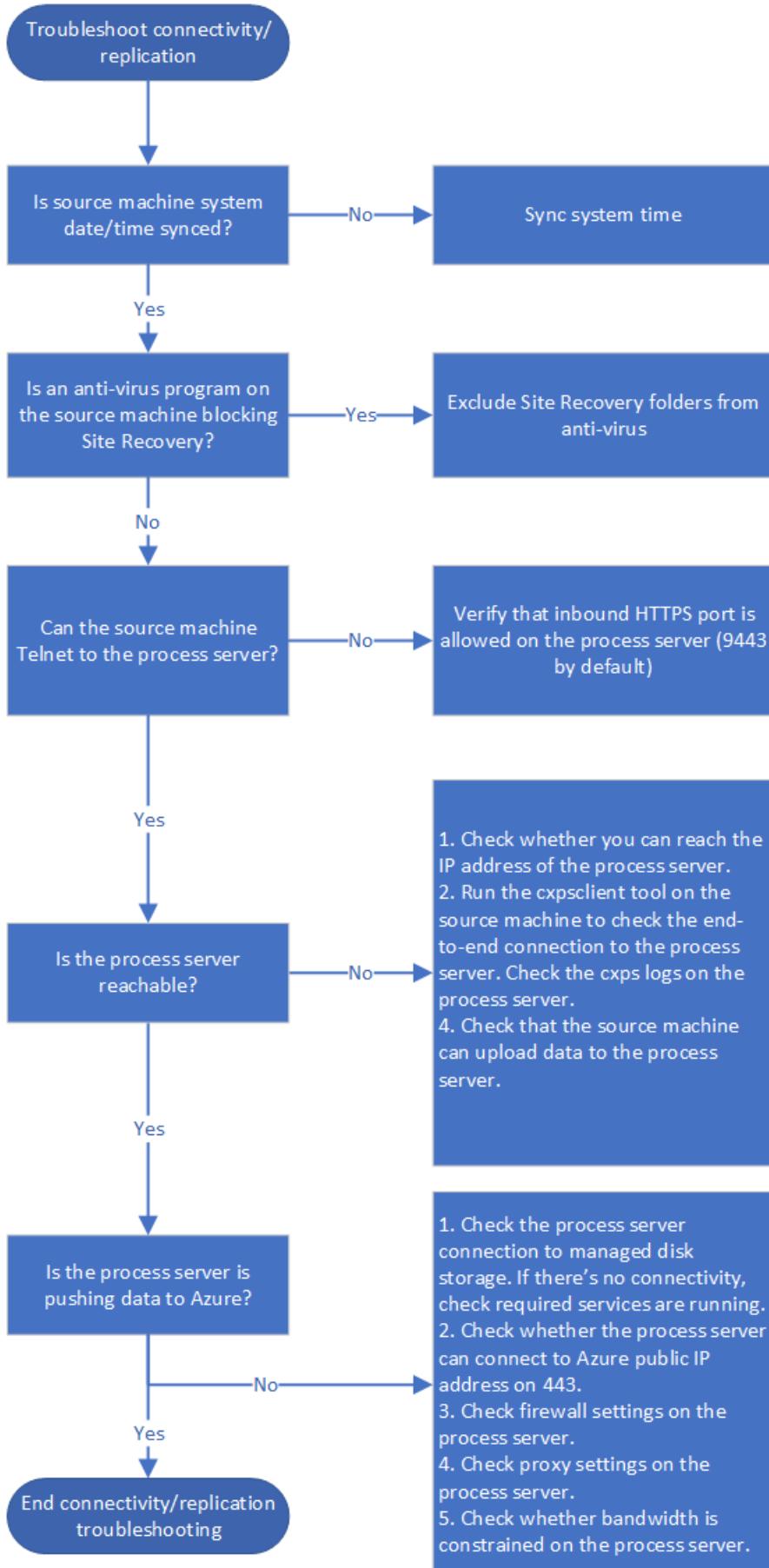
If there's no heartbeat from the process server (error code 806), do the following:

- Verify that the process server VM is up and running.
- Check these logs for errors.

C:\ProgramData\ASR\home\svsystems\eventmanager\*.log  
C:\ProgramData\ASR\home\svsystems\monitor\_protection\*.log

## Check connectivity and replication

Initial and ongoing replication failures are often caused by connectivity issues between source machines and the process server, or between the process server and Azure. These steps are summarized in the following graphic, followed by procedures to help you perform the steps.



## Step 4: Verify time sync on source machine

Ensure that the system date/time for the replicated machine is in sync. [Learn more](#)

## Step 5: Check anti-virus software on source machine

Check that no anti-virus software on the replicated machine is blocking Site Recovery. If you need to exclude Site Recovery from anti-virus programs, review [this article](#).

## Step 6: Check connectivity from source machine

1. Install the [Telnet client](#) on the source machine if you need to. Don't use Ping.
2. From the source machine, ping the process server on the HTTPS port with Telnet. By default 9443 is the HTTPS port for replication traffic.

```
telnet <process server IP address> <port>
```

3. Verify whether the connection is successful.

CONNECTIVITY	DETAILS	ACTION
<b>Successful</b>	Telnet shows a blank screen, and the process server is reachable.	No further action required.
<b>Unsuccessful</b>	You can't connect	Make sure that inbound port 9443 is allowed on the process server. For example, if you have a perimeter network or a screened subnet. Check connectivity again.
<b>Partially successful</b>	You can connect, but the source machine reports that the process server can't be reached.	Continue with the next troubleshooting procedure.

## Step 7: Troubleshoot an unreachable process server

If the process server isn't reachable from the source machine, error 78186 will be displayed. If not addressed, this issue will lead to both app-consistent and crash-consistent recovery points not being generated as expected.

Troubleshoot by checking whether the source machine can reach the IP address of the process server, and run the cxpsclient tool on the source machine, to check the end-to-end connection.

### Check the IP connection on the process server

If telnet is successful but the source machine reports that the process server can't be reached, check whether you can reach the IP address of the process server.

1. In a web browser, try to reach IP address `https://<PS_IP>:<PS_Data_Port>/`.
2. If this check shows an HTTPS certificate error, that's normal. If you ignore the error, you should see a 400 - Bad Request. This means that the server can't serve the browser request, and that the standard HTTPS connection is fine.
3. If this check doesn't work, then note the browser error message. For example, a 407 error will indicate an issue with proxy authentication.

### Check the connection with cxpsclient

Additionally, you can run the cxpsclient tool to check the end-to-end connection.

- Run the tool as follows:

```
<install folder>\cxpsclient.exe -i <PS_IP> -l <PS_Data_Port> -y <timeout_in_secs:recommended 300>
```

- On the process server, check the generated logs in these folders:

C:\ProgramData\ASR\home\svsystems\transport\log\cxps.err  
C:\ProgramData\ASR\home\svsystems\transport\log\cxps.xfer

#### Check source VM logs for upload failures (error 78028)

Issue with data uploads blocked from source machines to the process service can result in both crash-consistent and app-consistent recovery points not being generated.

- To troubleshoot network upload failures, you can look for errors in this log:

C:\Program Files (x86)\Microsoft Azure Site Recovery\agent\svagents\*.log

- Use the rest of the procedures in this article can help you to resolve data upload issues.

## Step 8: Check whether the process server is pushing data

Check whether the process server is actively pushing data to Azure.

- On the process server, open Task Manager (press Ctrl+Shift+Esc).
- Select the **Performance** tab > **Open Resource Monitor**.
- In **Resource Monitor** page, select the **Network** tab. Under **Processes with Network Activity**, check whether cbengine.exe is actively sending a large volume of data.

	PID	Send (B/sec)
cbengine.exe	8860	9,703
cxps.exe	3008	26
cxhost.exe (termsvc)	2024	4,131

If cbengine.exe isn't sending a large volume of data, complete the steps in the following sections.

## Step 9: Check the process server connection to Azure blob storage

- In Resource Monitor, select **cbengine.exe**.
- Under **TCP Connections**, check to see whether there is connectivity from the process server to the Azure storage.

Image	PID	Address	Send (B/sec)	Receive (B/sec)	Total (B/sec)
cbengine.exe	8860	blob.store.core.windows.net	3,907	72	3,979

## Check services

If there's no connectivity from the process server to the Azure blob storage URL, check that services are running.

1. In the Control Panel, select **Services**.
2. Verify that the following services are running:
  - cxprocessserver
  - InMage Scout VX Agent – Sentinel/Outpost
  - Microsoft Azure Recovery Services Agent
  - Microsoft Azure Site Recovery Service
  - tmansvc
3. Start or restart any service that isn't running.
4. Verify that the process server is connected and reachable.

## Step 10: check the process server connection to Azure public IP address

1. On the process server, in **%programfiles%\Microsoft Azure Recovery Services Agent\Temp**, open the latest CBEngineCurr.errlog file.
2. In the file, search for **443**, or for the string **connection attempt failed**.

This PC > Local Disk (C:) > Program Files > Microsoft Azure Recovery Services Agent > Temp			
Name	Date modified	Type	
CBEngine0.errlog	4/11/2017 5:15 PM	ERRLOG File	
CBEngine1.errlog	4/12/2017 4:34 AM	ERRLOG File	
CBEngine2.errlog	4/12/2017 2:13 PM	ERRLOG File	
CBEngine3.errlog	4/13/2017 1:28 AM	ERRLOG File	
CBEngine4.errlog	4/13/2017 11:36 AM	ERRLOG File	
CBEngine5.errlog	4/13/2017 10:56 PM	ERRLOG File	
CBEngine6.errlog	4/14/2017 10:16 AM	ERRLOG File	
CBEngine7.errlog	4/14/2017 9:32 PM	ERRLOG File	
CBEngine8.errlog	4/15/2017 8:43 AM	ERRLOG File	
CBEngine9.errlog	4/15/2017 8:01 PM	ERRLOG File	
CBEngine10.errlog	4/16/2017 7:12 AM	ERRLOG File	
CBEngine11.errlog	4/16/2017 6:25 PM	ERRLOG File	
CBEngine12.errlog	4/17/2017 5:37 AM	ERRLOG File	
CBEngine13.errlog	4/17/2017 10:19 AM	ERRLOG File	
CBEngine14.errlog	4/17/2017 3:55 PM	ERRLOG File	
CBEngine15.errlog	4/17/2017 9:33 PM	ERRLOG File	
CBEngine16.errlog	4/18/2017 3:11 AM	ERRLOG File	
CBEngine17.errlog	4/18/2017 8:44 AM	ERRLOG File	
<b>CBEngineCurr.errlog</b>	<b>4/18/2017 10:06 AM</b>	<b>ERRLOG File</b>	
CBUIOCurr.errlog	4/18/2017 10:05 AM	ERRLOG File	
GatewayProvider0Curr.errlog	4/18/2017 10:09 AM	ERRLOG File	

```
18E4 0604 04/12 11:22:14.702 71 calexternalunmanagedutils.h(194)
914728FF-AF2B-4F3E-B649-4A3DDAF5E73A WARNING-->System.Net.WebException: Unable to connect to
the remote server --> System.Net.Sockets.SocketException A connection attempt failed because the
connected party did not properly respond after a period of time, or established connection failed
because connected host has failed to respond [REDACTED]:443
```

3. If you see issues, located your Azure public IP address in the CBEngineCurr.currLog file by using port 443:

```
telnet <your Azure Public IP address as seen in CBEngineCurr.errlog> 443
```

5. At the command line on the process server, use Telnet to ping your Azure public IP address.
6. If you can't connect, follow the next procedure.

## Step 11: Check process server firewall settings.

Check whether the IP address-based firewall on the process server is blocking access.

1. For IP address-based firewall rules:

- a) Download the complete list of [Microsoft Azure datacenter IP ranges](#).
- b) Add the IP address ranges to your firewall configuration, to ensure that the firewall allows communication to Azure (and to the default HTTPS port, 443).
- c) Allow IP address ranges for the Azure region of your subscription, and for the Azure West US region (used for access control and identity management).

2. For URL-based firewalls, add the URLs listed in the following table to the firewall configuration.

NAME	COMMERCIAL URL	GOVERNMENT URL	DESCRIPTION
Azure Active Directory	login.microsoftonline.com	login.microsoftonline.us	Used for access control and identity management by using Azure Active Directory.
Backup	*.backup.windowsazure.com	*.backup.windowsazure.us	Used for replication data transfer and coordination.
Replication	*.hypervrecoverymanager.wir	*.hypervrecoverymanager.wirk	Used for replication management operations and coordination.
Storage	*.blob.core.windows.net	*.blob.core.usgovcloudapi.net	Used for access to the storage account that stores replicated data.
Telemetry (optional)	dc.services.visualstudio.cc	dc.services.visualstudio.co	Used for telemetry.
Time synchronization	time.windows.com	time.nist.gov	Used to check time synchronization between system and global time in all deployments.

## Step 12: Verify process server proxy settings

1. If you use a proxy server, ensure that the proxy server name is resolved by the DNS server. Check the value that you provided when you set up the configuration server in registry key **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Azure Site Recovery\ProxySettings**.
2. Ensure that the same settings are used by the Azure Site Recovery agent to send data.
  - a) Search for **Microsoft Azure Backup**.
  - b) Open **Microsoft Azure Backup**, and select **Action > Change Properties**.
  - c) On the **Proxy Configuration** tab, the proxy address should be same as the proxy address that's shown in the registry settings. If not, change it to the same address.

## Step 13: Check bandwidth

Increase the bandwidth between the process server and Azure, and then check whether the problem still occurs.

## Next steps

If you need more help, post your question in the [Azure Site Recovery forum](#).

# Troubleshoot Mobility Service push installation

11/12/2019 • 15 minutes to read • [Edit Online](#)

Installation of Mobility service is a key step during Enable Replication. The success of this step depends solely on meeting prerequisites and working with supported configurations. The most common failures you face during Mobility service installation are due to:

- [Credential/Privilege errors](#)
- [Login failures](#)
- [Connectivity errors](#)
- [File and printer sharing errors](#)
- [WMI failures](#)
- [Unsupported Operating systems](#)
- [Unsupported Boot configurations](#)
- [VSS installation failures](#)
- [Device name in GRUB configuration instead of device UUID](#)
- [LVM volume](#)
- [Reboot warnings](#)

When you enable replication, Azure Site Recovery tries to push install mobility service agent on your virtual machine. As part of this, Configuration server tries to connect with the virtual machine and copy the Agent. To enable successful installation, follow the step by step troubleshooting guidance given below.

## Credentials check (ErrorID: 95107 & 95108)

- Verify if the user account chosen during enable replication is **valid, accurate**.
- Azure Site Recovery requires **ROOT** account or user account with **administrator privileges** to perform push installation. Else, push installation will be blocked on the source machine.
  - For Windows (**error 95107**), verify if the user account has administrative access, either local or domain, on the source machine.
  - If you are not using a domain account, you need to disable Remote User Access control on the local computer.
    - To disable Remote User Access control, under HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System registry key, add a new DWORD: LocalAccountTokenFilterPolicy. Set the value to 1. To execute this step, run the following command from command prompt:

```
REG ADD HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v LocalAccountTokenFilterPolicy /t REG_DWORD /d 1
```

- For Linux (**error 95108**), you must choose the root account for successful installation of mobility agent. Additionally, SFTP services should be running. To enable SFTP subsystem and password authentication in the sshd\_config file:
  1. Sign in as root.
  2. Go to /etc/ssh/sshd\_config file, find the line that begins with PasswordAuthentication.
  3. Uncomment the line, and change the value to yes.
  4. Find the line that begins with Subsystem, and uncomment the line.
  5. Restart the sshd service.

If you wish to modify the credentials of chosen user account, follow the instructions given [here](#).

## Insufficient privileges failure (ErrorID: 95517)

When the user chosen to install mobility agent does not have administrator privileges, Configuration server/scale-out process server will not be allowed to copy the mobility agent software on to source machine. So, this error is a result of access denied failure. Ensure that the user account has administrator privileges.

If you wish to modify the credentials of chosen user account, follow the instructions given [here](#).

## Insufficient privileges failure (ErrorID: 95518)

When domain trust relationship establishment between the primary domain and workstation fails while trying to sign in to the source machine, mobility agent installation fails with error ID 95518. So, ensure that the user account used to install mobility agent has administrative privileges to sign in through primary domain of the source machine.

If you wish to modify the credentials of chosen user account, follow the instructions given [here](#).

## Login Failures (ErrorID: 95519, 95520, 95521, 95522)

### Credentials of the user account have been disabled (ErrorID: 95519)

The user account chosen during Enable Replication has been disabled. To enable the user account, refer to the article [here](#) or run the following command by replacing text *username* with the actual user name.

```
net user 'username' /active:yes
```

### Credentials locked out due to multiple failed login attempts (ErrorID: 95520)

Multiple failed retry efforts to access a machine will lock the user account. The failure can be due to:

- Credentials provided during Configuration setup are incorrect OR
- The user account chosen during Enable Replication is wrong

So, modify the credentials chosen by following the instructions given [here](#) and retry the operation after sometime.

### Logon servers are not available on the source machine (ErrorID: 95521)

This error occurs when the logon servers are not available on source machine. Unavailability of logon servers will lead to failure of login request and thus mobility agent cannot be installed. For successful Login, ensure that Logon servers are available on the source machine and start the Logon service. For detailed instructions, see the KB [139410](#) Err Msg: There are Currently No Logon Servers Available.

### Logon service isn't running on the source machine (ErrorID: 95522)

The login service isn't running on your source machine and caused failure of login request. So, mobility agent cannot be installed. To resolve, ensure that Logon service is running on the source machine for successful Login. To start the logon service, run the command "net start Logon" from command prompt or start "NetLogon" service from task manager.

## Connectivity failure (ErrorID: 95117 & 97118)

Configuration server/ scale-out process server tries to connect to the source VM to install Mobility agent. This error occurs when source machine is not reachable due to network connectivity issues. To resolve,

- Ensure you are able to ping your Source machine from the Configuration server. If you have chosen scale-out process server during enable replication, ensure you are able to ping your Source machine from process server.
  - From Source Server machine command line, use Telnet to ping the configuration server/ scale-out

process server with https port (135) as shown below to see if there are any network connectivity issues or firewall port blocking issues.

```
telnet <CS/ scale-out PS IP address> <135>
```

- Additionally, for **Linux VM**,
  - Check if latest openssh, openssh-server, and openssl packages are installed.
  - Check and ensure that Secure Shell (SSH) is enabled and is running on port 22.
  - SFTP services should be running. To enable SFTP subsystem and password authentication in the sshd\_config file,
    - Sign in as root.
    - Go to /etc/ssh/sshd\_config file, find the line that begins with PasswordAuthentication.
    - Uncomment the line, and change the value to yes
    - Find the line that begins with Subsystem, and uncomment the line
    - Restart the sshd service.
- A connection attempt could have failed if there is no proper response after a period of time, or established connection failed because connected host has failed to respond.
- It may be a Connectivity/network/domain related issue. It could also be due to DNS name resolving issue or TCP port exhaustion issue. Check if there are any such known issues in your domain.

## Connectivity failure (ErrorID: 95523)

This error occurs when the network in which the source machine resides is not found or might have been deleted or is no longer available. The only way to resolve the error is by ensuring that the network exists.

## File and Printer sharing services check (ErrorID: 95105 & 95106)

After connectivity check, verify if File and printer sharing service is enabled on your virtual machine. These settings are required to copy Mobility agent on to the source machine.

### For windows 2008 R2 and prior versions,

- To enable file and print sharing through Windows Firewall,
  - Open control panel -> System and Security -> Windows Firewall -> on left pane, click Advanced settings -> click Inbound Rules in console tree.
  - Locate rules File and Printer Sharing (NB-Session-In) and File and Printer Sharing (SMB-In). For each rule, right-click the rule, and then click **Enable Rule**.
- To enable file sharing with Group Policy,
  - Go to Start, type gpmc.msc and search.
  - In the navigation pane, open the following folders: Local Computer Policy, User Configuration, Administrative Templates, Windows Components, and Network Sharing.
  - In the details pane, double-click **Prevent users from sharing files within their profile**. To disable the Group Policy setting, and enable the user's ability to share files, click Disabled. Click OK to save your changes. To learn more, see [Enable or disable File Sharing with Group Policy](#).

For **later versions**, follow the instructions provided in [Install the Mobility service for disaster recovery of VMware VMs and physical servers](#) to enable file and printer sharing.

## Windows Management Instrumentation (WMI) configuration check (Error code: 95103)

After file and printer services check, enable WMI service for private, public, and domain profiles through firewall.

These settings are required to complete remote execution on the source machine. To enable,

- Go to Control Panel, click Security, and then click Windows Firewall.
- Click Change Settings and then click the Exceptions tab.
- In the Exceptions window, select the check box for Windows Management Instrumentation (WMI) to enable WMI traffic through the firewall.

You can also enable WMI traffic through the firewall at the command prompt. Use the following command

```
netsh advfirewall firewall set rule group="windows management instrumentation (wmi)" new enable=yes
```

Other WMI troubleshooting articles could be found at the following articles.

- [Basic WMI testing](#)
- [WMI troubleshooting](#)
- [Troubleshooting problems with WMI scripts and WMI services](#)

## Unsupported Operating Systems

Another most common reason for failure could be due to unsupported operating system. Ensure you are on the supported Operating System/Kernel version for successful installation of Mobility service. Avoid the usage of private patch. To view the list of operating systems and kernel versions supported by Azure Site Recovery, refer to our [support matrix document](#).

## Unsupported boot disk configurations (ErrorID: 95309, 95310, 95311)

### **Boot and system partitions / volumes are not the same disk (ErrorID: 95309)**

Before 9.20 version, boot and system partitions/ volumes on different disks was an unsupported configuration.

From [9.20 version](#), this configuration is supported. Use latest version for this support.

### **The boot disk is not available (ErrorID: 95310)**

A virtual machine without a boot disk cannot be protected. This is to ensure smooth recovery of virtual machine during failover operation. Absence of boot disk results in failure to boot the machine after failover. Ensure that the virtual machine contains boot disk and retry the operation. Also, note that multiple boot disks on the same machine is not supported.

### **Multiple Boot disks present on the source machine (ErrorID: 95311)**

A virtual machine with multiple boot disks is not a [supported configuration](#).

## System partition on multiple disks (ErrorID: 95313)

Before 9.20 version, root partition or volume laid on multiple disks was an unsupported configuration. From [9.20 version](#), this configuration is supported. Use latest version for this support.

## Enable protection failed as device name mentioned in the GRUB configuration instead of UUID (ErrorID: 95320)

### **Possible Cause:**

The GRUB configuration files ("`/boot/grub/menu.lst`", "`/boot/grub/grub.cfg`", "`/boot/grub2/grub.cfg`" or "`/etc/default/grub`") may contain the value for the parameters **root** and **resume** as the actual device names instead of UUID. Site Recovery mandates UUID approach as devices name may change across reboot of the VM as VM may not come-up with the same name on failover resulting in issues. For example:

- The following line is from the GRUB file **/boot/grub2/grub.cfg**.

```
linux /boot/vmlinuz-3.12.49-11-default root=/dev/sda2 ${extra_cmdline} resume=/dev/sda1
splash=silent quiet showopts
```

- The following line is from the GRUB file **/boot/grub/menu.lst**

```
kernel /boot/vmlinuz-3.0.101-63-default
root=/dev/sda2 resume=/dev/sda1 splash=silent crashkernel=256M-:128M showopts vga=0x314
```

If you observe the bold string above, GRUB has actual device names for the parameters "root" and "resume" instead of UUID.

#### **How to Fix:**

The device names should be replaced with the corresponding UUID.

- Find the UUID of the device by executing the command "blkid <device name>". For example:

```
blkid /dev/sda1
/dev/sda1: UUID="6f614b44-433b-431b-9ca1-4dd2f6f74f6b" TYPE="swap"
blkid /dev/sda2
/dev/sda2: UUID="62927e85-f7ba-40bc-9993-cc1feeb191e4" TYPE="ext3"
```

- Now replace the device name with its UUID in the format like "root=UUID=<UUID>". For example, if we replace the device names with UUID for root and resume parameter mentioned above in the files "/boot/grub2/grub.cfg", "/boot/grub2/grub.cfg" or "/etc/default/grub": then the lines in the files look like.
 

```
kernel /boot/vmlinuz-3.0.101-63-default root=UUID=62927e85-f7ba-40bc-9993-cc1feeb191e4
resume=UUID=6f614b44-433b-431b-9ca1-4dd2f6f74f6b splash=silent crashkernel=256M-:128M
showopts vga=0x314
```
- Restart the protection again

## Install Mobility Service completed with warning to reboot (ErrorID: 95265 & 95266)

Site Recovery mobility service has many components, one of which is called filter driver. Filter driver gets loaded into system memory only at a time of system reboot. It means that the filter driver fixes can only be realized when a new filter driver is loaded; which can happen only at the time of system reboot.

**Please note** that this is a warning and existing replication will work even after the new agent update. You can choose to reboot anytime you want to get the benefits of new filter driver but if you don't reboot the old filter driver keeps on working. So, after an update without reboot, apart from filter driver, **benefits of other enhancements and fixes in mobility service gets realized**. So, though recommended, it is not mandatory to reboot after every upgrade. For information on when a reboot is mandatory, set the [Reboot of source machine after mobility agent upgrade](#) section in Service updates in Azure Site Recovery.

#### **TIP**

For best practices on scheduling upgrades during your maintenance window, see the [Support for latest OS/kernel versions in Service updates in Azure Site Recovery](#).

## LVM support from 9.20 version

Before 9.20 version, LVM was supported for data disks only. /boot should be on a disk partition and not be an LVM volume.

From [9.20 version, OS disk on LVM](#) is supported. Use latest version for this support.

## Insufficient space (ErrorID: 95524)

When Mobility agent is copied on to the source machine, at least 100 MB free space is required. So, ensure that your source machine has required free space and retry the operation.

# VSS Installation failures

VSS installation is a part of Mobility agent installation. This service is used in the process of generating application consistent recovery points. Failures during VSS installation can occur due to multiple reasons. To identify the exact errors, refer to **c:\ProgramData\ASRSetupLogs\ASRUNifiedAgentInstaller.log**. Few common errors and the resolution steps are highlighted in the following section.

## **VSS error -2147023170 [0x800706BE] - exit code 511**

This issue is mostly seen when anti-virus software is blocking the operations of Azure Site Recovery services. To resolve this issue:

1. Exclude all folders mentioned [here](#).
2. Follow the guidelines published by your anti-virus provider to unblock the registration of DLL in Windows.

## **VSS error 7 [0x7] - exit code 511**

This is a runtime error and is caused due to insufficient memory to install VSS. Ensure to increase the disk space for successful completion of this operation.

## **VSS error -2147023824 [0x80070430] - exit code 517**

This error occurs when Azure Site Recovery VSS Provider service is [marked for deletion](#). Try to install VSS manually on the source machine by running the following command line

```
C:\Program Files (x86)\Microsoft Azure Site Recovery\agent>"C:\Program Files (x86)\Microsoft Azure Site Recovery\agent\InMageVSSProvider_Install.cmd"
```

## **VSS error -2147023841 [0x8007041F] - exit code 512**

This error occurs when Azure Site Recovery VSS Provider service database is [locked](#). Try to install VSS manually on the source machine by running the following command line

```
C:\Program Files (x86)\Microsoft Azure Site Recovery\agent>"C:\Program Files (x86)\Microsoft Azure Site Recovery\agent\InMageVSSProvider_Install.cmd"
```

In case of failure, check if any antivirus program or other services are stuck in "Starting" state. This could retain the lock on database services. It will lead to failures in installing VSS provider. Ensure that no service is in a "Starting" state and then retry the above operation.

## **VSS exit code 806**

This error occurs when the user account used for installation does not have permissions to execute the CSScript command. Provide necessary permissions to the user account to execute the script and retry the operation.

## **Other VSS errors**

Try to install VSS provider service manually on the source machine by running the following command line

```
C:\Program Files (x86)\Microsoft Azure Site Recovery\agent>"C:\Program Files (x86)\Microsoft Azure Site Recovery\agent\InMageVSSProvider_Install.cmd"
```

# **VSS error - 0x8004E00F**

This error is typically encountered during the installation of the mobility agent due to issues in DCOM and DCOM is in a critical state.

Use the following procedure to determine the cause of the error.

## **Examine the installation logs**

1. Open the installation log located at **c:\ProgramData\ASRSetupLogs\ASRUNifiedAgentInstaller.log**.
2. The presence of the following error indicates this issue:

Unregistering the existing application... Create the catalogue object Get the collection of Applications

ERROR:

- Error code: -2147164145 [0x8004E00F]
- Exit code: 802

To resolve the issue:

Contact the [Microsoft Windows platform team](#) to obtain assistance with resolving the DCOM issue.

When the DCOM issue is resolved, reinstall the Azure Site Recovery VSS Provider manually using the following command:

**C:\Program Files (x86)\Microsoft Azure Site Recovery\agent>"C:\Program Files (x86)\Microsoft Azure Site Recovery\agent\InMageVSSProvider\_Install.cmd**

If application consistency is not critical for your Disaster Recovery requirements, you can bypass the VSS Provider installation.

To bypass the Azure Site Recovery VSS Provider installation and manually install Azure Site Recovery VSS Provider post installation:

1. Install the mobility service.

**NOTE**

The Installation will fail at 'Post install configuration' step.

2. To bypass the VSS installation:

a. Open the Azure Site Recovery Mobility Service installation directory located at:

C:\Program Files (x86)\Microsoft Azure Site Recovery\agent

b. Modify the Azure Site Recovery VSS Provider installation scripts **nMageVSSProvider\_Install** and **InMageVSSProvider\_Uninstall.cmd** to always succeed by adding the following lines:

```
rem @echo off
setlocal
exit /B 0
```

3. Rerun the Mobility Agent installation manually.

4. When the Installation succeeds and moves to the next step, **Configure**, remove the lines you added.

5. To install the VSS provider, open a command prompt as Administrator and run the following command:

**C:\Program Files (x86)\Microsoft Azure Site Recovery\agent> .\InMageVSSProvider\_Install.cmd**

6. Verify that the ASR VSS Provider is installed as a service in Windows Services and open the Component Service MMC to verify that ASR VSS Provider is listed.

7. If the VSS Provider install continues to fail, work with CX to resolve the permissions errors in CAPI2.

## VSS Provider installation fails due to the cluster service being enabled on non-cluster machine

This issue causes the Azure Site Recovery Mobility Agent installation to fail during the ASAzure Site RecoveryR

VSS Provider installation step due to an issue with COM+ that prevents the installation of the VSS provider.

### To identify the issue

In the log located on configuration server at C:\ProgramData\ASRSetupLogs\UploadedLogs<date-time>UA\_InstallLogFile.log, you will find the following exception:

COM+ was unable to talk to the Microsoft Distributed Transaction Coordinator (Exception from HRESULT: 0x8004E00F)

To resolve the issue:

1. Verify that this machine is a non-cluster machine and that the cluster components are not being used.
2. If the components are not being used, remove the cluster components from the machine.

## Drivers are missing on the Source Server

If the Mobility Agent installation fails, examine the logs under C:\ProgramData\ASRSetupLogs to determine if some of the required drivers are missing in some control sets.

To resolve the issue:

1. Using a registry editor such as regedit.msc, open the registry.
2. Open the HKEY\_LOCAL\_MACHINE\SYSTEM node.
3. In the SYSTEM node, locate the control Sets.
4. Open each control set and verify that following Windows drivers are present:
  - Atapi
  - Vmbus
  - Storflt
  - Storvsc
  - intelide

Reinstall any missing drivers.

## Next steps

[Learn how](#) to set up disaster recovery for VMware VMs.

# Troubleshoot errors when failing over VMware VM or physical machine to Azure

1/8/2020 • 7 minutes to read • [Edit Online](#)

You may receive one of the following errors while doing failover of a virtual machine to Azure. To troubleshoot, use the described steps for each error condition.

## Failover failed with Error ID 28031

Site Recovery was not able to create a failed over virtual machine in Azure. It could happen because of one of the following reasons:

- There isn't sufficient quota available to create the virtual machine: You can check the available quota by going to Subscription -> Usage + quotas. You can open a [new support request](#) to increase the quota.
- You are trying to failover virtual machines of different size families in same availability set. Ensure that you choose same size family for all virtual machines in the same availability set. Change size by going to Compute and Network settings of the virtual machine and then retry failover.
- There is a policy on the subscription that prevents creation of a virtual machine. Change the policy to allow creation of a virtual machine and then retry failover.

## Failover failed with Error ID 28092

Site Recovery was not able to create a network interface for the failed over virtual machine. Make sure you have sufficient quota available to create network interfaces in the subscription. You can check the available quota by going to Subscription -> Usage + quotas. You can open a [new support request](#) to increase the quota. If you have sufficient quota, then this might be an intermittent issue, try the operation again. If the issue persists even after retries, then leave a comment at the end of this document.

## Failover failed with Error ID 70038

Site Recovery was not able to create a failed over Classic virtual machine in Azure. It could happen because:

- One of the resources such as a virtual network that is required for the virtual machine to be created doesn't exist. Create the virtual network as provided under Compute and Network settings of the virtual machine or modify the setting to a virtual network that already exists and then retry failover.

## Failover failed with Error ID 170010

Site Recovery was not able to create a failed over virtual machine in Azure. It could happen because an internal activity of hydration failed for the on-premises virtual machine.

To bring up any machine in Azure, the Azure environment requires some of the drivers to be in boot start state and services like DHCP to be in autostart state. Thus, hydration activity, at the time of failover, converts the startup type of **atapi, intelide, storflt, vmbus, and storvsc drivers** to boot start. It also converts the startup type of a few services like DHCP to autostart. This activity can fail due to environment specific issues.

To manually change the startup type of drivers for **Windows Guest OS**, follow the below steps:

1. [Download](#) the no-hydration script and run it as follows. This script checks if VM requires hydration.

```
.\Script-no-hydration.ps1
```

It gives the following result if hydration is required:

```
REGISTRY::HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\storvsc start = 3 expected value
= 0

This system doesn't meet no-hydration requirement.
```

In case the VM meets no-hydration requirement, the script will give the result "This system meets no-hydration requirement". In this case, all drivers and services are in the state as required by Azure and hydration on the VM is not required.

- Run the no-hydration-set script as follows if the VM does not meet no-hydration requirement.

```
.\Script-no-hydration.ps1 -set
```

This will convert the startup type of drivers and will give the result like below:

```
REGISTRY::HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\storvsc start = 3 expected value = 0

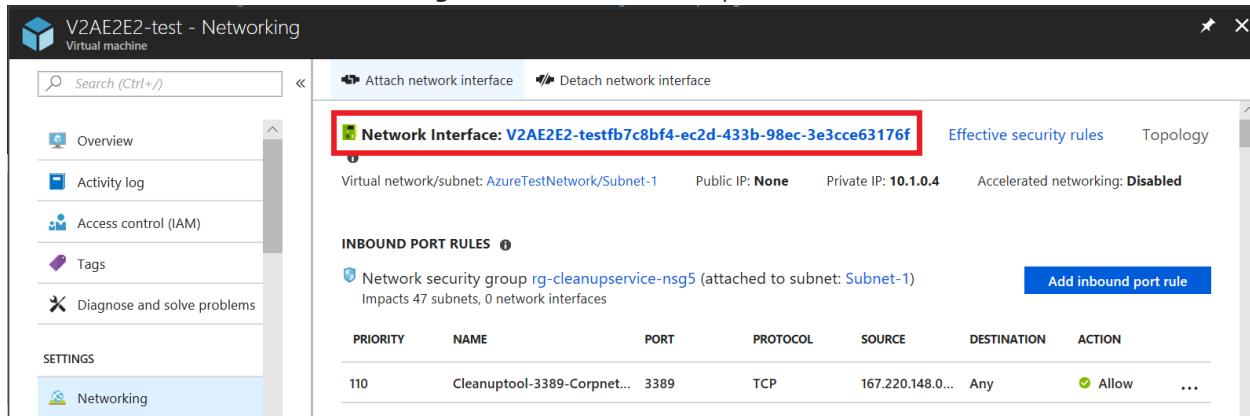
Updating registry: REGISTRY::HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\storvsc start = 0

This system is now no-hydration compatible.
```

## Unable to connect/RDP/SSH to the failed over virtual machine due to grayed out Connect button on the virtual machine

If the **Connect** button on the failed over VM in Azure is grayed out and you are not connected to Azure via an Express Route or Site-to-Site VPN connection, then,

- Go to **Virtual machine > Networking**, click on the name of required network interface.



V2AE2E2-test - Networking

Virtual machine

Search (Ctrl+ /)

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

SETTINGS

Networking

Attach network interface

Detach network interface

Network Interface: V2AE2E2-testfb7c8bf4-ec2d-433b-98ec-3e3cce63176f

Effective security rules

Topology

Virtual network/subnet: AzureTestNetwork/Subnet-1

Public IP: None

Private IP: 10.1.0.4

Accelerated networking: Disabled

INBOUND PORT RULES

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
110	CleanupTool-3389-Corpnet...	3389	TCP	167.220.148.0...	Any	Allow

- Navigate to **Ip Configurations**, then click on the name field of required IP configuration.

V2AE2E2-testfb7c8bf4-ec2d-433b-98ec-3e3cce63176f - IP configurations

Network interface

Overview Activity log Access control (IAM) Tags

SETTINGS

IP configurations (highlighted with a red box)

DNS servers Network security group Properties

IP forwarding settings

IP forwarding: Enabled

Virtual network: AzureTestNetwork

IP configurations

\* Subnet: Subnet-1 (10.1.0.0/24)

NAME	IP VERSION	TYPE	PRIVATE IP ADDRESS	PUBLIC IP ADDRESS
ipConfigV2A...	IPv4	Primary	10.1.0.4 (Dynamic)	52.187.65.13 (ambhatvm1-ip) ...

3. To enable Public IP address, click on **Enable**.

ipConfigV2AE2E2-testfb7c8bf4-ec2d-433b-98ec-3e3cce63176f

V2AE2E2-testfb7c8bf4-ec2d-433b-98ec-3e3cce63176f

Save Discard

Public IP address settings

Public IP address: Enabled (highlighted with a red box)

Private IP address settings

Virtual network/subnet: AzureTestNetwork/Subnet-1

Assignment: Dynamic (highlighted with a red box)

\* IP address: 10.1.0.4

4. Click on **Configure required settings > Create new**.

The screenshot shows the Azure portal interface for managing a virtual machine's network settings. On the left, under 'Public IP address settings', the 'IP address' dropdown is set to 'Enabled'. Below it, there's a red box highlighting the 'Configure required settings' section, which includes a note about dynamic vs static assignment and a specific IP address (10.1.0.4). On the right, a sidebar titled 'Choose public IP address' lists several existing public IP addresses and a prominent 'Create new' button.

5. Enter the name of public address, choose the default options for **SKU** and **assignment**, then click **OK**.
6. Now, to save the changes made, click **Save**.
7. Close the panels and navigate to **Overview** section of virtual machine to connect/RDP.

## Unable to connect/RDP/SSH - VM Connect button available

If the **Connect** button on the failed over VM in Azure is available (not grayed out), then check **Boot diagnostics** on your Virtual Machine and check for errors as listed in [this article](#).

1. If the virtual machine has not started, try failing over to an older recovery point.
2. If the application inside the virtual machine is not up, try failing over to an app-consistent recovery point.
3. If the virtual machine is domain joined, then ensure that domain controller is functioning accurately. This can be done by following the below given steps:
  - a. Create a new virtual machine in the same network.
  - b. Ensure that it is able to join to the same domain on which the failed over virtual machine is expected to come up.
  - c. If the domain controller is **not** functioning accurately, then try logging into the failed over virtual machine using a local administrator account.
4. If you are using a custom DNS server, then ensure that it is reachable. This can be done by following the below given steps:
  - a. Create a new virtual machine in the same network and
  - b. Check if the virtual machine is able to do name resolution using the custom DNS Server

### NOTE

Enabling any setting other than Boot Diagnostics would require Azure VM Agent to be installed in the virtual machine before the failover

## Unable to open serial console after failover of a UEFI based machine into Azure

If you are able to connect to the machine using RDP but cannot open serial console, follow the below steps:

- If the machine OS is Red Hat or Oracle Linux 7.\*/8.0, run the following command on the failover Azure VM

with root permissions. Reboot the VM after the command.

```
grub2-mkconfig -o /boot/efi/EFI/redhat/grub.cfg
```

- If the machine OS is CentOS 7.\*, run the following command on the failover Azure VM with root permissions. Reboot the VM after the command.

```
grub2-mkconfig -o /boot/efi/EFI/centos/grub.cfg
```

## Unexpected shutdown message (Event ID 6008)

When booting up a Windows VM post failover, if you receive an unexpected shutdown message on the recovered VM, it indicates that a VM shutdown state was not captured in the recovery point used for failover. This happens when you recover to a point when the VM had not been fully shut down.

This is normally not a cause for concern and can usually be ignored for unplanned failovers. If the failover is planned, ensure that the VM is properly shut down prior to failover and provide sufficient time for pending replication data on-premises to be sent to Azure. Then use the **Latest** option on the [Failover screen](#) so that any pending data on Azure is processed into a recovery point, which is then used for VM failover.

## Unable to select the Datastore

This issue is indicated when you are unable to see the datastore in Azure the portal when trying to reprotect the virtual machine that has experienced a failover. This is because the Master target is not recognized as a virtual machine under vCenters added to Azure Site Recovery.

For more information about reprotecting a virtual machine, see [Reprotect and fail back machines to an on-premises site after failover to Azure](#).

To resolve the issue:

Manually create the Master target in the vCenter that manages your source machine. The datastore will be available after the next vCenter discovery and refresh fabric operations.

### NOTE

The discovery and refresh fabric operations can take up to 30 minutes to complete.

## Linux Master Target registration with CS fails with an SSL error 35

The Azure Site Recovery Master Target registration with the configuration server fails due to the Authenticated Proxy being enabled on the Master Target.

This error is indicated by the following strings in the installation log:

```
RegisterHostStaticInfo encountered exception config/talwrapper.cpp(107)[post] CurlWrapper Post failed : server : 10.38.229.221, port : 443, phpUrl : request_handler.php, secure : true, ignoreCurlPartialError : false with error: [at curlwrapperlib/curlwrapper.cpp:processCurlResponse:231] failed to post request: (35) - SSL connect error.
```

To resolve the issue:

1. On the configuration server VM, open a command prompt and verify the proxy settings using the following commands:

```
cat /etc/environment echo $http_proxy echo $https_proxy
```

2. If the output of the previous commands shows that either the http\_proxy or https\_proxy settings are defined, use one of the following methods to unblock the Master Target communications with configuration server:

- Download the [PsExec tool](#).
- Use the tool to access the System user context and determine whether the proxy address is configured.
- If the proxy is configured, open IE in a system user context using the PsExec tool.

```
psexec -s -i "%programfiles%\Internet Explorer\iexplore.exe"
```

- To ensure that the master target server can communicate with the configuration server:
  - Modify the proxy settings in Internet Explorer to bypass the Master Target server IP address through the proxy.  
Or
  - Disable the proxy on Master Target server.

## Next steps

- Troubleshoot [RDP connection to Windows VM](#)
- Troubleshoot [SSH connection to Linux VM](#)

If you need more help, then post your query on [Site Recovery forum](#) or leave a comment at the end of this document. We have an active community that should be able to assist you.

# Troubleshoot failback to on-premises from Azure

12/26/2019 • 4 minutes to read • [Edit Online](#)

This article describes how to troubleshoot issues you might encounter when you fail back Azure VMs to your on-premises VMware infrastructure, after failover to Azure by using [Azure Site Recovery](#).

Failback essentially involves two main steps. For the first step, after failover, you need to reprotect Azure VMs to on-premises so that they start replicating. The second step is to run a failover from Azure to fail back to your on-premises site.

## Common issues

- If you perform a read-only user vCenter discovery and protect virtual machines, protection succeeds, and failover works. During reprottection, failover fails because the datastores can't be discovered. A symptom is that the datastores aren't listed during reprottection. To resolve this problem, you can update the vCenter credentials with an appropriate account that has permissions and then retry the job.
- When you fail back a Linux virtual machine and run it on-premises, you can see that the Network Manager package has been uninstalled from the machine. This uninstallation occurs because the Network Manager package is removed when the virtual machine is recovered in Azure.
- When a Linux virtual machine is configured with a static IP address and is failed over to Azure, the IP address is acquired from DHCP. When you fail over to on-premises, the virtual machine continues to use DHCP to acquire the IP address. Manually sign in to the machine, and then set the IP address back to a static address if necessary. A Windows virtual machine can acquire its static IP address again.
- If you use either the ESXi 5.5 free edition or the vSphere 6 Hypervisor free edition, failover succeeds, but failback doesn't succeed. To enable failback, upgrade to either program's evaluation license.
- If you can't reach the configuration server from the process server, use Telnet to check connectivity to the configuration server on port 443. You can also try to ping the configuration server from the process server. A process server should also have a heartbeat when it's connected to the configuration server.
- A Windows Server 2008 R2 SP1 server that is protected as a physical on-premises server can't be failed back from Azure to an on-premises site.
- You can't fail back in the following circumstances:
  - You migrated machines to Azure. [Learn more](#).
  - You moved a VM to another resource group.
  - You deleted the Azure VM.
  - You disabled protection of the VM.
  - You created the VM manually in Azure. The machine should have been initially protected on-premises and failed over to Azure before reprottection.
  - You can fail only to an ESXi host. You can't failback VMware VMs or physical servers to Hyper-V hosts, physical machines, or VMware workstations.

## Troubleshoot reprottection errors

This section details common reprottection errors and how to correct them.

### Error code 95226

**Reprotect failed as the Azure virtual machine was not able to reach the on-premises configuration server.**

This error occurs when:

- The Azure VM can't reach the on-premises configuration server. The VM can't be discovered and registered to the configuration server.
- The InMage Scout application service isn't running on the Azure VM after failover. The service is needed for communications with the on-premises configuration server.

To resolve this issue:

- Check that the Azure VM network allows the Azure VM to communicate with the on-premises configuration server. You can either set up a site-to-site VPN to your on-premises datacenter or configure an Azure ExpressRoute connection with private peering on the virtual network of the Azure VM.
- If the VM can communicate with the on-premises configuration server, sign in to the VM. Then check the InMage Scout application service. If you see that it's not running, start the service manually. Check that the service start type is set to **Automatic**.

### Error code 78052

**Protection couldn't be completed for the virtual machine.**

This issue can happen if there's already a VM with the same name on the master target server to which you're failing back.

To resolve this issue:

- Select a different master target server on a different host so that reprottection creates the machine on a different host, where the names don't collide.
- You also can use vMotion to move the master target to a different host where the name collision won't happen. If the existing VM is a stray machine, rename it so that the new VM can be created on the same ESXi host.

### Error code 78093

**The VM is not running, in a hung state, or not accessible.**

To resolve this issue:

To reprotect a failed-over VM, the Azure VM must be running so that Mobility Service registers with the configuration server on-premises and can start replicating by communicating with the process server. If the machine is on an incorrect network or isn't running (not responding or shut down), the configuration server can't reach Mobility Service on the VM to begin reprottection.

- Restart the VM so that it can start communicating back on-premises.
- Restart the reprotect job after you start the Azure virtual machine.

### Error code 8061

**The datastore is not accessible from ESXi host.**

Check the [master target prerequisites and supported data stores](#) for failback.

## Troubleshoot failback errors

This section describes common errors you might encounter during failback.

### Error code 8038

**Failed to bring up the on-premises virtual machine due to the error.**

This issue happens when the on-premises VM is brought up on a host that doesn't have enough memory provisioned.

To resolve this issue:

- Provision more memory on the ESXi host.
- In addition, you can use vMotion to move the VM to another ESXi host that has enough memory to boot the VM.

# Troubleshoot Microsoft Azure Site Recovery Provider upgrade failures

1/10/2020 • 2 minutes to read • [Edit Online](#)

This article helps you resolve issues that can cause failures during a Microsoft Azure Site Recovery Provider upgrade.

## The upgrade fails reporting that the latest Site Recovery Provider is already installed

When upgrading Microsoft Azure Site Recovery Provider (DRA), the Unified Setup upgrade fails and issues the error message:

Upgrade is not supported as a higher version of the software is already installed.

To upgrade, use the following steps:

1. Download the Microsoft Azure Site Recovery Unified Setup:
  - a. In the "Links to currently supported update rollups" section of the [Service updates in Azure Site Recovery](#) article, select the provider to which you are upgrading.
  - b. On the rollout page, locate the **Update information** section and download the Update Rollup for Microsoft Azure Site Recovery Unified Setup.
2. Open a command prompt and navigate to the folder to which you downloaded Unified Setup file. Extract the setup files from the download using the following command,  
MicrosoftAzureSiteRecoveryUnifiedSetup.exe /q /x:<folder path for the extracted files>.

Example command:

```
MicrosoftAzureSiteRecoveryUnifiedSetup.exe /q /x:C:\Temp\Extracted
```

3. In the command prompt, navigate to the folder to which you extracted the files and run the following installation commands:

```
CX_THIRDPARTY_SETUP.EXE /VERYSILENT /SUPPRESSMSGBOXES /NORESTART
UCX_SERVER_SETUP.EXE /VERYSILENT /SUPPRESSMSGBOXES /NORESTART /UPGRADE
```

4. Return to the folder to which you downloaded the Unified Setup and run MicrosoftAzureSiteRecoveryUnifiedSetup.exe to finish the upgrade.

## Upgrade failure due to the 3rd-party folder being renamed

For the upgrade to succeed, the 3rd-party folder must not be renamed.

To resolve the issue.

1. Start the Registry Editor (regedit.exe) and open the HKEY\_LOCAL\_MACHINE\SOFTWARE\WOW6432Node\InMage Systems\Installed Products\10 branch.
2. Inspect the `Build_Version` key value. If it is set to the latest version, reduce version number. For example, if latest version is 9.22.\* and the `Build_Version` key set to that value, then reduce it to 9.21.\*.
3. Download the latest Microsoft Azure Site Recovery Unified Setup:

- a. In the "Links to currently supported update rollups" section of the [Service updates in Azure Site Recovery](#) article, select the provider to which you are upgrading.
  - b. On the rollup page, locate the **Update information** section and download the Update Rollup for Microsoft Azure Site Recovery Unified Setup.
4. Open a command prompt and navigate to the folder to which you downloaded Unified Setup file and then extract the setup files from the download using the following command,  
MicrosoftAzureSiteRecoveryUnifiedSetup.exe /q /x:<folder path for the extracted files>.

Example command:

```
MicrosoftAzureSiteRecoveryUnifiedSetup.exe /q /x:C:\Temp\Extracted
```

5. In the command prompt, navigate to the folder to which you extracted the files and run the following installation commands:

```
CX_THIRDPARTY_SETUP.EXE /VERYSILENT /SUPPRESSMSGBOXES /NORESTART
```

6. Use task manager to monitor the progress of the installation. When the process for CX\_THIRDPARTY\_SETUP.EXE is no longer visible in task manager, proceed to the next step.
7. Verify that C:\thirdparty exists and that the folder contains the RRD libraries.
8. Return to the folder to which you downloaded the Unified Setup and run MicrosoftAzureSiteRecoveryUnifiedSetup.exe to finish the upgrade.

# Troubleshoot vCenter Server discovery failures

11/14/2019 • 2 minutes to read • [Edit Online](#)

This article helps you to troubleshoot issues that occur because of VMware vCenter discovery failures.

## Non-numeric values in the maxSnapShots property

On versions prior to 9.20, vCenter disconnects when it retrieves a non-numeric value for the property `snapshot.maxSnapshots` property on a VM.

This issue is identified by error ID 95126.

```
ERROR :: Hit an exception while fetching the required information from vCenter/vSphere. Exception details:
System.FormatException: Input string was not in a correct format.
at System.Number.StringToNumber(String str, NumberStyles options, NumberBuffer& number, NumberFormatInfo
info, Boolean parseDecimal)
at System.Number.ParseInt32(String s, NumberStyles style, NumberFormatInfo info)
at VMware.VSphere.Management.InfraContracts.VirtualMachineInfo.get_MaxSnapshots()
```

To resolve the issue:

- Identify the VM and set the value to a numeric value (VM Edit settings in vCenter).

Or

- Upgrade your configuration server to version 9.20 or later.

## Proxy configuration issues for vCenter connectivity

vCenter Discovery honors the System default proxy settings configured by the System user. The DRA service honors the proxy settings provided by the user during the installation of configuration server using the unified setup installer or OVA template.

In general, the proxy is used to communicate to public networks; such as communicating with Azure. If the proxy is configured and vCenter is in a local environment, it won't be able to communicate with DRA.

The following situations occur when this issue is encountered:

- The vCenter server <vCenter> is not reachable because of the error: The remote server returned an error: (503) Server Unavailable
- The vCenter server <vCenter> is not reachable because of the error: The remote server returned an error: Unable to connect to the remote server.
- Unable to connect to vCenter/ESXi server.

To resolve the issue:

Download the [PsExec tool](#).

Use the PsExec tool to access the System user context and determine whether the proxy address is configured. You can then add vCenter to the bypass list using the following procedures.

For Discovery proxy configuration:

- Open IE in system user context using the PsExec tool.

```
psexec -s -i "%programfiles%\Internet Explorer\iexplore.exe"
```

2. Modify the proxy settings in Internet Explorer to bypass the vCenter IP address.
3. Restart the tmanssvc service.

For DRA proxy configuration:

1. Open a command prompt and open the Microsoft Azure Site Recovery Provider folder.

**cd C:\Program Files\Microsoft Azure Site Recovery Provider**

2. From the command prompt, run the following command.

**DRCONFIGULATOR.EXE /configure /AddBypassUrls [IP Address/FQDN of vCenter Server provided at the time of add vCenter]**

3. Restart the DRA provider service.

## Next steps

[Manage the configuration server for VMware VM disaster recovery](#)

# Troubleshoot Hyper-V to Azure replication and failover

11/12/2019 • 7 minutes to read • [Edit Online](#)

This article describes common issues that you might come across when replicating on-premises Hyper-V VMs to Azure, using [Azure Site Recovery](#).

## Enable protection issues

If you experience issues when you enable protection for Hyper-V VMs, check the following recommendations:

1. Check that your Hyper-V hosts and VMs meet all [requirements and prerequisites](#).
2. If Hyper-V servers are located in System Center Virtual Machine Manager (VMM) clouds, verify that you've prepared the [VMM server](#).
3. Check that the Hyper-V Virtual Machine Management service is running on Hyper-V hosts.
4. Check for issues that appear in the Hyper-V-VMMS\Admin sign in to the VM. This log is located in **Applications and Services Logs > Microsoft > Windows**.
5. On the guest VM, verify that WMI is enabled and accessible.
  - [Learn about](#) basic WMI testing.
  - [Troubleshoot](#) WMI.
  - [Troubleshoot](#) problems with WMI scripts and services.
6. On the guest VM, ensure that the latest version of Integration Services is running.
  - [Check](#) that you have the latest version.
  - [Keep](#) Integration Services up-to-date.

## Replication issues

Troubleshoot issues with initial and ongoing replication as follows:

1. Make sure you're running the [latest version](#) of Site Recovery services.
2. Verify whether replication is paused:
  - Check the VM health status in the Hyper-V Manager console.
  - If it's critical, right-click the VM > **Replication > View Replication Health**.
  - If replication is paused, click **Resume Replication**.
3. Check that required services are running. If they aren't, restart them.
  - If you're replicating Hyper-V without VMM, check that these services are running on the Hyper-V host
    - Virtual Machine Management service
    - Microsoft Azure Recovery Services Agent service
    - Microsoft Azure Site Recovery service
    - WMI Provider Host service
  - If you're replicating with VMM in the environment, check that these services are running:
    - On the Hyper-V host, check that the Virtual Machine Management service, the Microsoft Azure Recovery Services Agent, and the WMI Provider Host service are running.
    - On the VMM server, ensure that the System Center Virtual Machine Manager Service is running.
4. Check connectivity between the Hyper-V server and Azure. To check connectivity, open Task Manager on the Hyper V host. On the **Performance** tab, click **Open Resource Monitor**. On the **Network** tab > **Process with**

**Network Activity**, check whether cbengine.exe is actively sending large volumes (Mbs) of data.

5. Check if the Hyper-V hosts can connect to the Azure storage blob URL. To check if the hosts can connect, select and check **cbengine.exe**. View **TCP Connections** to verify connectivity from the host to the Azure storage blob.
6. Check performance issues, as described below.

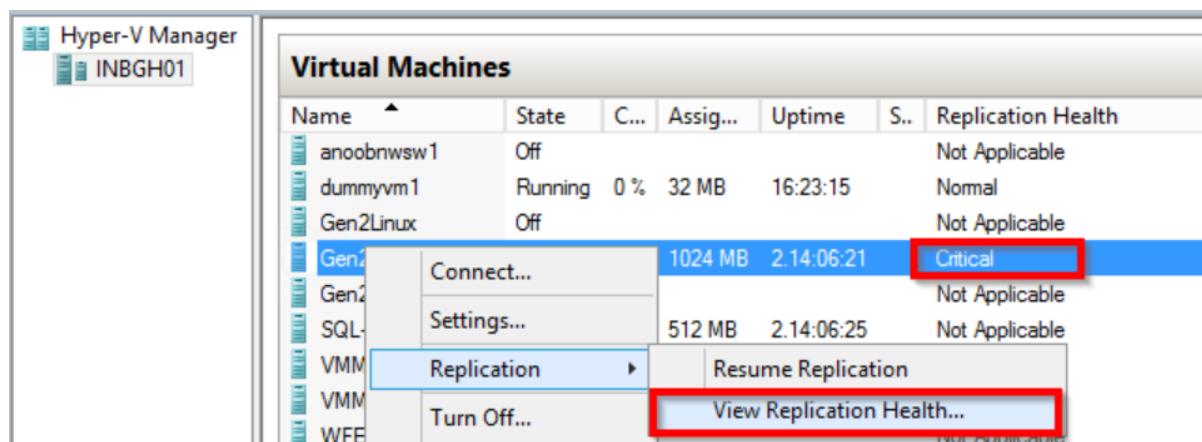
## Performance issues

Network bandwidth limitations can impact replication. Troubleshoot issues as follows:

1. [Check](#) if there are bandwidth or throttling constraints in your environment.
2. Run the [Deployment Planner profiler](#).
3. After running the profiler, follow the [bandwidth](#) and [storage](#) recommendations.
4. Check [data churn limitations](#). If you see high data churn on a VM, do the following:
  - Check if your VM is marked for resynchronization.
  - Follow [these steps](#) to investigate the source of the churn.
  - Churn can occur when the HRL log files exceed 50% of the available disk space. If this is the issue, provision more storage space for all VMs on which the issue occurs.
  - Check that replication isn't paused. If it is, it continues writing the changes to the hrl file, which can contribute to its increased size.

## Critical replication state issues

1. To check replication health, connect to the on-premises Hyper-V Manager console, select the VM, and verify health.



2. Click **View Replication Health** to see the details:

- If replication is paused, right-click the VM > **Replication** > **Resume replication**.
- If a VM on a Hyper-V host configured in Site Recovery migrates to a different Hyper-V host in the same cluster, or to a standalone machine, replication for the VM isn't impacted. Just check that the new Hyper-V host meets all prerequisites, and is configured in Site Recovery.

## App-consistent snapshot issues

An app-consistent snapshot is a point-in-time snapshot of the application data inside the VM. Volume Shadow Copy Service (VSS) ensures that apps on the VM are in a consistent state when the snapshot is taken. This section details some common issues you might experience.

### VSS failing inside the VM

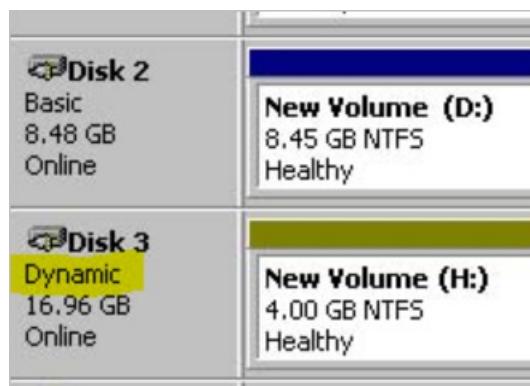
1. Check that the latest version of Integration services is installed and running. Check if an update is available by running the following command from an elevated PowerShell prompt on the Hyper-V host: **get-vm |**

**select Name, State, IntegrationServicesState.**

2. Check that VSS services are running and healthy:

- To check the services, sign in to the guest VM. Then open an admin command prompt, and run the following commands to check whether all the VSS writers are healthy.
  - **Vssadmin list writers**
  - **Vssadmin list shadows**
  - **Vssadmin list providers**
- Check the output. If writers are in a failed state, do the following:
  - Check the application event log on the VM for VSS operation errors.
- Try restarting these services associated with the failed writer:
  - Volume Shadow Copy
    - Azure Site Recovery VSS Provider
- After you do this, wait for a couple of hours to see if app-consistent snapshots are generated successfully.
- As a last resort try rebooting the VM. This might resolve services that are in unresponsive state.

3. Check you don't have dynamic disks in the VM. THis isn't supported for app-consistent snapshots. You can check in Disk Management (diskmgmt.msc).



4. Check that you don't have an iSCSI disk attached to the VM. This isn't supported.

5. Check that the Backup service is enabled. Verify that it is enabled in **Hyper-V settings > Integration Services**.

6. Make sure there are no conflicts with apps taking VSS snapshots. If multiple apps are trying to take VSS snapshots at the same time conflicts can occur. For example, if a Backup app is taking VSS snapshots when Site Recovery is scheduled by your replication policy to take a snapshot.

7. Check if the VM is experiencing a high churn rate:

- You can measure the daily data change rate for the guest VMs, using performance counters on Hyper-V host. To measure the data change rate, enable the following counter. Aggregate a sample of this value across the VM disks for 5-15 minutes, to get the VM churn.
  - Category: "Hyper-V Virtual Storage Device"
  - Counter: "Write Bytes / Sec"
  - This data churn rate will increase or remain at a high level, depending on how busy the VM or its apps are.
  - The average source disk data churn is 2 MB/s for standard storage for Site Recovery. [Learn more](#)
- In addition you can [verify storage scalability targets](#).

8. Run the [Deployment Planner](#).

9. Review the recommendations for [network](#) and [storage](#).

## **VSS failing inside the Hyper-V Host**

- Check event logs for VSS errors and recommendations:
  - On the Hyper-V host server, open the Hyper-V Admin event log in **Event Viewer > Applications and Services Logs > Microsoft > Windows > Hyper-V > Admin**.
  - Verify whether there are any events that indicate app-consistent snapshot failures.
  - A typical error is: "Hyper-V failed to generate VSS snapshot set for virtual machine 'XYZ': The writer experienced a non-transient error. Restarting the VSS service might resolve issues if the service is unresponsive."
- To generate VSS snapshots for the VM, check that Hyper-V Integration Services are installed on the VM, and that the Backup (VSS) Integration Service is enabled.
  - Ensure that the Integration Services VSS service/daemons are running on the guest, and are in an **OK** state.
  - You can check this from an elevated PowerShell session on the Hyper-V host with command **Get-VMIntegrationService -VMName<VMName>-Name VSS** You can also get this information by logging into the guest VM. [Learn more](#).
  - Ensure that the Backup/VSS integration Services on the VM are running and in healthy state. If not, restart these services, and the Hyper-V Volume Shadow Copy requestor service on the Hyper-V host server.

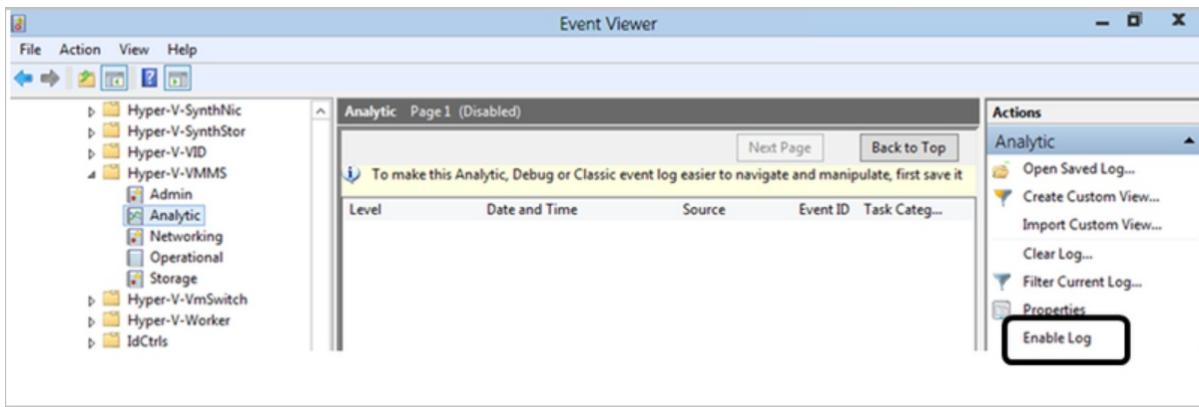
## Common errors

Error code	Message	Details
<b>0x800700EA</b>	"Hyper-V failed to generate VSS snapshot set for virtual machine: More data is available. (0x800700EA). VSS snapshot set generation can fail if backup operation is in progress.  Replication operation for virtual machine failed: More data is available."	Check if your VM has dynamic disk enabled. This isn't supported.
<b>0x80070032</b>	"Hyper-V Volume Shadow Copy Requestor failed to connect to virtual machine <./VMname> because the version does not match the version expected by Hyper-V"	Check if the latest Windows updates are installed.  <a href="#">Upgrade</a> to the latest version of Integration Services.

## Collect replication logs

All Hyper-V replication event are logged in the Hyper-V-VMMS\Admin log, located in **Applications and Services Logs > Microsoft > Windows**. In addition, you can enable an Analytic log for the Hyper-V Virtual Machine Management Service, as follows:

- Make the Analytic and Debug logs viewable in the Event Viewer. To make the logs available, in the Event Viewer, click **View > Show Analytic and Debug Logs..** The Analytic log appears under **Hyper-V-VMMS**.
- In the **Actions** pane, click **Enable Log**.



3. After it's enabled, it appears in **Performance Monitor**, as an **Event Trace Session** under **Data Collector Sets**.
4. To view the collected information, stop the tracing session by disabling the log. Then save the log, and open it again in Event Viewer, or use other tools to convert it as required.

### Event log locations

EVENT LOG	DETAILS
<b>Applications and Service Logs/Microsoft/VirtualMachineManager/Server/Admin</b> (VMM server)	Logs to troubleshoot VMM issues.
<b>Applications and Service Logs/Microsoft/AzureRecoveryServices/Replication</b> (Hyper-V host)	Logs to troubleshoot Microsoft Azure Recovery Services Agent issues.
<b>Applications and Service Logs/Microsoft/Azure Site Recovery/Provider/Operational</b> (Hyper-V host)	Logs to troubleshoot Microsoft Azure Site Recovery Service issues.
<b>Applications and Service Logs/Microsoft/Windows/Hyper-V-VMMS/Admin</b> (Hyper-V host)	Logs to troubleshoot Hyper-V VM management issues.

### Log collection for advanced troubleshooting

These tools can help with advanced troubleshooting:

- For VMM, perform Site Recovery log collection using the [Support Diagnostics Platform \(SDP\) tool](#).
- For Hyper-V without VMM, [download this tool](#), and run it on the Hyper-V host to collect the logs.

# Troubleshoot errors when failing over VMware VM or physical machine to Azure

1/8/2020 • 7 minutes to read • [Edit Online](#)

You may receive one of the following errors while doing failover of a virtual machine to Azure. To troubleshoot, use the described steps for each error condition.

## Failover failed with Error ID 28031

Site Recovery was not able to create a failed over virtual machine in Azure. It could happen because of one of the following reasons:

- There isn't sufficient quota available to create the virtual machine: You can check the available quota by going to Subscription -> Usage + quotas. You can open a [new support request](#) to increase the quota.
- You are trying to failover virtual machines of different size families in same availability set. Ensure that you choose same size family for all virtual machines in the same availability set. Change size by going to Compute and Network settings of the virtual machine and then retry failover.
- There is a policy on the subscription that prevents creation of a virtual machine. Change the policy to allow creation of a virtual machine and then retry failover.

## Failover failed with Error ID 28092

Site Recovery was not able to create a network interface for the failed over virtual machine. Make sure you have sufficient quota available to create network interfaces in the subscription. You can check the available quota by going to Subscription -> Usage + quotas. You can open a [new support request](#) to increase the quota. If you have sufficient quota, then this might be an intermittent issue, try the operation again. If the issue persists even after retries, then leave a comment at the end of this document.

## Failover failed with Error ID 70038

Site Recovery was not able to create a failed over Classic virtual machine in Azure. It could happen because:

- One of the resources such as a virtual network that is required for the virtual machine to be created doesn't exist. Create the virtual network as provided under Compute and Network settings of the virtual machine or modify the setting to a virtual network that already exists and then retry failover.

## Failover failed with Error ID 170010

Site Recovery was not able to create a failed over virtual machine in Azure. It could happen because an internal activity of hydration failed for the on-premises virtual machine.

To bring up any machine in Azure, the Azure environment requires some of the drivers to be in boot start state and services like DHCP to be in autostart state. Thus, hydration activity, at the time of failover, converts the startup type of **atapi, intelide, storflt, vmbus, and storvsc drivers** to boot start. It also converts the startup type of a few services like DHCP to autostart. This activity can fail due to environment specific issues.

To manually change the startup type of drivers for **Windows Guest OS**, follow the below steps:

1. [Download](#) the no-hydration script and run it as follows. This script checks if VM requires hydration.

```
.\\Script-no-hydration.ps1
```

It gives the following result if hydration is required:

```
REGISTRY::HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\storvsc start = 3 expected
value = 0

This system doesn't meet no-hydration requirement.
```

In case the VM meets no-hydration requirement, the script will give the result "This system meets no-hydration requirement". In this case, all drivers and services are in the state as required by Azure and hydration on the VM is not required.

- Run the no-hydration-set script as follows if the VM does not meet no-hydration requirement.

```
.\\Script-no-hydration.ps1 -set
```

This will convert the startup type of drivers and will give the result like below:

```
REGISTRY::HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\storvsc start = 3 expected value = 0

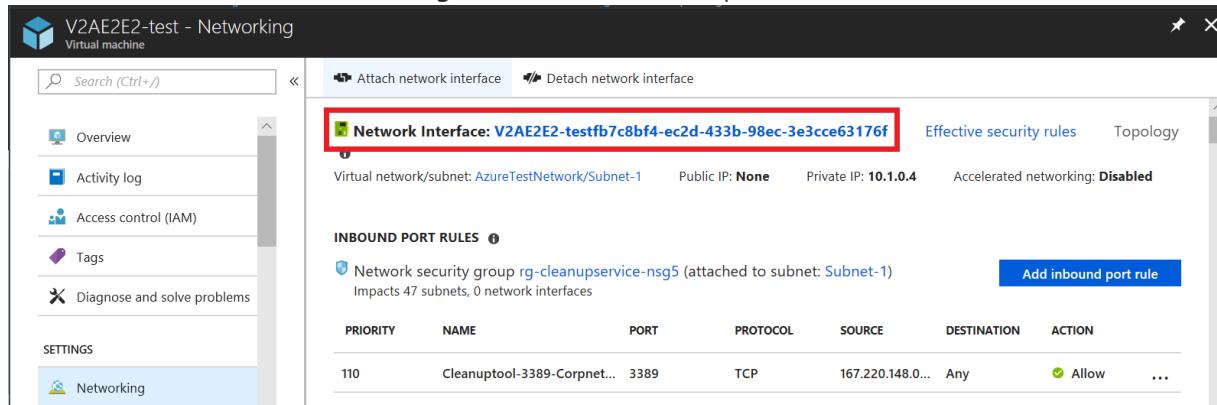
Updating registry: REGISTRY::HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\storvsc start = 0

This system is now no-hydration compatible.
```

## Unable to connect/RDP/SSH to the failed over virtual machine due to grayed out Connect button on the virtual machine

If the **Connect** button on the failed over VM in Azure is grayed out and you are not connected to Azure via an Express Route or Site-to-Site VPN connection, then,

- Go to **Virtual machine > Networking**, click on the name of required network interface.



PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
110	Cleanuptool-3389-Corpnet...	3389	TCP	167.220.148.0...	Any	<input checked="" type="checkbox"/> Allow

- Navigate to **Ip Configurations**, then click on the name field of required IP configuration.

The screenshot shows the Azure portal interface for managing IP configurations. On the left, there's a sidebar with options like Overview, Activity log, Access control (IAM), Tags, and SETTINGS. Under SETTINGS, the 'IP configurations' option is selected and highlighted with a red box. The main content area shows 'IP forwarding settings' with 'IP forwarding' set to 'Enabled'. It also displays 'Virtual network' as 'AzureTestNetwork'. The 'IP configurations' section lists a single entry: 'Subnet-1 (10.1.0.0/24)'. Below this is a table with columns: NAME, IP VERSION, TYPE, PRIVATE IP ADDRESS, and PUBLIC IP ADDRESS. A row in the table is highlighted with a red box, showing 'ipConfigV2A...' under NAME, 'IPv4' under IP VERSION, 'Primary' under TYPE, '10.1.0.4 (Dynamic)' under PRIVATE IP ADDRESS, and '52.187.65.13 (ambhatvm1-ip)' under PUBLIC IP ADDRESS.

3. To enable Public IP address, click on **Enable**.

This screenshot shows the configuration details for a specific IP configuration named 'ipConfigV2AE2E2-testfb7c8bf4-ec2d-433b-98ec-3e3cce63176f'. At the top, there are 'Save' and 'Discard' buttons. The main section is titled 'Public IP address settings'. It includes a 'Public IP address' field where 'Enabled' is selected (highlighted with a red box). Below this is a 'Private IP address settings' section. It shows 'Virtual network/subnet' as 'AzureTestNetwork/Subnet-1'. Under 'Assignment', 'Dynamic' is selected (highlighted with a red box). The 'IP address' field is marked with a red asterisk (\*) and contains the value '10.1.0.4'.

4. Click on **Configure required settings > Create new**.

The screenshot shows the Azure portal interface for managing network settings. On the left, under 'Public IP address settings', there's a section for a specific IP address (10.1.0.4) with 'Dynamic' selected for assignment. A red box highlights the 'IP address' field and the 'Configure required settings' link. On the right, a panel titled 'Choose public IP address' lists several public IP addresses and includes a 'Create new' button.

5. Enter the name of public address, choose the default options for **SKU** and **assignment**, then click **OK**.
6. Now, to save the changes made, click **Save**.
7. Close the panels and navigate to **Overview** section of virtual machine to connect/RDP.

## Unable to connect/RDP/SSH - VM Connect button available

If the **Connect** button on the failed over VM in Azure is available (not grayed out), then check **Boot diagnostics** on your Virtual Machine and check for errors as listed in [this article](#).

1. If the virtual machine has not started, try failing over to an older recovery point.
2. If the application inside the virtual machine is not up, try failing over to an app-consistent recovery point.
3. If the virtual machine is domain joined, then ensure that domain controller is functioning accurately. This can be done by following the below given steps:
  - a. Create a new virtual machine in the same network.
  - b. Ensure that it is able to join to the same domain on which the failed over virtual machine is expected to come up.
  - c. If the domain controller is **not** functioning accurately, then try logging into the failed over virtual machine using a local administrator account.
4. If you are using a custom DNS server, then ensure that it is reachable. This can be done by following the below given steps:
  - a. Create a new virtual machine in the same network and
  - b. Check if the virtual machine is able to do name resolution using the custom DNS Server

### NOTE

Enabling any setting other than Boot Diagnostics would require Azure VM Agent to be installed in the virtual machine before the failover

## Unable to open serial console after failover of a UEFI based machine into Azure

If you are able to connect to the machine using RDP but cannot open serial console, follow the below steps:

- If the machine OS is Red Hat or Oracle Linux 7.\*/8.0, run the following command on the failover Azure

VM with root permissions. Reboot the VM after the command.

```
grub2-mkconfig -o /boot/efi/EFI/redhat/grub.cfg
```

- If the machine OS is CentOS 7.\*, run the following command on the failover Azure VM with root permissions. Reboot the VM after the command.

```
grub2-mkconfig -o /boot/efi/EFI/centos/grub.cfg
```

## Unexpected shutdown message (Event ID 6008)

When booting up a Windows VM post failover, if you receive an unexpected shutdown message on the recovered VM, it indicates that a VM shutdown state was not captured in the recovery point used for failover. This happens when you recover to a point when the VM had not been fully shut down.

This is normally not a cause for concern and can usually be ignored for unplanned failovers. If the failover is planned, ensure that the VM is properly shut down prior to failover and provide sufficient time for pending replication data on-premises to be sent to Azure. Then use the **Latest** option on the [Failover screen](#) so that any pending data on Azure is processed into a recovery point, which is then used for VM failover.

## Unable to select the Datastore

This issue is indicated when you are unable to see the datastore in Azure the portal when trying to reprotect the virtual machine that has experienced a failover. This is because the Master target is not recognized as a virtual machine under vCenters added to Azure Site Recovery.

For more information about reprotecting a virtual machine, see [Reprotect and fail back machines to an on-premises site after failover to Azure](#).

To resolve the issue:

Manually create the Master target in the vCenter that manages your source machine. The datastore will be available after the next vCenter discovery and refresh fabric operations.

### NOTE

The discovery and refresh fabric operations can take up to 30 minutes to complete.

## Linux Master Target registration with CS fails with an SSL error 35

The Azure Site Recovery Master Target registration with the configuration server fails due to the Authenticated Proxy being enabled on the Master Target.

This error is indicated by the following strings in the installation log:

```
RegisterHostStaticInfo encountered exception config/talwrapper.cpp(107)[post] CurlWrapper Post failed :
server : 10.38.229.221, port : 443, phpUrl : request_handler.php, secure : true, ignoreCurlPartialError :
false with error: [at curlwrapperlib/curlwrapper.cpp:processCurlResponse:231] failed to post request: (35)
- SSL connect error.
```

To resolve the issue:

1. On the configuration server VM, open a command prompt and verify the proxy settings using the following commands:

```
cat /etc/environment echo $http_proxy echo $https_proxy
```

2. If the output of the previous commands shows that either the http\_proxy or https\_proxy settings are defined, use one of the following methods to unblock the Master Target communications with configuration server:

- Download the [PsExec tool](#).
- Use the tool to access the System user context and determine whether the proxy address is configured.
- If the proxy is configured, open IE in a system user context using the PsExec tool.

```
psexec -s -i "%programfiles%\Internet Explorer\iexplore.exe"
```

- To ensure that the master target server can communicate with the configuration server:
  - Modify the proxy settings in Internet Explorer to bypass the Master Target server IP address through the proxy.  
Or
  - Disable the proxy on Master Target server.

## Next steps

- Troubleshoot [RDP connection to Windows VM](#)
- Troubleshoot [SSH connection to Linux VM](#)

If you need more help, then post your query on [Site Recovery forum](#) or leave a comment at the end of this document. We have an active community that should be able to assist you.