

Contents

[Site Recovery Documentation](#)

[Overview](#)

[About Site Recovery](#)

[Quickstarts](#)

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

[Tutorials](#)

[Azure VMs](#)

[Set up disaster recovery](#)

[Run a disaster recovery drill](#)

[Run failover and failback](#)

[VMware VMs](#)

[Prepare Azure](#)

[Prepare on-premises VMware](#)

[Set up disaster recovery](#)

[Run a disaster recovery drill](#)

[Run failover and failback](#)

[Hyper-V VMs](#)

[Prepare Azure](#)

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

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

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

[Run a disaster recovery drill](#)

[Run failover and failback](#)

[Migrate to Azure](#)

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

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

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

[Migrate AWS instances to Azure](#)

[Migrate Azure VMs to another region](#)

Concepts

Azure VMs

Azure to Azure architecture

Azure to Azure support matrix

VMware VMs and physical servers

Replication to Azure

Common questions for VMware to Azure replication

VMware/physical to Azure support matrix

VMware to Azure architecture

Physical to Azure architecture

Multi-tenant support for VMware replication to Azure

About the Mobility service

Fallback location options

Replication to a secondary site

VMware/physical to secondary site support matrix

VMware/physical to secondary site architecture

Hyper-V VMs

Replication to Azure

Common questions for Hyper-V to Azure replication

Hyper-V to Azure support matrix

Hyper-V to Azure architecture

Replication to a secondary site

Hyper-V to secondary site support matrix

Hyper-V to secondary site architecture

Networking

Azure Traffic Manager with Site Recovery

ExpressRoute with Site Recovery

Network Security Groups with Site Recovery

Disaster recovery for apps

About recovery plans

About migration

About role-based access control with Site Recovery

FAQ

How-to Guides

Azure to Azure

Networking

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

[Prepare network mapping in Azure VM disaster recovery](#)

[Set up IP addressing for failover](#)

[ExpressRoute with Azure VM disaster recovery](#)

Disaster recovery

[Disaster recovery of Azure VMs after migration to Azure](#)

[Disaster recovery of Azure VMs using PowerShell](#)

Replication, failover, and failback

[Enable Azure to Azure replication](#)

[Reprotect from an Azure secondary region to primary](#)

Troubleshooting

[Troubleshoot Azure to Azure replication](#)

[Troubleshoot Azure Site Recovery extension](#)

Manage

[Automatic update of mobility service extension](#)

VMware/physical to Azure

Networking

[Manage network interfaces for on-premises to Azure replication](#)

[Set up IP addressing for failover](#)

Capacity planning

[Capacity planning for VMware replication to Azure](#)

[Deployment Planner tool for VMware replication to Azure](#)

[Overview and prerequisites](#)

[Run the Deployment Planner tool](#)

[Analyze the generated report](#)

[Analyze the cost estimation report](#)

[Scale out process servers for VMware replication](#)

Disaster recovery

- [Replicate VMware virtual machines to Azure using PowerShell](#)
- [Disaster recovery of physical servers to Azure](#)
- [Set up the source environment for VMware VMs](#)
- [Set up the source environment for physical servers](#)
- [Deploy the configuration server for VMware replication](#)
- [Set up the target environment for VMware VMs](#)
- [Set up the target environment for physical servers](#)
- [Configure replication settings](#)
- [Exclude disks from replication](#)
- [Enable VMware VM replication](#)
- [Multi-tenancy with CSP for VMWare VMs](#)
- [Deploy the Mobility service](#)
 - [Mobility service overview](#)
 - [Deploy the Mobility service with System Center Configuration Manager](#)
- [Failover and failback](#)
 - [Run a disaster recovery drill to Azure](#)
 - [Set up recovery plans](#)
 - [Add Azure runbooks to recovery plans](#)
 - [Set up and manage a failback process server in Azure](#)
 - [Set up a Linux master target server for failback](#)
 - [Run a failover to Azure](#)
 - [Run a failover and failback for physical servers](#)
 - [Fail back from Azure to VMware](#)
 - [Reprotect from Azure to on-premises VMware](#)
- [Manage](#)
 - [Manage the configuration server for VMware replication](#)
 - [Manage the configuration server for physical server replication](#)
 - [Manage process servers](#)
 - [Manage vCenter servers](#)
 - [Remove servers and disable protection](#)
 - [Delete a vault](#)
- [Monitor and troubleshoot](#)

- [Monitor Azure Site Recovery](#)
- [Troubleshoot VMware to Azure replication](#)
- [Troubleshoot the Mobility service in VMware and physical server replication](#)
- [Troubleshoot failover to Azure](#)
- [Troubleshoot reprotection and failback of VMware VMs from Azure](#)
- [VMware/physical to a secondary site](#)
- [Disaster recovery of VMware VMs and physical servers to a secondary site](#)
- [Hyper-V to Azure](#)
 - [Networking](#)
 - [Manage network interfaces for on-premises to Azure replication](#)
 - [Set up IP addressing for failover](#)
 - [Capacity planning](#)
 - [Deployment Planner tool for Hyper-V replication to Azure](#)
 - [Overview and prerequisites](#)
 - [Run the Deployment Planner tool](#)
 - [Analyze the generated report](#)
 - [Analyze the cost estimation report](#)
 - [Disaster recovery](#)
 - [Set up Hyper-V replication to Azure \(no VMM\) using PowerShell](#)
 - [Set up Hyper-V replication to Azure \(with VMM\) using PowerShell](#)
 - [Prepare network mapping for Hyper-V VM disaster recovery](#)
 - [Exclude disks from replication for Hyper-V to Azure](#)
 - [Failover and fallback](#)
 - [Run a disaster recovery drill to Azure](#)
 - [Set up recovery plans](#)
 - [Add VMM scripts to recovery plans](#)
 - [Add Azure runbooks to recovery plans](#)
 - [Run a failover to Azure](#)
 - [Fail back from Azure to Hyper-V](#)
 - [Manage](#)
 - [Remove servers and disable protection](#)
 - [Delete a vault](#)

[Monitor and troubleshoot](#)

[Troubleshoot Hyper-V replication](#)

[Monitor Azure Site Recovery](#)

[Hyper-V to secondary](#)

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

[Set up Hyper-V replication to a secondary VMM site using PowerShell](#)

[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 failback between on-premises sites](#)

[Performance scale tests for Hyper-V replication to a secondary site](#)

[Replicate 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](#)

[Reference](#)

[Azure PowerShell](#)

[Azure PowerShell classic](#)

[REST](#)

[Related](#)

[Azure Automation](#)

[Resources](#)

[Azure Roadmap](#)

[Blog](#)

[Forum](#)

[Learning path](#)

[Pricing](#)

[Pricing calculator](#)

[Service updates](#)

About Site Recovery

7/9/2018 • 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 and physical servers replicating to Azure, or to a secondary site.

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
Replication scenarios <ul style="list-style-type: none"> Replicate Azure VMs from one Azure region to another. Replicate on-premises VMware VMs, Hyper-V VMs, physical servers (Windows and Linux) to Azure. Replicate on-premises VMware VMs, Hyper-V VMs managed by System Center VMM, and physical servers to a secondary site. 	
Regions	Review supported regions for Site Recovery.

SUPPORTED	DETAILS
Replicated machines	Review the replication requirements for Azure VM replication , on-premises VMware VMs and physical servers , and on-premises Hyper-V VMs .
VMware servers/hosts	VMware VMs you want to replicate can be located on supported host and virtualization servers .
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](#).

Replicate an Azure VM to another Azure region

8/21/2018 • 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 replicate an Azure VM to a different Azure region.

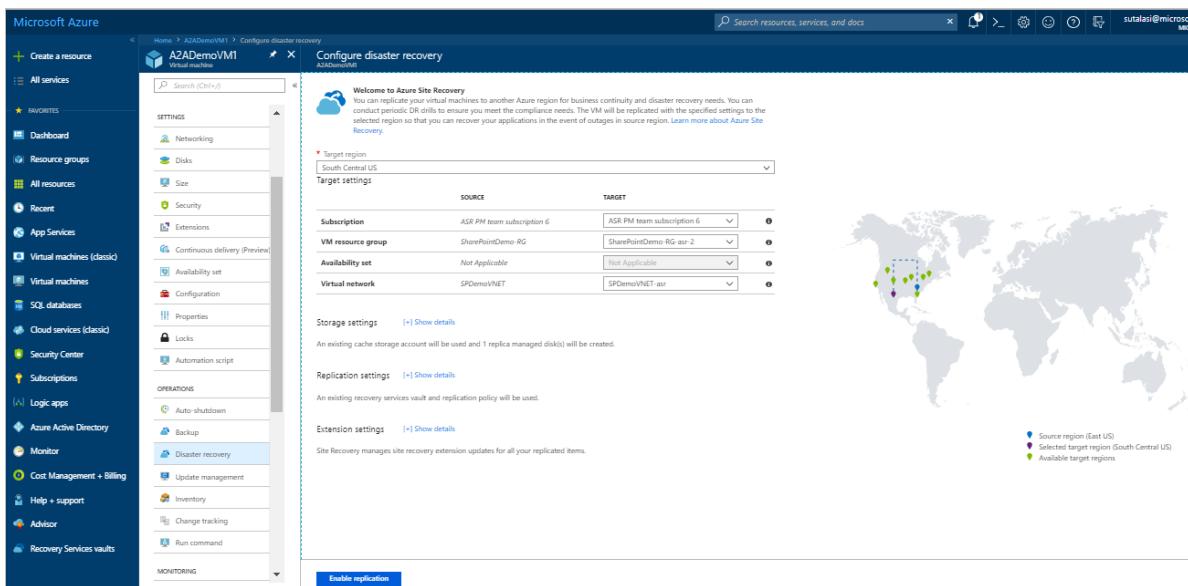
If you don't have an Azure subscription, create a [free account](#) before you begin.

Log in to Azure

Log in to the Azure portal at <http://portal.azure.com>.

Enable replication for the Azure VM

1. In the Azure portal, click **Virtual machines**, and select the VM you want to replicate.
2. In **Operations**, click **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. Click **Enable replication**. This starts a job to enable replication for the VM.



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

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.
- Site Recovery billing for the VM also stops.

Stop replication as follows:

1. Select the VM.
2. In **Disaster recovery**, click **Disable Replication**.

Next steps

In this quickstart, you replicated a single VM to a secondary region.

[Configure disaster recovery for Azure VMs](#)

Set up disaster recovery for Azure VMs to a secondary Azure region

8/22/2018 • 8 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 to a secondary Azure region for Azure VMs. In this tutorial, you learn how to:

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

Prerequisites

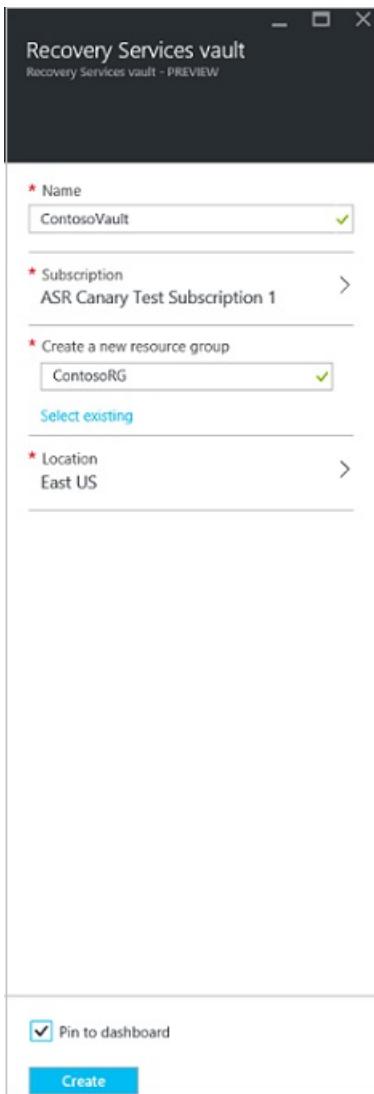
To complete this tutorial:

- Make sure that you understand the [scenario architecture and components](#).
- Review the [support requirements](#) for all components.

Create a vault

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

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. To check supported regions, see geographic availability in [Azure Site Recovery Pricing Details](#).
5. 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.

Verify target resources

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. Site Recovery picks the same size or the closest possible size for the target VM.

Configure outbound network connectivity

For Site Recovery to work as expected, you need to make some changes in outbound network connectivity, from VMs that you want to replicate.

- Site Recovery doesn't support use of an authentication proxy to control network connectivity.
- If you have an authentication proxy, replication can't be enabled.

Outbound connectivity for URLs

If you're using a URL-based firewall proxy to control outbound connectivity, allow access to the following URLs used by Site Recovery.

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

If you want to control outbound connectivity using IP addresses instead of URLs, whitelist the appropriate datacenter ranges; Office 365 addresses; and service endpoint addresses, for IP-based firewalls, proxy, or NSG rules.

- [Microsoft Azure Datacenter IP Ranges](#)
- [Windows Azure Datacenter IP Ranges in Germany](#)
- [Windows Azure Datacenter IP Ranges in China](#)
- [Office 365 URLs and IP address ranges](#)
- [Site Recovery service endpoint IP addresses](#)

You can use this [script](#) to create required NSG rules.

Verify Azure VM certificates

Check that all the latest root certificates are present on the Windows or Linux VMs you want to replicate. If the latest root certificates aren't, the VM can't register to Site Recovery, due to 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 DR 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 on [Azure RBAC built-in roles](#)

Enable replication

Select the source

1. In Recovery Services vaults, click the vault name > **+Replicate**.
2. In **Source**, select **Azure**.
3. In **Source location**, select the source Azure region where your VMs are currently running.
4. Select the **Azure virtual machine deployment model** for VMs: **Resource Manager** or **Classic**.
5. 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.
6. Select the **Source resource group** for Resource Manager VMs, or **cloud service** for classic VMs.
7. Click **OK** to save the settings.

Select the VMs

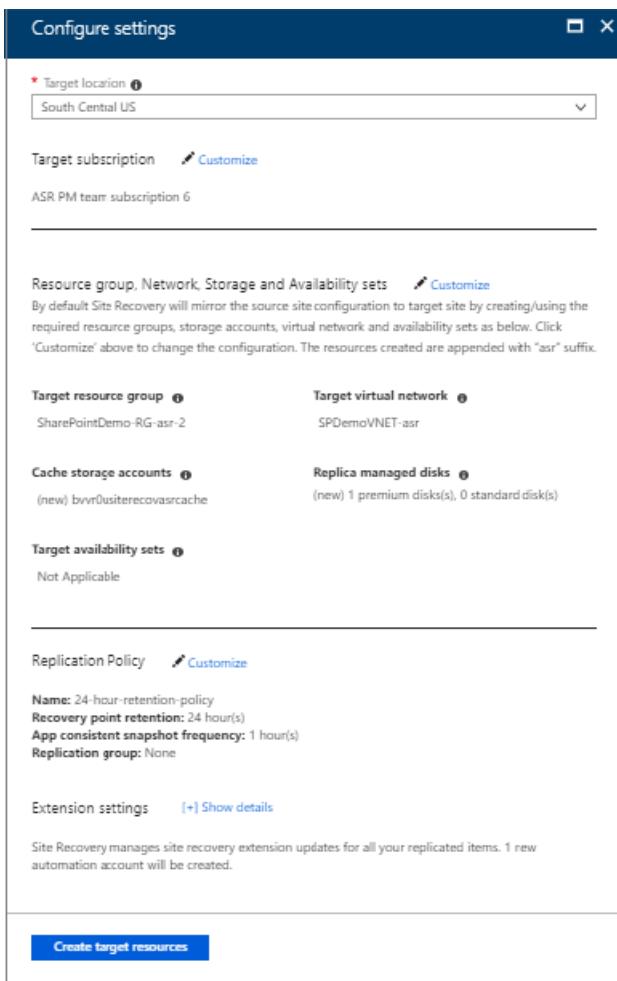
Site Recovery retrieves a list of the VMs associated with the subscription and resource group/cloud service.

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

Configure replication settings

Site Recovery creates default settings and replication policy for the target region. You can change the settings based on your requirements.

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



- **Target subscription:** The target subscription used for disaster recovery. By default, the target subscription will be same as the source subscription. Click 'Customize' to select a different target subscription within the same Azure Active Directory tenant.
- **Target location:** The target region used for disaster recovery. We recommend that the target location matches the location of the Site Recovery vault.
- **Target resource group:** The resource group in the target region that holds Azure VMs after failover. By default, Site Recovery creates a new resource group in the target region with an "asr" suffix. resource group location of the target resource group can be any region except the region where your source virtual machines are hosted.
- **Target virtual network:** The network in the target region that VMs are located after failover. By default, Site Recovery creates a new virtual network (and subnets) in the target region with an "asr" suffix.
- **Cache storage accounts:** 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.
- **Target storage accounts (If source VM does not use managed disks):** By default, Site Recovery creates a new storage account in the target region to mirror the source VM storage account.
- **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.
- **Target availability sets:** By default, Site Recovery creates a new availability set in the target region with the "asr" suffix. You can only add availability sets if VMs are part of a set in the source region.

To override the default replication policy settings, click **Customize** next to **Replication policy**.

- **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:** By default, Site Recovery takes an app-consistent snapshot every 4 hours. You can configure any value between 1 and 12 hours. A 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.
- **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.

Click **Customize** next to **Replication policy** and then select **Yes** for multi-VM consistency to make VMs part of a replication group. You can create a new replication group or use an existing replication group. Select the VMs to be part of the replication group and click **OK**.

IMPORTANT

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 and should be used only if machines are running the same workload and you need consistency across multiple machines.

IMPORTANT

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.

Track replication status

1. In **Settings**, click **Refresh** to get the latest status.
2. You can track progress of the **Enable protection** job in **Settings > Jobs > Site Recovery Jobs**.
3. In **Settings > Replicated Items**, you can view the status of VMs and the initial replication progress. Click the VM to drill down into its settings.

Next steps

In this tutorial, you configured disaster recovery for an Azure VM. Next step is to test your configuration.

[Run a disaster recovery drill](#)

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

7/9/2018 • 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

Prerequisites

- Before you run a test failover, we recommend that you verify the VM properties to make sure everything's as expected. Access the VM properties in **Replicated items**. The **Essentials** blade shows information about machines settings and status.
- 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.

Run a test failover

1. In **Settings > Replicated Items**, click the VM +**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 Azure VMs in the secondary region will be connected, after the failover occurs.
4. To start the failover, 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. To delete the VMs that were created during the test failover, click **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 fail back Azure VMs between Azure regions

7/9/2018 • 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 over a single Azure VM to a secondary Azure region. After you've failed over, you fail back to the primary region when it's available. In this tutorial, you learn how to:

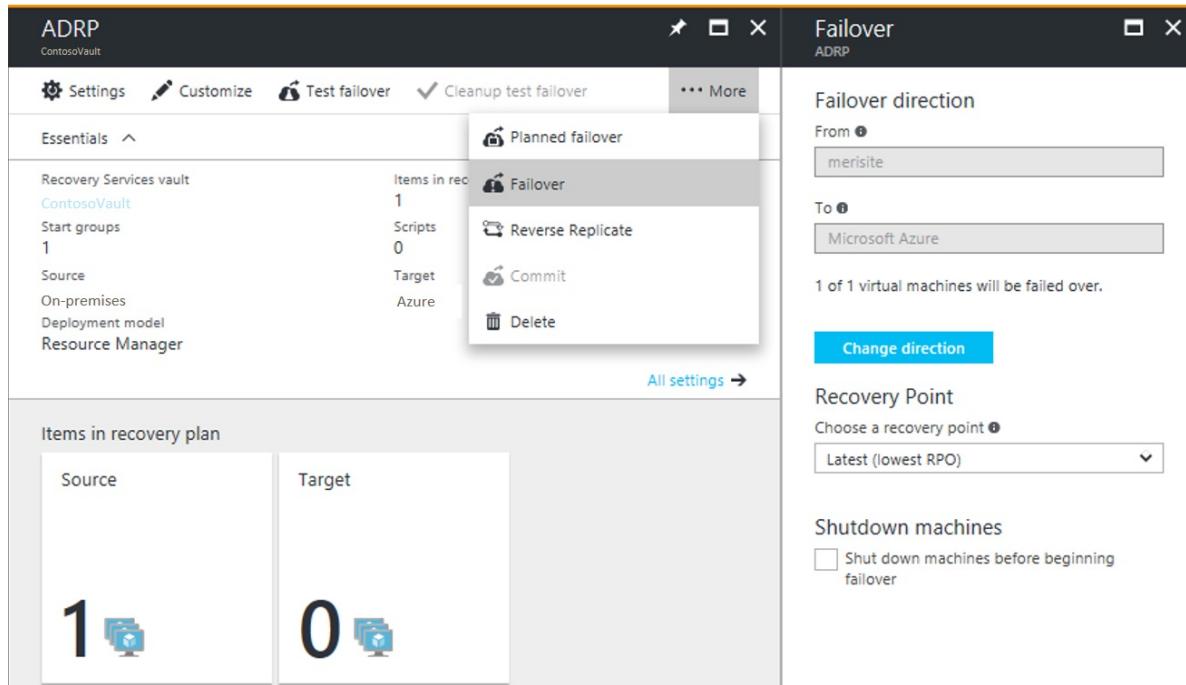
- Fail over the Azure VM
- Reprotect the secondary Azure VM, so that it replicates to the primary region
- Fail back the secondary VM
- Reprotect the primary VM back to the secondary region

Prerequisites

- 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): This option processes all the data in the Site Recovery service and provides the lowest Recovery Point Objective (RPO).
- **Latest processed**: This option reverts the virtual machine to the latest recovery point that has been processed by Site Recovery service.
- **Custom**: Use this option to fail over to a particular recovery point. This option is useful for performing a

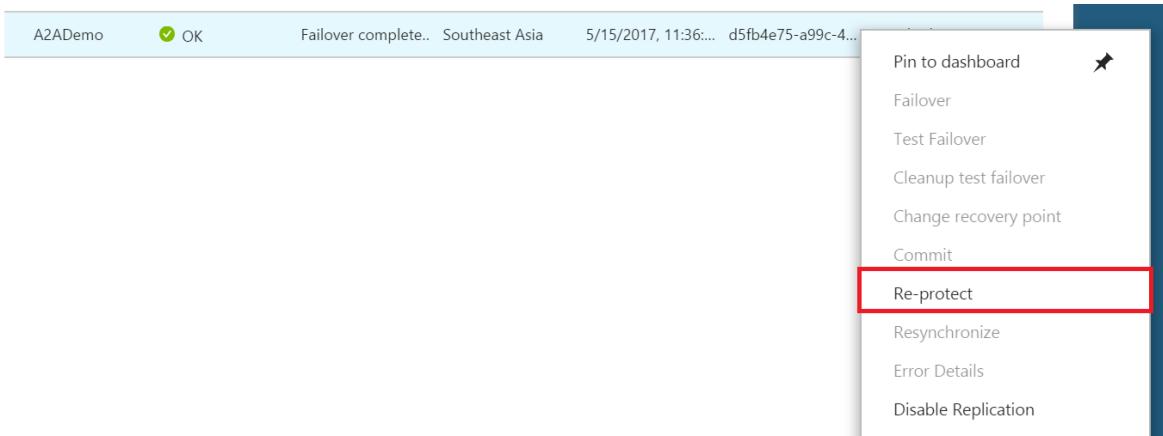
test failover.

3. Select **Shut down machine before beginning failover** if you want Site Recovery to attempt to do a shutdown of source virtual machines before triggering the failover. Failover continues even if shutdown fails.
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. The **Change recovery point** option is no longer available.

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. Notice 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 (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.

Fail back to the primary region

After VMs are reprotected, you can fail back to the primary region as you need to. To do this, follow the [failover](#) instructions.

Prepare Azure resources for replication of on-premises machines

7/9/2018 • 4 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), including replication, failover, and recovery.

This article is the first tutorial in a series that shows you how to set up disaster recovery for on-premises VMs. It's relevant whether you're protecting on-premises VMware VMs, Hyper-V VMs, or physical servers.

Tutorials are designed to show you the simplest deployment path for a scenario. They use default options where possible, and don't show all possible settings and paths.

This article shows you how to prepare Azure components when you want to replicate on-premises VMs (Hyper-V or VMware) or Windows/Linux physical servers to Azure. In this tutorial, you learn how to:

- Verify that your Azure account has replication permissions.
- Create an Azure storage account. Images of replicated machines are stored in it.
- Create a Recovery Services vault. A vault holds 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 Azure network.

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

Sign in to Azure

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

Verify account permissions

If you just 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 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.

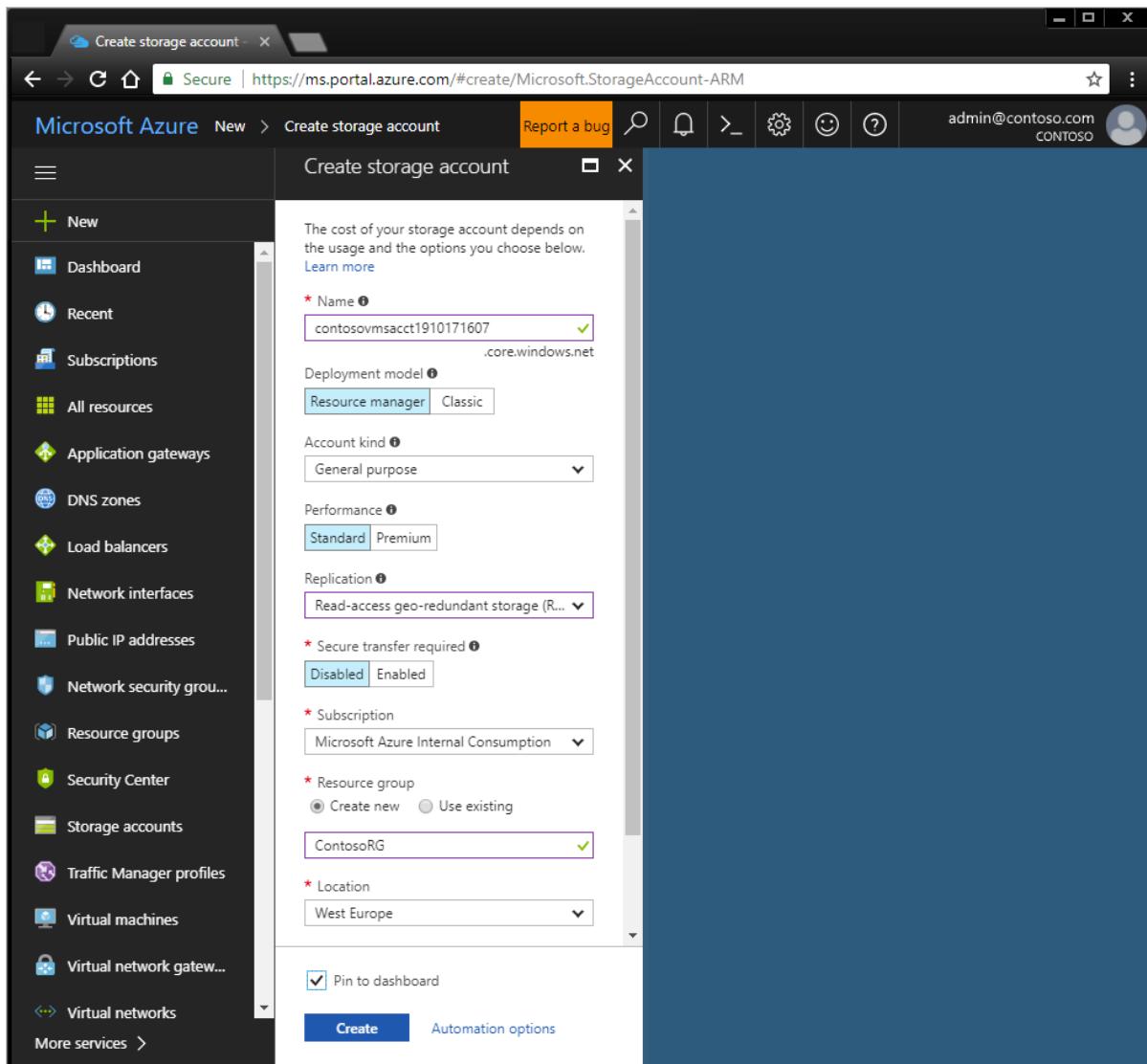
To complete these tasks your account should be assigned the Virtual Machine Contributor built-in role. In addition, to manage Site Recovery operations in a vault, your account should be assigned the Site Recovery Contributor build-in role.

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. We're using West Europe in this tutorial.

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

2. On **Create storage account**, enter a name for the account. For these tutorials, we're using **contosovmsacct1910171607**. The name you select must be unique within Azure and be between 3 and 24 characters, with numbers and lowercase letters only.
3. In **Deployment model**, select **Resource Manager**.
4. In **Account kind**, select **Storage (general purpose v1)**. Don't select blob storage.
5. In **Replication**, select the default **Read-access geo-redundant storage** for storage redundancy. We're leaving **Secure transfer required** as **Disabled**.
6. In **Performance**, select **Standard** and in **Access tier** choose the default option of **Hot**.
7. In **Subscription**, select the subscription in which you want to create the new storage account.
8. In **Resource group**, enter a new resource group. An Azure resource group is a logical container into which Azure resources are deployed and managed. For these tutorials, we're using **ContosoRG**.
9. In **Location**, select the geographic location for your storage account.



10. Select **Create** to create the storage account.

Create a Recovery Services vault

1. In the Azure portal, select **Create a resource > Storage > Backup and Site Recovery (OMS)**.
2. In **Name**, enter a friendly name to identify the vault. For this set of tutorials we're using **ContosoVMVault**.
3. In **Resource group**, we're using **contosoRG**.
4. In **Location**. We're using **West Europe**.
5. To quickly access the vault from the dashboard, select **Pin to dashboard > Create**.

Recovery Services vault

Name: ContosoVMVault

Subscription: Contoso Subscription

Resource group: contosoRG

Location: West Europe

Pin to dashboard

Create Automation options

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**.
2. We're leaving **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. Specify the resource group in which the network will be created. We're using the existing resource group **contosoRG**.
5. In **Address range**, enter the range for the network **10.0.0.0/24**. In this network we're not using a subnet.
6. In **Subscription**, select the subscription in which to create the network.
7. In **Location**, select **West Europe**. The network must be in the same region as the Recovery Services vault.
8. We're leaving the default options of basic DDoS protection, with no service endpoint on the network.
9. Click **Create**.

Home > New > Create virtual network

Create virtual network

* Name
ContosoASRnet ✓

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

* Subscription
Microsoft Azure Internal Consumption (e12l) ▾

* Resource group
 Create new Use existing
ContosoRG ▾

* Location
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

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

Useful links

- [Learn about](#) Azure networks.
- [Learn about](#) types of Azure storage.
- [Learn more](#) about storage redundancy, and [secure transfer](#) for storage.

Next steps

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

Prepare on-premises VMware servers for disaster recovery to Azure

7/9/2018 • 5 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), including replication, failover, and recovery.

- 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.
- Tutorials are designed to show you the simplest deployment path for a scenario. They use default options where possible, and don't show all possible settings and paths.

In this article, we show you how to prepare your on-premises VMware environment when you want to replicate VMware VMs to Azure using Azure Site Recovery. 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
- Prepare to connect to Azure VMs after failover

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
VM discovery	At least a read-only user 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. To restrict access, assign the No access role with the Propagate to child object, to the child objects (vSphere hosts, datastores, VMs and networks).

Task	Role/Permissions	Details
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](#).

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 log 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.

Useful links

If you're replicating multiple VMs, you should plan capacity and deployment before you start. [Learn more](#).

Next steps

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

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

7/9/2018 • 9 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), including replication, failover, and recovery.

In this tutorial, we show you how to set up and enable replication of a VMware VM to Azure, using Azure Site Recovery. Tutorials are designed to show you how to deploy Site Recovery with basic settings. They use the simplest path, and don't show all options. In this tutorial, you learn how to:

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

Before you start

Before you start, it's helpful to:

- [Review the architecture](#) for this disaster recovery scenario.
- If you want to learn about setting up disaster recovery for VMware VMs in more detail, review and use the following resources:
 - [Read common questions](#) about disaster recovery for VMware.
 - [Learn](#) what's supported and required for VMware.
- Read our **How To guides** for detailed instructions that cover all deployment options for VMware:
 - Set up the [replication source](#) and [configuration server](#).
 - Set up the [replication target](#).
 - Configure a [replication policy](#), and [enable replication](#).

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**.

Plan your deployment

In this tutorial we're showing you how to replicate a single VM, and in **Deployment Planning**, we'll select **Yes, I have done it**. If you're deploying multiple VMs we recommend that you don't skip this step. We provide the [Deployment Planner Tool](#) to help you. [Learn more](#) about this tool.

Set up the source environment

As a first deployment step, you set up your source environment. You need a single, highly available, on-premises machine to host on-premises Site Recovery components. Components include the configuration server, process server, and master target server:

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

To set up the configuration server as a highly available VMware VM, download a prepared Open Virtualization Application (OVA) template and import the template into VMware to create the VM. After you set up the configuration server, register it in the vault. After registration, Site Recovery discovers on-premises VMware VMs.

TIP

This tutorial uses an OVA template to create the configuration server VMware VM. If you're unable to do this, you can [set up the configuration server manually](#).

TIP

In this tutorial, Site Recovery downloads and installs MySQL to the configuration server. If you don't want Site Recovery to do this, you can set it up manually. [Learn more](#).

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.

TIP

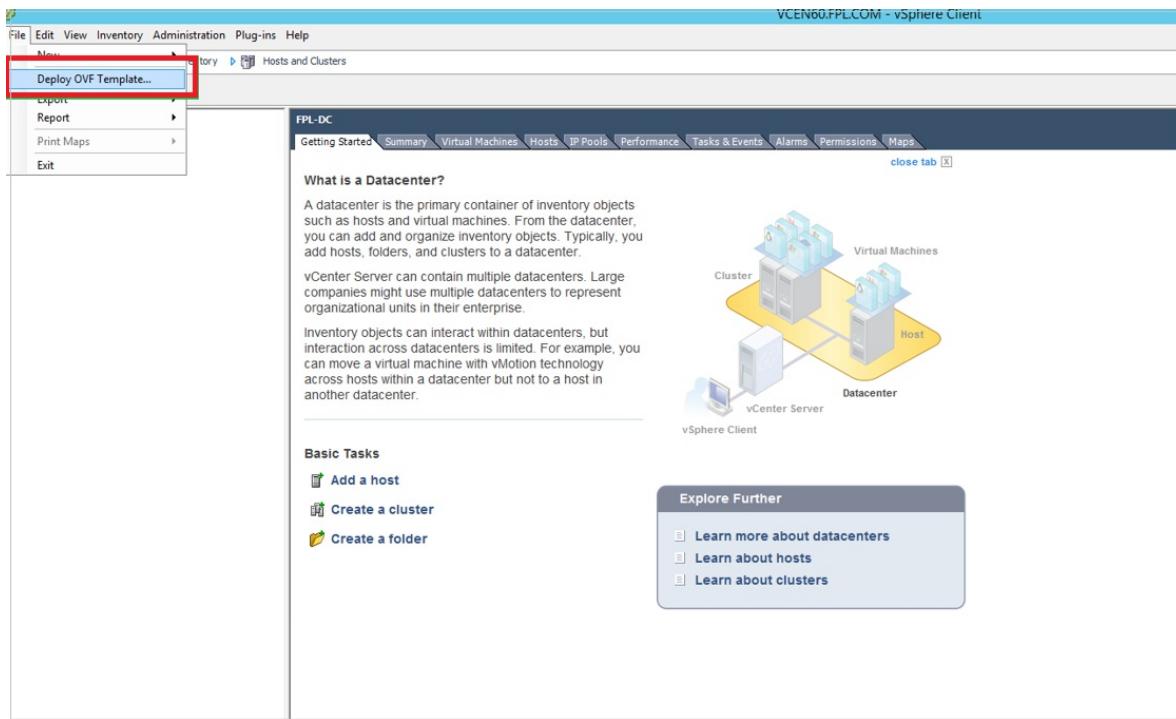
You can download the latest version of the configuration server template directly from the [Microsoft Download Center](#).

NOTE

The licence provided with OVF template is an evaluation licence valid for 180 days. Customer needs to activate the windows with a procured licence.

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

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

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.
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

1. In the configuration server management wizard, select **Setup connectivity**, and then select the NIC that the process server uses to receive replication traffic from VMs. Then select **Save**. You can't 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 is skipped.
4. Select **Install VMware PowerCLI**. Make sure all browser windows are closed before you do this. Then select **Continue**.
5. In **Validate appliance configuration**, prerequisites are verified before you continue.
6. 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.
7. 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**, and then select **Continue**.
8. 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.
9. Select **Finalize configuration** to complete registration.
10. After registration finishes, in the Azure portal, verify that the configuration server and VMware server are listed on the **Source** page in the vault. Then select **OK** to configure target settings.

Site Recovery connects to VMware servers by using the specified settings and discovers VMs.

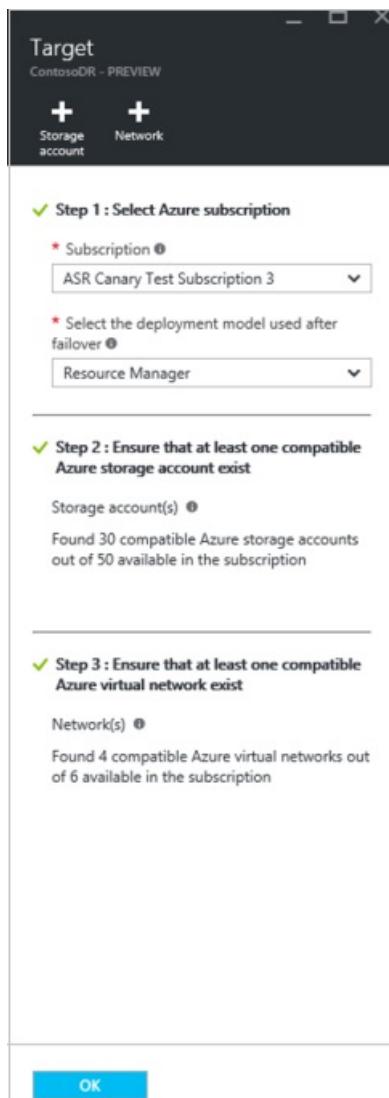
NOTE

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

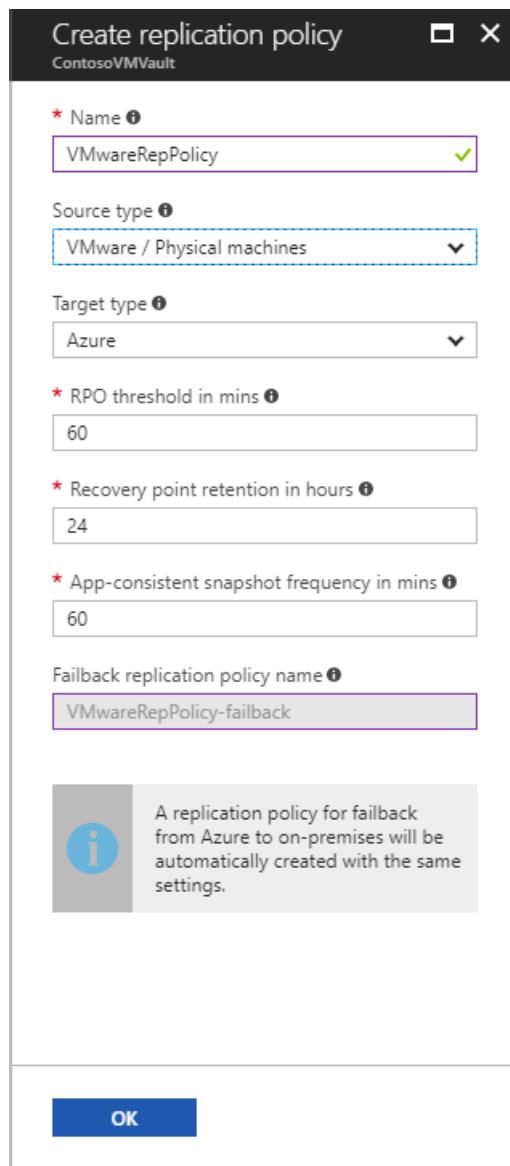
Select and verify target resources.

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 compatible Azure storage accounts and 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](#), and select **All resources**.
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 can be performed 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**.
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 storage account you want to use to replicate data, and 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**.

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, 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

[Run a disaster recovery drill](#)

Run a disaster recovery drill to Azure

8/13/2018 • 3 minutes to read • [Edit Online](#)

In this article, we show you how to run a disaster recovery drill for an on-premises machine to Azure, using a test failover. 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 VMware VMs, or Hyper-V VMs.

This tutorial presumes that you've completed the first three tutorials:

- In the [first tutorial](#), we set up the Azure components needed for VMware disaster recovery.
- In the [second tutorial](#), we prepared on-premises components for disaster recovery, and reviewed prerequisites.
- In the [third tutorial](#) we set up and enabled replication for our on-premises VMware VM.
- Tutorials are designed to 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 test failover steps in more detail, read the [How To Guide](#).

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

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 **Disks**, you can see information about the operating system and data disks on the VM.

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.

Next steps

[Run a failover and failback for on-premises VMware VMs](#). [Run a failover and failback for on-premises Hyper-V VMs](#).

Fail over and fail back VMware VMs and physical servers replicated to Azure

7/9/2018 • 8 minutes to read • [Edit Online](#)

This tutorial describes how to fail over a VMware VM to Azure. 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 VMware VM properties to check conform with Azure requirements
- Run a failover to Azure
- Create a process server and master target server for failback
- Reprotect Azure VMs to the on-premises site
- Fail over from Azure to on-premises
- Reprotect on-premises VMs, to start replicating to Azure again

NOTE

Tutorials are designed to 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 test failover steps in detail, read the [How-to Guide](#).

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

1. [Prepare Azure](#)
2. [Prepare on-premises VMware](#)
3. [Set up disaster recovery](#)
4. [Run a disaster recovery drill](#)
5. In addition to the above steps, it is helpful to [review the architecture](#) for the disaster recovery scenario.

Failover and failback

Failover and failback have four stages:

1. **Fail over to Azure:** Fail machines over from the on-premises site to Azure.
2. **Reprotect Azure VMs:** Reprotect the Azure VMs, so that they start replicating back to the on-premises VMware VMs. The on-premises VM is turned off during reprottection. This helps ensure data consistency during replication.
3. **Fail over to on-premises:** Run a failover, to fail back from Azure.
4. **Reprotect on-premises VMs:** After data has failed back, reprotect the on-premises VMs that you failed back to, so that they start replicating to Azure.

Verify VM properties

Verify the VM properties, and make sure that the VM complies with [Azure requirements](#).

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**, 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 operating system and data disks on the VM.

Run a failover to Azure

1. In **Settings > Replicated items**, click the VM > **Failover**.
2. In **Failover**, select a **Recovery Point** to fail over to. You can use one of the following options:
 - **Latest** (default): 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 VM 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 VM to the latest app-consistent recovery point processed by Site Recovery.
 - **Custom**: Specify a recovery point.
3. Select **Shut down machine before beginning failover** to attempt to do a shutdown of source virtual machines before triggering the failover. Failover continues even if shutdown fails. You can follow the failover progress on the **Jobs** page.

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 virtual machines using mobility service of version older than 9.8, physical servers, VMware Linux virtual machines, Hyper-V virtual machines protected as physical servers, 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.

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 virtual machine in Azure

1. After failover, go to the virtual machine and validate by [connecting](#) to it.
2. Post validation, click on **Commit** to finalize the recovery point of the virtual machine after failover. Post commit, all the other available recovery points are deleted. This completes the failover activity.

TIP

Change recovery point helps you in choosing a different recovery point after failover if you are not satisfied with the failed over virtual machine. After **commit**, this option will no longer be available.

Preparing for reprotection of Azure VM

Create a process server in Azure

The process server receives data from the Azure VM, and sends it to the on-premises site. A low-latency network

is required between the process server and the protected VM.

- For test purposes, if you have an Azure ExpressRoute connection, you can use the on-premises process server (in-built process server) that's automatically installed on the configuration server.
- If you have a VPN connection, or you're running failback in a production environment, you must set up an Azure VM as an Azure-based process server for failback.
- To set up a process server in Azure, follow the instructions in [this article](#).

Configure the master target server

A master target server receives and handles replication data during failback from Azure. By default, it is available on the on-premises configuration server. In this tutorial, let's use the default master target server.

NOTE

Protecting a Linux based virtual machine requires creation of a separate Master Target Server. [Click here](#) to learn more.

If the VM is on an **ESXi host that's managed by a vCenter** server, the master target server must have access to the VM's datastore (VMDK), to write replicated data to the VM disks. Make sure that the VM datastore is mounted on the master target's host, with read/write access.

If the VM is on an **ESXi that isn't managed by a vCenter server**, Site Recovery service creates a new VM during reprottection. The VM is created on the ESX host on which you create the master target. 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.

If the VM **doesn't use vCenter**, you should complete discovery of the host on which the master target server is running, before you can reprotect the machine. This is true for failing back physical servers too. Another option, if the on-premises VM exists, is to delete it before you do a failback. Failback then creates a new VM on the same host as the master target ESX host. When you fail back to an alternate location, the data is recovered to the same datastore and the same ESX host as that used by the on-premises master target server.

You can't use Storage vMotion on the master target server. If you do, failback won't work, because the disks aren't available to it. Exclude the master target servers from your vMotion list.

WARNING

If you use a different master target server to reprotect a replication group, the server cannot provide a common point in time.

Reprotect Azure VMs

Reprotecting Azure VM leads to replication of data on to on-premises VM. This is a mandatory step before performing failover from Azure to on-premises VM. Follow the below given instructions to execute reprottection.

1. In **Settings > Replicated items**, right-click the VM 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. If the VM has been deleted, new disks are created on this datastore. This setting is ignored if the disks already exist, but you do need to specify a value.
5. Select the master target retention drive. The failback policy is automatically selected.
6. Click **OK** to begin reprottection. A job begins to replicate the virtual machine from Azure to the on-premises site. You can track the progress on the **Jobs** tab.
7. After the status of VM on **Replicated items** changes to **Protected**, the machine is ready for failover to on-

premises.

NOTE

Azure VM can be recovered to an existing on-premises VM or an alternate location. Read [this article](#) to learn more.

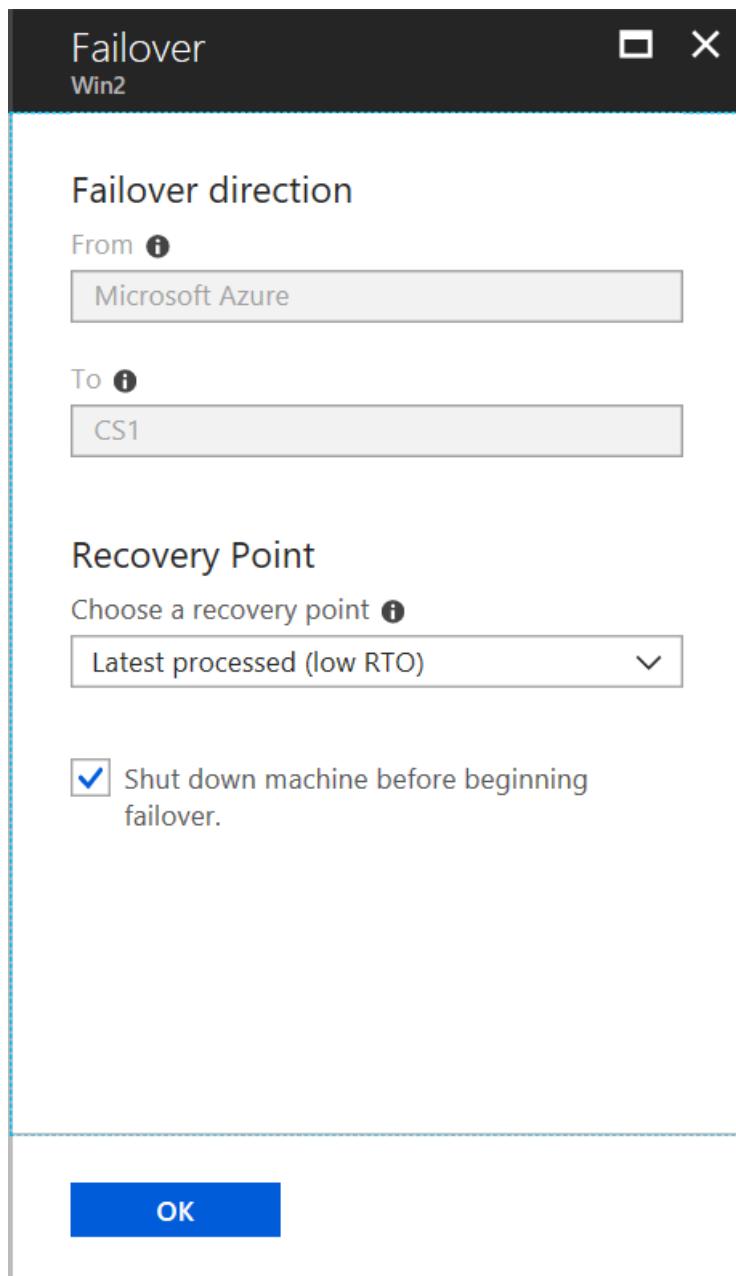
Run a failover from Azure to on-premises

To replicate back to on-premises, a fallback policy is used. This policy is automatically created when you created a replication policy for replication to Azure:

- The policy is automatically associated with the configuration server.
- The policy can't be modified.
- The policy values are:
 - RPO threshold = 15 minutes
 - Recovery point retention = 24 hours
 - App-consistent snapshot frequency = 60 minutes

Run the failover as follows:

1. On the **Replicated Items** page, right-click the machine > **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. An app-consistent recovery point occurs before the most recent point in time, and it will cause some data loss.

WARNING

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.

4. The progress of the job can be tracked on **Recovery Services Vault > Monitoring and Reports > Site Recovery Jobs**.
5. After completion of failover, right-click the virtual machine, and click **Commit**. This triggers a job that removes the Azure VMs.
6. 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 > **Protected items > Replicated Items**, select the failed back VM, and click **Re-Protect**.

2. Select the process server that is to be used to send the replicated data to Azure, and click **OK**.

After the reprotection finishes, the VM replicates back to Azure, and you can run a failover as required.

Prepare Azure resources for replication of on-premises machines

7/9/2018 • 4 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), including replication, failover, and recovery.

This article is the first tutorial in a series that shows you how to set up disaster recovery for on-premises VMs. It's relevant whether you're protecting on-premises VMware VMs, Hyper-V VMs, or physical servers.

Tutorials are designed to show you the simplest deployment path for a scenario. They use default options where possible, and don't show all possible settings and paths.

This article shows you how to prepare Azure components when you want to replicate on-premises VMs (Hyper-V or VMware) or Windows/Linux physical servers to Azure. In this tutorial, you learn how to:

- Verify that your Azure account has replication permissions.
- Create an Azure storage account. Images of replicated machines are stored in it.
- Create a Recovery Services vault. A vault holds 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 Azure network.

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

Sign in to Azure

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

Verify account permissions

If you just 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 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.

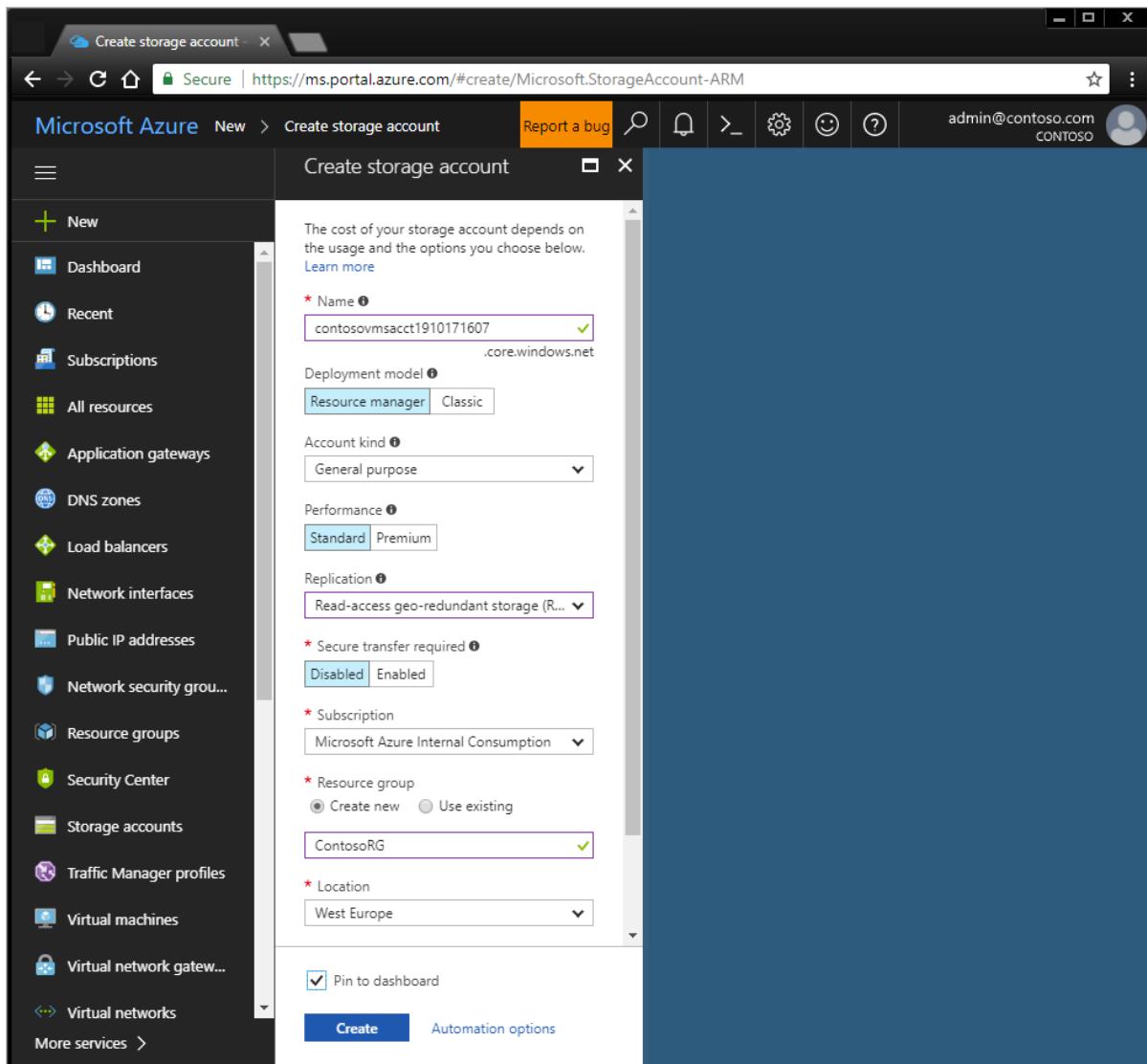
To complete these tasks your account should be assigned the Virtual Machine Contributor built-in role. In addition, to manage Site Recovery operations in a vault, your account should be assigned the Site Recovery Contributor build-in role.

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. We're using West Europe in this tutorial.

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

2. On **Create storage account**, enter a name for the account. For these tutorials, we're using **contosovmsacct1910171607**. The name you select must be unique within Azure and be between 3 and 24 characters, with numbers and lowercase letters only.
3. In **Deployment model**, select **Resource Manager**.
4. In **Account kind**, select **Storage (general purpose v1)**. Don't select blob storage.
5. In **Replication**, select the default **Read-access geo-redundant storage** for storage redundancy. We're leaving **Secure transfer required** as **Disabled**.
6. In **Performance**, select **Standard** and in **Access tier** choose the default option of **Hot**.
7. In **Subscription**, select the subscription in which you want to create the new storage account.
8. In **Resource group**, enter a new resource group. An Azure resource group is a logical container into which Azure resources are deployed and managed. For these tutorials, we're using **ContosoRG**.
9. In **Location**, select the geographic location for your storage account.



10. Select **Create** to create the storage account.

Create a Recovery Services vault

1. In the Azure portal, select **Create a resource > Storage > Backup and Site Recovery (OMS)**.
2. In **Name**, enter a friendly name to identify the vault. For this set of tutorials we're using **ContosoVMVault**.
3. In **Resource group**, we're using **contosoRG**.
4. In **Location**. We're using **West Europe**.
5. To quickly access the vault from the dashboard, select **Pin to dashboard > Create**.

Recovery Services vault

Name: ContosoVMVault

Subscription: Contoso Subscription

Resource group: contosoRG

Location: West Europe

Pin to dashboard

Create Automation options

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**.
2. We're leaving **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. Specify the resource group in which the network will be created. We're using the existing resource group **contosoRG**.
5. In **Address range**, enter the range for the network **10.0.0.0/24**. In this network we're not using a subnet.
6. In **Subscription**, select the subscription in which to create the network.
7. In **Location**, select **West Europe**. The network must be in the same region as the Recovery Services vault.
8. We're leaving the default options of basic DDoS protection, with no service endpoint on the network.
9. Click **Create**.

Home > New > Create virtual network

Create virtual network

* Name
ContosoASRnet ✓

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

* Subscription
Microsoft Azure Internal Consumption (e12l) ▾

* Resource group
 Create new Use existing
ContosoRG ▾

* Location
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

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

Useful links

- [Learn about](#) Azure networks.
- [Learn about](#) types of Azure storage.
- [Learn more](#) about storage redundancy, and [secure transfer](#) for storage.

Next steps

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

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

7/9/2018 • 3 minutes to read • [Edit Online](#)

This tutorial shows you how to prepare your on-premises Hyper-V infrastructure when you want to replicate Hyper-V VMs to Azure, for the purposes of disaster recovery. Hyper-V hosts can be managed by System Center Virtual Machine Manager (VMM), but it's not required. In this tutorial you learn how to:

- Review Hyper-V requirements, and VMM requirements if applicable.
- Prepare VMM if applicable
- Verify internet access to Azure locations
- Prepare VMs so that you can access them after failover to Azure

This is the second tutorial in the series. Make sure that you have [set up the Azure components](#) as described in the previous tutorial.

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 these URLs:

Name Commercial URL Government URL Description	--- --- --- ---	Azure AD
login.microsoftonline.com	login.microsoftonline.us	Used for access control and identity management using AAD
Backup	*.backup.windowsazure.com	*.backup.windowsazure.us
Transfer and coordination	Replication	*.hypervrecoverymanager.windowsazure.com
Storage	*.blob.core.windows.net	*.blob.core.usgovcloudapi.net
Telemetry (optional)	dc.services.visualstudio.com	dc.services.visualstudio.com
	Used for telemetry	time.nist.gov and time.windows.com are used to check time synchronization between system and global time in all deployments.

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.

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 log 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

7/9/2018 • 4 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 Hyper-V VMs to Azure. The tutorial is relevant for Hyper-V VMs that are not managed by 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.

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

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

Before you start, it's helpful to [review the architecture](#) for this disaster recovery scenario.

Select a replication goal

1. In **All Services > Recovery Services vaults**, select the vault that was prepared in the previous tutorial, **ContosoVMVault**.
2. In **Getting Started**, click **Site Recovery**. Then click **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 you using System Center VMM to manage your Hyper-V hosts**, select **No**. Then click **OK**.

Prepare infrastructure

ContosoVMVault

These are long running tasks done on-premises.

- 1 Protection goal > Select
- 2 Source Prepare
- 3 Target Prepare
- 4 Replication settings > Prepare
- 5 Deployment planning > Select

Protection goal

ContosoVMVault

* Where are your machines located?

On-premises

* Where do you want to replicate your machines to?

To Azure

* Are your machines virtualized?

Yes, with Hyper-V

* Are you using System Center VMM to manage your Hyper-V hosts?

No

Confirm deployment planning

When you're planning a large deployment, you should make sure you complete [deployment planning for Hyper-V replication](#). For the purposes of this tutorial, In **Have you completed deployment planning?**, select **I will do it later** in the dropdown list.

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. Status: >
- 4 Target**: Prepare. Status: >
- 5 Replication settings**: Prepare. Status: >

To the right, 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 Hyper-V hosts to the site. 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.

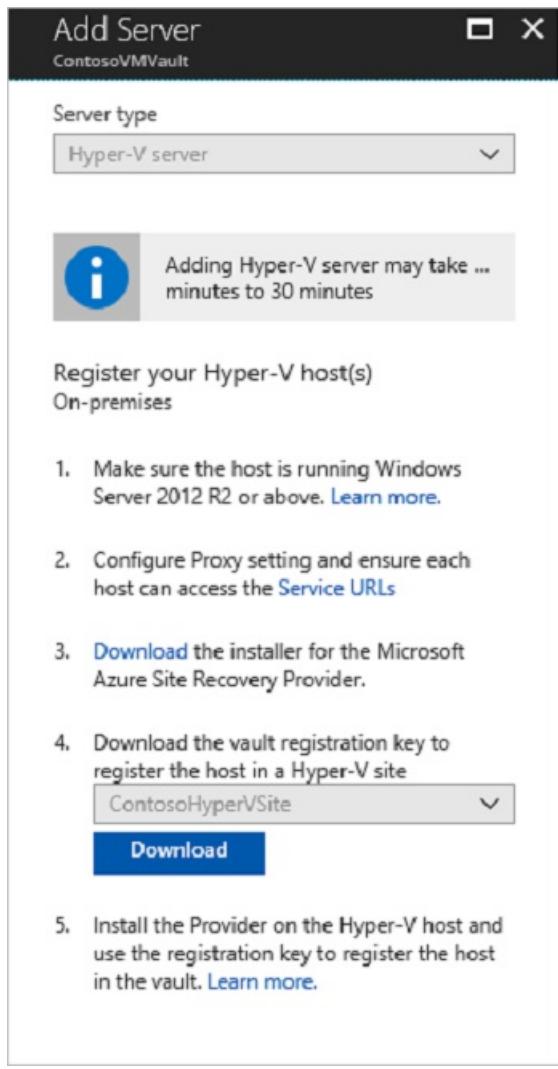
1. In **Prepare Infrastructure**, click **Source**.
2. Click **+Hyper-V Site**, and specify the name of the site created in the previous tutorial, **ContosoHyperVSite**.

These are long running tasks done on-premises.		+ Hyper-V Site	Hyper-V Server
<p>1 Protection goal Hyper-V VMs to Azure</p> <p>2 Deployment planning I will do it later</p> <p>3 Source Prepare ></p> <p>4 Target Prepare ></p> <p>5 Replication settings Prepare ></p>		<p>→ Step 1: Select Hyper-V site</p>  <p>(0 sites found) Click on +Hyper-V Site in the command bar above to add a site.</p> <p>Step 2: Ensure Hyper-V servers are added</p> <p>Complete previous step(s).</p>	

3. After the site is created, click **+Hyper-V Server**.

These are long running tasks done on-premises.		+ Hyper-V Site	+ Hyper-V Server
<p>1 Protection goal Hyper-V VMs to Azure</p> <p>2 Deployment planning I will do it later</p> <p>3 Source Prepare ></p> <p>4 Target Prepare ></p> <p>5 Replication settings Prepare ></p>		<p>✓ Step 1: Select Hyper-V site</p> <p>* Hyper-V Site ContosoHyperVSite</p> <p>→ Step 2: Ensure Hyper-V servers are added</p>  <p>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.</p>	

4. Download the Provider setup file.
5. Download the vault registration key. You need this key to run Provider setup. The key is valid for five days after you generate it.



Install the Provider

Run the Provider setup file (AzureSiteRecoveryProvider.exe) on each Hyper-V host you added to the **ContosoHyperVSite** site. Setup installs the Azure Site Recovery Provider and Recovery Services agent, on each Hyper-V host.

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 agent, and click **Install**.
3. After installation, in the Microsoft Azure Site Recovery Registration Wizard > **Vault Settings**, click **Browse**, and in **Key File**, select the vault key file that you downloaded.
4. Specify the Azure Site Recovery subscription, the vault name (**ContosoVMVault**), and the Hyper-V site (**ContosoHyperVSite**) to which the Hyper-V server belongs.
5. In **Proxy Settings**, select **Connect directly to Azure Site Recovery without a proxy**.
6. In **Registration**, After the server is registered in the vault, click **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.

Set up the target environment

Select and verify target resources.

1. Click **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.

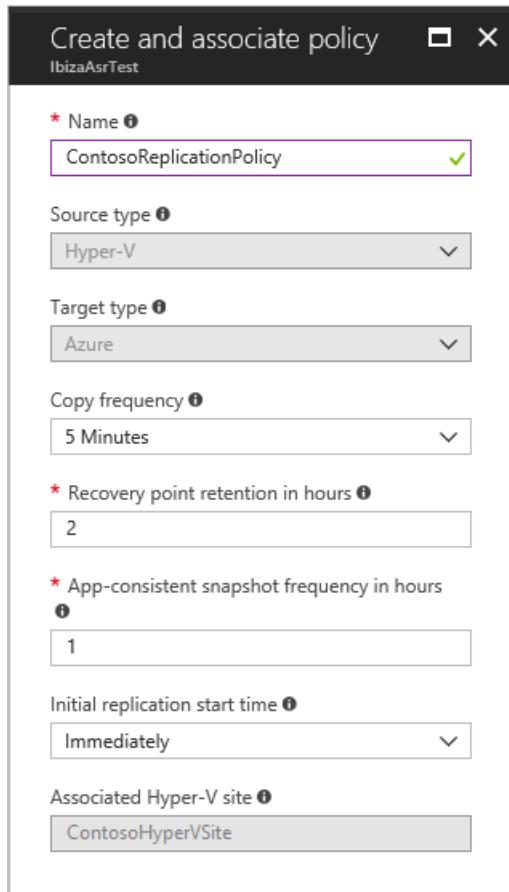
Site Recovery checks that you have one or more compatible Azure storage accounts and networks.

Set up a replication policy

NOTE

For Hyper-V to Azure replication policies, the 15-minute copy frequency option is being retired in favor of the 5-minute, and 30-second copy frequency settings. Replication policies using a 15-minute copy frequency will automatically be updated to use the 5-minute copy frequency setting. The 5-minute, and 30-second copy frequency options provides improved replication performance and better recovery point objectives compared to a 15-minute copy frequency, with minimal impact on bandwidth usage and data transfer volume.

1. Click **Prepare infrastructure > Replication Settings > +Create and associate**.
2. In **Create and associate policy**, specify a policy name, **ContosoReplicationPolicy**.
3. Leave the default settings and click **OK**.
 - **Copy frequency** indicates that delta data (after initial replication) will replicate every five minutes.
 - **Recovery point retention** indicates that the retention windows for each recovery point will be 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, click **OK**. When you create a new policy, it's automatically associated with the specified Hyper-V site (**ContosoHyperVSite**)



Enable replication

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

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 virtual machine 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

7/23/2018 • 4 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 Hyper-V VMs to Azure. The tutorial is relevant for Hyper-V VMs that are managed by 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.
- Set up network mapping, to map between VMM VM networks, and Azure virtual networks.
- Create a replication policy
- Enable replication for a VM

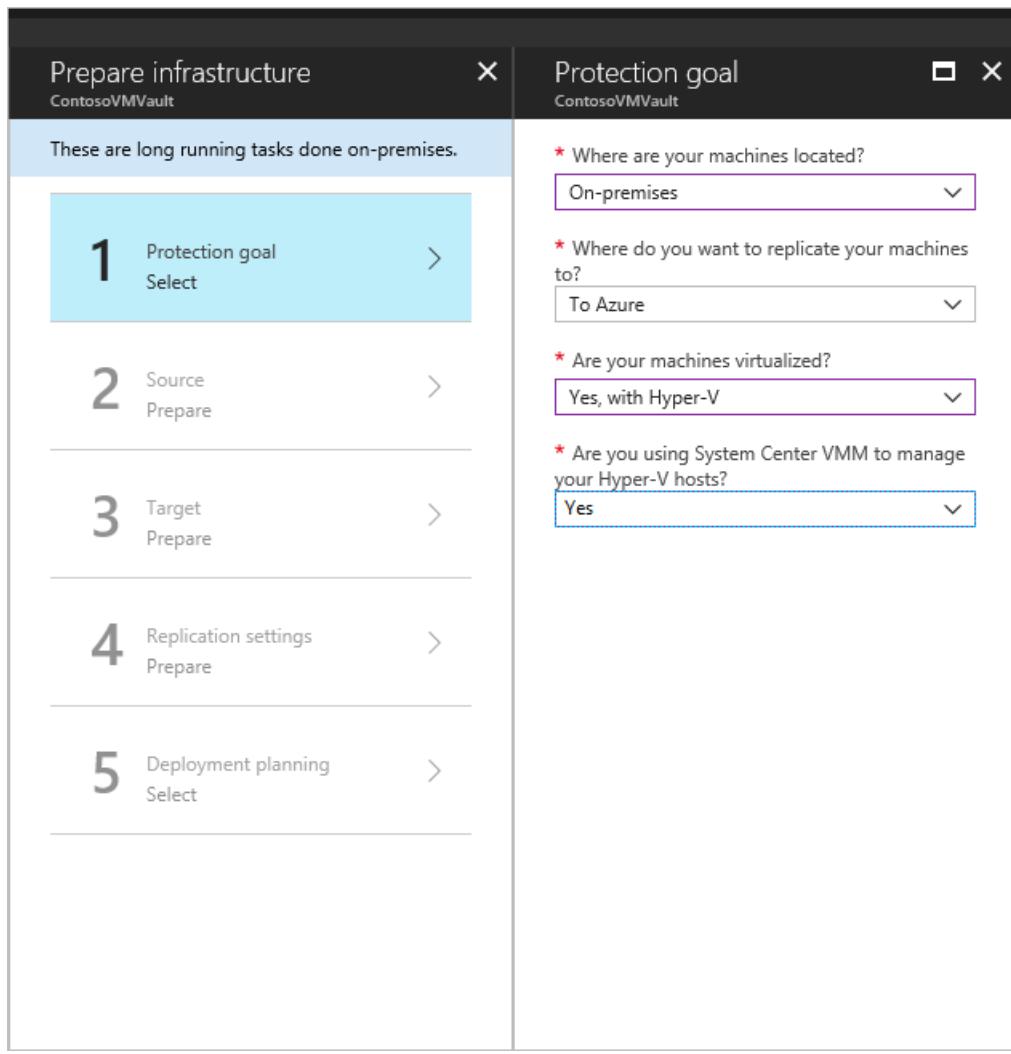
This is the third tutorial in a series. This tutorial assumes that you have already completed the tasks in the previous tutorials:

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

Before you start, it's helpful to [review the architecture](#) for this disaster recovery scenario.

Select a replication goal

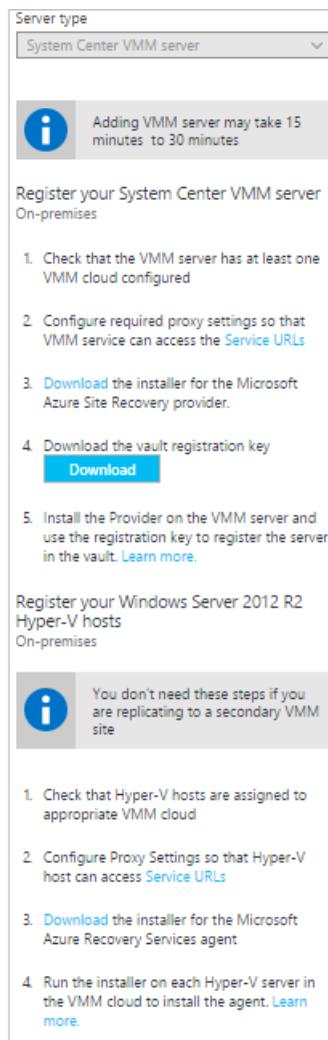
1. In **All Services > Recovery Services vaults**, click the vault name we use in these tutorials, **ContosoVMVault**.
2. In **Getting Started**, click **Site Recovery**. Then click **Prepare Infrastructure**
3. In **Protection goal > Where are your machines located**, select **On-premises**.
4. In **Where 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**, select **Yes**. Then click **OK**.



Set up the source environment

When you set up the source environment, you install the Azure Site Recovery Provider and the Azure Recovery Services agent, and register on-premises servers in the vault.

1. In **Prepare Infrastructure**, click **Source**.
2. In **Prepare source**, click **+ 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 when you run Provider setup. The key is valid for five days after you generate it.
5. Download the Recovery Services agent.



Install the Provider on the VMM server

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

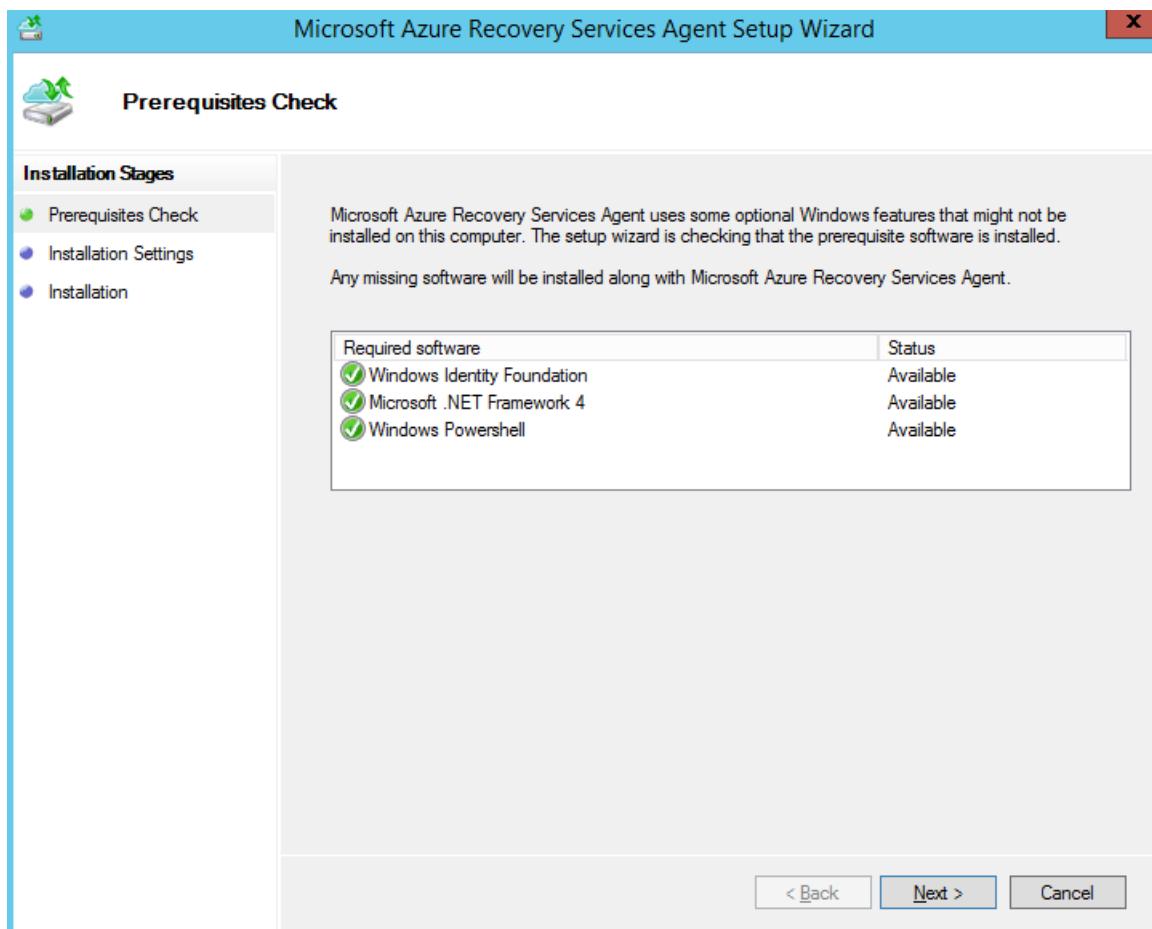
After registration finishes, metadata from the server is retrieved by Azure Site Recovery, and the VMM server is displayed in **Site Recovery Infrastructure**.

Install the Recovery Services agent

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

- In the Microsoft Azure Recovery Services Agent Setup Wizard > **Prerequisites Check**, click **Next**. Any missing prerequisites will automatically be installed.
- 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 click **Install**.

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



Set up the target environment

1. Click **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**, click 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 click **OK**.

* Source System Center VMM	* Target
CP-L2B18-X64-48.drtest.nttest.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. Click **Prepare infrastructure > Replication Settings > +Create and associate**.
2. In **Create and associate policy**, specify a policy name, **ContosoReplicationPolicy**.
3. Leave the default settings and click **OK**.
 - **Copy frequency** indicates that delta data (after initial replication) will replicate every five minutes.
 - **Recovery point retention** indicates that the retention windows for each recovery point will be 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** - the default **Off** setting indicates that at rest data in Azure isn't encrypted.
4. After the policy is created, click **OK**. When you create a new policy it's automatically associated with the VMM cloud.

Enable replication

1. In **Replicate application**, click **Source**.
2. In **Source**, select the VMM cloud. Then click **OK**.
3. In **Target**, verify Azure as the target, 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 you want to replicate. Then click **OK**.

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 disaster recovery drill to Azure

8/13/2018 • 3 minutes to read • [Edit Online](#)

In this article, we show you how to run a disaster recovery drill for an on-premises machine to Azure, using a test failover. 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 VMware VMs, or Hyper-V VMs.

This tutorial presumes that you've completed the first three tutorials:

- In the [first tutorial](#), we set up the Azure components needed for VMware disaster recovery.
- In the [second tutorial](#), we prepared on-premises components for disaster recovery, and reviewed prerequisites.
- In the [third tutorial](#) we set up and enabled replication for our on-premises VMware VM.
- Tutorials are designed to 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 test failover steps in more detail, read the [How To Guide](#).

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

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 **Disks**, you can see information about the operating system and data disks on the VM.

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.

Next steps

[Run a failover and failback for on-premises VMware VMs](#). [Run a failover and failback for on-premises Hyper-V VMs](#).

Failover and failback Hyper-V VMs replicated to Azure

7/9/2018 • 3 minutes to read • [Edit Online](#)

This tutorial describes how to failover a Hyper-V VM to Azure. After you've failed over, you failback 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
- Run a failover to Azure
- Failback from Azure to on-premises
- Reverse replicate on-premises VMs, to start replicating to Azure again

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](#)

Prepare for failover and failback

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.

Failover 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.

Fallback Azure VM to on-premises and reverse replicate the on-premises VM

Fallback operation is basically a failover from Azure to the on-premises site and in reverse replicate it again starts replicating VMs from the on-premises site to Azure.

1. In **Settings > Replicated items**, click the VM > **Planned Failover**.
2. In **Confirm Planned Failover**, verify the failover direction (from Azure), and select the source and target locations.
3. Select **Synchronize data before failover (synchronize delta changes only)**. This option minimizes VM downtime because it synchronizes without shutting down the VM.
4. Initiate the failover. You can follow the failover progress on the **Jobs** tab.
5. After the initial data synchronization is done and you're ready to shut down the Azure VMs click **Jobs > planned-failover-job-name > Complete Failover**. It shuts down the Azure VM, transfers the latest changes on-premises, and starts the on-premises VM.
6. Log on to the on-premises VM to check it's available as expected.
7. The on-premises VM is now in a **Commit Pending** state. Click **Commit**. It deletes the Azure VMs and its disks, and prepares the on-premises VM for reverse replication. To start replicating the on-premises VM to Azure, enable **Reverse Replicate**. It triggers replication of delta changes that have occurred since the Azure VM was switched off.

Prepare Azure resources for replication of on-premises machines

7/9/2018 • 4 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), including replication, failover, and recovery.

This article is the first tutorial in a series that shows you how to set up disaster recovery for on-premises VMs. It's relevant whether you're protecting on-premises VMware VMs, Hyper-V VMs, or physical servers.

Tutorials are designed to show you the simplest deployment path for a scenario. They use default options where possible, and don't show all possible settings and paths.

This article shows you how to prepare Azure components when you want to replicate on-premises VMs (Hyper-V or VMware) or Windows/Linux physical servers to Azure. In this tutorial, you learn how to:

- Verify that your Azure account has replication permissions.
- Create an Azure storage account. Images of replicated machines are stored in it.
- Create a Recovery Services vault. A vault holds 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 Azure network.

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

Sign in to Azure

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

Verify account permissions

If you just 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 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. In addition, to manage Site Recovery operations in a vault, your account should be assigned the Site Recovery Contributor build-in role.

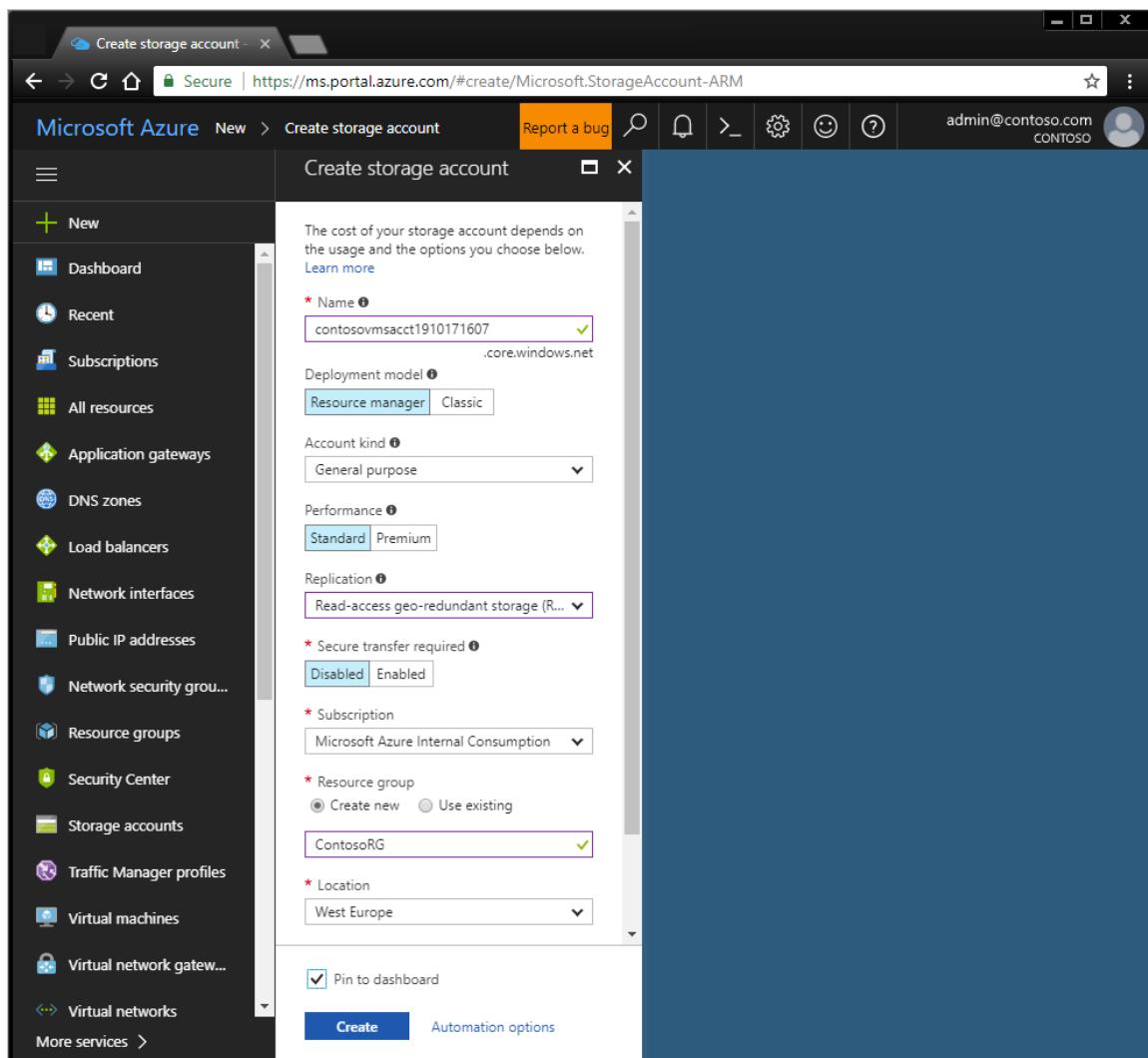
Create a storage account

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. We're using West Europe in this tutorial.

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

queue.

2. On **Create storage account**, enter a name for the account. For these tutorials, we're using **contosovmsacct1910171607**. The name you select must be unique within Azure and be between 3 and 24 characters, with numbers and lowercase letters only.
3. In **Deployment model**, select **Resource Manager**.
4. In **Account kind**, select **Storage (general purpose v1)**. Don't select blob storage.
5. In **Replication**, select the default **Read-access geo-redundant storage** for storage redundancy. We're leaving **Secure transfer required** as **Disabled**.
6. In **Performance**, select **Standard** and in **Access tier** choose the default option of **Hot**.
7. In **Subscription**, select the subscription in which you want to create the new storage account.
8. In **Resource group**, enter a new resource group. An Azure resource group is a logical container into which Azure resources are deployed and managed. For these tutorials, we're using **ContosoRG**.
9. In **Location**, select the geographic location for your storage account.



10. Select **Create** to create the storage account.

Create a Recovery Services vault

1. In the Azure portal, select **Create a resource > Storage > Backup and Site Recovery (OMS)**.
2. In **Name**, enter a friendly name to identify the vault. For this set of tutorials we're using **ContosoVMVault**.
3. In **Resource group**, we're using **contosoRG**.
4. In **Location**. We're using **West Europe**.
5. To quickly access the vault from the dashboard, select **Pin to dashboard > Create**.

Recovery Services vault □ X

Recovery Services vault

* Name
ContosoVMVault ✓

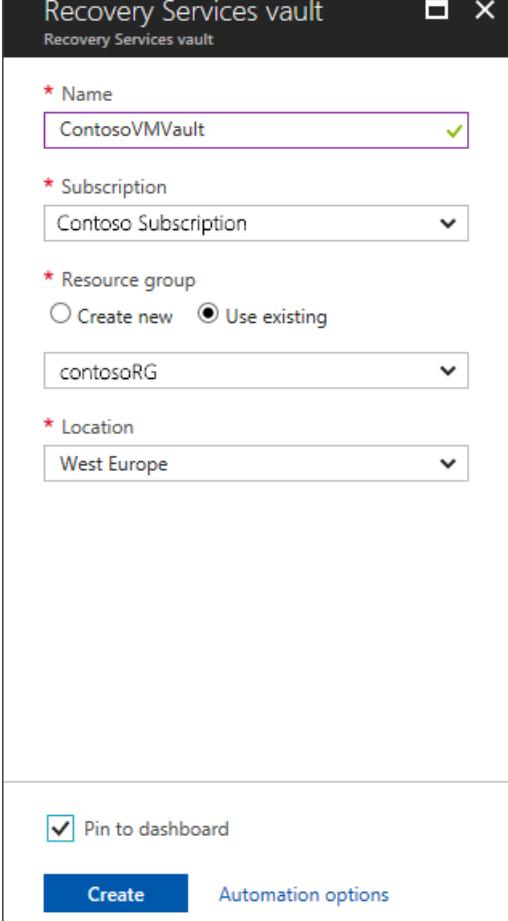
* Subscription
Contoso Subscription ▼

* Resource group
 Create new Use existing
contosoRG ▼

* Location
West Europe ▼

Pin to dashboard

Create Automation options



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**.
2. We're leaving **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. Specify the resource group in which the network will be created. We're using the existing resource group **contosoRG**.
5. In **Address range**, enter the range for the network **10.0.0.0/24**. In this network we're not using a subnet.
6. In **Subscription**, select the subscription in which to create the network.
7. In **Location**, select **West Europe**. The network must be in the same region as the Recovery Services vault.
8. We're leaving the default options of basic DDoS protection, with no service endpoint on the network.
9. Click **Create**.

Home > New > Create virtual network

Create virtual network

* Name
ContosoASRnet

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

* Subscription
Microsoft Azure Internal Consumption (e12l)

* Resource group
 Create new Use existing
ContosoRG

* Location
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

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

Useful links

- [Learn about](#) Azure networks.
- [Learn about](#) types of Azure storage.
- [Learn more](#) about storage redundancy, and [secure transfer](#) for storage.

Next steps

Prepare the on-premises VMware infrastructure for disaster recovery to Azure

Migrate on-premises machines to Azure

7/16/2018 • 3 minutes to read • [Edit Online](#)

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 migration of on-premises machines to Azure.

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

- Select a replication goal
- Set up the source and target environment
- 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

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

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

Before you start, it's helpful to review the [VMware](#) or [Hyper-V](#) architectures for disaster recovery.

Prerequisites

- Devices exported by paravirtualized drivers aren't supported.

WARNING

It is possible to migrate VMs on other virtualization platforms(other than VMware, Hyper-V) such as XenServer by treating the VMs like Physical servers. This approach however, hasn't been tested and validated by Microsoft and may or may not work. For example, VMs running on the XenServer platform may not run in Azure unless XenServer tools and para-virtualized storage and network drivers are uninstalled from the VM before starting the migration.

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 the friendly name **ContosoVMVault**. If you have more than one 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. To quickly access the vault from the dashboard, click **Pin to dashboard** and then click **Create**.

The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with various service icons and links like 'Dashboard', 'Resource groups', and 'All resources'. The main area has a breadcrumb navigation path: 'Home > Recovery Services vaults > Recovery Services vault'. A search bar at the top right contains the URL 'ms.portal.azure.com/#create/Microsoft.RecoveryServices'. The central part of the screen displays a list of existing Recovery Services vaults on the left, with names such as 'a2ajpnvault', 'a2ajpnwvault', 'A2ATestVault', etc. On the right, a form is open for creating a new vault. It requires filling in fields for 'Name' (set to 'ContosoVMVault'), 'Subscription' (set to 'ContosoSubscription'), 'Resource group' (radio button selected for 'Create new', with 'ContosoRG' chosen), and 'Location' (set to 'West Europe').

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

Select a replication 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

- [Set up](#) the source environment for VMware VMs.
- [Set up](#) the source environment for physical servers.
- [Set up](#) the source environment for Hyper-V VMs.

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

- [Set up a replication policy](#) for VMware VMs.
- [Set up a replication policy](#) for physical servers.
- [Set up a replication policy](#) for Hyper-V VMs.

Enable replication

- [Enable replication](#) for VMware VMs.
- [Enable replication](#) for physical servers.
- Enable replication for Hyper-V VMs [with](#) or [without VMM](#).

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 finishes the migration process, stops replication for the VM, and stops Site Recovery billing for the VM.

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 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.

Next steps

In this tutorial you migrated on-premises VMs to Azure VMs. Now that you've successfully migrated VMs:

- [Set up disaster recovery](#) for the migrated VMs.
- Take advantage of Azure's [Secure and well managed cloud](#) capabilities to manage your VMs in Azure.

Migrate servers running Windows Server 2008 to Azure

7/27/2018 • 8 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.

Supported Operating Systems and environments

OPERATING SYSTEM	ON-PREMISE 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.

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 9.18.0.1 of the Azure Site Recovery software. The unified setup for version 9.18.0.1 of the Configuration Server and process server can be downloaded from <https://aka.ms/asr-w2k8-migration-setup>.
- An existing Configuration Server or process server cannot be used to migrate servers running Windows Server 2008 SP2. A new Configuration Server should be provisioned with version 9.18.0.1 of the Azure Site Recovery software. This Configuration Server should only be used for migration of Windows servers to Azure.
- 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 atleast 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

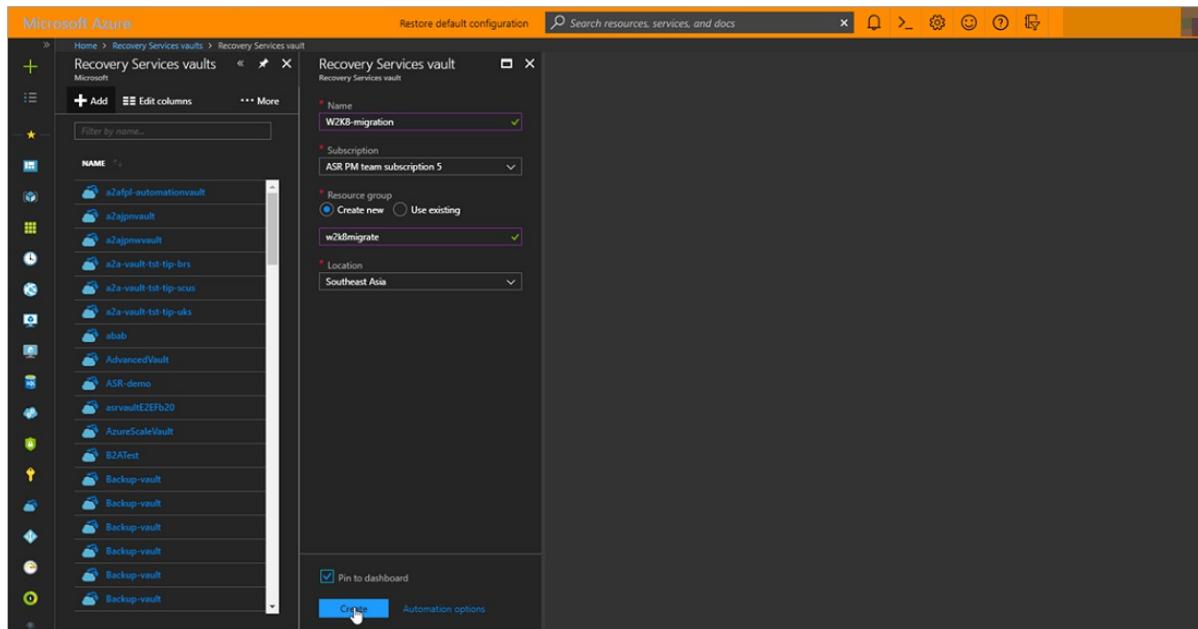
Perform the following tasks to prepare the Azure subscription and on-premises VMware/Physical environment:

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** > **Monitoring & Management** > **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

- Download the Configuration Server installer (Unified Setup) from <https://aka.ms/asr-w2k8-migration-setup>
- Follow the steps outlined below to set up the source environment using the installer file downloaded in the previous step.

IMPORTANT

- Ensure that you use the setup file downloaded in the first step above to install and register the Configuration Server. Do not download the setup file from the Azure portal. The setup file available at <https://aka.ms/asr-w2k8-migration-setup> is the only version that supports Windows Server 2008 migration.
- You cannot use an existing Configuration Server to migrate machines running Windows Server 2008. You'll need to setup a new Configuration Server using the link provided above.
- Follow the steps provided below to install the Configuration Server. Do not attempt to use the GUI based install procedure by running the unified setup directly. Doing so will result in the install attempt failing with an incorrect error stating that there is no internet connectivity.

- 1) Download the vault credentials file from the portal: On the Azure portal, select the Recovery Services vault created in the previous step. From the menu on the vault page select **Site Recovery Infrastructure** > **Configuration Servers**. Then click **+Server**. Select *Configuration Server for Physical* from the drop down form

on the page that opens. Click the download button on step 4 to download the vault credentials file.

The screenshot shows the Microsoft Azure portal interface. On the left, there's a navigation pane with sections for 'FOR AZURE VIRTUAL MACHINES', 'FOR SYSTEM CENTER VMM', 'FOR VMWARE & PHYSICAL MACHINES', and 'FOR HYPER-V SITES'. The 'Configuration Servers' option under 'FOR VMWARE & PHYSICAL MACHINES' is selected. In the main content area, it says 'Finished loading data from service.' and 'No servers are registered yet. Click on + Servers to read more on how to get started'. A right-side panel titled 'Add Server W2K8-migration' shows steps for registering a Configuration server. Step 4, 'Download the vault registration key', has a blue 'Download' button highlighted with a mouse cursor. Below the steps, it says '7. If you're protecting VMware VMs make sure the management accounts have'.

- 2) Copy the vault credentials file downloaded in the previous step and the unified setup file downloaded previously to the desktop of the Configuration Server machine (the Windows Server 2012 R2 or Windows Server 2016 machine on which you are going to install the configuration server software.)
- 3) Ensure that the Configuration Server has internet connectivity, and that the system clock and time zone settings on the machine are configured correctly. Download the [MySQL 5.7](#) installer and place it at `C:\Temp\ASRSetup` (create the directory if it doesn't exist.)
- 4) Create a MySQL credentials file with the following lines and place it on the desktop at `C:\Users\Administrator\MySQLCreds.txt`. Replace "Password~1" below with a suitable and strong password:

```
[MySQLCredentials]
MySQLRootPassword = "Password~1"
MySQLUserPassword = "Password~1"
```

- 5) Extract the contents of the downloaded unified setup file to the desktop by running the following command:

```
cd C:\Users\Administrator\Desktop
MicrosoftAzureSiteRecoveryUnifiedSetup.exe /q /x:C:\Users\Administrator\Desktop\9.18
```

- 6) Install the configuration server software using the extracted contents by executing the following commands:

```
cd C:\Users\Administrator\Desktop\9.18.1
UnifiedSetup.exe /AcceptThirdpartyEULA /ServerMode CS /InstallLocation "C:\Program Files (x86)\Microsoft Azure Site Recovery" /MySQLCredsFilePath "C:\Users\Administrator\Desktop\MySQLCreds.txt" /VaultCredsFilePath <vault credentials file path> /EnvType VMWare /SkipSpaceCheck
```

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.

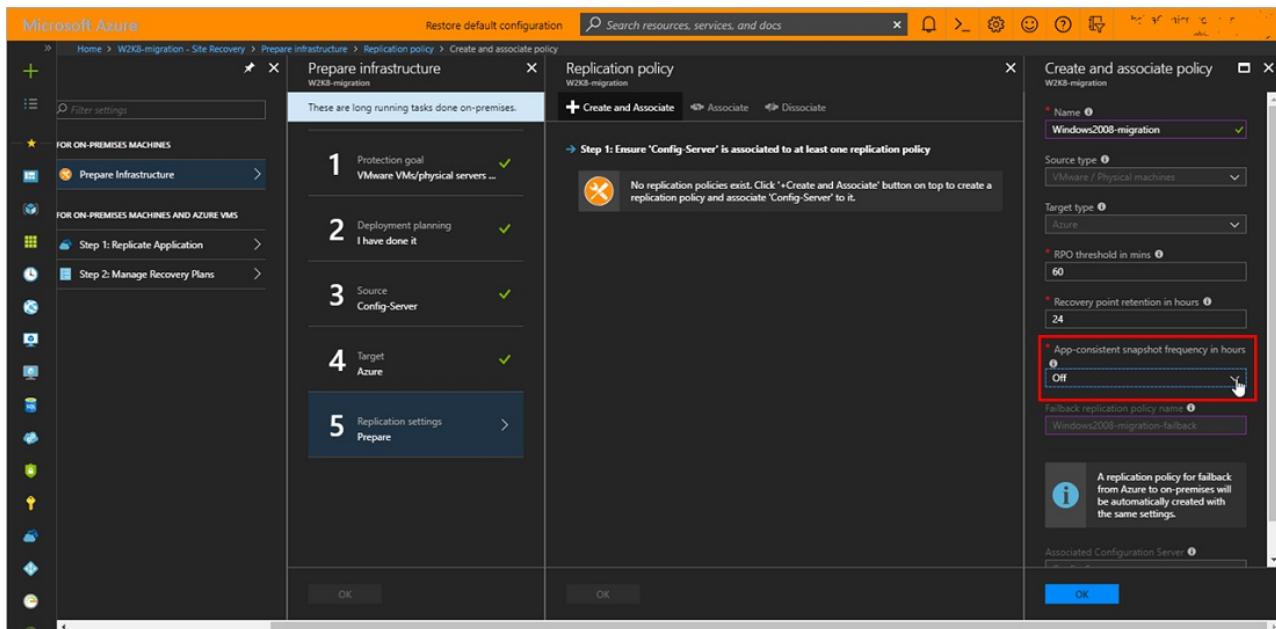
Set up a replication policy

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 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 **Off**. Click **OK** to create the policy.

The policy is automatically associated with the configuration server.

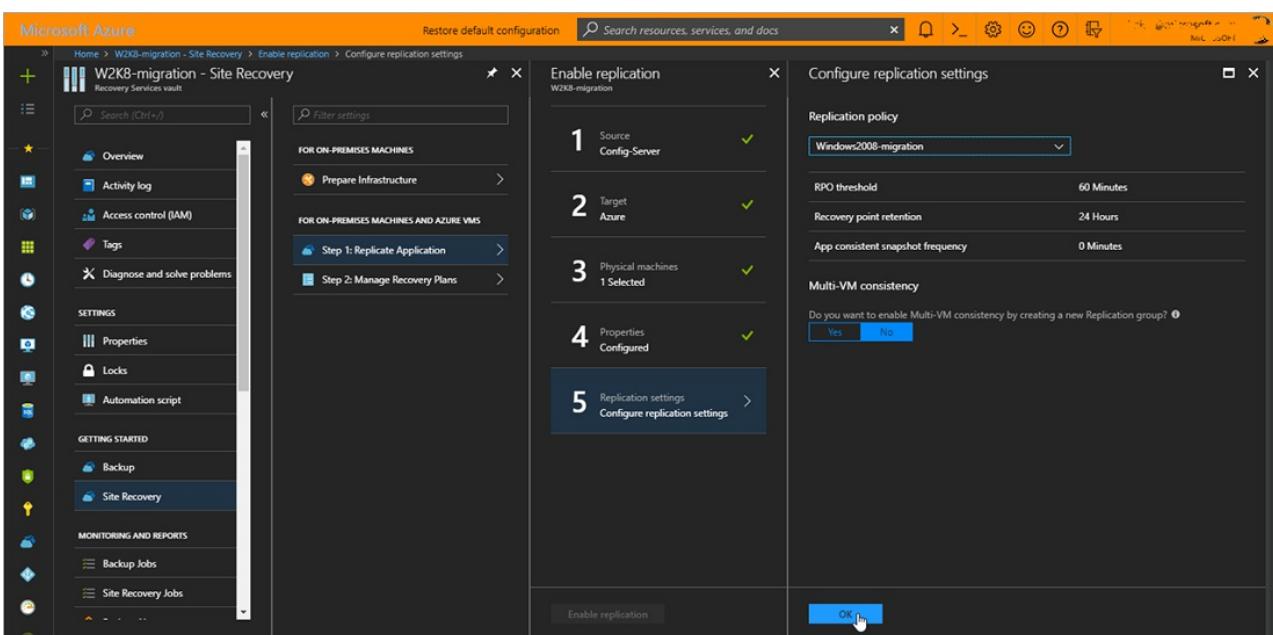
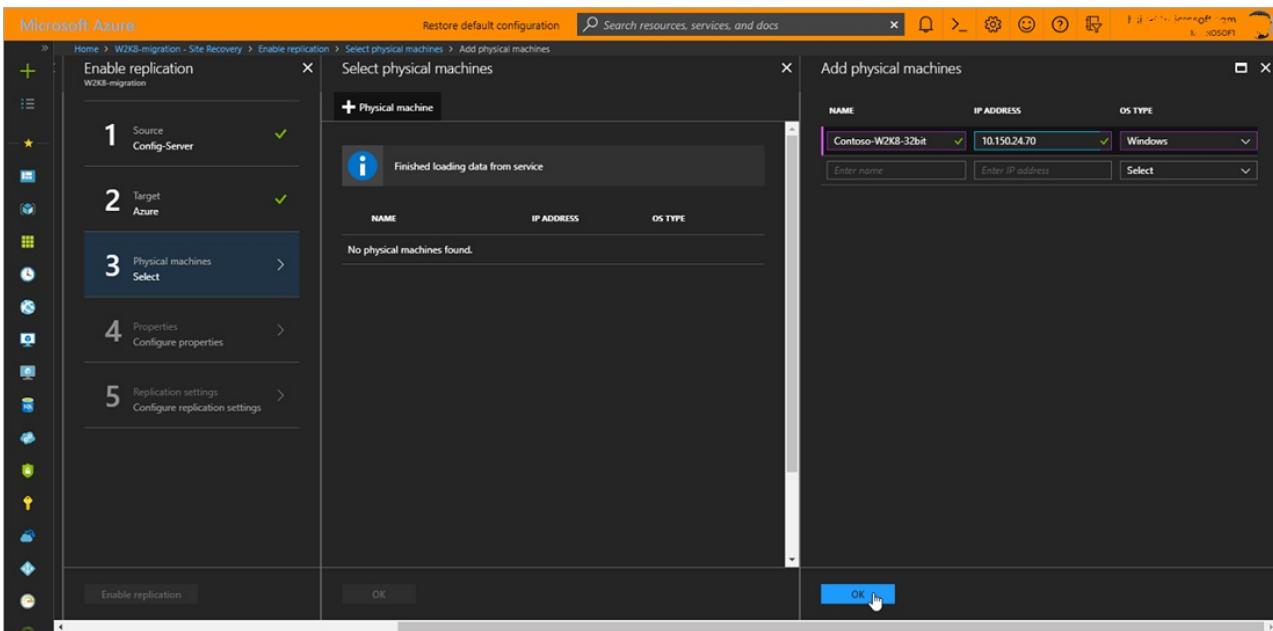
WARNING

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 portal interface. On the left, there's a navigation sidebar with various 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 is titled 'W2K8-migration - Replicated items' under 'Recovery Services vault'. It displays a table with one row for 'Contoso-W2K8-32bit'. The columns are NAME, REPLICATION HEALTH, STATUS, ACTIVE LOCATION, and RPO. The 'REPLICATION HEALTH' column shows a green dot and 'Healthy'. The 'STATUS' column shows 'Protected'. The 'ACTIVE LOCATION' column shows 'Config-Server'. The 'RPO' column has a dropdown menu with several 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 VM > **Complete Migration**. This finishes the migration process, stops replication for the VM, and stops Site Recovery billing for the VM.

This screenshot is similar to the one above, showing the 'W2K8-migration - Replicated items' service vault. The table now shows the 'Contoso-W2K8-32bit' VM with a status of 'Failover completed' in the 'STATUS' column. The 'Complete Migration' option in the context menu is highlighted with a red box.

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.

Migrate Amazon Web Services (AWS) VMs to Azure

7/9/2018 • 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.

Prerequisites

- Ensure that the VMs that you want to migrate are running a supported OS version. Supported versions include:
 - Windows Server 2016
 - Red Hat Enterprise Linux 6.7 (HVM virtualized instances only) and must have only Citrix PV or AWS PV drivers. Instances running Red Hat PV drivers **aren't** supported.
- 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**.
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**.
8. Leave the **Service Endpoints** option disabled.
9. 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 your machines virtualized?	Select Not virtualized / Other .

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

2: 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.

3: 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**.

4: Prepare replication settings

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

1. Select **Replicate 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.

5: Select deployment planning

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

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**.

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

- In **Protected items > Replicated items**, select the AWS instances, and then select **Failover**.
- In **Failover**, select a **Recovery Point** to failover to. Select the latest recovery point.
- Select **Shutdown machine before beginning failover** if you want Site Recovery to attempt to do a shutdown of source virtual machines before triggering the failover. Failover continues even if shutdown fails. You can follow the failover progress on the **Jobs** page.
- Ensure that the VM appears in **Replicated items**.
- Right-click each VM, and then select **Complete Migration**. This finishes the migration process, stops replication for the AWS VM, and stops Site Recovery billing for the VM.

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](#)

Migrate Azure VMs to another region

7/23/2018 • 4 minutes to read • [Edit Online](#)

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 migration of Azure VMs to a secondary region. To migrate Azure VMs, you enable replication for them, and fail them over from the primary region to the secondary region of your choice.

This tutorial shows you how to migrate Azure VMs to another region. In this tutorial, you learn how to:

- Create a Recovery services vault
- Enable replication for a VM
- Run a failover to migrate the VM

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

Prerequisites

- Make sure you have Azure VMs in the Azure region from which you want to migrate.
- Make sure that you understand the [scenario architecture and components](#).
- Review the [support limitations and requirements](#).

Before you start

Before you set up replication, complete these steps.

Verify target resources

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.
Site Recovery picks the same size or the closest possible size for the target VM.

Verify account permissions

If you have just created your free Azure account then you are the administrator of your subscription. If you are not the subscription administrator, work with the administrator to assign the permissions you need. To enable replication for a new VM, you must have:

1. 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
2. You also need permission to manage Azure Site Recovery operations. The 'Site Recovery Contributor' role has all permissions required to manage Site Recovery operations in a Recovery Services vault.

Verify VM outbound access

1. Make sure you're not using an authentication proxy to control network connectivity for VMs you want to migrate.
2. For the purposes of this tutorial we assume that the VMs you want to migrate can access the internet, and are

not using a firewall proxy to control outbound access. If you are, check the requirements [here](#).

Verify VM certificates

Check that all the latest root certificates are present on the Azure VMs you want to migrate. If the latest root certificates aren't, the VM can't be registered to Site Recovery, due to 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.

Create a vault

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

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

The screenshot shows the Azure portal interface for creating a Recovery Services vault. On the left, the navigation bar includes 'Create a resource', 'All services', 'Dashboard', 'Resource groups', 'All resources', 'Recent', 'App Services', 'SQL databases', 'Virtual machines (classic)', 'Cloud services (classic)', 'Subscriptions', 'Azure Active Directory', 'Monitor', 'Security Center', and 'Cost Management + Billing'. The main area shows 'Recovery Services vaults' with a list of existing vaults: a2ajpnvault, a2ajpnwvault, A2ATestVault, a2a-vault-acan-ak-ccy, a2a-vault-acan-apk-ccy, a2a-vault-acan-fos-ccy, a2a-vault-acan-sa-ccy, a2a-vault-acan-sak-ccy, a2a-vault-acan-sakk-ccy, a2a-vault-acan-saki-ccy, a2a-vault-acan-sfs-ccy, a2a-vault-acan-siv-ccy, a2a-vault-acan-ski-ccy, a2a-vault-acan-skl-ccy, and a2a-vault-acan-sof-ccy. The right panel is titled 'Recovery Services vault' and contains fields for 'Name' (ContosoVMVault), 'Subscription' (ContosoSubscription), 'Resource group' (radio buttons for 'Create new' or 'Use existing', with 'ContosoRG' selected), and 'Location' (West Europe). The URL in the browser bar is ms.portal.azure.com/#create/Microsoft.RecoveryServices.

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

Select the source

1. In Recovery Services vaults, click **ConsotoVMVault** > **+Replicate**.
2. In **Source**, select **Azure**.
3. In **Source location**, select the source Azure region where your VMs are currently running.
4. Select the Resource Manager deployment model. Then select the **Source resource group**.
5. Click **OK** to save the settings.

Enable replication for Azure VMs

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

1. In the Azure portal, click **Virtual machines**.
2. Select the VM you want to migrate. Then click **OK**.
3. In **Settings**, click **Disaster recovery**.
4. In **Configure disaster recovery** > **Target region** select the target region to which you'll replicate.
5. For this tutorial, accept the other default settings.
6. Click **Enable replication**. This starts a job to enable replication for the VM.

The screenshot shows the 'Configure settings' dialog box. At the top, it says 'Resource group, Network, Storage and Availability sets' with a 'Customize' link. Below that, there's a note about ASR creating resources with an 'asr' suffix. The configuration sections include:

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)

Run a failover

1. In **Settings** > **Replicated items**, click the machine, and then click **Failover**.
2. In **Failover**, select **Latest**. The encryption key setting isn't relevant for this scenario.
3. 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.

4. Check that the Azure VM appears in Azure as expected.
5. In **Replicated items**, right-click the VM > **Commit**. This finishes the migration process,
6. After the commit finishes, click **Disable Replication**. This stops replication for the VM.

Next steps

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

[Set up disaster recovery after migration](#)

Azure to Azure replication architecture

7/9/2018 • 2 minutes to read • [Edit Online](#)

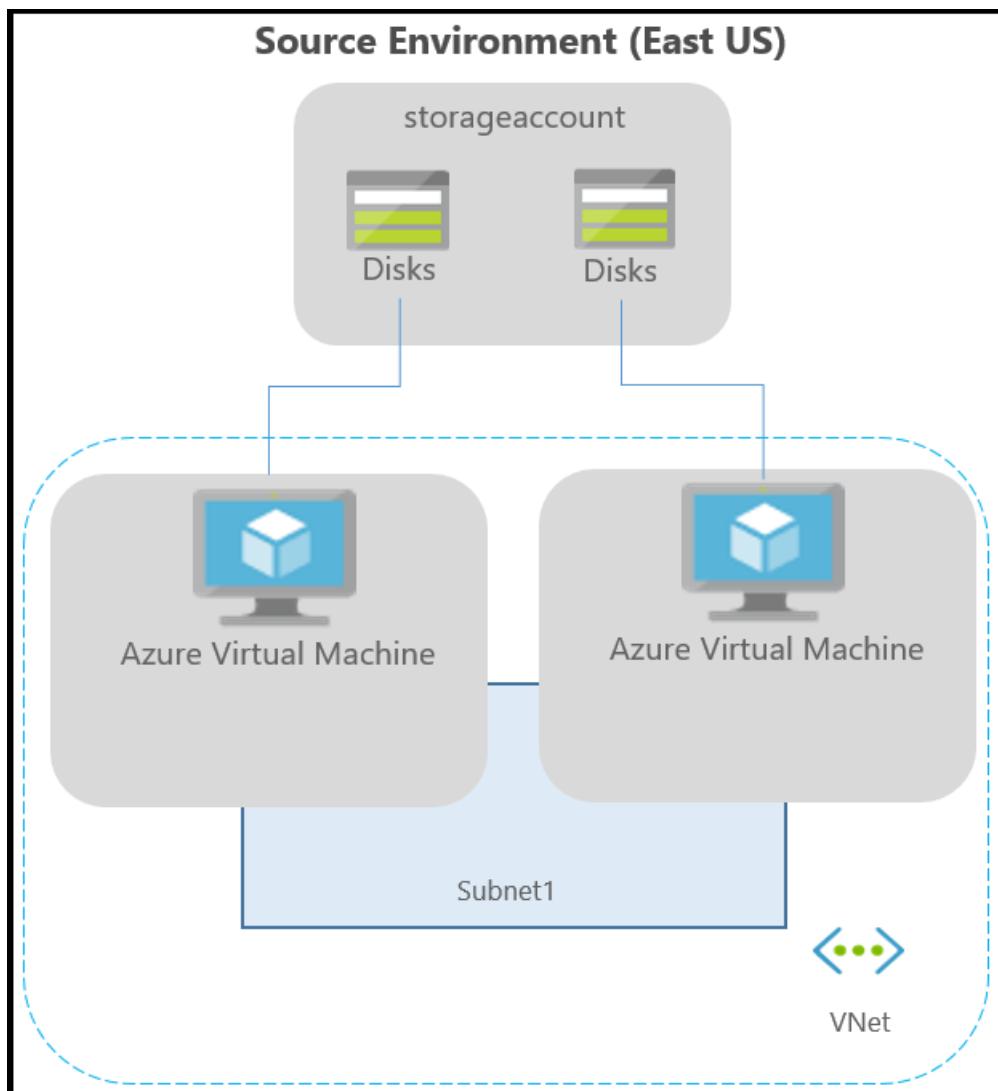
This article describes the architecture used when you replicate, fail over, and recover Azure virtual machines (VMs) between Azure regions, using the [Azure Site Recovery](#) service.

Architectural components

The following graphic provides a high-level view of an Azure VM environment in a specific region (in this example, the East US location). In an Azure VM environment:

- Apps can be running on VMs with managed disks or non-managed disks spread across storage accounts.
- The VMs can be included in one or more subnets within a virtual network.

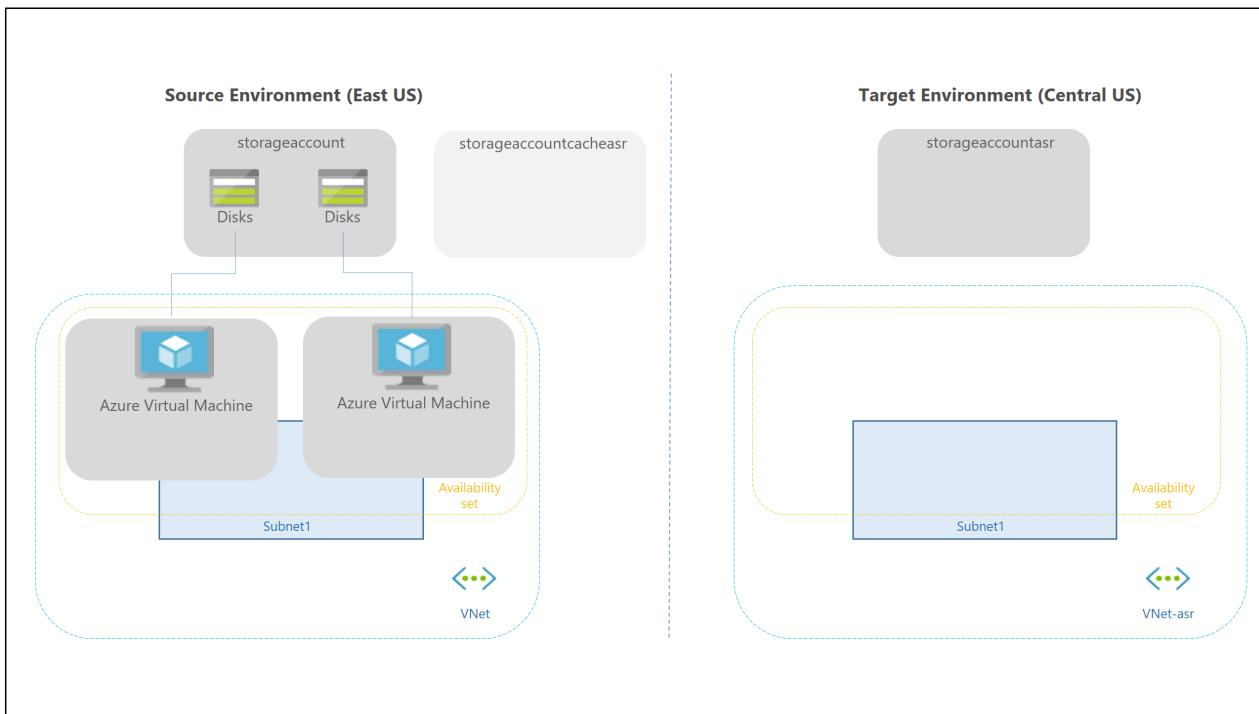
Azure to Azure replication



Replication process

Step 1

When you enable Azure VM replication, the following resources are automatically created in the target region, based on the source region settings. You can customize target resources settings as required.

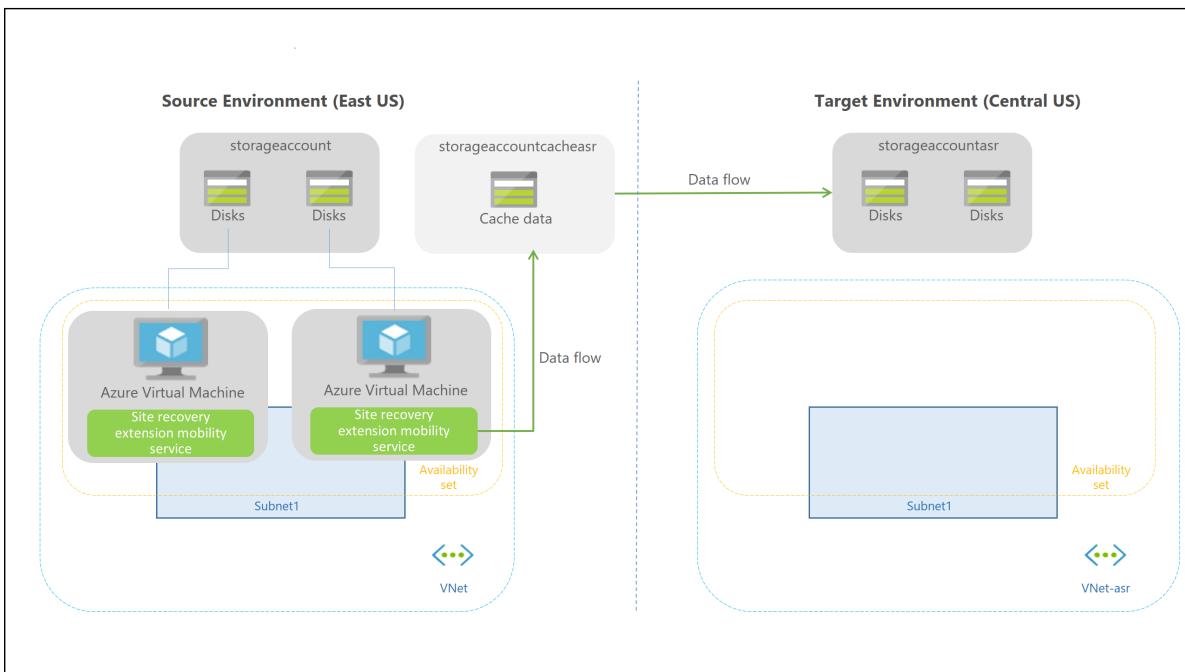


RESOURCE	DETAILS
Target resource group	The resource group to which replicated VMs belong after failover. The location of this resource group can be in any Azure region except the Azure region in which the source virtual machines are hosted.
Target virtual network	The virtual network in which replicated VMs are located after failover. A network mapping is created between source and target virtual networks, and vice versa.
Cache storage accounts	Before source VM changes are replicated to a target storage account, they are tracked and sent to the cache storage account in source location. This step ensures minimal impact on production applications running on the VM.
Target storage accounts (If source VM does not use managed disks)	Storage accounts in the target location to which the data is replicated.
** Replica managed disks (If source VM is on managed disks)**	Managed disks in the target location to which data is replicated.
Target availability sets	Availability sets in which the replicated VMs are located after failover.

Step 2

As replication is enabled, the Site Recovery extension Mobility service is automatically installed on the VM:

1. The VM is registered with Site Recovery.
2. Continuous replication is configured for the VM. Data writes on the VM disks are continuously transferred to the cache storage account, in the source location.



Site Recovery never needs inbound connectivity to the VM. Only outbound connectivity is needed for the following.

- Site Recovery service URLs/IP addresses
- Office 365 authentication URLs/IP addresses
- Cache storage account IP addresses

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.

IMPORTANT

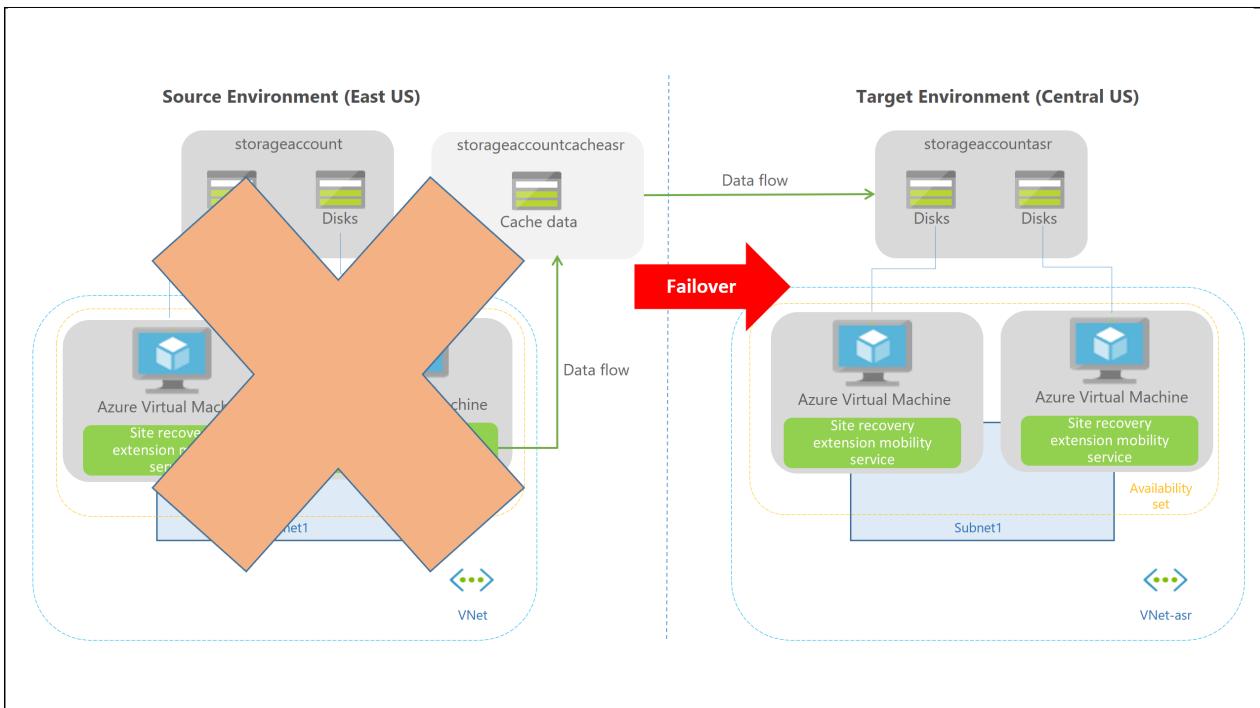
If you want Linux VMs to be part of a replication group, ensure the outbound traffic on port 20004 is manually opened as per the guidance of the specific Linux version.

Step 3

After continuous replication is in progress, disk writes are immediately transferred to the cache storage account. Site Recovery processes the data, and sends it to the target storage account or replica managed disks. After the data is processed, recovery points are generated in the target storage account every few minutes.

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.

Support matrix for replicating from one Azure region to another

8/22/2018 • 10 minutes to read • [Edit Online](#)

This article summarizes supported configurations and components when you replicate and recovering Azure virtual machines from one region to another region, using the [Azure Site Recovery](#) service.

User interface options

USER INTERFACE	SUPPORTED / NOT SUPPORTED
Azure portal	Supported
PowerShell	Azure to Azure replication with PowerShell
REST API	Not currently supported
CLI	Not currently supported

Resource support

RESOURCE MOVE TYPE	DETAILS
Move vault across resource groups	Not supported You can't move a Recovery services vault across resource groups.
Move compute/storage/network resources across resource groups	Not supported. If you move a VM or associated components such as storage/network after it's replicating, you need to disable replication and reenable 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 subscriptions	Not supported.
Migrate VMs within the same region	Not supported.

Support for replicated machine OS versions

The below support is applicable for any workload running on the mentioned OS.

Windows

- Windows Server 2016 (Server Core, Server with Desktop Experience)*
- Windows Server 2012 R2
- Windows Server 2012

- Windows Server 2008 R2 with at least SP1

NOTE

* Windows Server 2016 Nano Server is not supported.

Linux

- Red Hat Enterprise Linux 6.7, 6.8, 6.9, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5
- CentOS 6.5, 6.6, 6.7, 6.8, 6.9, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5
- Ubuntu 14.04 LTS Server ([supported kernel versions](#))
- Ubuntu 16.04 LTS Server ([supported kernel versions](#))
- Debian 7 ([supported kernel versions](#))
- Debian 8 ([supported kernel versions](#))
- SUSE Linux Enterprise Server 12 SP1,SP2,SP3 ([supported kernel versions](#))
- SUSE Linux Enterprise Server 11 SP3
- SUSE Linux Enterprise Server 11 SP4
- Oracle Enterprise Linux 6.4, 6.5 running either the Red Hat compatible kernel or Unbreakable Enterprise Kernel Release 3 (UEK3)

(Upgrade of replicating machines from SLES 11 SP3 to SLES 11 SP4 is not supported. If a replicated machine has been upgraded from SLES 11SP3 to SLES 11 SP4, you need to disable replication and protect the machine again post the upgrade.)

NOTE

Ubuntu servers using password-based authentication and login, and using the cloud-init package to configure cloud virtual machines, may have password-based login disabled upon failover (depending on the cloudinit configuration.) Password-based login can be re-enabled on the virtual machine by resetting the password from the settings menu (under the SUPPORT + TROUBLESHOOTING section) of the failed over virtual machine on the Azure portal.

Supported Ubuntu kernel versions for Azure virtual machines

RELEASE	MOBILITY SERVICE VERSION	KERNEL VERSION
14.04 LTS	9.18	3.13.0-24-generic to 3.13.0-151-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 4.4.0-128-generic
14.04 LTS	9.17	3.13.0-24-generic to 3.13.0-147-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 4.4.0-124-generic
14.04 LTS	9.16	3.13.0-24-generic to 3.13.0-144-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 4.4.0-119-generic

RELEASE	MOBILITY SERVICE VERSION	KERNEL VERSION
14.04 LTS	9.15	3.13.0-24-generic to 3.13.0-143-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 4.4.0-116-generic
16.04 LTS	9.18	4.4.0-21-generic to 4.4.0-128-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, 4.11.0-1009-azure to 4.11.0-1016-azure, 4.13.0-1005-azure to 4.13.0-1018-azure
16.04 LTS	9.17	4.4.0-21-generic to 4.4.0-124-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 4.13.0-41-generic, 4.11.0-1009-azure to 4.11.0-1016-azure, 4.13.0-1005-azure to 4.13.0-1016-azure
16.04 LTS	9.16	4.4.0-21-generic to 4.4.0-119-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 4.13.0-38-generic, 4.11.0-1009-azure to 4.11.0-1016-azure, 4.13.0-1005-azure to 4.13.0-1012-azure
16.04 LTS	9.15	4.4.0-21-generic to 4.4.0-116-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 4.13.0-37-generic, 4.11.0-1009-azure to 4.11.0-1016-azure, 4.13.0-1005-azure to 4.13.0-1012-azure

Supported Debian kernel versions for Azure virtual machines

RELEASE	MOBILITY SERVICE VERSION	KERNEL VERSION
Debian 7	9.17, 9.18	3.2.0-4-amd64 to 3.2.0-6-amd64, 3.16.0-0.bpo.4-amd64
Debian 7	9.15, 9.16	3.2.0-4-amd64 to 3.2.0-5-amd64, 3.16.0-0.bpo.4-amd64

RELEASE	MOBILITY SERVICE VERSION	KERNEL VERSION
Debian 8	9.17, 9.18	3.16.0-4-amd64 to 3.16.0-6-amd64, 4.9.0-0.bpo.4-amd64 to 4.9.0-0.bpo.6-amd64
Debian 8	9.15, 9.16	3.16.0-4-amd64 to 3.16.0-5-amd64, 4.9.0-0.bpo.4-amd64 to 4.9.0-0.bpo.5-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)	9.18	SP1 3.12.49-11-default to 3.12.74-60.64.40-default SP1(LTSS) 3.12.74-60.64.45-default to 3.12.74-60.64.93-default SP2 4.4.21-69-default to 4.4.120-92.70-default SP2(LTSS) 4.4.121-92.73-default to 4.4.121-92.80-default SP3 4.4.73-5-default to 4.4.138-94.39-default
SUSE Linux Enterprise Server 12 (SP1,SP2,SP3)	9.17	SP1 3.12.49-11-default to 3.12.74-60.64.40-default SP1(LTSS) 3.12.74-60.64.45-default to 3.12.74-60.64.88-default SP2 4.4.21-69-default to 4.4.120-92.70-default SP2(LTSS) 4.4.121-92.73-default SP3 4.4.73-5-default to 4.4.126-94.22-default

Supported file systems and guest storage configurations on Azure virtual machines running Linux OS

- File systems: ext3, ext4, ReiserFS (Suse Linux Enterprise Server only), XFS
- Volume manager: LVM2
- Multipath software: Device Mapper

Region support

You can replicate and recover VMs between any two regions within the same geographic cluster.

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
Asia	South India, Central India, Southeast Asia, East Asia, Japan East, Japan West, Korea Central, Korea South
Australia	Australia East, Australia Southeast
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

NOTE

For Brazil South region, you can only replicate and fail over to one of South Central US, West Central US, East US, East US 2, West US, West US 2, and North Central US regions and fail back.

Support for VM/disk management

ACTION	DETAILS
Resize disk on replicated VM	Supported
Add disk to replicated VM	Not supported. You need to disable replication for the VM, add the disk, and then enable replication again.

Support for Compute configuration

CONFIGURATION	SUPPORTED/NOT SUPPORTED	REMARKS
Size	Any Azure VM size with at least 2 CPU cores and 1-GB RAM	Refer to Azure virtual machine sizes
Availability sets	Supported	If you use the default option during 'Enable replication' step in portal, the availability set is auto created based on source region configuration. You can change the target availability set in 'Replicated item > Settings > Compute and Network > Availability set' any time.

Configuration	Supported/Not Supported	Remarks
Hybrid Use Benefit (HUB) VMs	Supported	If the source VM has HUB license enabled, the Test failover or Failover VM also uses the HUB license.
Virtual machine scale sets	Not supported	
Azure Gallery Images - Microsoft published	Supported	Supported as long as the VM runs on a supported operating system by Site Recovery
Azure Gallery images - Third party published	Supported	Supported as long as the VM runs on a supported operating system by Site Recovery.
Custom images - Third party published	Supported	Supported as long as the VM runs on a supported operating system by Site Recovery.
VMs migrated using Site Recovery	Supported	If it is a VMware/Physical machine migrated to Azure using Site Recovery, you need to uninstall the older version of mobility service and restart the machine before replicating it to another Azure region.

Support for Storage configuration

Configuration	Supported/Not Supported	Remarks
Maximum OS disk size	2048 GB	Refer to Disks used by VMs .
Maximum data disk size	4095 GB	Refer to Disks used by VMs .
Number of data disks	Up to 64 as supported by a specific Azure VM size	Refer to Azure virtual machine sizes
Temporary disk	Always excluded from replication	Temporary disk is excluded from replication always. You should not put any persistent data on temporary disk as per Azure guidance. Refer to Temporary disk on Azure VMs for more details.
Data change rate on the disk	Maximum of 10 MBps per disk for Premium storage and 2 MBps per disk for Standard storage	If the average data change rate on the disk is beyond 10 MBps (for Premium) and 2 MBps (for Standard) continuously, replication will not catch up. However, if it is an occasional data burst and the data change rate is greater than 10 MBps (for Premium) and 2 MBps (for Standard) for some time and comes down, replication will catch up. In this case, you might see slightly delayed recovery points.

Configuration	Supported/Not Supported	Remarks
Disks on standard storage accounts	Supported	
Disks on premium storage accounts	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 target region
Standard Managed disks	Supported in Azure regions in which Azure Site Recovery is supported.	
Premium Managed disks	Supported in Azure regions in which Azure Site Recovery is supported.	
Storage spaces	Supported	
Encryption at rest (SSE)	Supported	SSE is the default setting on storage accounts.
Azure Disk Encryption (ADE)	Not supported	
Hot add/remove disk	Not supported	If you add or remove data disk on the VM, you need to disable replication and enable replication again for the VM.
Exclude disk	Not supported	Temporary disk is excluded by default.
Storage Spaces Direct	Not supported	
Scale-out File Server	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	No	Allowing access to specific Azure virtual networks on cache storage accounts used to store replicated data is not supported.
General purpose V2 storage accounts (Both Hot and Cool tier)	No	Transaction costs increase substantially compared to General purpose V1 storage accounts

IMPORTANT

Ensure that you observe the VM disk scalability and performance targets for [Linux](#) or [Windows](#) virtual machines to avoid any performance issues. If you follow the default settings, Site Recovery will create the required disks and storage accounts based on the source configuration. If you customize and select your own settings, ensure that you follow the disk scalability and performance targets for your source VMs.

Support for Network configuration

CONFIGURATION	SUPPORTED/NOT SUPPORTED	REMARKS
Network interface (NIC)	Up to maximum number of NICs supported by a specific Azure VM size	NICs are created when the VM is created as part of Test failover or Failover operation. The number of NICs on the failover VM depends on the number of NICs the source VM has at the time of enabling replication. If you add/remove NIC after enabling replication, it does not impact NIC count on the failover VM.
Internet Load Balancer	Supported	You need to associate the pre-configured load balancer using an azure automation script in a recovery plan.
Internal Load balancer	Supported	You need to associate the pre-configured load balancer using an azure automation script in a recovery plan.
Public IP	Supported	You need to associate an already existing public IP to the NIC or create one and associate to the NIC using an azure automation script in a recovery plan.
NSG on NIC (Resource Manager)	Supported	You need to associate the NSG to the NIC using an azure automation script in a recovery plan.
NSG on subnet (Resource Manager and Classic)	Supported	You need to associate the NSG to the subnet using an azure automation script in a recovery plan.
NSG on VM (Classic)	Supported	You need to associate the NSG to the NIC using an azure automation script in a recovery plan.

Configuration	Supported/Not Supported	Remarks
Reserved IP (Static IP) / Retain source IP	Supported	If the NIC on the source VM has static IP configuration and the target subnet has the same IP available, it is assigned to the failover VM. If the target subnet does not have the same IP available, one of the available IPs in the subnet is reserved for this VM. You can specify a fixed IP of your choice in 'Replicated item > Settings > Compute and Network > Network interfaces'. You can select the NIC and specify the subnet and IP of your choice.
Dynamic IP	Supported	If the NIC on the source VM has dynamic IP configuration, the NIC on the failover VM is also Dynamic by default. You can specify a fixed IP of your choice in 'Replicated item > Settings > Compute and Network > Network interfaces'. You can select the NIC and specify the subnet and IP of your choice.
Traffic Manager integration	Supported	You can pre-configure your traffic manager in such a way that the traffic is routed to the endpoint in source region on a regular basis and to the endpoint in target region in case of failover.
Azure managed DNS	Supported	
Custom DNS	Supported	
Unauthenticated Proxy	Supported	Refer to networking guidance document .
Authenticated Proxy	Not supported	If the VM is using an authenticated proxy for outbound connectivity, it cannot be replicated using Azure Site Recovery.
Site to Site VPN with 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. Refer to networking guidance document .
VNET to VNET connection	Supported	Refer to networking guidance document .
Virtual Network Service Endpoints	Supported	Azure Storage firewalls for virtual networks are not supported. Allowing access to specific Azure virtual networks on cache storage accounts used to store replicated data is not supported.

CONFIGURATION	SUPPORTED/NOT SUPPORTED	REMARKS
Accelerated Networking	Not supported	A VM with Accelerated Networking enabled can be replicated, but the failover VM will not have Accelerated Networking enabled. Accelerated Networking will also be disabled for source VM on failback.

Next steps

- Learn more about [networking guidance for replicating Azure VMs](#)
- Start protecting your workloads by [replicating Azure VMs](#)

Common questions - VMware to Azure replication

7/24/2018 • 9 minutes to read • [Edit Online](#)

This article provides answers to common questions we see when replicating on-premises VMware VMs to Azure. If you have questions after reading this article, post them on the [Azure Recovery Services Forum](#).

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.

What can I do with VMware to Azure replication?

- **Disaster recovery:** You can set up full disaster recovery. In this scenario, you replicate on-premises VMware VMs to Azure storage. Then, if your on-premises infrastructure is unavailable, you can 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, until your on-premises datacenter is available again. Then, you can fail back from Azure to your on-premises site.
- **Migration:** You can 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.

Azure

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](#).

On-premises

What do I need on-premises?

On on-premises you need Site Recovery components, installed on a single VMware VM. You also need a VMware infrastructure, with at least one ESXi host, and we recommend a vCenter server. In addition, you need one or more VMware VMs to replicate. [Learn more](#) about VMware to Azure architecture.

The on-premises configuration server can be deployed in one of the two following ways

1. Deploy it using a VM template that has the configuration server pre-installed. [Read more here.](#)
2. Deploy it using the setup on a Windows Server 2016 machine of your choice. [Read more here.](#)

To discover the getting started steps of deploying the configuration server on your own Windows Server machines, in the Protection goal of enable protection, choose **To Azure > Not virtualized/Other**.

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 on a VMware 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.

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 public 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 [public 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 (public peering), and VPN doesn't work.

What are the replicated VM requirements?

For replication, a VMware 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?

Replication is continuous when replicating VMware VMs to Azure.

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.

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. You can't add a

VM to an existing replication group after replication is initiated, and 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. If you want to add new disks you need to add the disk and reenable protection for the VM.

Configuration server

What does the configuration server do?

The configuration server runs the on-premises Site Recovery components, including:

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

Where do I set up the configuration server?

You need a single highly available on-premises VMware VM for the configuration server.

What are the requirements for the configuration server?

Review the [prerequisites](#).

Can I manually set up the configuration server instead of using a template?

We recommend that you use the latest version of the OVF template to [create the configuration server VM](#). If for some reason you can't, for example you don't have access to the VMware server, you can [download the Unified Setup file](#) from the portal, and run it on a VM.

Can a configuration server replicate to more than one region?

No. To do this, you need to set up a configuration server in each region.

Can I host a configuration server in Azure?

While possible, the Azure VM running the configuration server would need to communicate with your on-premises VMware infrastructure and VMs. The overhead probably isn't viable.

Where can I get the latest version of the configuration server template?

Download the latest version from the [Microsoft Download Center](#).

How do I update the configuration server?

You install update rollups. You can find the latest update information in the [wiki updates page](#).

Mobility service

Where can I find the Mobility service installers?

The installers are held in the **%ProgramData%\ASR\home\svsystems\pushinstallsvc\repository** folder on the configuration server.

How do I install the Mobility service?

You install on each VM you want to replicate, using a [push installation](#), or manual installation from [the UI](#), or [using PowerShell](#). Alternatively, you can deploy using a deployment tool such as [System Center Configuration Manager](#), or [Azure Automation and DSC](#).

Security

What access does Site Recovery need to VMware servers?

Site Recovery needs access to VMware servers to:

- Set up a VMware VM running the configuration server, and other on-premises Site Recovery components.
[Learn more](#)
- Automatically discover VMs for replication. Learn about preparing an account for automatic discovery. [Learn more](#)

What access does Site Recovery need to VMware VMs?

- In order to replicate, an VMware VM must have the Site Recovery Mobility service installed and running. You can deploy the tool manually, or specify that Site Recovery should do a push installation of the service when you enable replication for a VM. For the push installation, Site Recovery needs an account that it can use to install the service component. [Learn more](#). The process server (running by default on the configuration server) performs this installation. [Learn more](#) about Mobility service installation.
- During replication, VMs communicate with Site Recovery as follows:
 - VMs communicate with the configuration server on port HTTPS 443 for replication management.
 - VMs send replication data to the process server on port HTTPS 9443 (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 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 regions?

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.

Failover and fallback

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. 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.

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 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 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 VMware and physical server replication to Azure

8/9/2018 • 9 minutes to read • [Edit Online](#)

This article summarizes supported components and settings for disaster recovery of VMware VMs to Azure by using [Azure Site Recovery](#).

To start using Azure Site Recovery with the simplest deployment scenario, visit our [tutorials](#). You can learn more about Azure Site Recovery architecture [here](#).

Replication scenario

SCENARIO	DETAILS
VMware VMs	Replication of on-premises VMware VMs to Azure. You can deploy this scenario in the Azure portal or by using PowerShell .
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
VMware	vCenter Server 6.7, 6.5, 6.0, or 5.5 or vSphere 6.7, 6.5, 6.0, or 5.5	We recommend that you use a vCenter server. We recommend that vSphere hosts and vCenter servers are located in the same network as the process server. By default the process server components runs on the configuration server, so this will be the network in which you set up the configuration server, unless you set up a dedicated process server.
Physical	N/A	

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 replication you set the configuration server up with all requirements, using an OVF template to create a VMware VM. For physical server replication, you set the configuration server machine up manually.

COMPONENT	REQUIREMENTS
CPU cores	8

COMPONENT	REQUIREMENTS
RAM	16 GB
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 required for process server cache.
Disk free space	600 GB of space required for retention drive.
Operating system	Windows Server 2012 R2 or Windows Server 2016
Operating system locale	English (en-us)
PowerCLI	PowerCLI 6.0 should be installed.
Windows Server roles	Don't enable: - Active Directory Domain Services - Internet Information Services - Hyper-V
Group policies	Don't enable: - 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 used for data transport

Replicated machines

Site Recovery supports replication of any workload running on a supported machine.

COMPONENT	DETAILS
Machine settings	Machines that replicate to Azure must meet Azure requirements .

COMPONENT	DETAILS
Windows operating system	<p>64-bit Windows Server 2016 (Server Core, Server with Desktop Experience), Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2 with at least SP1. Windows Server 2008 with at least SP2 - 32 bit and 64 bit (migration only).</p> <p>Windows 2016 Nano Server isn't supported.</p>
Linux operating system	<p>Red Hat Enterprise Linux: 5.2 to 5.11**, 6.1 to 6.9**, 7.0 to 7.5 CentOS: 5.2 to 5.11**, 6.1 to 6.9**, 7.0 to 7.5 Ubuntu 14.04 LTS server (supported kernel versions) Ubuntu 16.04 LTS server (supported kernel versions) Debian 7/Debian 8 (supported kernel versions) SUSE Linux Enterprise Server 12 SP1,SP2,SP3 (supported kernel versions) SUSE Linux Enterprise Server 11 SP3**, SUSE Linux Enterprise Server 11 SP4 * Oracle Enterprise Linux 6.4, 6.5 running the Red Hat compatible kernel or Unbreakable Enterprise Kernel Release 3 (UEK3)</p> <p>* <i>Upgrading replicated machines from SUSE Linux Enterprise Server 11 SP3 to SP4 isn't supported. To upgrade, disable replication and enable it again after the upgrade.</i></p> <p>** <i>Refer to support for Linux virtual machines in Azure to understand support for Linux and open source technology in Azure. Azure Site Recovery lets you failover and run Linux servers in Azure, however Linux vendors may limit support to only those versions of their distribution that have not reached end of life.</i></p>

NOTE

- On Linux distributions, only the stock kernels that are part of the distribution minor version release/update are supported.
- Upgrading protected machines across major Linux distribution versions isn't supported. To upgrade, disable replication, upgrade the operating system, and then enable replication again.
- Servers running Red Hat Enterprise Linux 5.2 to 5.11 or CentOS 5.2 to 5.11 should have the Linux Integration Services(LIS) components installed in order for the machines to boot in Azure.

Ubuntu kernel versions

SUPPORTED RELEASE	AZURE SITE RECOVERY MOBILITY SERVICE VERSION	KERNEL VERSION
-------------------	--	----------------

SUPPORTED RELEASE	AZURE SITE RECOVERY MOBILITY SERVICE VERSION	KERNEL VERSION
14.04 LTS	9.18	3.13.0-24-generic to 3.13.0-153-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 4.4.0-130-generic
14.04 LTS	9.17	3.13.0-24-generic to 3.13.0-149-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 4.4.0-127-generic
14.04 LTS	9.16	3.13.0-24-generic to 3.13.0-144-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 4.4.0-119-generic
14.04 LTS	9.15	3.13.0-24-generic to 3.13.0-144-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 4.4.0-119-generic
16.04 LTS	9.18	4.4.0-21-generic to 4.4.0-130-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
16.04 LTS	9.17	4.4.0-21-generic to 4.4.0-127-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 4.13.0-43-generic
16.04 LTS	9.16	4.4.0-21-generic to 4.4.0-119-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 4.13.0-38-generic
16.04 LTS	9.15	4.4.0-21-generic to 4.4.0-119-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 4.13.0-38-generic

Debian kernel versions

SUPPORTED RELEASE	AZURE SITE RECOVERY MOBILITY SERVICE VERSION	KERNEL VERSION
Debian 7	9.17, 9.18	3.2.0-4-amd64 to 3.2.0-6-amd64, 3.16.0-0.bpo.4-amd64
Debian 7	9.15, 9.16	3.2.0-4-amd64 to 3.2.0-5-amd64, 3.16.0-0.bpo.4-amd64
Debian 8	9.17, 9.18	3.16.0-4-amd64 to 3.16.0-6-amd64, 4.9.0-0.bpo.4-amd64 to 4.9.0-0.bpo.6-amd64
Debian 8	9.16	3.16.0-4-amd64 to 3.16.0-5-amd64, 4.9.0-0.bpo.4-amd64 to 4.9.0-0.bpo.6-amd64
Debian 8	9.15	3.16.0-4-amd64 to 3.16.0-5-amd64, 4.9.0-0.bpo.4-amd64 to 4.9.0-0.bpo.5-amd64

SUSE Linux Enterprise Server 12 supported kernel versions

RELEASE	MOBILITY SERVICE VERSION	KERNEL VERSION
SUSE Linux Enterprise Server 12 (SP1,SP2,SP3)	9.18	SP1 3.12.49-11-default to 3.12.74-60.64.40-default SP1(LTSS) 3.12.74-60.64.45-default to 3.12.74-60.64.96-default SP2 4.4.21-69-default to 4.4.120-92.70-default SP2(LTSS) 4.4.121-92.73-default to 4.4.121-92.85-default SP3 4.4.73-5-default to 4.4.138-94.39-default

Linux file systems/guest storage

COMPONENT	SUPPORTED
File systems	ext3, ext4, XFS.
Volume manager	LVM2. LVM is supported for data disks only. Azure VMs have only a single OS disk.
Paravirtualized storage devices	Devices exported by paravirtualized drivers aren't supported.
Multi-queue block IO devices	Not supported.
Physical servers with the HP CCISSTorage controller	Not supported.

COMPONENT	SUPPORTED
Directories	<p>These directories (if set up as separate partitions/file-systems) all 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>.</p> <p><code>/boot</code> should be on a disk partition and not be an LVM volume.</p>
Free space requirements	<p>2 GB on the <code>/root</code> partition</p> <p>250 MB on the installation folder</p>
XFSv5	XFSv5 features on XFS file systems, such as metadata checksum, are supported from Mobility Service version 9.10 onward. Use the <code>xfs_info</code> utility to check the XFS superblock for the partition. If <code>ftype</code> is set to 1, then XFSv5 features are in use.

VM/Disk management

ACTION	DETAILS
Resize disk on replicated VM	Supported.
Add disk on replicated VM	Disable replication for the VM, add the disk, and then reenable replication. Adding a disk on a replicating VM isn't currently supported.

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 fallback.</p>

COMPONENT	SUPPORTED
Guest/server network multiple NICs	Yes.

Azure VM network (after failover)

COMPONENT	SUPPORTED
Azure ExpressRoute	Yes
ILB	Yes
ELB	Yes
Azure Traffic Manager	Yes
Multi-NIC	Yes
Reserved IP address	Yes
IPv4	Yes
Retain source IP address	Yes
Azure Virtual Network service endpoints (without Azure Storage firewalls)	Yes
Accelerated Networking	No

Storage

COMPONENT	SUPPORTED
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

COMPONENT	SUPPORTED
Guest/server EFI/UEFI	Partial (migration to Azure for Windows Server 2012 and later VMware virtual machines only) See the note at the end of the table
Guest/server shared cluster disk	No
Guest/server encrypted disk	No
Guest/server NFS	No
Guest/server SMB 3.0	No
Guest/server RDM	Yes N/A for physical servers
Guest/server disk > 1 TB	Yes Up to 4,095 GB
Guest/server disk with 4K logical and 4k physical sector size	Yes
Guest/server disk with 4K logical and 512 bytes physical sector size	Yes
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

NOTE

UEFI boot VMware virtual machines running Windows Server 2012 or later can be migrated to Azure. The following restrictions apply:

- Only migration to Azure is supported. Fallback to on-premises VMware site isn't supported.
- The server shouldn't have more than four partitions on the OS disk.
- Requires Mobility Service version 9.13 or later.
- Not supported for physical servers.

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 (Storage Service Encryption)	Yes
Premium storage	Yes
Import/export service	No
Azure Storage firewalls for virtual networks configured on target storage/cache storage account (used to store replication data)	No
General purpose v2 storage accounts (both hot and cool tiers)	No

Azure compute

FEATURE	SUPPORTED
Availability sets	Yes
HUB	Yes
Managed disks	Yes

Azure VM requirements

On-premises VMs that you replicate to Azure must meet the Azure VM requirements summarized in this table. When Site Recovery runs a prerequisites check, it 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.

COMPONENT	REQUIREMENTS	DETAILS
Data disk count	64 or less.	Check fails if unsupported.
Data disk size	Up to 4,095 GB	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	<p>From 1 to 63 characters.</p> <p>Restricted to letters, numbers, and hyphens.</p> <p>The machine name must start and end with a letter or number.</p>	Update the value in the machine properties in Site Recovery.

Vault tasks

ACTION	SUPPORTED
Move vault across resource groups	No
Within and across subscriptions	
Move storage, network, Azure VMs across resource groups	No
Within and across subscriptions	

Download latest Azure Site Recovery components

NAME	DESCRIPTION	LATEST VERSION DOWNLOAD INSTRUCTIONS
Configuration server	<p>Coordinates communications between on-premises VMware servers and Azure</p> <p>Installed on on-premises VMware servers</p>	For fresh installation, click here . For upgrading existing component to latest version, click here .
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. As your deployment grows, you can add additional, separate process servers to handle larger volumes of replication traffic.	For fresh installation, click here . For upgrading existing component to latest version, click here .

NAME	DESCRIPTION	LATEST VERSION DOWNLOAD INSTRUCTIONS
Mobility Service	<p>Coordinates replication between on-premises VMware servers/physical servers and Azure/secondary site</p> <p>Installed on VMware VM or physical servers you want to replicate</p>	For fresh installation, click here . For upgrading existing component to latest version, click here .

To learn about the latest features and fixes, click [here](#).

Next steps

[Learn how](#) to prepare Azure for disaster recovery of VMware VMs.

VMware to Azure replication architecture

7/9/2018 • 8 minutes to read • [Edit Online](#)

This article describes the architecture and processes used when you replicate, fail over, and recover VMware virtual machines (VMs) between an on-premises VMware site and Azure by using [Azure Site Recovery](#).

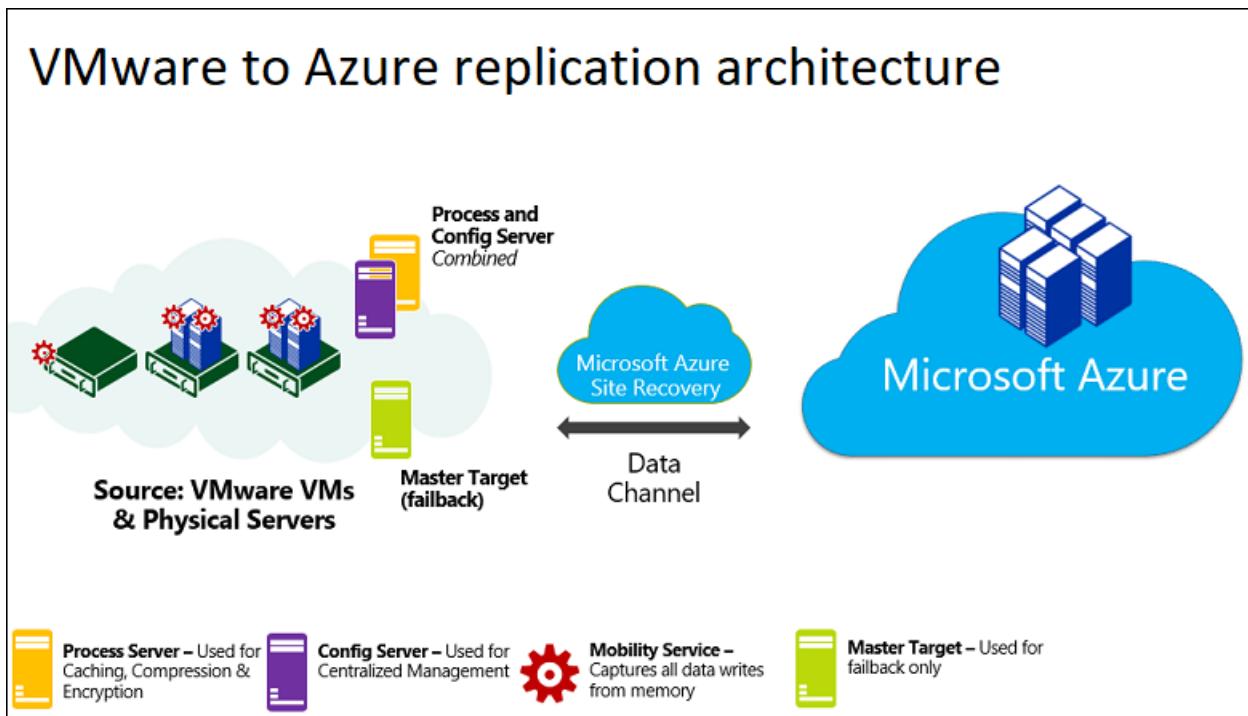
Architectural components

The following table and graphic provide a high-level view of the components used for VMware replication to Azure.

COMPONENT	REQUIREMENT	DETAILS
Azure	An Azure subscription, Azure Storage account, and Azure network.	Replicated data from on-premises VMs is stored in the storage account. 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	A single on-premises machine. We recommend that you run it as a VMware VM that can be deployed from a downloaded OVF template. The machine runs all on-premises Site Recovery components, which include the configuration server, process server, and master target server.	Configuration server: Coordinates communications between on-premises and Azure, and manages data replication. 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. 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.
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 System Center Configuration Manager.

VMware to Azure architecture



Configuration steps

The broad steps for setting up VMware to Azure disaster recovery or migration are as follows:

- Set up Azure components.** You need an Azure account with the right permissions, an Azure storage account, an Azure virtual network, and a Recovery Services vault. [Learn more](#).
- Set up on-premises.** These include setting up an account on the VMware server so that Site Recovery can automatically discover VMs to replicate, setting up an account that can be used to install the Mobility service component on VMs you want to replicate, and verifying that VMware servers and VMs comply with prerequisites. You can also optionally prepare to connect to these Azure VMs after failover. Site Recovery replicates VM data to an Azure storage account, and creates Azure VMs using the data when you run a failover to Azure. [Learn more](#).
- Set up replication.** You choose where you want to replicate to. You configure the source replication environment by setting up a single on-premises VMware VM (the configuration server) that runs all of the on-premises Site Recovery components that you need. After setup you register the configuration server machine in the Recovery Services vault. Then, you select the target settings. [Learn more](#).
- Create a replication policy.** You create a replication policy that specifies how replication should happen.
 - RPO threshold:** This monitoring setting states that if replication doesn't occur within the time specified, an alert (and optionally an email) is issued. For example, if you set the RPO threshold to 30 minutes, and an issue prevents replication from happening for 30 minutes, an event is generated. This setting doesn't affect replication. Replication is continuous, and recovery points are created every few minutes
 - Retention:** Recovery point retention specifies how long recovery points should be kept in Azure. You

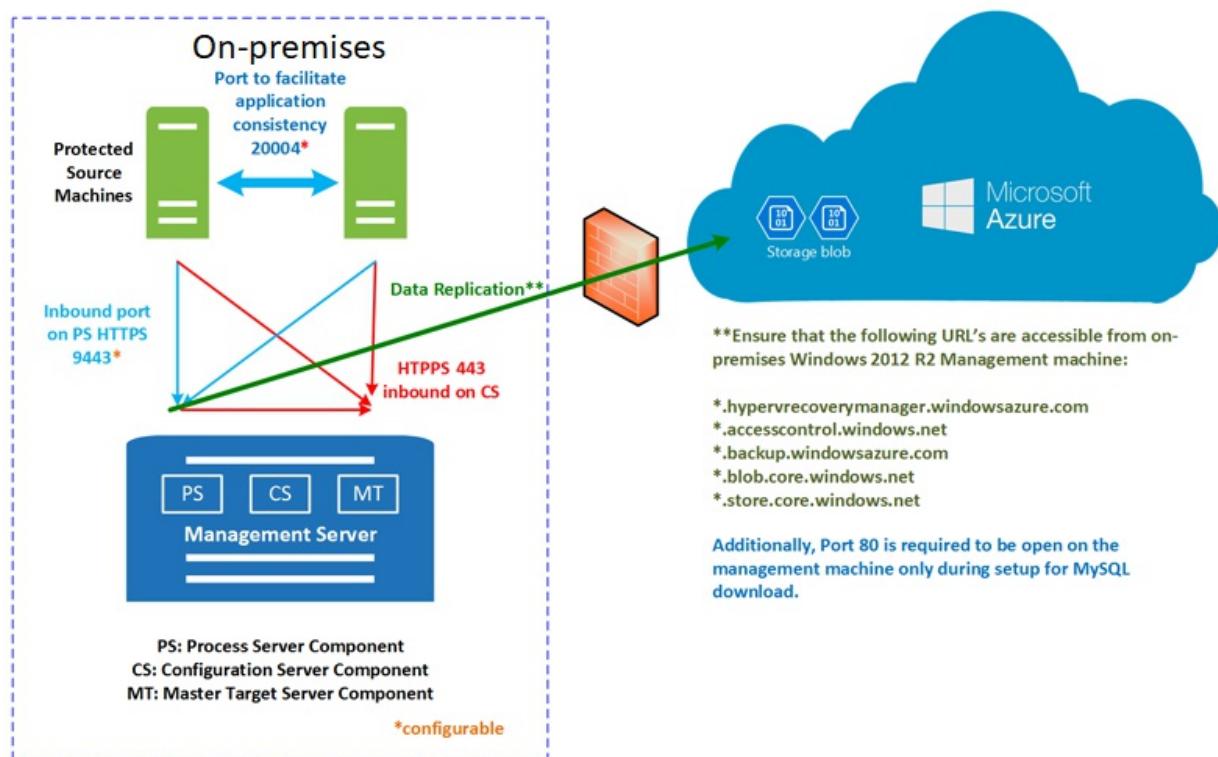
can specify a value between 0 and 24 hours for premium storage, or up to 72 hours for standard storage. You can fail over to the latest recovery point, or to a stored point if you set the value higher than zero. After the retention window, recovery points are purged.

- **Crash-consistent snapshots:** By default, Site Recovery takes crash-consistent snapshots and creates recovery points with them every few minutes. A recovery point is crash consistent if all of the interrelated data components are write-order consistent, as they were at the instant the recovery point was created. To better understand, imagine the status of the data on your PC hard drive after a power outage or similar event. A crash-consistent recovery point is usually sufficient if your application is designed to recover from a crash without any data inconsistencies.
 - **App-consistent snapshots:** If this value isn't zero, the Mobility service running on the VM attempts to generate file system-consistent snapshots and recovery points. The first snapshot is taken after initial replication is complete. Then, snapshots are taken at the frequency you specify. A recovery point is application-consistent if, in addition to being write-order consistent, running applications complete all of their operations, and flush their buffers to disk (application quiescing). App-consistent recovery points are recommended for database applications such as SQL, Oracle, and Exchange. If a crash-consistent snapshot is sufficient, this value can be set to 0.
 - **Multi-VM consistency:** You can optionally create a replication group. Then, when you enable replication, you can gather VMs into that group. VMs in a replication group replicate together, and have shared crash-consistent and app-consistent recovery points when failed over. You should use this option carefully, since it can affect workload performance as snapshots needed to be gathered across multiple machines. Only do this if VMs run the same workload and need to be consistent, and VMs have similar chucks. You can add up to 8 VMs to a group.
5. **Enable VM replication.** Finally, you enable replication for your on-premises VMware VMs. If you created an account to install the Mobility service, and specified that Site Recovery should do a push installation, then the Mobility service will be installed on each VM for which you enable replication. [Learn more](#). If you have created a replication group for multi-VM consistency, you can add VMs to that group.
 6. **Test failover.** After everything's set up, you can do a test failover to check that VMs fail over to Azure as expected. [Learn more](#).
 7. **Failover.** If you're just migrating the VMs to Azure - you run a full failover to do that. If you're setting up disaster recovery, you can run a full failover as you need to. For full disaster recovery, after failover to Azure, you can fail back to your on-premises site as and when it's available. [Learn more](#).

Replication process

1. When you enable replication for a VM, it begins to replicate in accordance with the replication policy.
2. Traffic replicates to Azure storage public endpoints over the internet. Alternately, you can use Azure ExpressRoute with [public peering](#). Replicating traffic over a site-to-site virtual private network (VPN) from an on-premises site to Azure isn't supported.
3. An initial copy of the VM 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. 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.

VMware to Azure replication process

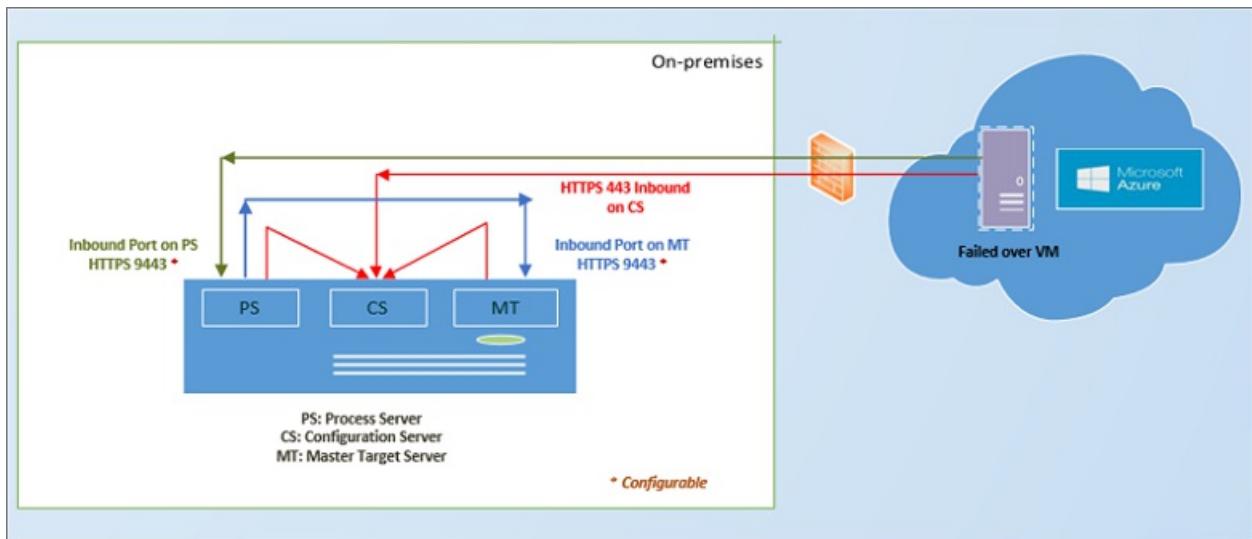


Failover and failback process

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 fail for a single machine, or create a recovery plans 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 was automatically created when you created your 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.

Physical server to Azure replication architecture

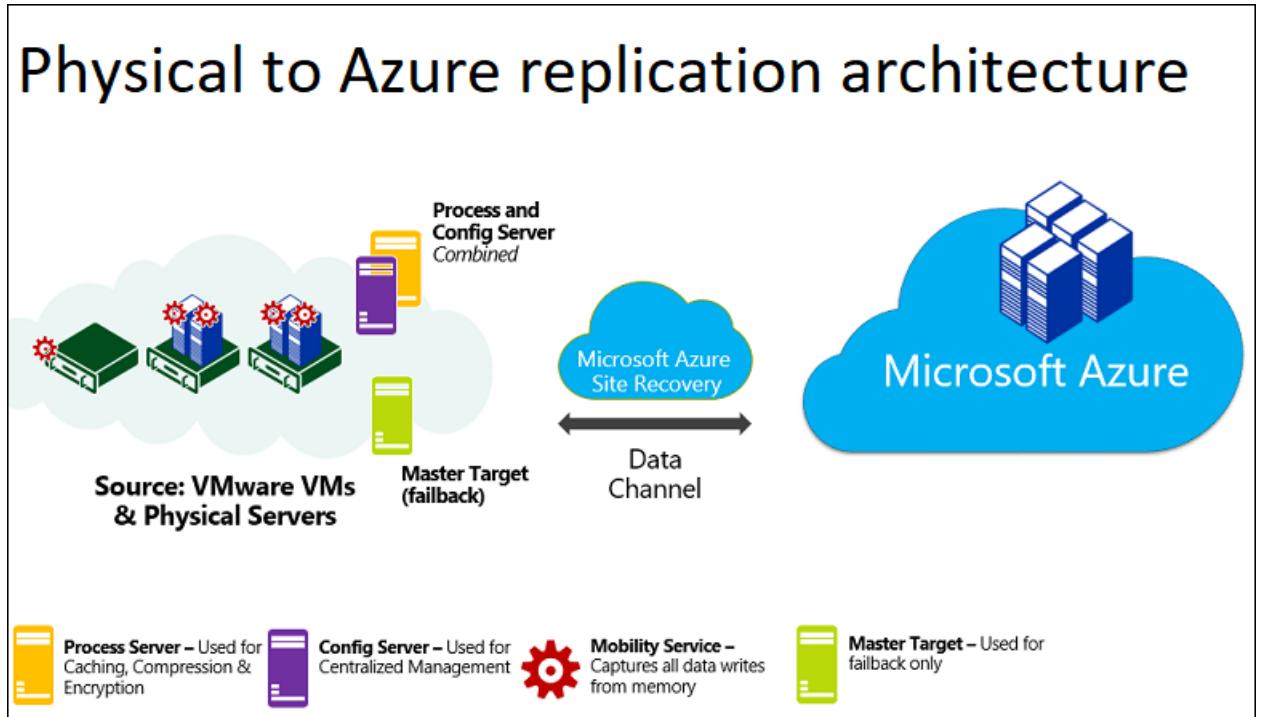
7/9/2018 • 4 minutes to read • [Edit Online](#)

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 provide a high-level view of the components used for physical server replication to Azure.

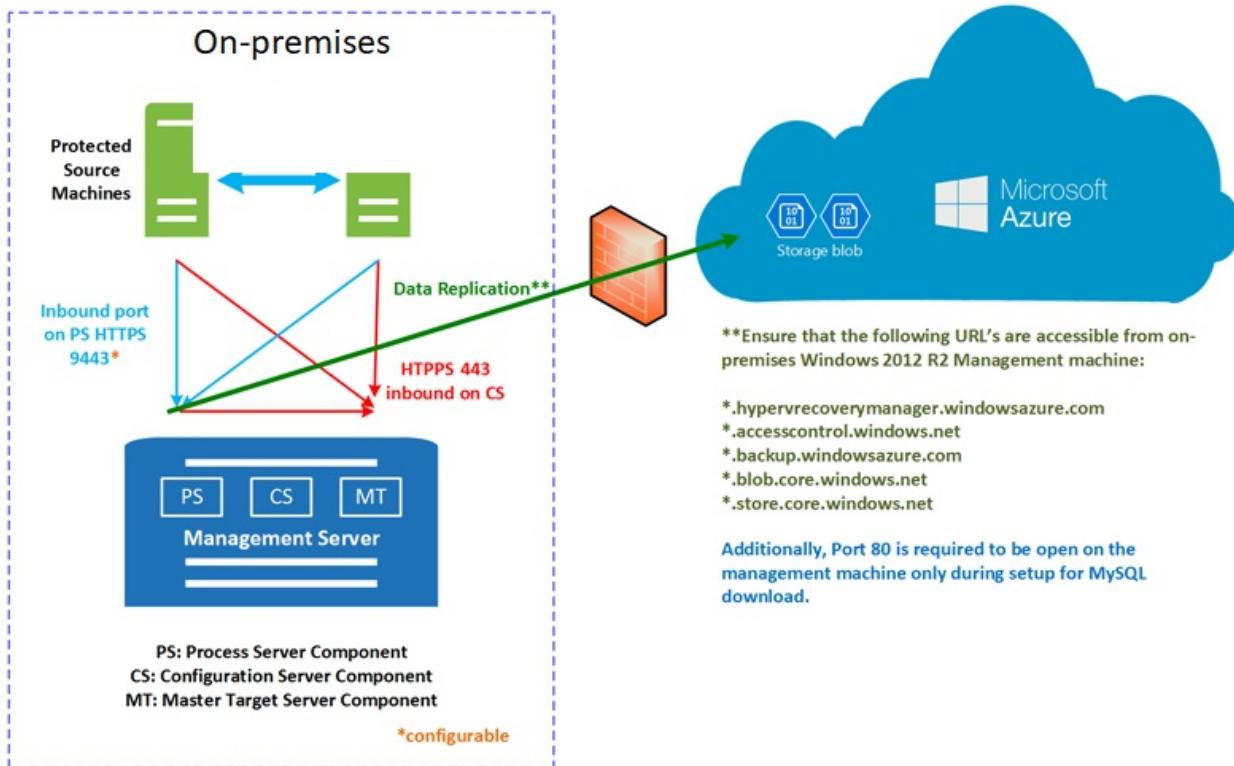
COMPONENT	REQUIREMENT	DETAILS
Azure	An Azure subscription, Azure storage account, and Azure network.	Replicated data from on-premises VMs is stored in the storage account. Azure VMs are created with the replicated data when you run a fail over from on-premises to Azure. The Azure VMs connect to the Azure virtual network when they're created.
Configuration server	A single on-premises physical machine or VMware VM is deployed to run all of the on-premises Site Recovery components. The VM runs the configuration server, process server, and master target server.	The configuration server coordinates communications between on-premises and Azure, and manages data replication.
Process server:	Installed by default together with the configuration server.	Acts as a replication gateway. Receives replication data, optimizes it with caching, compression, and encryption, and sends it to Azure storage. The process server also installs the Mobility service on servers you want to replicate. As your deployment grows, you can add additional, separate process servers to handle larger volumes of replication traffic.
Master target server	Installed by default together with the configuration server.	Handles replication data during failback from Azure. For large deployments, you can add an additional, separate master target server for failback.
Replicated servers	The Mobility service is installed on each server you replicate.	We recommend you allow automatic installation from the process server. Alternatively you can install the service manually, or use an automated deployment method such as System Center Configuration Manager.



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 in accordance with 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 .hrl file.
 - Machines communicate with the configuration server on port HTTPS 443 inbound, for replication management.
 - Machines send replication data to the process server on port HTTPS 9443 inbound (can be modified).
 - The configuration server orchestrates replication management with Azure over port HTTPS 443 outbound.
 - The process server receives data from source machines, optimizes and encrypts it, and sends it to Azure storage over 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. This is 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](#). Replicating traffic over a site-to-site VPN from an on-premises site to Azure isn't supported.

Physical to Azure replication process

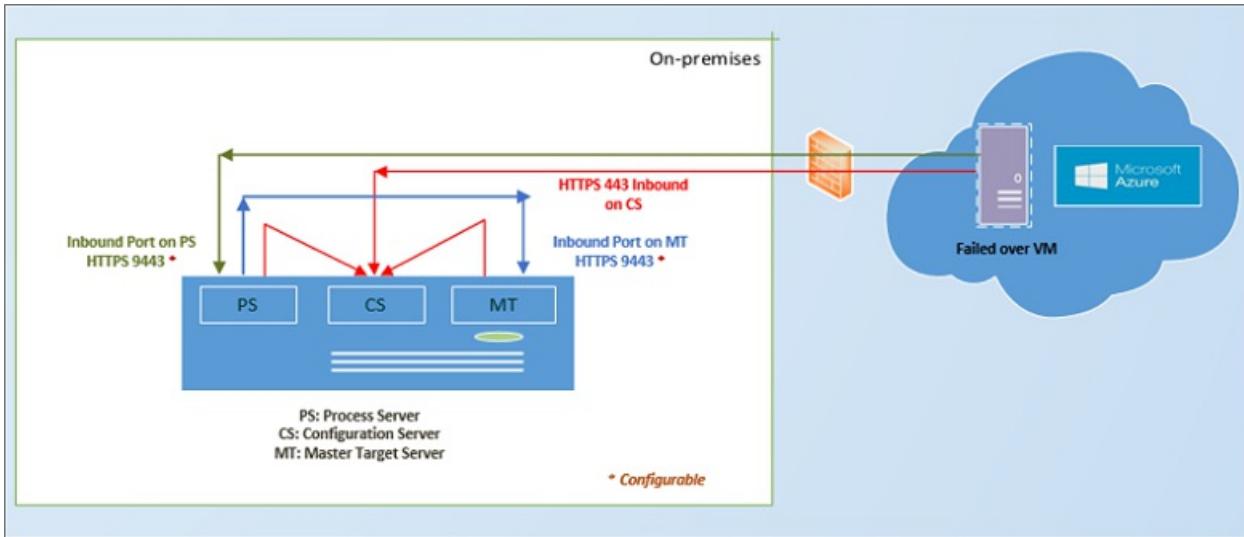


Failover and fallback process

After replication is set up and you've run a disaster recovery drill (test failover) to check everything's working as expected, you can run failover and failback as you need to. Note that:

- Planned failover isn't supported.
- You must fail back to an on-premises VMware VM. This means 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 triggering the initial failover, 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.
- 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 Azure 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. However, if you need to fail back large volumes of traffic, you should 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 was automatically created when you created your replication policy from on-premises to Azure.
 - **VMware infrastructure:** You need a VMware infrastructure for failback. You can't fail back to a physical server.
- After the components are in place, failback 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

Follow [this tutorial](#) to enable physical server to Azure replication.

Overview of multi-tenant support for VMware replication to Azure with CSP

7/9/2018 • 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:

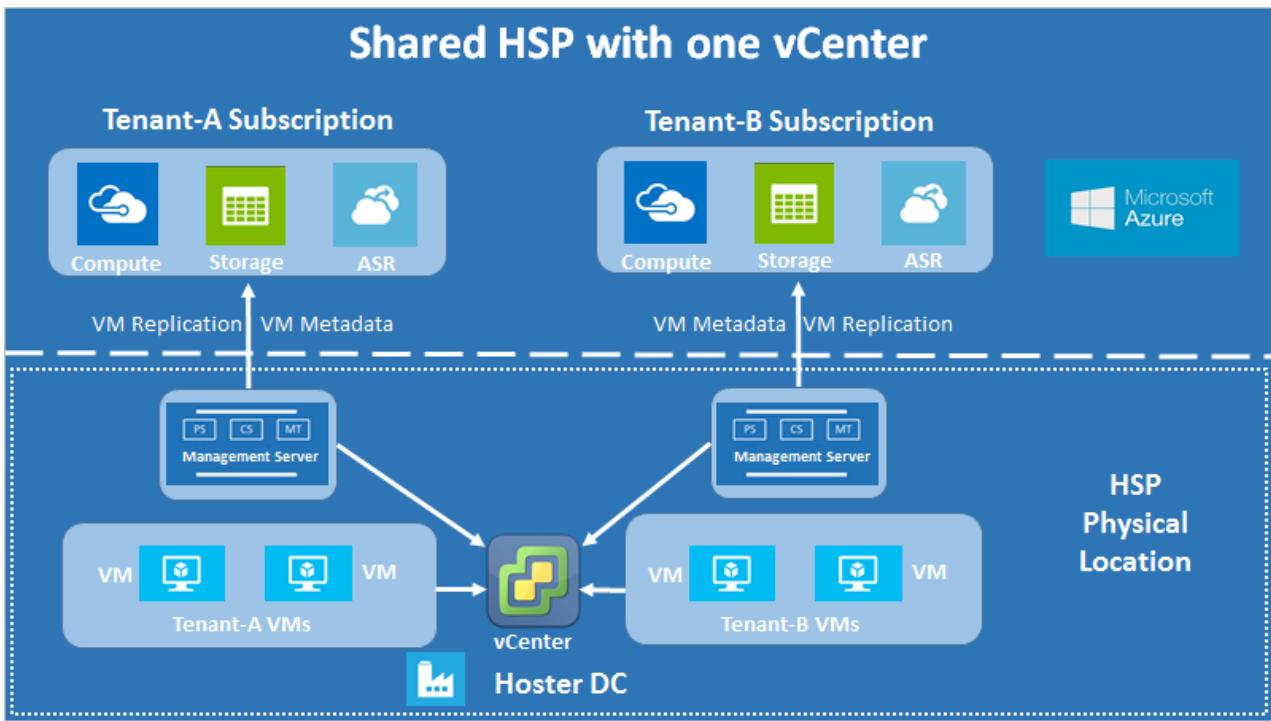
- **Shared Hosting Services Provider (HSP):** The partner owns the physical infrastructure, and uses shared resources (vCenter, datacenters, physical storage, and so on) to host multiple tenant VMs on the same infrastructure. The partner can provide disaster-recovery management as a managed service, 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:

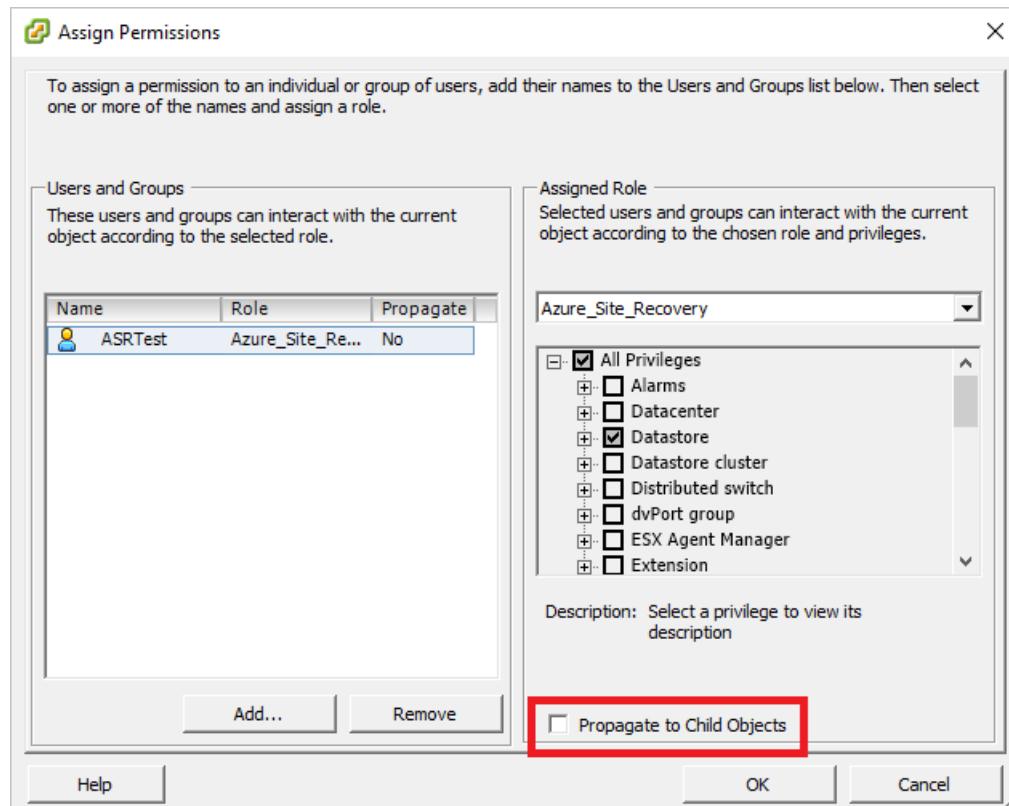
- **vCenter access account:** This account is used to discover tenant VMs. It has vCenter access permissions assigned to it. To help avoid access leaks, we recommend that partners enter these credentials themselves in the configuration tool.
- **Virtual machine access account:** This account is used 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

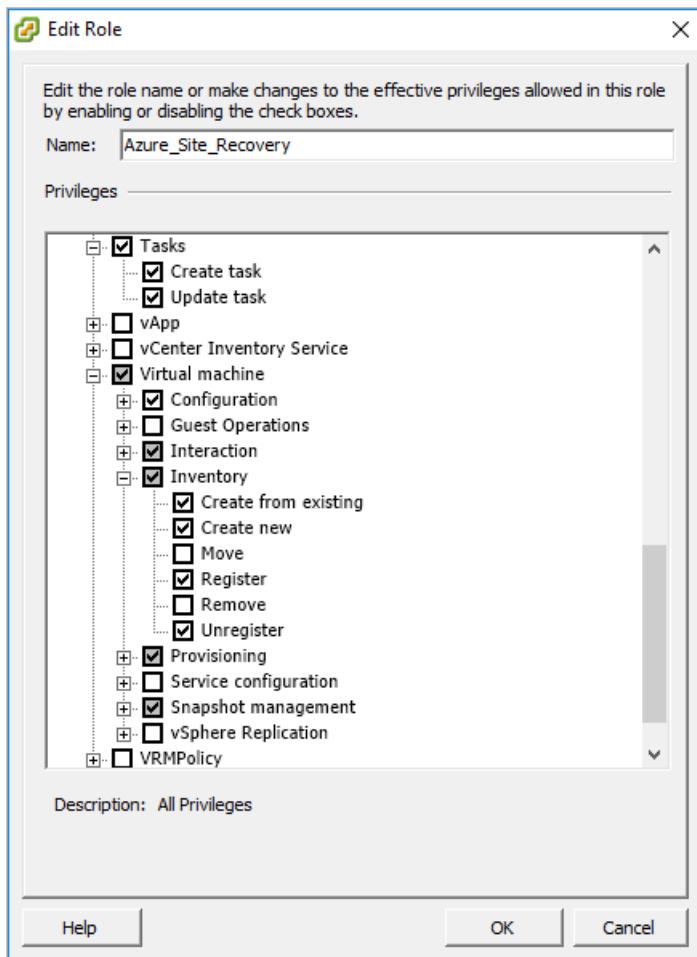
propagated to the child objects. This configuration ensures tenant isolation, because access propagation can result in accidental access to other objects.



- 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.

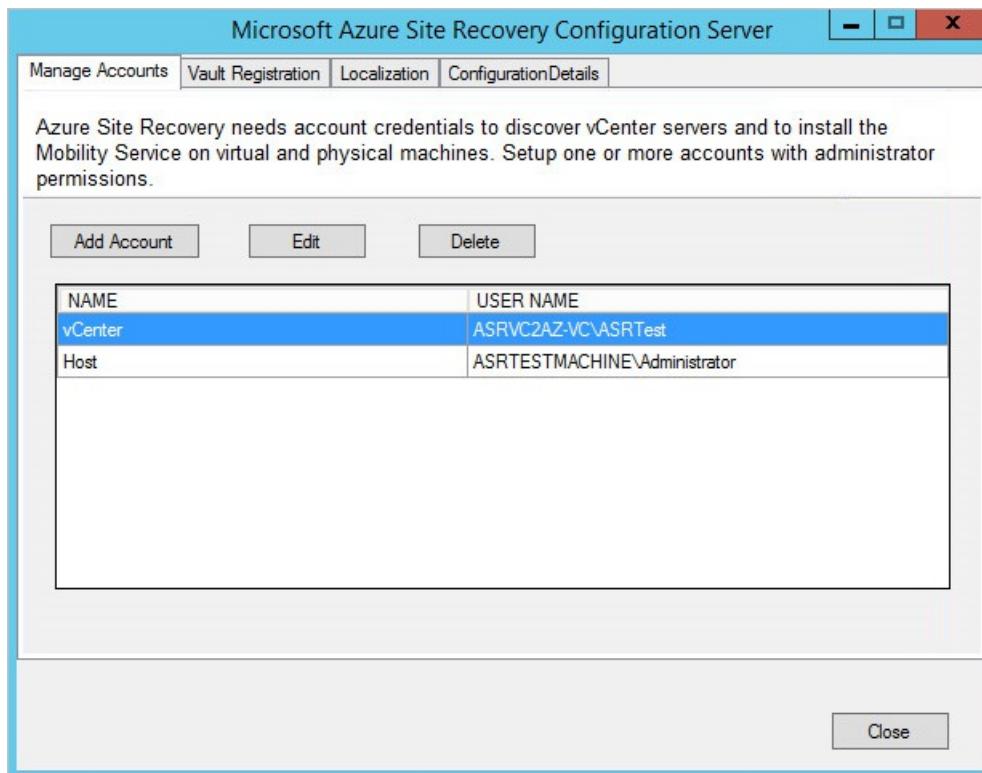
Failover only

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.



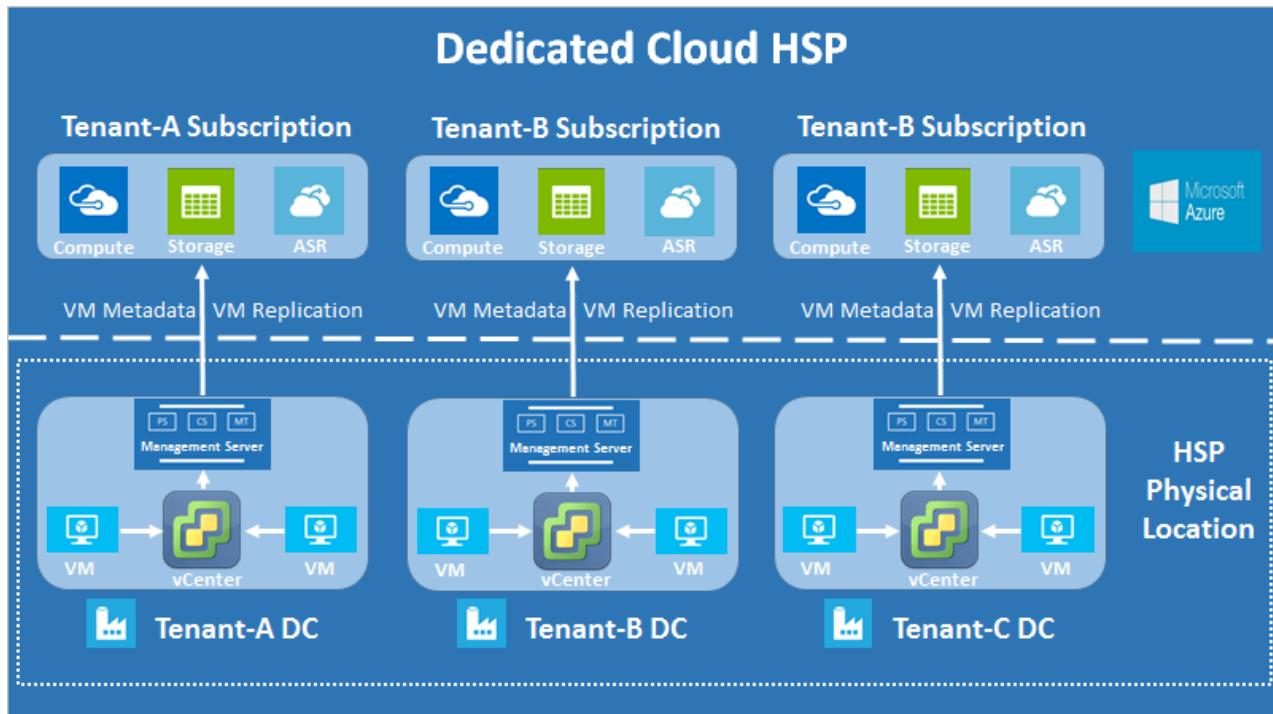
Register servers in the vault

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

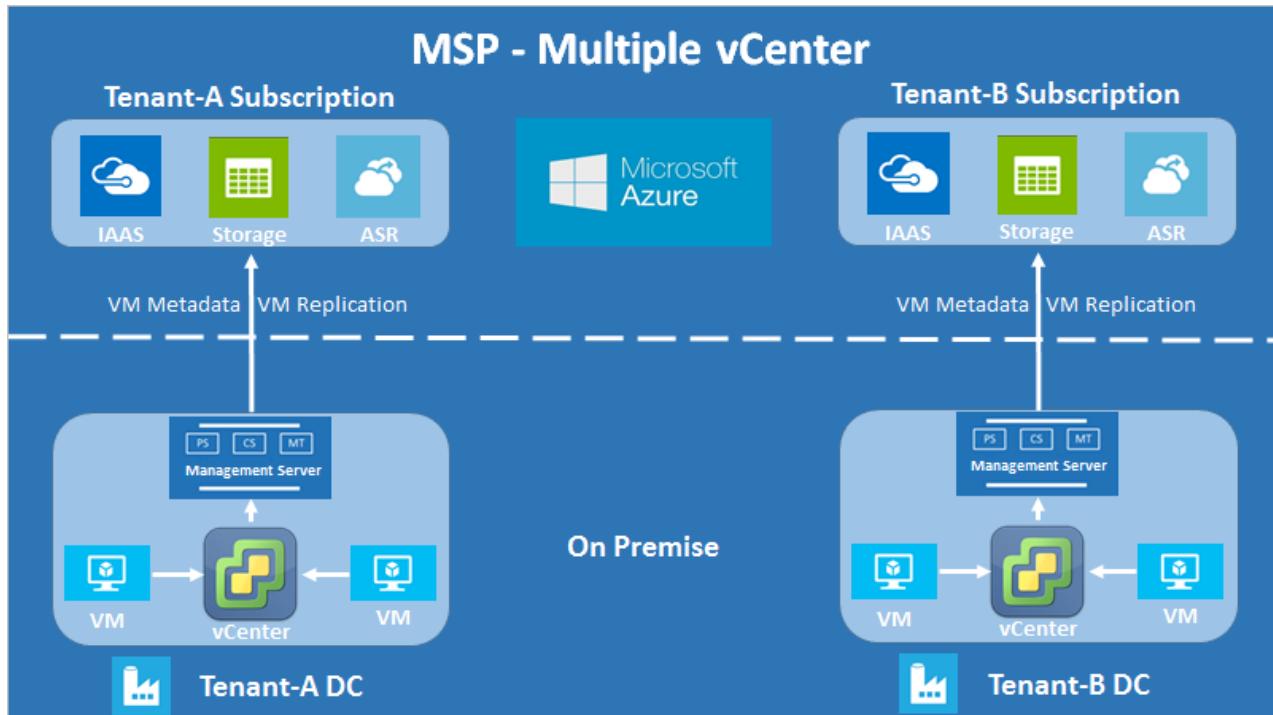
As shown in the following diagram, the architectural difference in a dedicated hosting solution is that each tenant's infrastructure is set up for that tenant only.



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](#).

Install the Mobility service

8/6/2018 • 8 minutes to read • [Edit Online](#)

Azure Site Recovery Mobility Service is installed on VMware VMs and physical servers that you want to replicate to Azure. The service captures data writes on a computer and then forwards them to the process server. Deploy Mobility Service to every computer (VMware VM or physical server) that you want to replicate to Azure. You can deploy the Mobility Service on the servers and VMware VMs you want to protect using the following methods:

- [Install using software deployment tools like System Center Configuration Manager](#)
- [Install with Azure Automation and Desired State Configuration \(Automation DSC\)](#)
- [Install manually from the UI](#)
- [Install manually from a command prompt](#)
- [Install using the Site Recovery push installation](#)

IMPORTANT

Beginning with version 9.7.0.0, **on Windows VMs**, the Mobility Service installer also installs the latest available [Azure VM agent](#). When a computer fails over to Azure, the computer meets the agent installation prerequisite for using any VM extension.

On **Linux VMs**, WALinuxAgent has to be manually installed.

Prerequisites

Complete these prerequisite steps before you manually install Mobility Service on your server:

1. Sign in to your configuration server, and then open a command prompt window as an administrator.
2. Change the directory to the bin folder, and then create a passphrase file.

```
cd %ProgramData%\ASR\home\svsystems\bin  
genpassphrase.exe -v > MobSvc.passphrase
```

3. Store the passphrase file in a secure location. You use the file during Mobility Service installation.
4. Mobility Service installers for all supported operating systems are in the %ProgramData%\ASR\home\svsystems\pushinstallsvc\repository folder.

Mobility Service installer-to-operating system mapping

To see a list of Operating System versions with a compatible Mobility Service package refer to the list of [supported operating systems for VMware virtual machines and physical servers](#).

INSTALLER FILE TEMPLATE NAME	OPERATING SYSTEM
Microsoft-ASR_UA*Windows*release.exe	Windows Server 2008 R2 SP1 (64-bit) Windows Server 2012 (64-bit) Windows Server 2012 R2 (64-bit) Windows Server 2016 (64-bit)
Microsoft-ASR_UA*RHEL6-64*release.tar.gz	Red Hat Enterprise Linux (RHEL) 6.* (64-bit only) CentOS 6.* (64-bit only)

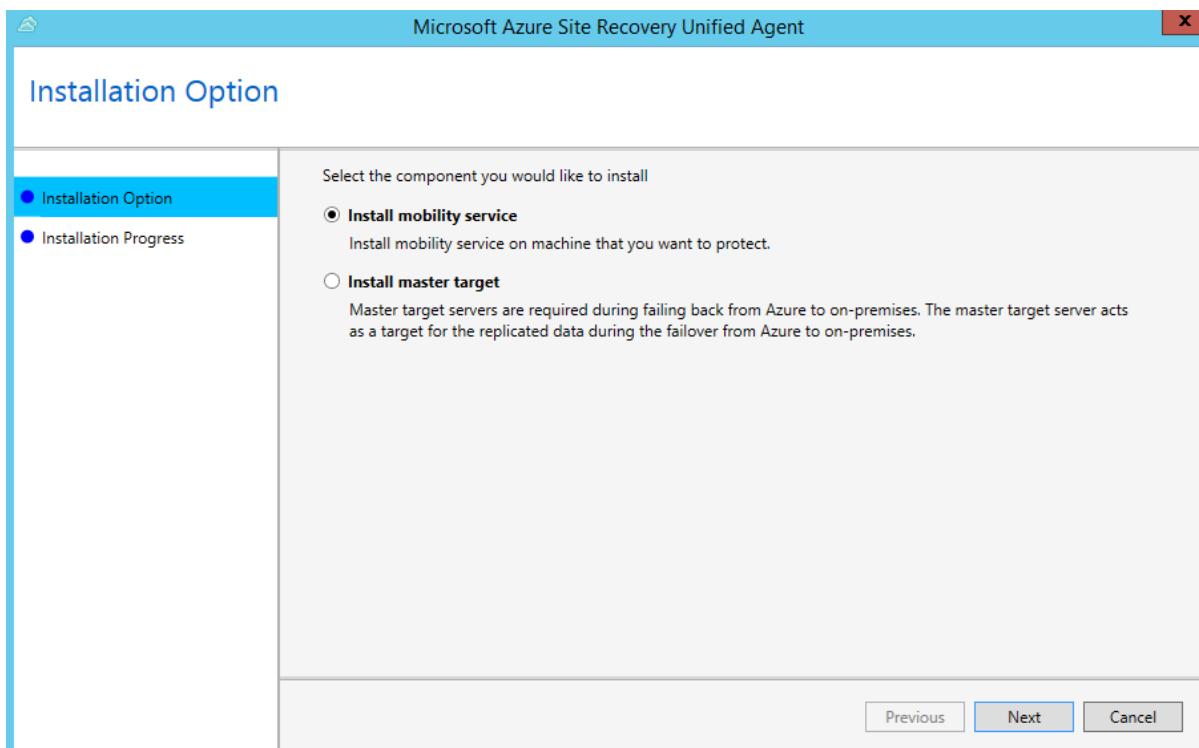
INSTALLER FILE TEMPLATE NAME	OPERATING SYSTEM
Microsoft-ASR_UA*RHEL7-64*release.tar.gz	Red Hat Enterprise Linux (RHEL) 7.* (64-bit only) CentOS 7.* (64-bit only)
Microsoft-ASR_UA*SLES12-64*release.tar.gz	SUSE Linux Enterprise Server 12 SP1,SP2,SP3 (64-bit only)
Microsoft-ASR_UA*SLES11-SP3-64*release.tar.gz	SUSE Linux Enterprise Server 11 SP3 (64-bit only)
Microsoft-ASR_UA*SLES11-SP4-64*release.tar.gz	SUSE Linux Enterprise Server 11 SP4 (64-bit only)
Microsoft-ASR_UA*OL6-64*release.tar.gz	Oracle Enterprise Linux 6.4, 6.5 (64-bit only)
Microsoft-ASR_UA*UBUNTU-14.04-64*release.tar.gz	Ubuntu Linux 14.04 (64-bit only)
Microsoft-ASR_UA*UBUNTU-16.04-64*release.tar.gz	Ubuntu Linux 16.04 LTS server (64-bit only)
Microsoft-ASR_UA*DEBIAN7-64*release.tar.gz	Debian 7 (64-bit only)
Microsoft-ASR_UA*DEBIAN8-64*release.tar.gz	Debian 8 (64-bit only)

Install Mobility Service manually by using the GUI

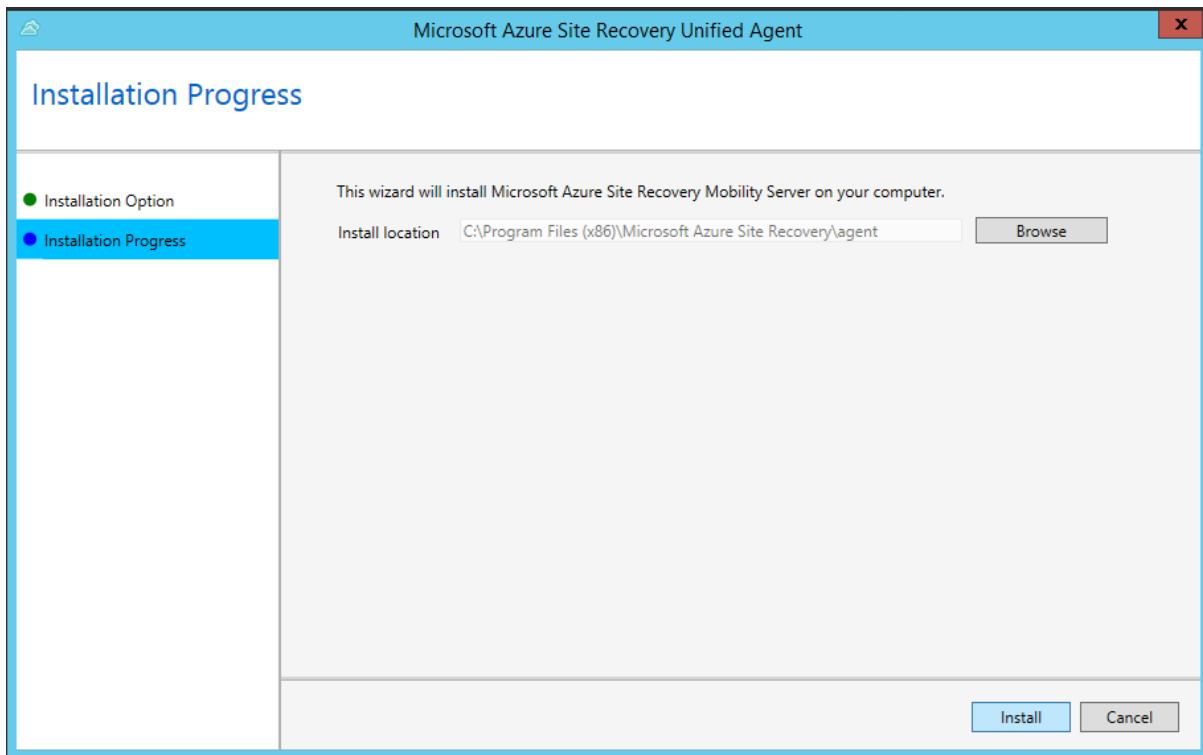
IMPORTANT

If you use a configuration server to replicate Azure IaaS virtual machines from one Azure subscription/region to another, use the command-line-based installation method.

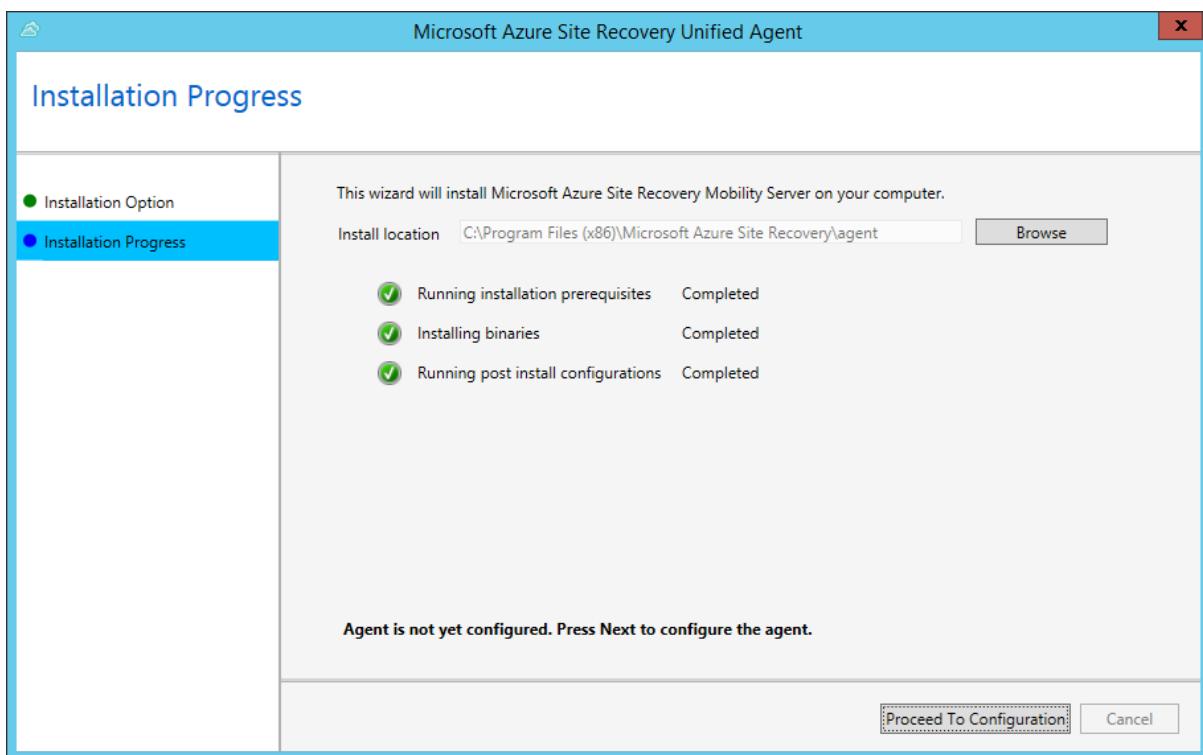
1. Copy the installation to the server, and then open the installer.
2. On **Installation Option**, select **Install mobility service**.



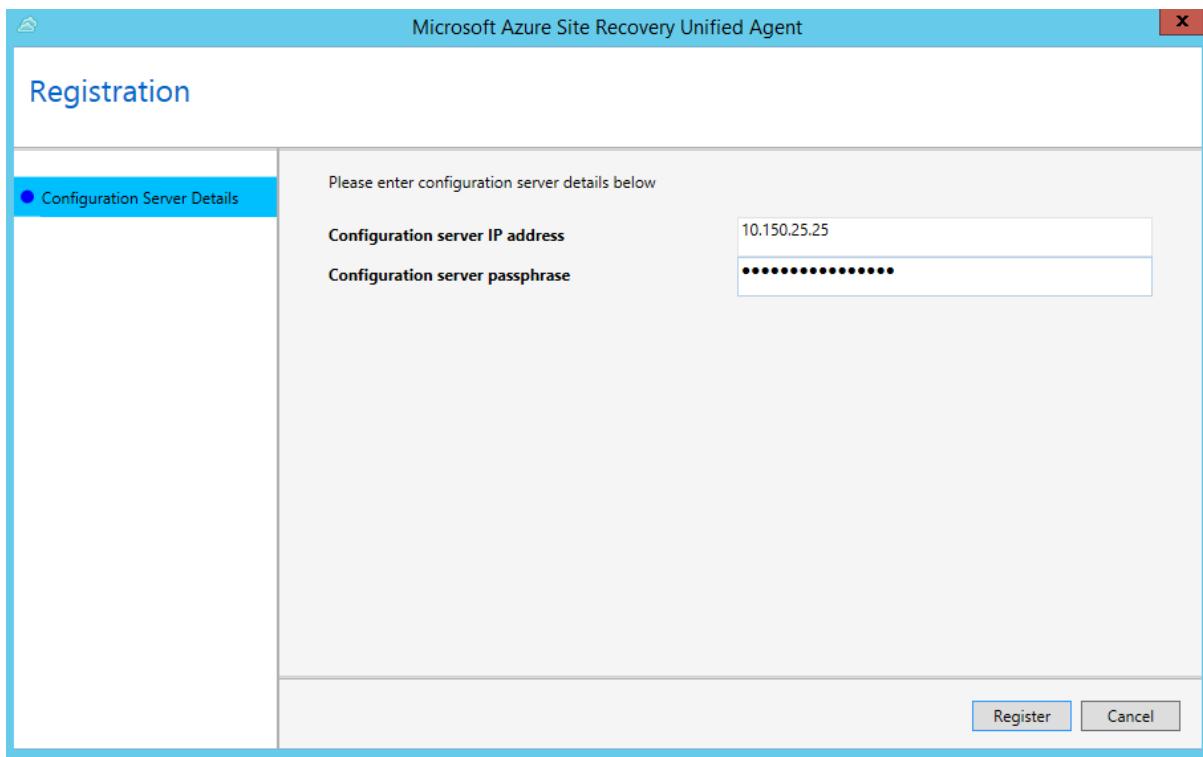
3. Select the installation location, and then select **Install** to start the installation procedure.



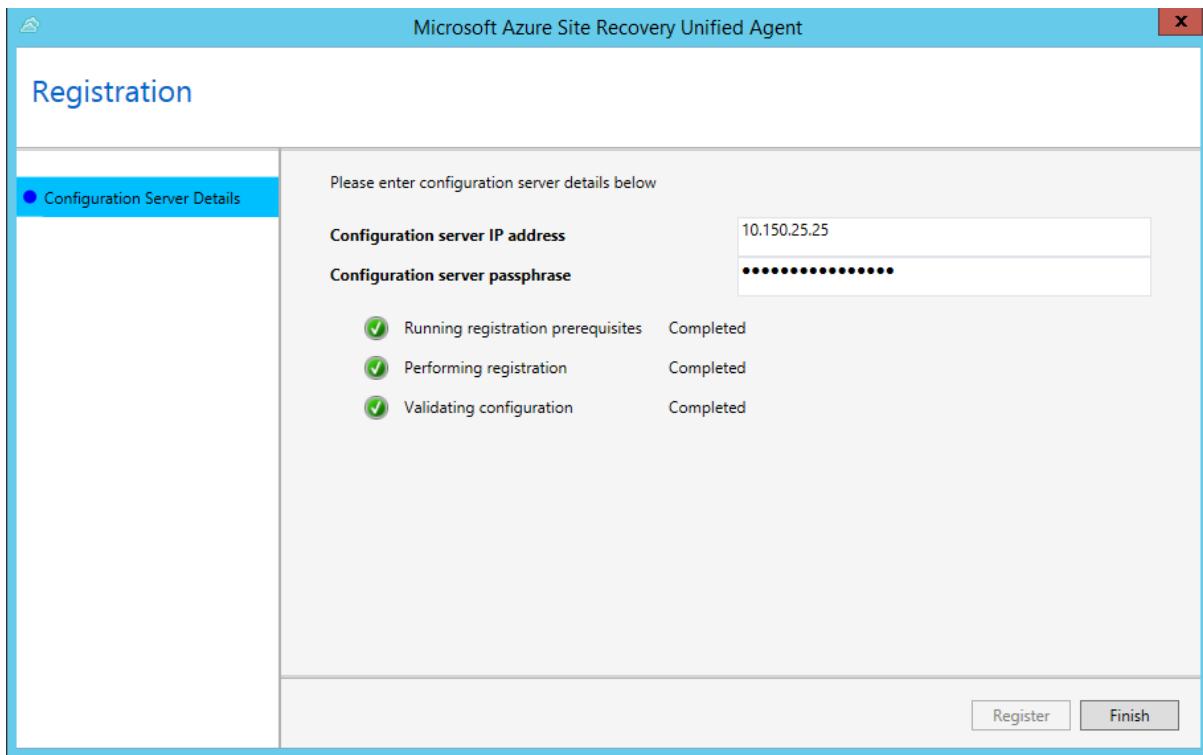
4. Use the **Installation Progress** page to monitor the installer's progress.



5. After the installation is finished, select **Proceed to Configuration** to register Mobility Service with your configuration server.



6. Select **Register** to finish the registration.



Install Mobility Service manually at a command prompt

Command-line installation on a Windows computer

1. Copy the installer to a local folder (for example, C:\Temp) on the server that you want to protect. Run the following commands as an administrator at a command prompt:

```
cd C:\Temp  
ren Microsoft-ASR_UA*Windows*release.exe MobilityServiceInstaller.exe  
MobilityServiceInstaller.exe /q /x:C:\Temp\Extracted  
cd C:\Temp\Extracted.
```

2. To install Mobility Service, run the following command:

```
UnifiedAgent.exe /Role "MS" /InstallLocation "C:\Program Files (x86)\Microsoft Azure Site Recovery"  
/Platform "VmWare" /Silent
```

3. Now the agent needs to be registered with the configuration server.

```
cd C:\Program Files (x86)\Microsoft Azure Site Recovery\agent  
UnifiedAgentConfigurator.exe /CSEndPoint <CSIP> /PassphraseFilePath <PassphraseFilePath>
```

Mobility Service installer command-line arguments

Usage :
UnifiedAgent.exe /Role <MS|MT> /InstallLocation <Install Location> /Platform "VmWare" /Silent

PARAMETER	TYPE	DESCRIPTION	POSSIBLE VALUES
/Role	Mandatory	Specifies whether Mobility Service (MS) should be installed or MasterTarget (MT) should be installed.	MS MT
/InstallLocation	Optional	Location where Mobility Service is installed.	Any folder on the computer
/Platform	Mandatory	Specifies the platform on which Mobility Service is installed. - VMware : Use this value if you install Mobility Service on a VM running on <i>VMware vSphere ESXi hosts, Hyper-V hosts, and physical servers</i> . - Azure : Use this value if you install an agent on an Azure IaaS VM.	VMware Azure
/Silent	Optional	Specifies to run the installer in silent mode.	N/A

TIP

The setup logs can be found under %ProgramData%\ASRSetupLogs\ASRUnifiedAgentInstaller.log.

Mobility Service registration command-line arguments

Usage :
UnifiedAgentConfigurator.exe /CSEndPoint <CSIP> /PassphraseFilePath <PassphraseFilePath>

PARAMETER	TYPE	DESCRIPTION	POSSIBLE VALUES
-----------	------	-------------	-----------------

PARAMETER	TYPE	DESCRIPTION	POSSIBLE VALUES
/CSEndPoint	Mandatory	IP address of the configuration server	Any valid IP address
/PassphraseFilePath	Mandatory	Location of the pass phrase	Any valid UNC or local file path

TIP

The Agent Configuration logs can be found under %ProgramData%\ASRSetupLogs\ASRUnifiedAgentConfigurator.log.

Command-line installation on a Linux computer

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 -xvzf Microsoft-ASR_UA*release.tar.gz
```

2. To install Mobility Service, run the following command:

```
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
```

Mobility Service installer command line

```
Usage:
./install -d <Install Location> -r <MS|MT> -v VmWare -q
```

PARAMETER	TYPE	DESCRIPTION	POSSIBLE VALUES
-r	Mandatory	Specifies whether Mobility Service (MS) should be installed or MasterTarget (MT) should be installed.	MS MT
-d	Optional	Location where Mobility Service is installed.	/usr/local/ASR

PARAMETER	TYPE	DESCRIPTION	POSSIBLE VALUES
-v	Mandatory	<p>Specifies the platform on which Mobility Service is installed.</p> <ul style="list-style-type: none"> - VMware: Use this value if you install Mobility Service on a VM running on <i>VMware vSphere ESXi hosts, Hyper-V hosts, and physical servers</i>. - Azure: Use this value if you install an agent on an Azure IaaS VM. 	VMware Azure
-q	Optional	Specifies to run the installer in silent mode.	N/A

Mobility Service configuration command line

```
Usage:  
cd /usr/local/ASR/Vx/bin  
UnifiedAgentConfigurator.sh -i <CSIP> -P <PassphraseFilePath>
```

PARAMETER	TYPE	DESCRIPTION	POSSIBLE VALUES
-i	Mandatory	IP of the configuration server	Any valid IP Address
-P	Mandatory	Full file path for the file where the connection pass phrase is saved	Any valid folder

Install Mobility Service by push installation from Azure Site Recovery

You can do a push installation of Mobility Service by using Site Recovery. All target computers must meet the following prerequisites.

Prepare for a push installation on a Windows computer

1. Ensure that there's network connectivity between the Windows computer and the process 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.

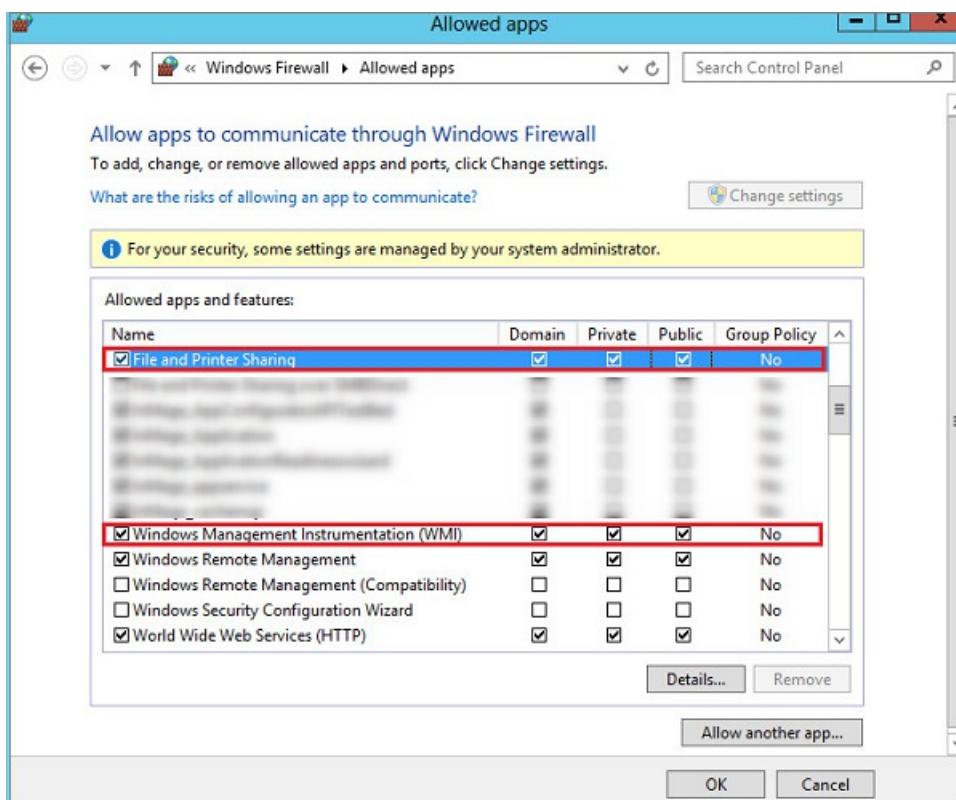
NOTE

If you don't use a domain account, 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 do this task 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 1
```

3. In Windows Firewall on the computer 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).



4. Add the account that you created in CSPSConfigtool. Follow these steps:

- Sign in to your configuration server.
- Open **cspconfigtool.exe**. It's available as a shortcut on the desktop and in the %ProgramData%\home\svsystems\bin folder.
- On the **Manage Accounts** tab, select **Add Account**.
- Add the account you created.
- Enter the credentials you use when you enable replication for a computer.

Prepare for a push installation on a Linux server

- Ensure that there's network connectivity between the Linux computer and the process server.
- 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.
- 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. Follow these steps:
 - Sign in as **root**.
 - In the **/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.

```
# override default of no subsystems
Subsystem      sftp      /usr/libexec.openssh/sftp-server
```

- e. Restart the **sshd** service.
7. Add the account that you created in CSPSConfigtool. Follow these steps:
- Sign in to your configuration server.
 - Open **cspscfgtool.exe**. It's available as a shortcut on the desktop and in the %ProgramData%\home\svsystems\bin folder.
 - On the **Manage Accounts** tab, select **Add Account**.
 - Add the account you created.
 - Enter the credentials you use when you enable replication for a computer.

NOTE

After Mobility Service is installed, in the Azure portal, select + **Replicate** to start protecting these VMs.

Update Mobility Service

WARNING

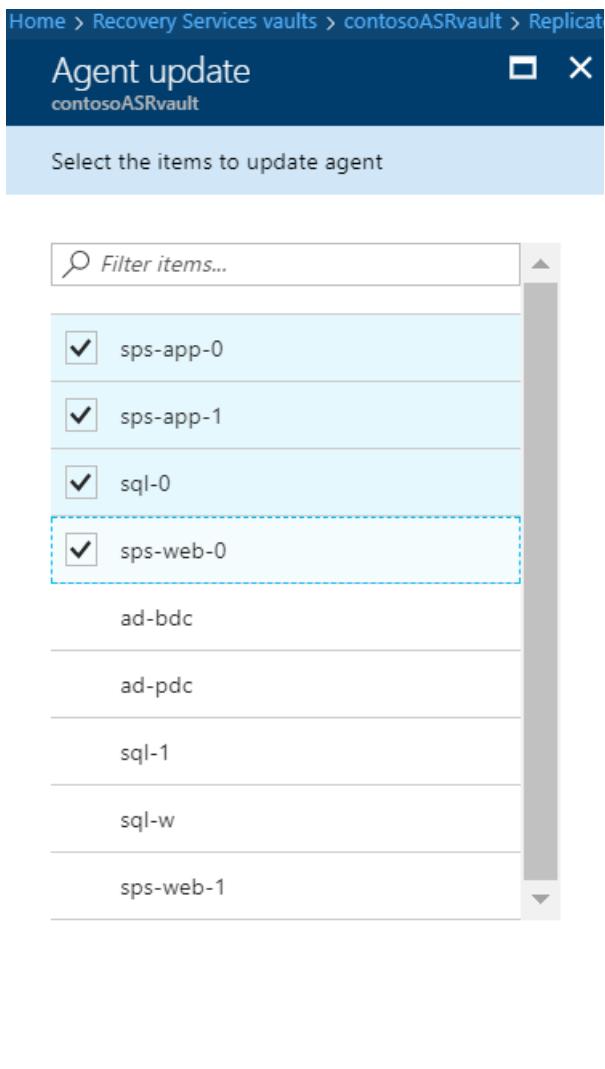
Ensure that the configuration server, scale-out process servers, and any master target servers that are a part of your deployment are updated before you start updating Mobility Service on the protected servers.

- On the Azure portal, browse to the *name of your vault* > **Replicated items** view.
- If the configuration server was already updated to 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's a navigation bar with 'Home', 'Recovery Services vaults', 'contosoASRVault', and 'Replicated items'. Below the navigation is a toolbar with 'Refresh', 'Replicate', and 'Columns' buttons. A prominent yellow notification bar at the top contains the message 'New Site recovery replication agent update is available. Click to install' with a right-pointing arrow. Below the notification, a message says 'Last refreshed at: 18/10/2017, 12:04:22 PM'. A progress indicator shows 'Finished loading data from service.' A search bar with 'Filter items...' is present. The main table lists four virtual machines with their names, health status (all critical), and protection status (all protected). The table has columns for NAME, HEALTH, and STATUS.

NAME	HEALTH	STATUS
sps-app-0	! Critical	Protected
sps-app-1	! Critical	Protected
sql-0	! Critical	Protected
sps-web-0	! Critical	Protected

- Select the notification to open the virtual machine selection page.
- Select the virtual machines you want to upgrade mobility service on, and select **OK**.



The Update Mobility Service job starts for each of the selected virtual machines.

NOTE

[Read more](#) on how to update the password for the account used to install Mobility Service.

Uninstall Mobility Service on a Windows Server computer

Use one of the following methods to uninstall Mobility Service on a Windows Server computer.

Uninstall by using the GUI

1. In Control Panel, select **Programs**.
2. Select **Microsoft Azure Site Recovery Mobility Service/Master Target server**, and then select **Uninstall**.

Uninstall at a command prompt

1. Open a command prompt window as an administrator.
2. To uninstall Mobility Service, run the following command:

```
MsiExec.exe /qn /x {275197FC-14FD-4560-A5EB-38217F80CBD1} /L+*V  
"C:\ProgramData\ASRSetupLogs\UnifiedAgentMSIUninstall.log"
```

Uninstall Mobility Service on a Linux computer

1. On your Linux server, sign in as a **root** user.
2. In a terminal, go to /user/local/ASR.
3. To uninstall Mobility Service, run the following command:

```
uninstall.sh -Y
```

Overview of failback

7/9/2018 • 3 minutes to read • [Edit Online](#)

After you have failed over to Azure, 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 failback 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 failback 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](#).

Support matrix for replication of VMware VMs and physical servers to a secondary site

7/9/2018 • 2 minutes to read • [Edit Online](#)

This article summarizes what's supported when you use the [Azure Site Recovery](#) service to replicate 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.

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
Windows Server	64-bit Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2 with at least SP1.
Linux	Red Hat Enterprise Linux 6.7, 6.8, 6.9, 7.1, 7.2 Centos 6.5, 6.6, 6.7, 6.8, 6.9, 7.0, 7.1, 7.2 Oracle Enterprise Linux 6.4, 6.5, 6.8 running the Red Hat compatible kernel, or Unbreakable Enterprise Kernel Release 3 (UEK3) SUSE Linux Enterprise Server 11 SP3, 11 SP4

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	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

CONFIGURATION	SUPPORTED
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
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	Learn about and download the latest Scout updates
Component updates	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. Learn more.

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

VMware VM/Physical server to VMware replication architecture

7/9/2018 • 2 minutes to read • [Edit Online](#)

This article describes the architecture and processes used when you replicate, fail over, and recover on-premises VMware virtual machines (VMs) or physical Windows/Linux servers to a secondary VMware site using [Azure Site Recovery](#).

Architectural components

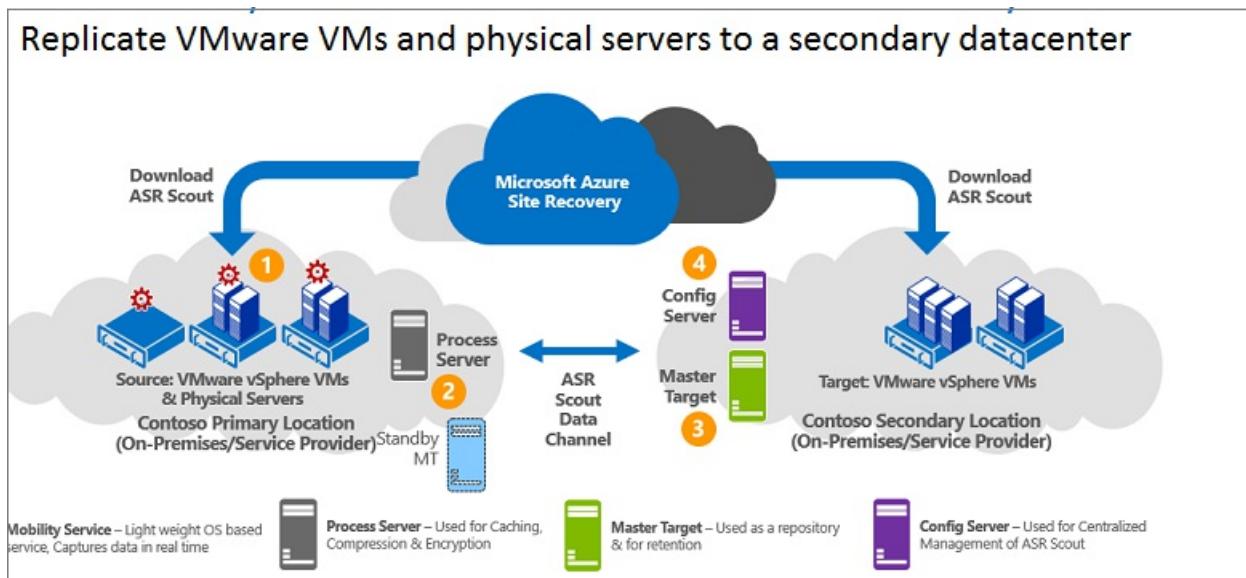
AREA	COMPONENT	DETAILS
Azure	You deploy this scenario using InMage Scout.	To obtain InMage Scout you need an Azure subscription. After you create a Recovery Services vault, you download InMage Scout and install the latest updates to set up the deployment.
Process server	Located in primary site	You deploy 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.](#)

Common questions - Hyper-V to Azure replication

8/16/2018 • 11 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 charges. 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.

Azure

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 regions?

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). 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 needs 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 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 public 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 [public 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 (public 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.

- During replication, VMs communicate with Site Recovery as follows:
 - VMs communicate with the configuration server on port HTTPS 443 for replication management.
 - VMs send replication data to the process server on port HTTPS 9443 (can be modified).
 - If you enable multi-VM consistency, VMs communicate with each other over port 20004.

Failover and failback

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.
- 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. 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 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.
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 Hyper-V replication to Azure

8/14/2018 • 5 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 2016 (including server core installation), Windows Server 2012 R2 with latest updates	<p>When you configure a Hyper-V site in Site Recovery, mixing hosts running Windows Server 2016 and 2012 R2 isn't supported.</p> <p>For VMs located on a host running Windows Server 2016, recovery to an alternate location isn't supported.</p>

SERVER	REQUIREMENTS	DETAILS
Hyper-V (running with Virtual Machine Manager)	Virtual Machine Manager 2016, Virtual Machine Manager 2012 R2	If Virtual Machine Manager is used, Windows Server 2016 hosts should be managed in Virtual Machine Manager 2016. A Virtual Machine Manager cloud that mixes Hyper-V hosts running on Windows Server 2016 and 2012 R2 isn't currently supported. Environments that include an upgrade of an existing Virtual Machine Manager 2012 R2 server to 2016 aren't supported.

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 reenable replication for the VM.
Add disk on replicated Hyper-V VM	Not supported. Disable replication, make the change, and then reenable 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	
Host network: VLAN	Yes	
Host network: IPv4	Yes	
Host network: IPv6	No	
Guest VM network: NIC Teaming	No	

COMPONENT	HYPER-V WITH VIRTUAL MACHINE MANAGER	HYPER-V WITHOUT VIRTUAL MACHINE MANAGER
Guest VM network: IPv4	Yes	
Guest VM network: IPv6	No	
Guest VM network: Static IP (Windows)	Yes	
Guest VM network: Static IP (Linux)	No	
Guest VM network: Multi-NIC	Yes	

Azure VM network configuration (after failover)

COMPONENT	HYPER-V WITH VIRTUAL MACHINE MANAGER	HYPER-V WITHOUT VIRTUAL MACHINE MANAGER
Azure ExpressRoute	Yes	Yes
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

STORAGE	HYPER-V WITH VIRTUAL MACHINE MANAGER	HYPER-V WITHOUT VIRTUAL MACHINE MANAGER
Multi-path (MPIO). Tested with: Microsoft DSM, EMC PowerPath 5.7 SP4 EMC PowerPath DSM for CLARiiON	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
EFI/UEFI	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	Yes	Yes
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
Cool storage	No	No
Hot storage	No	No
Block blobs	No	No
Encryption at rest (SSE)	Yes	Yes
Premium storage	Yes	Yes
Import/export service	No	No
Azure Storage firewalls for virtual networks configured on target storage/cache storage account (used to store replication data)	No	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	64-bit	Prerequisites check fails if unsupported.

Component	Requirements	Details
Operating system disk size	Up to 2,048 GB for generation 1 VMs.	Prerequisites check fails if unsupported.
	Up to 300 GB for generation 2 VMs.	
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 Virtual Machine Manager	Hyper-V without Virtual Machine Manager
Move vault across resource groups	No	No
Within and across subscriptions		
Move storage, network, Azure VMs across resource groups	No	No
Within and across subscriptions		

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 replication architecture

7/9/2018 • 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.

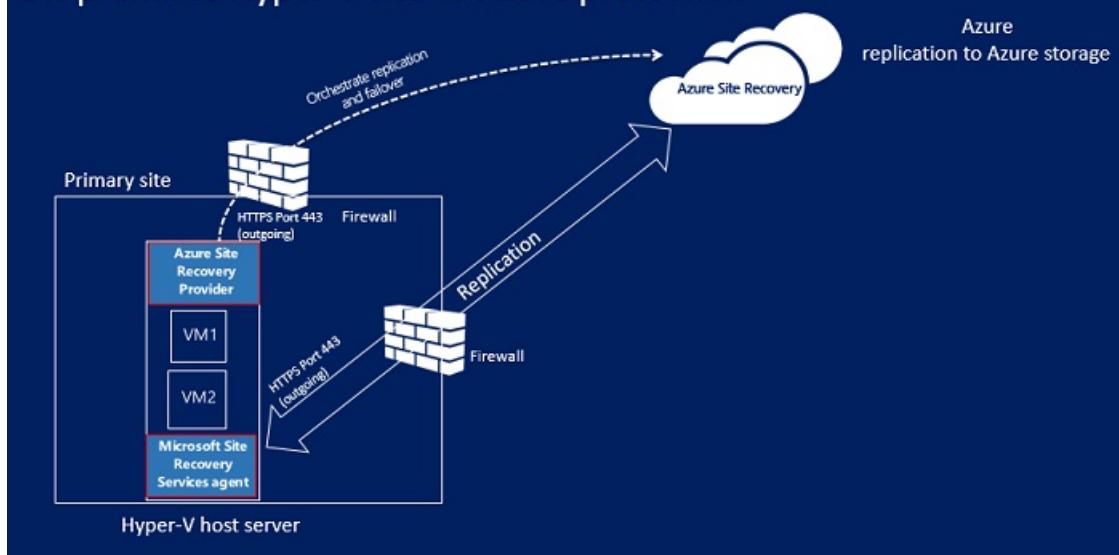
Architectural components - Hyper-V without VMM

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



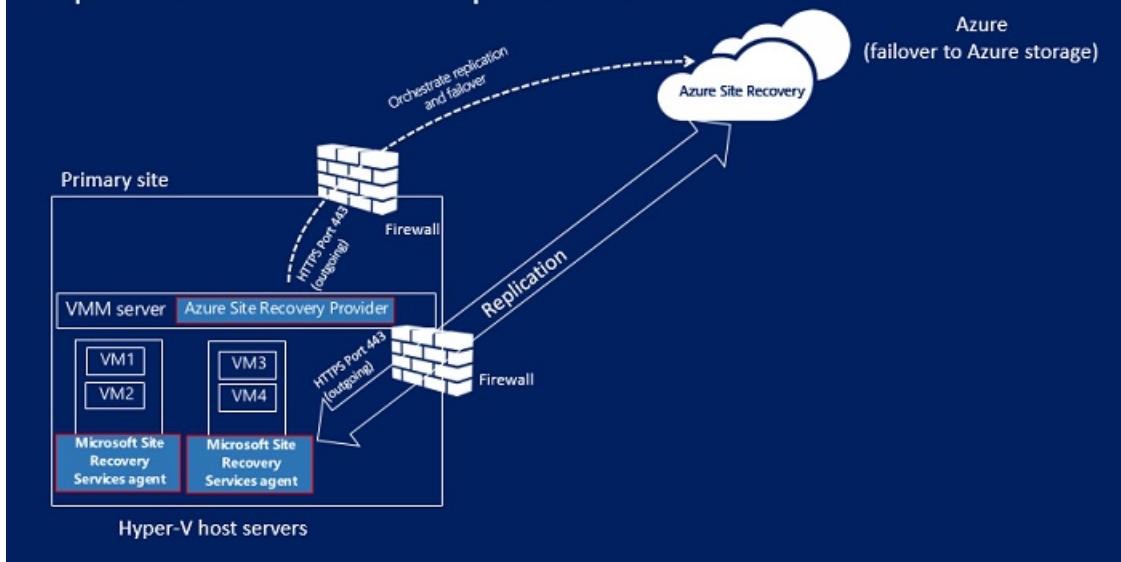
Architectural components - Hyper-V with VMM

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.

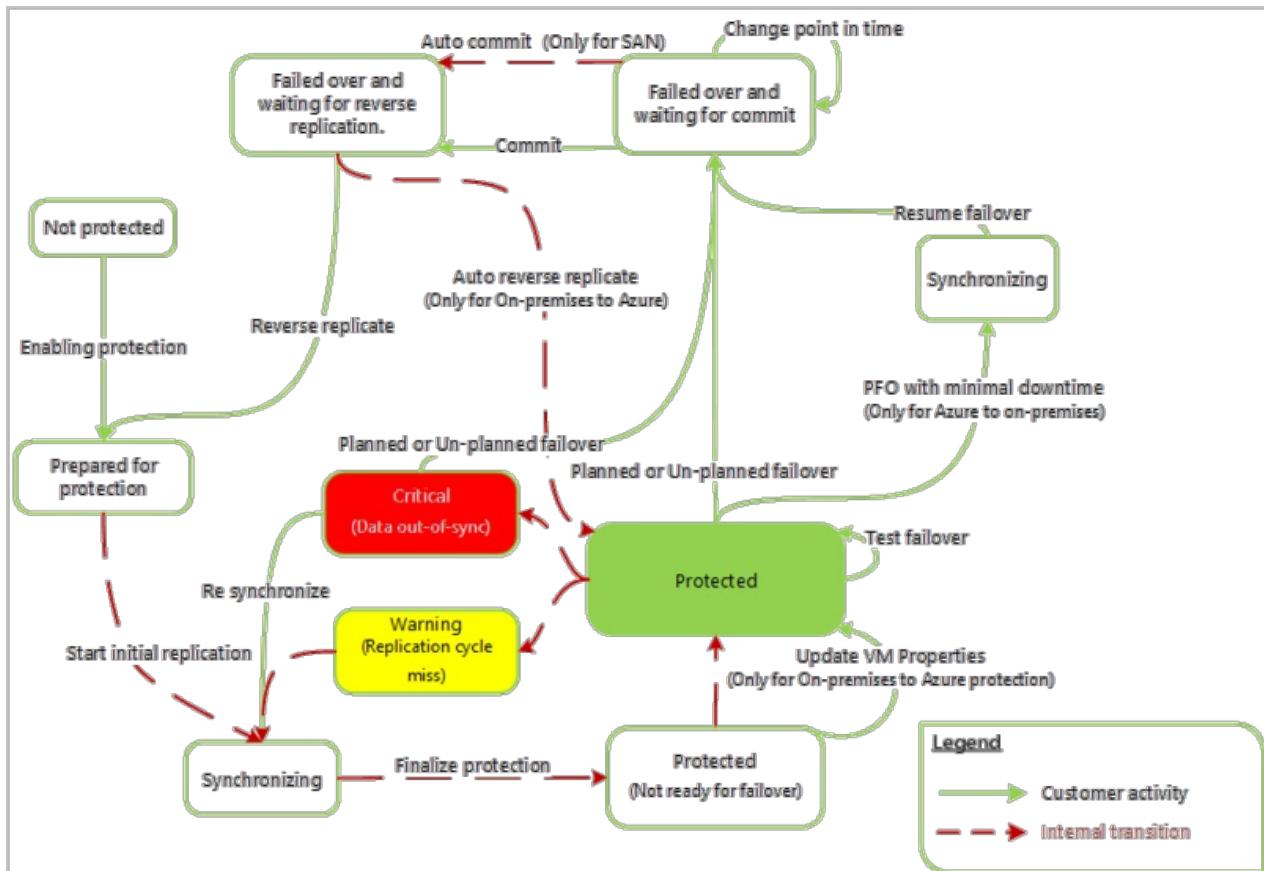
COMPONENT	REQUIREMENT	DETAILS
Azure	An Azure subscription, Azure storage account, and Azure network.	Replicated data from on-premises VM workloads is stored in the storage account. Azure VMs are created with the replicated data when failover from your on-premises site occurs. The Azure VMs connect to 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

- After you enable protection for a Hyper-V VM, in the Azure portal or on-premises, the **Enable protection** starts.
- The job checks that the machine complies with prerequisites, before invoking the [CreateReplicationRelationship](#), to set up replication with the settings you've configured.
- 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.
- You can monitor the job in the **Jobs** tab.

The screenshot shows the 'Jobs' section of the Site Recovery interface. At the top, there are buttons for 'Filter' and 'Export jobs'. A message indicates 'More than 200 jobs found. Please refine your query.' Below this is a table of job details:

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

Below the table, a specific job is selected: 'Enable protection' (Site Recovery Job). The properties for this job are shown in a detailed view:

Property	Value
Vault	robinnehraVault1
Protected item	VMmissingFO
Job id	843e1b28-ba5f-40b2-9327-a32aacff47e-2016-08-30 07:06:50Z-lbz ActivityId: da7fa882-5958-4ff8-a3e!
Source server	ronehrB2Asite101
Target server	Microsoft Azure

Under the 'Job' section, a table lists the steps of the replication process:

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

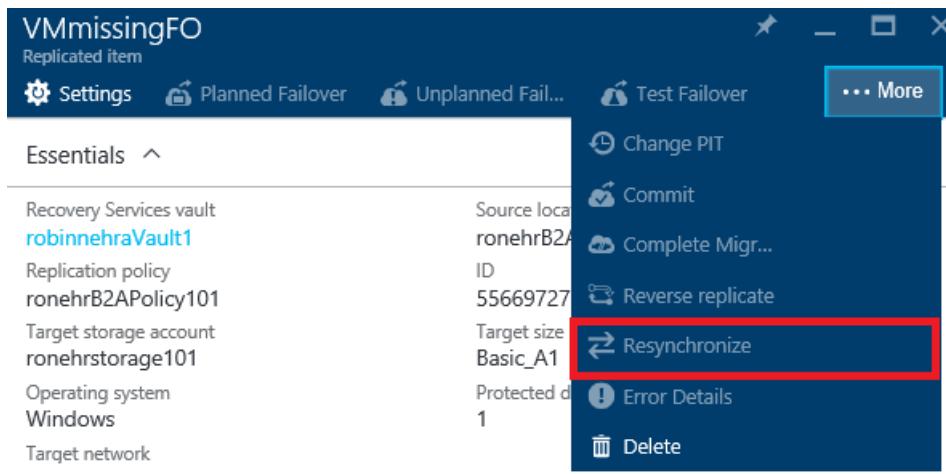
- After the initial replication, delta replication begins, in accordance with the replication policy.
- The Hyper-V Replica Replication Tracker tracks changes to a virtual hard disk as .hrl files. Each disk that's

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 fallback 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.

Support matrix for replication of Hyper-V VMs to a secondary site

7/9/2018 • 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
Gues 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](#)

Hyper-V replication to a secondary site

7/9/2018 • 2 minutes to read • [Edit Online](#)

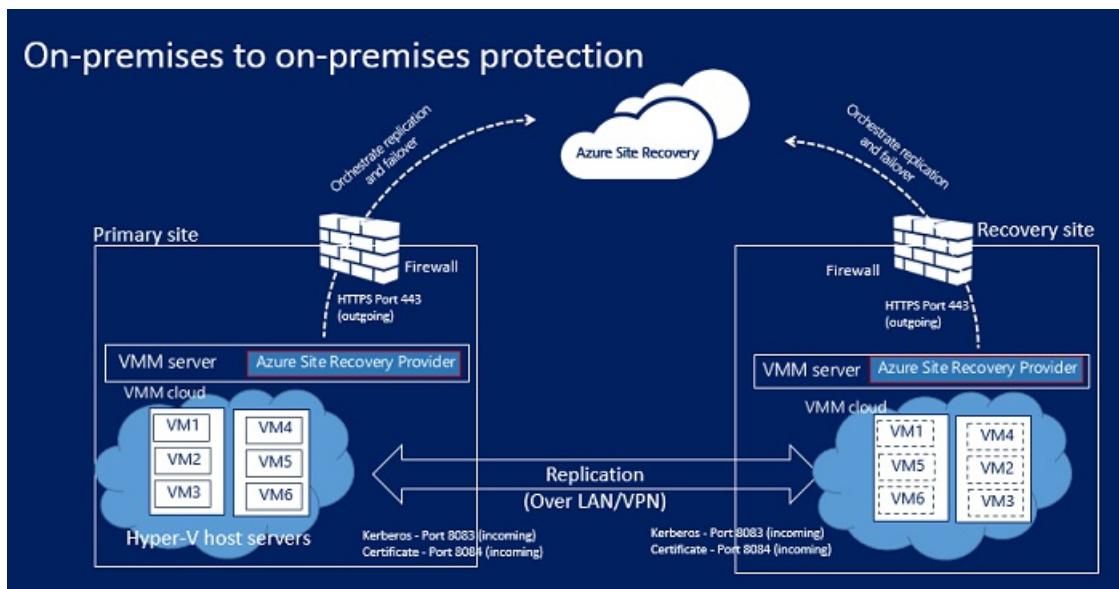
This article describes the components and processes involved when replicating on-premises Hyper-V virtual machines (VMs) in System Center Virtual Machine Manager (VMM) clouds, to a secondary VMM site using the [Azure Site Recovery](#) service in the Azure portal.

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.

Azure Traffic Manager with Azure Site Recovery

7/9/2018 • 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.

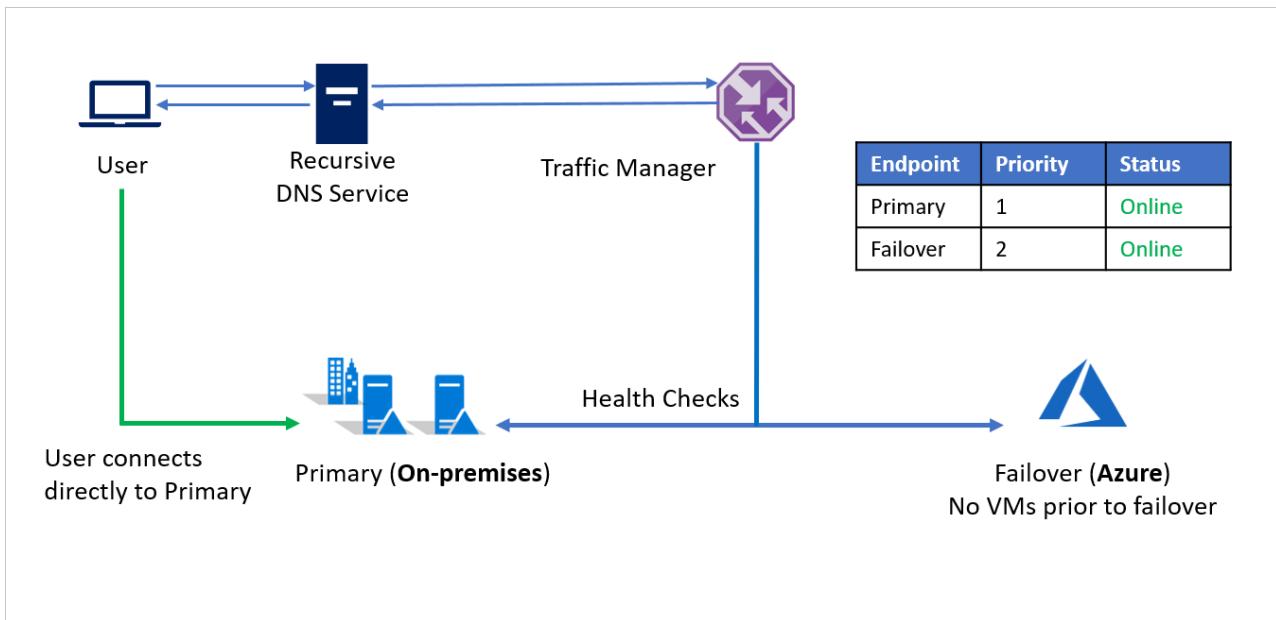
On-premises to Azure failover

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.

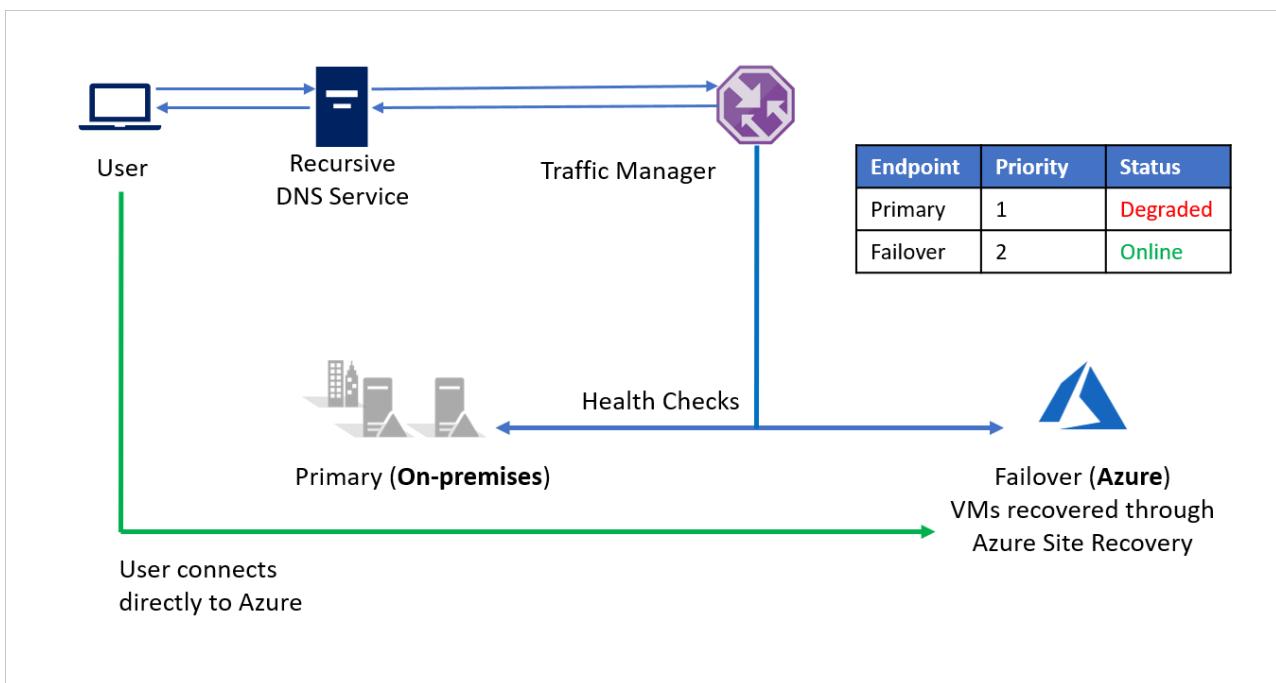
Company A is running applications with public endpoints and wants the ability to seamlessly redirect traffic to Azure in a disaster event. The [Priority](#) traffic-routing method in Azure Traffic Manager allows Company A to easily implement this failover pattern.

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.

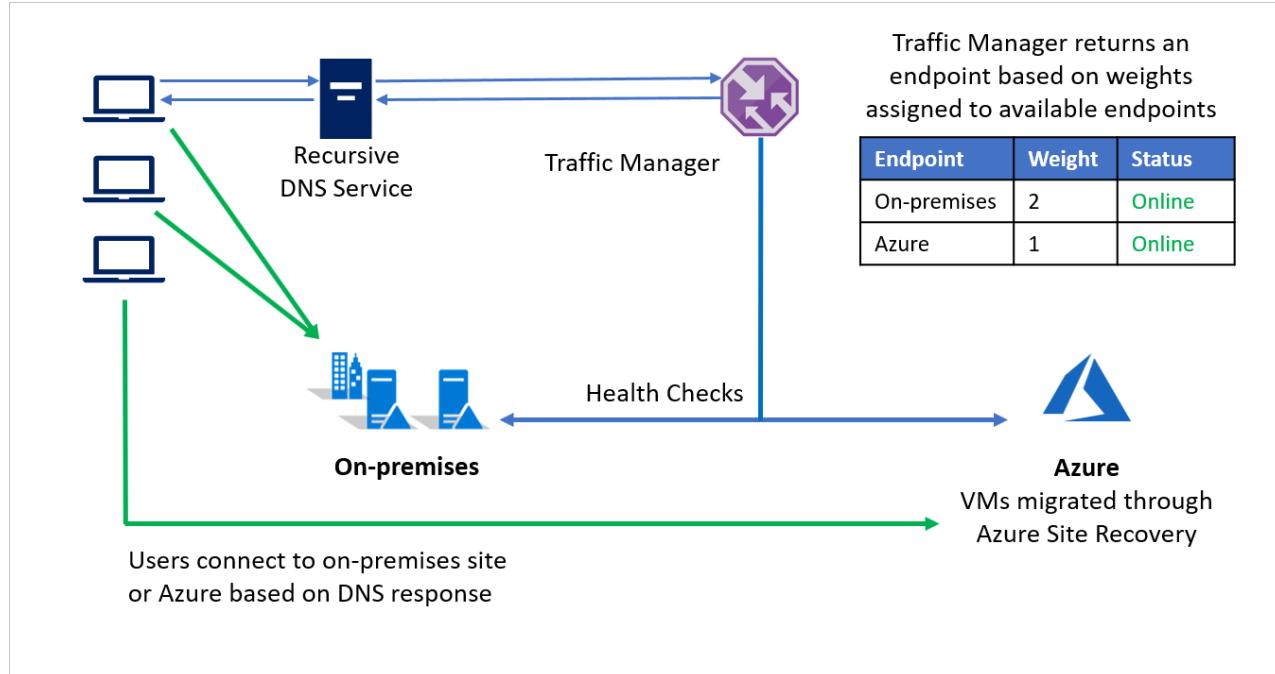
On-premises to Azure migration

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.

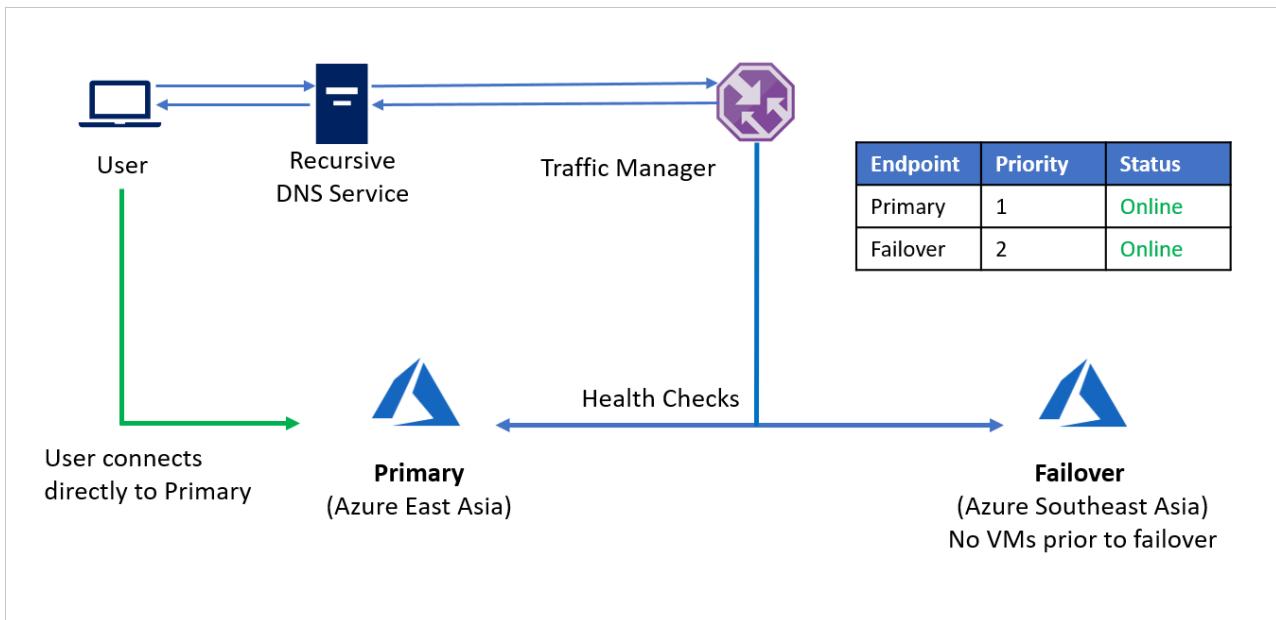
Azure to Azure failover

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.

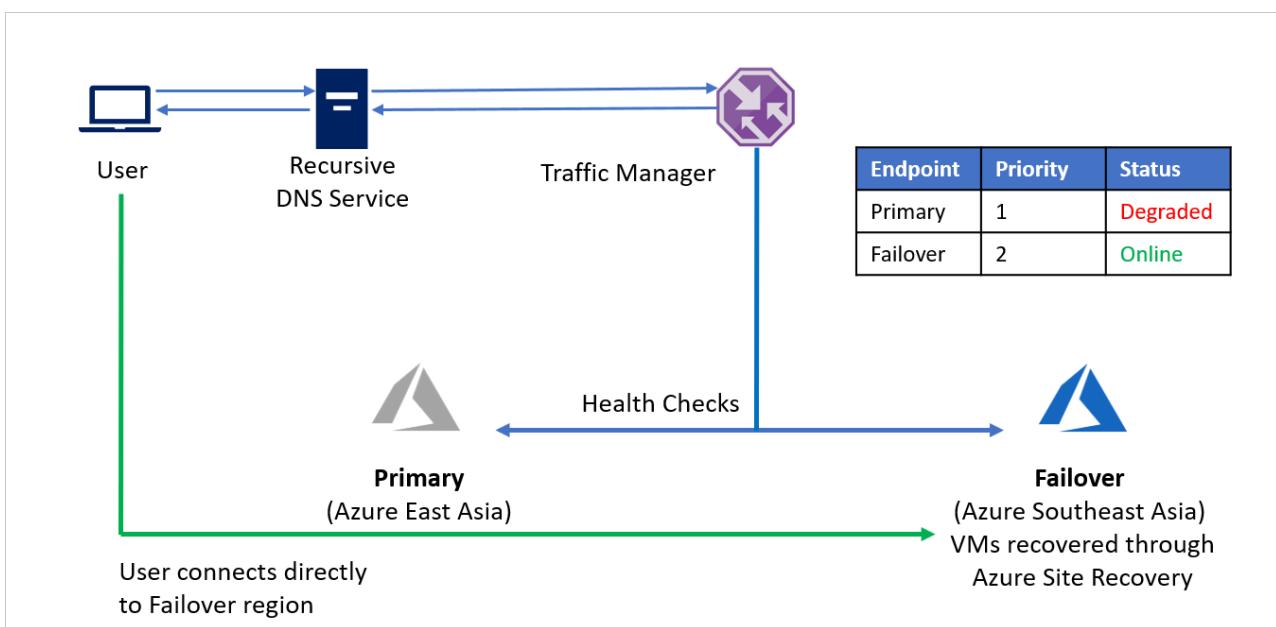
Company C is running applications with public endpoints and wants the ability to seamlessly redirect traffic to a different Azure region in a disaster event. The [Priority](#) traffic-routing method allows **Company C** to easily implement this failover pattern.

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.

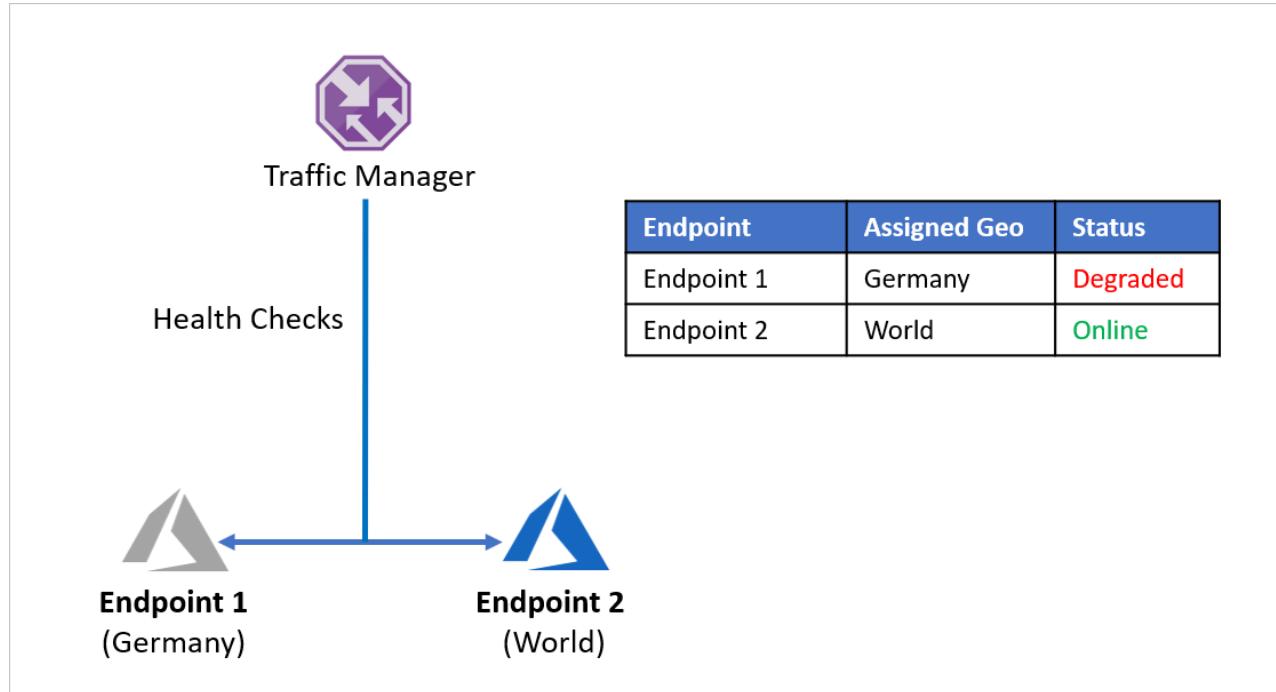
Protecting multi-region enterprise applications

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 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

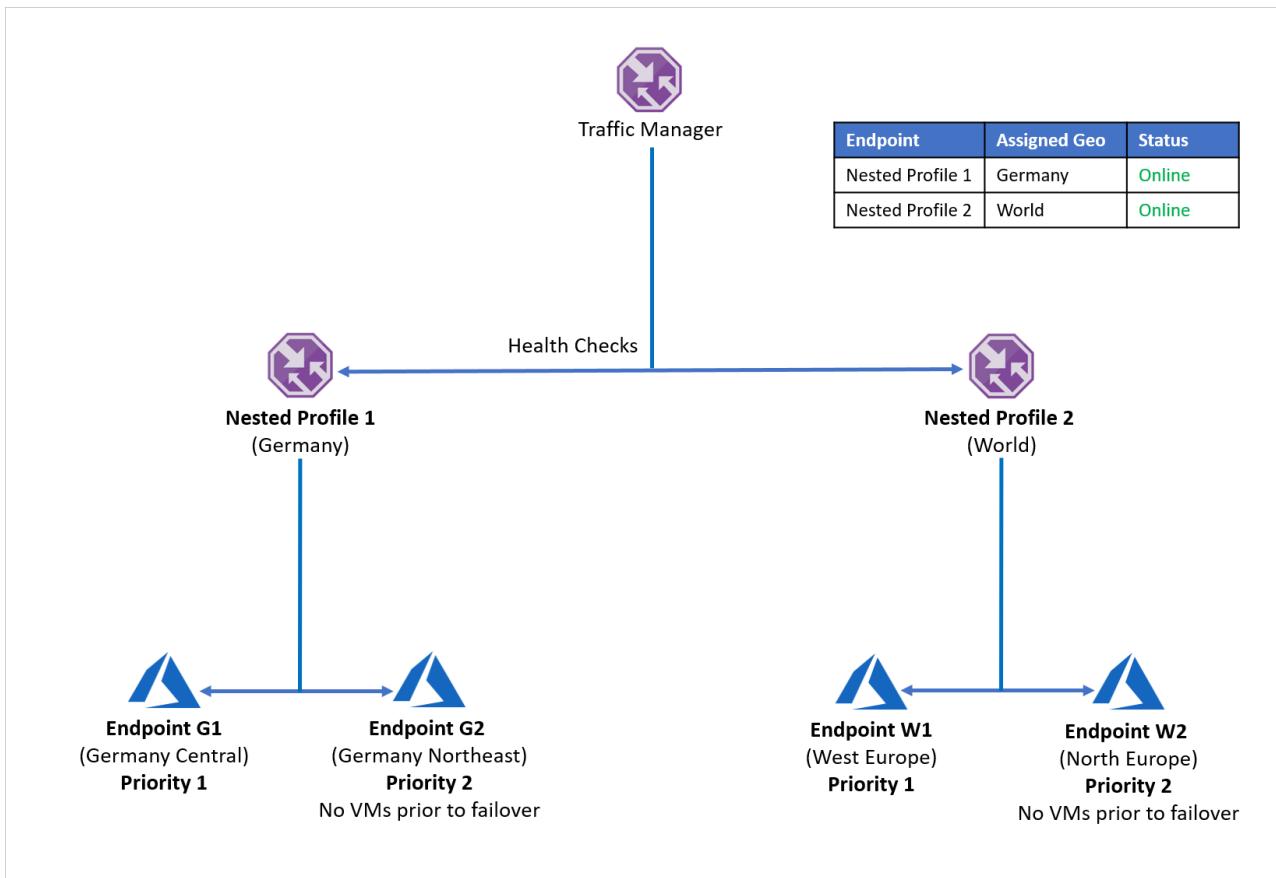
traffic originating from Germany is directed to **Endpoint 1** and any traffic originating outside Germany is directed to **Endpoint 2**.

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

7/9/2018 • 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](#).

ExpressRoute routing domains

An ExpressRoute circuit has multiple routing domains associated with it:

- [Azure Private peering](#) - Azure compute services, namely virtual machines (IaaS), and cloud services (PaaS) that are deployed within a virtual network can be connected through the private peering domain. The private peering domain is considered a trusted extension of your core network into Microsoft Azure.
- [Azure Public peering](#) - Services such as Azure Storage, SQL databases, and Websites are offered on public IP addresses. You can privately connect to services hosted on public IP addresses, including VIPs of your cloud services, through the public peering routing domain. Public peering has been deprecated for new creations and Microsoft Peering should be used instead for Azure PaaS services.
- [Microsoft peering](#) - Connectivity to Microsoft online services (Office 365, Dynamics 365, and Azure PaaS services) is through the Microsoft peering. Microsoft peering is the recommended routing domain to connect to Azure PaaS services.

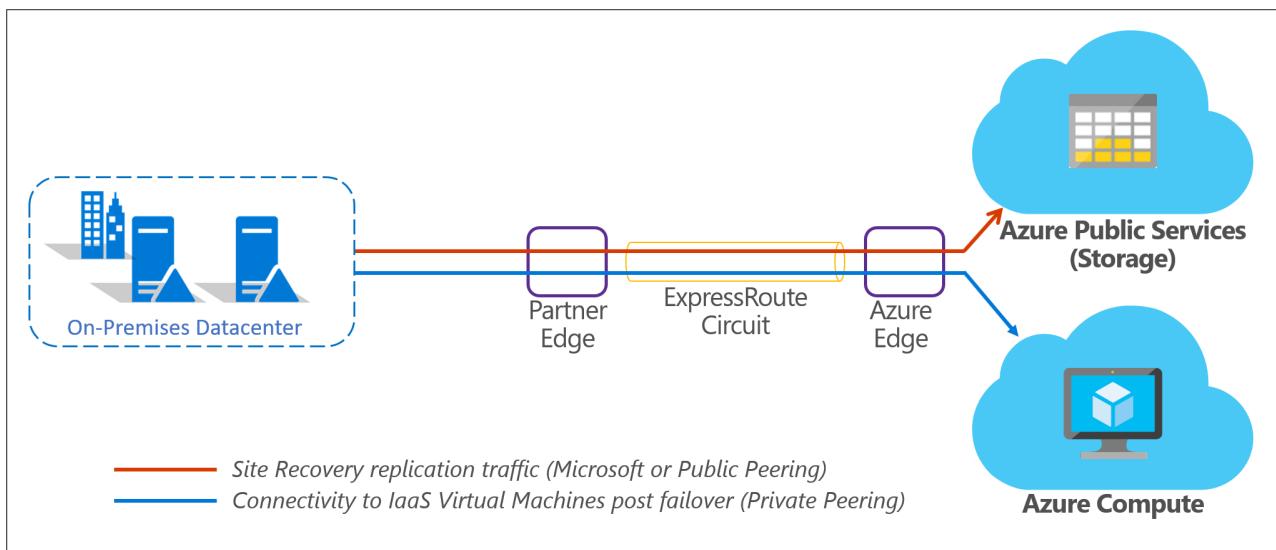
Learn more about and compare ExpressRoute routing domains [here](#).

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 over a public endpoint. To use ExpressRoute for Site Recovery replication, you can utilize [public peering](#) or [Microsoft peering](#). Microsoft peering is the recommended routing domain for replication. After virtual machines or servers fail over to an Azure virtual network, you can access them using [private peering](#). Replication is not supported over 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](#).

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

7/9/2018 • 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.

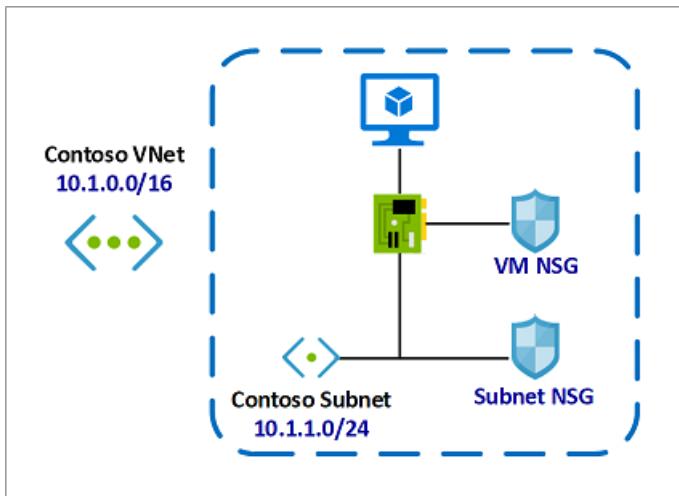
This article describes how you can use Network Security Groups with Azure Site Recovery.

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 NGs 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 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 NGs 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.

What workloads can you protect with Azure Site Recovery?

7/23/2018 • 8 minutes to read • [Edit Online](#)

This article describes workloads and applications you can replicate 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) and Oracle Data Guard.
- 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 app-specific testing.

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
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
Pooled Virtual Desktop (unmanaged)	No	Yes	No	Yes	No	Yes	No
Pooled Virtual Desktop (managed and without UPD)	No	Yes	No	Yes	No	Yes	No
Remote applications and Desktop sessions (without UPD)	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 recovery plans

7/9/2018 • 4 minutes to read • [Edit Online](#)

This article describes recovery plans in [Azure Site Recovery](#).

A recovery plan gathers machines into recovery groups. 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.

Why use a recovery plan?

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. Use recovery plans to:

- Model an app around its dependencies.
- Automate recovery tasks to reduce RTO.
- Verify that you're prepared for migration or disaster recovery by ensuring that your apps are part of a recovery plan.
- Run test failover 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 where 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

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

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.

Test failover

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.

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 the video

Watch a quick example video showing a on-click failover for a two-tier WordPress app.

Next steps

- [Create](#) a recovery plan.
- Learn about [running failovers](#).

About migration

7/23/2018 • 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.

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](#)

Use Role-Based Access Control to manage Site Recovery access

7/9/2018 • 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.

RESOURCE TYPE	DEPLOYMENT MODEL	PERMISSION
Compute	Resource Manager	Microsoft.Compute/availabilitySets/read

RESOURCE TYPE	DEPLOYMENT MODEL	PERMISSION
		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
		Microsoft.Network/virtualNetworks/subnets/join/action
	Classic	Microsoft.ClassicNetwork/virtualNetworks/read
		Microsoft.ClassicNetwork/virtualNetworks/join/action

RESOURCE TYPE	DEPLOYMENT MODEL	PERMISSION
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.

Azure Site Recovery: frequently asked questions (FAQ)

7/9/2018 • 10 minutes to read • [Edit Online](#)

This article includes frequently asked questions about Azure Site Recovery. If you have questions after reading this article, post them on the [Azure Recovery Services Forum](#).

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](#).

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.

Can I replicate Azure VMs?

Yes, you can replicate supported Azure VMs between Azure regions. [Learn more](#).

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](#).

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.

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 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 physical servers can I protect?

You can replicate physical servers running Windows and Linux to Azure or to a secondary site. Learn about requirements for [replication to Azure](#), and [replication to a secondary site](#).

Note that physical servers will run as VMs in Azure if your on-premises server goes down. Failback to an on-premises physical server isn't currently supported. For a machine protected as physical, you can only failback to a VMware virtual machine.

What VMware VMs can I protect?

To protect VMware VMs you'll need a vSphere hypervisor, and virtual machines running VMware tools. We also recommend that you have a VMware vCenter server to manage the hypervisors. Learn more about requirements for [replication to Azure](#), or [replication to a secondary site](#).

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.

Pricing

For pricing related questions, please refer to the FAQ at [Azure Site Recovery pricing](#).

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.

Replication

Can I replicate over a site-to-site VPN to Azure?

Azure Site Recovery replicates data to an Azure storage account, over a public endpoint. Replication isn't over a

site-to-site VPN. You can create a site-to-site VPN, with an Azure virtual network. This doesn't interfere with Site Recovery replication.

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 Account over a public endpoint. You need to set up [public peering](#) or [Microsoft peering](#) to use ExpressRoute for Site Recovery replication. Microsoft peering is the recommended routing domain for replication. 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. Replication is not supported over private peering.

Are there any prerequisites for replicating virtual machines to Azure?

[VMware VMs](#) and [Hyper-V VMs](#) you want to replicate to Azure should comply with Azure requirements.

Your Azure user account needs to have certain [permissions](#) to enable replication of a new virtual 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. [Read more](#).

If I replicate to Azure how do I pay for Azure VMs?

During regular replication, data is replicated to geo-redundant Azure storage and you don't need to pay any Azure IaaS virtual machine charges, providing a significant advantage. When you run a failover to Azure, Site Recovery automatically creates Azure IaaS virtual machines, and after that you'll be billed for the compute resources that you consume in Azure.

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](#)

If I replicate to Azure what kind of 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. 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.

How often can I replicate data?

- **Hyper-V:** Hyper-V VMs can be replicated every 30 seconds (except for premium storage), 5 minutes or 15 minutes. If you've set up SAN replication then replication is synchronous.
- **VMware and 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. They are also supported when

replicating VMware VMs and physical machines to Azure. The operating system disk must be a basic disk.

Can I add a new machine to an existing replication group?

Adding new machines to existing replication groups is supported. To do so, select the replication group (from 'Replicated items' blade) and right click/select context menu on the replication group and select the appropriate option.

The screenshot shows the 'Replicated items' blade in the Azure portal. It displays a list of replicated machines with columns for NAME, TARGET LOCATION, TARGET STORAGE, TARGET NETWORK, LAST DATA SYNC, and DATA CHANGE RATE. Two machines are listed under 'grp1 (3 machines)': W-MDS-02 and W-MDS-03. A context menu is open over the 'grp1 (3 machines)' row, with options: 'Pin to dashboard', 'Add virtual machine' (which is highlighted), and 'Add physical machine'.

NAME	TARGET LOCATION	TARGET STORAGE	TARGET NETWORK	LAST DATA SYNC	DATA CHANGE RATE	...
V2A-w2K12-651	Microsoft Azure	mmrstorage	ASRCanaryTestS...	19/10/2016, 12:1...	3064.2149434771	...
V2A-w2K12-652	Microsoft Azure	mmrstorage	ASRCanaryTestS...	19/10/2016, 12:1...	3026.0719214848	...
▶ grp1 (3 machines)	-	-	-	-	-	...
W-MDS-02	Microsoft Azure	madhavips	InMageS2SVPNS...	30/6/2016, 12:35...	0	
W-MDS-03	Microsoft Azure	madhavips	InMageS2SVPNS...	7/7/2016, 1:09:58...	0	
W-MDS-04	Microsoft Azure	madhavips	-	9/7/2016, 8:35:44...	499.53112945557	...

Can I throttle bandwidth allotted for Hyper-V replication traffic?

Yes. You can read more about throttling bandwidth in the deployment 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 virtual machines after failover?

You can access the 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](#)

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 the need arises. 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 failover back to a different host?

Yes, you can use the alternate location recovery to fallback to a different host from Azure. Read more about the options in the below links for VMware and Hyper-V virtual machines.

- [For VMware virtual machines](#)
- [For Hyper-V virtual machines](#)

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 an Azure storage account 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.

Next steps

- Read the [Site Recovery overview](#)
- Learn about [Site Recovery architecture](#)

About networking in Azure to Azure replication

7/9/2018 • 4 minutes to read • [Edit Online](#)

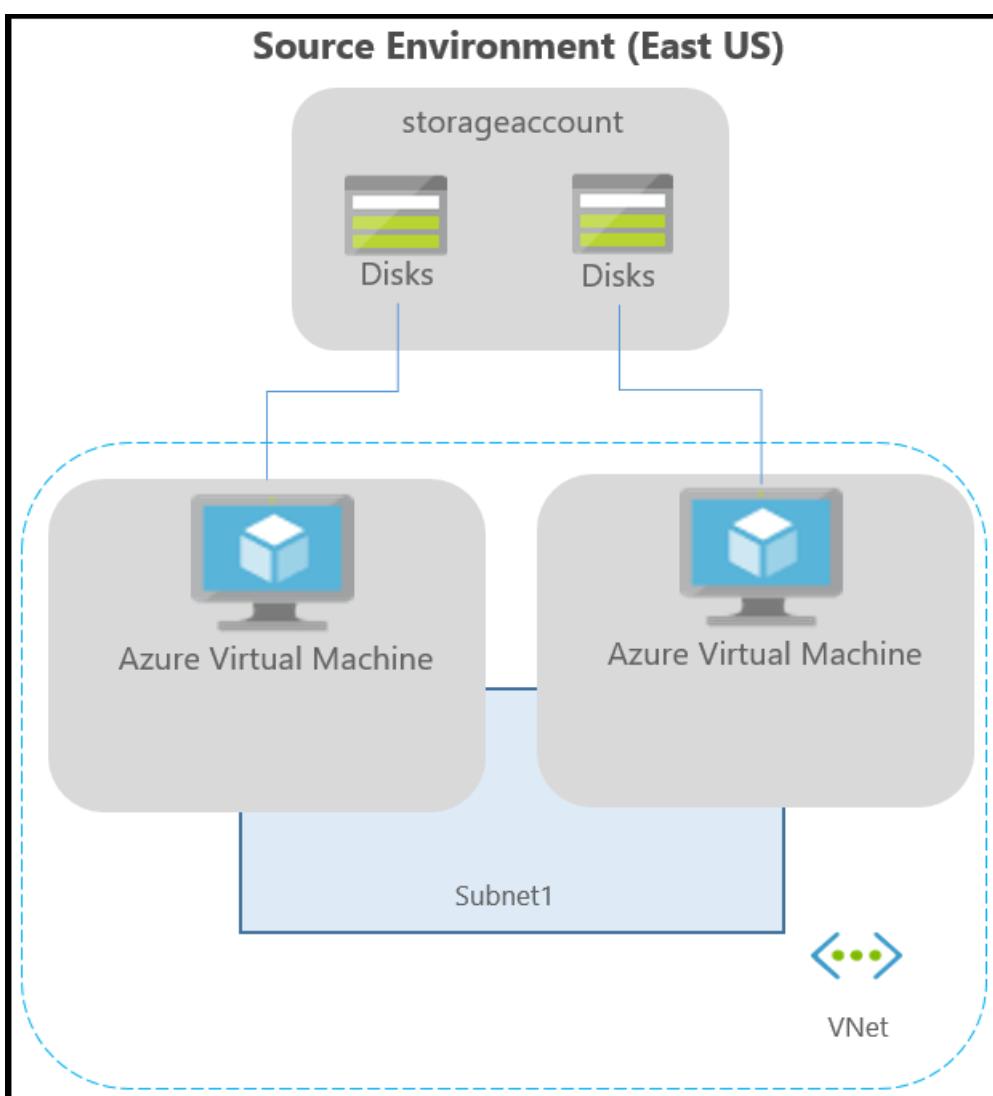
This article provides networking guidance when you're replicating and recovering Azure VMs from one region to another, using [Azure Site Recovery](#).

Before you start

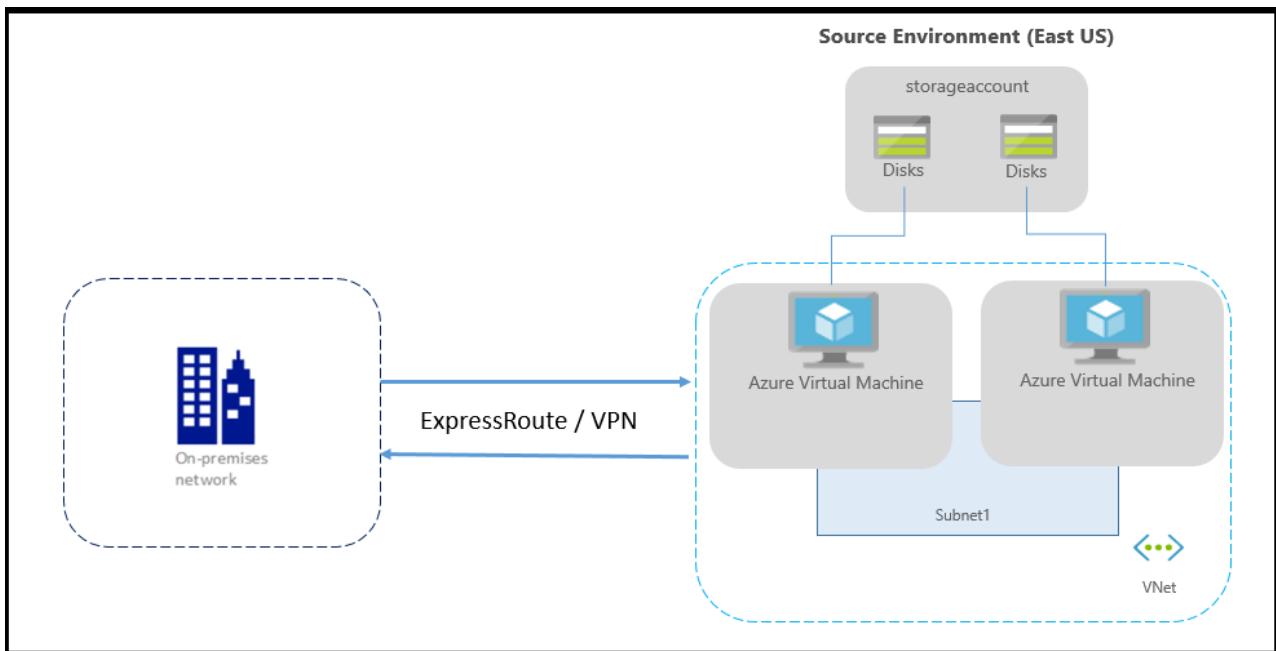
Learn how Site Recovery provides disaster recovery for [this scenario](#).

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.
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 IP-based firewall proxy, or NSG rules to control outbound connectivity, these IP ranges 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.
- All IP address ranges that correspond to Office 365 [authentication and identity IP V4 endpoints](#).

- If new addresses are added to the Office 365 ranges in the future, you need to create new NSG rules.
- Site Recovery service endpoint IP addresses - available in an [XML file](#) and depend on your target location.
- You can [download and use this script](#), to automatically create the required rules on the NSG.
- 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.

Site Recovery IP address ranges are as follows:

TARGET	SITE RECOVERY IP	SITE RECOVERY MONITORING IP
East Asia	52.175.17.132	13.94.47.61
Southeast Asia	52.187.58.193	13.76.179.223
Central India	52.172.187.37	104.211.98.185
South India	52.172.46.220	104.211.224.190
North Central US	23.96.195.247	168.62.249.226
North Europe	40.69.212.238	52.169.18.8
West Europe	52.166.13.64	40.68.93.145
East US	13.82.88.226	104.45.147.24
West US	40.83.179.48	104.40.26.199
South Central US	13.84.148.14	104.210.146.250
Central US	40.69.144.231	52.165.34.144
East US 2	52.184.158.163	40.79.44.59
Japan East	52.185.150.140	138.91.1.105
Japan West	52.175.146.69	138.91.17.38
Brazil South	191.234.185.172	23.97.97.36
Australia East	104.210.113.114	191.239.64.144
Australia Southeast	13.70.159.158	191.239.160.45
Canada Central	52.228.36.192	40.85.226.62
Canada East	52.229.125.98	40.86.225.142
West Central US	52.161.20.168	13.78.149.209
West US 2	52.183.45.166	13.66.228.204

TARGET	SITE RECOVERY IP	SITE RECOVERY MONITORING IP
UK West	51.141.3.203	51.141.14.113
UK South	51.140.43.158	51.140.189.52
UK South 2	13.87.37.4	13.87.34.139
UK North	51.142.209.167	13.87.102.68
Korea Central	52.231.28.253	52.231.32.85
Korea South	52.231.298.185	52.231.200.144
France Central	52.143.138.106	52.143.136.55
France South	52.136.139.227	52.136.136.62

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

2. Create outbound HTTPS (443) rules for all IP address ranges that correspond to Office 365 [authentication and identity IP V4 endpoints](#).
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 outbound HTTPS (443) rules for all IP address ranges that correspond to Office 365 [authentication and identity IP V4 endpoints](#).
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

Network virtual appliance configuration

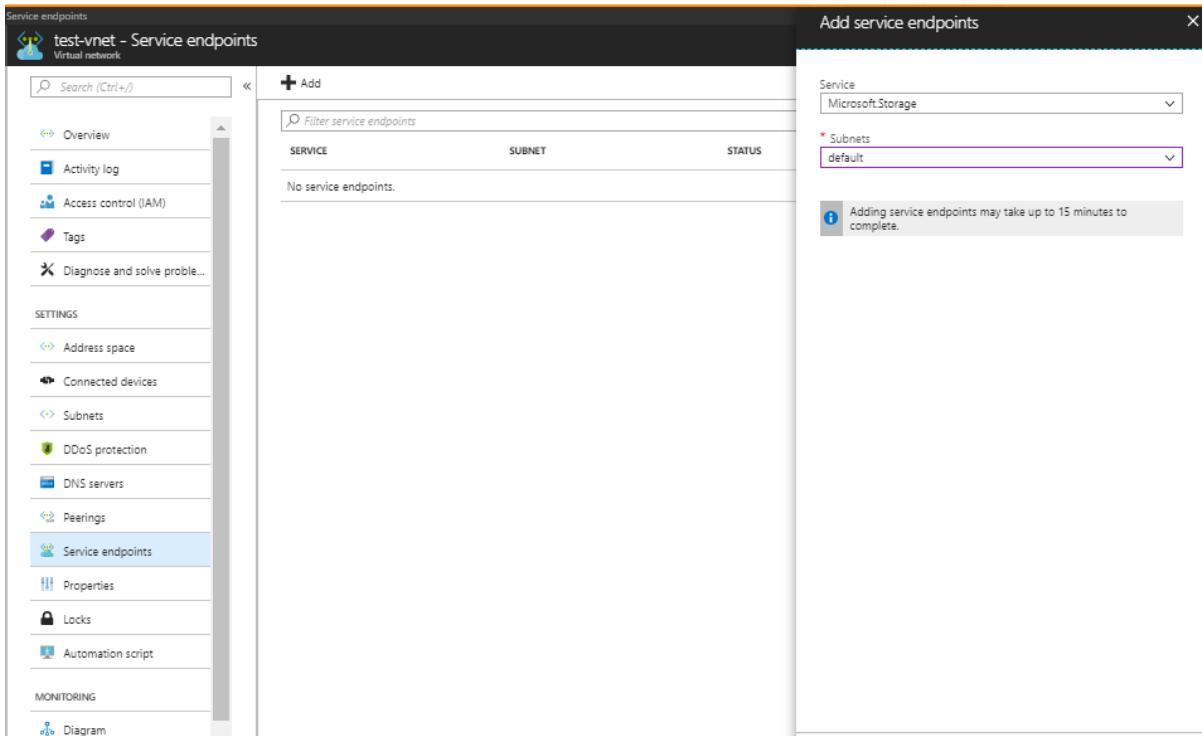
If you are using network virtual appliances (NVAs) to control outbound network traffic from VMs, the appliance

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](#).

Map virtual networks in different Azure regions

8/9/2018 • 4 minutes to read • [Edit Online](#)

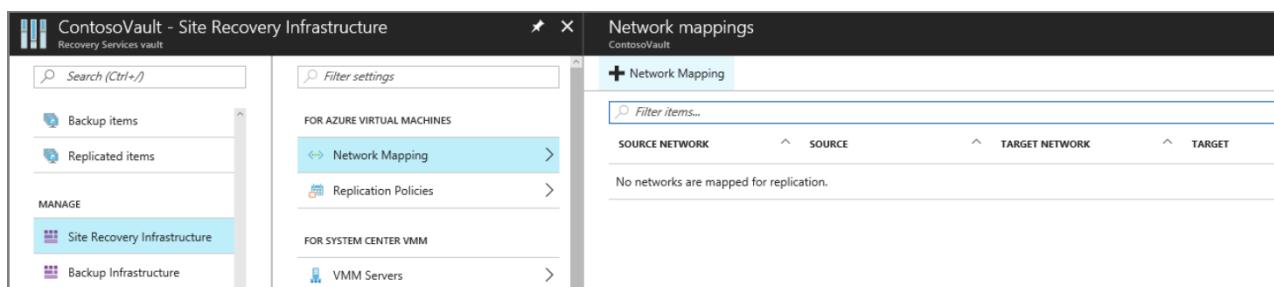
This article describes how to map two instances of Azure Virtual Network located in different Azure regions with each other. Network mapping ensures that when a replicated virtual machine is created in the target Azure region, the virtual machine is also created on the virtual network that's mapped to the virtual network of the source virtual machine.

Prerequisites

Before you map networks, ensure that you have created an [Azure virtual network](#) in both the source region and the target Azure region.

Map virtual networks

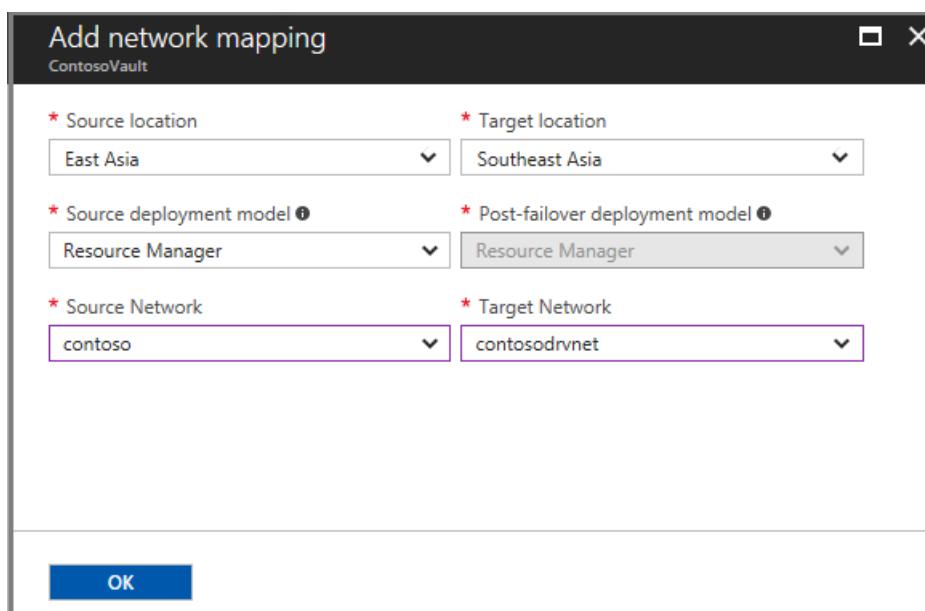
To map an Azure virtual network that's located in one Azure region (source network) to a virtual network that's located in another region (target network), for Azure virtual machines, go to **Site Recovery Infrastructure > Network Mapping**. Create a network mapping.



The screenshot shows the 'ContosoVault - Site Recovery Infrastructure' interface. On the left, there's a navigation sidebar with 'Search (Ctrl+J)', 'Backup items', 'Replicated items', 'MANAGE' (selected), 'Site Recovery Infrastructure' (highlighted in blue), and 'Backup Infrastructure'. The main area has a 'FOR AZURE VIRTUAL MACHINES' section with 'Network Mapping' and 'Replication Policies' options. Below that is a 'FOR SYSTEM CENTER VMM' section with 'VMM Servers' option. To the right, the 'Network mappings' page is displayed under 'ContosoVault'. It has a header with '+ Network Mapping' and a search bar. A table below shows columns for 'SOURCE NETWORK', 'TARGET NETWORK', and 'TARGET'. A message at the bottom states 'No networks are mapped for replication.'

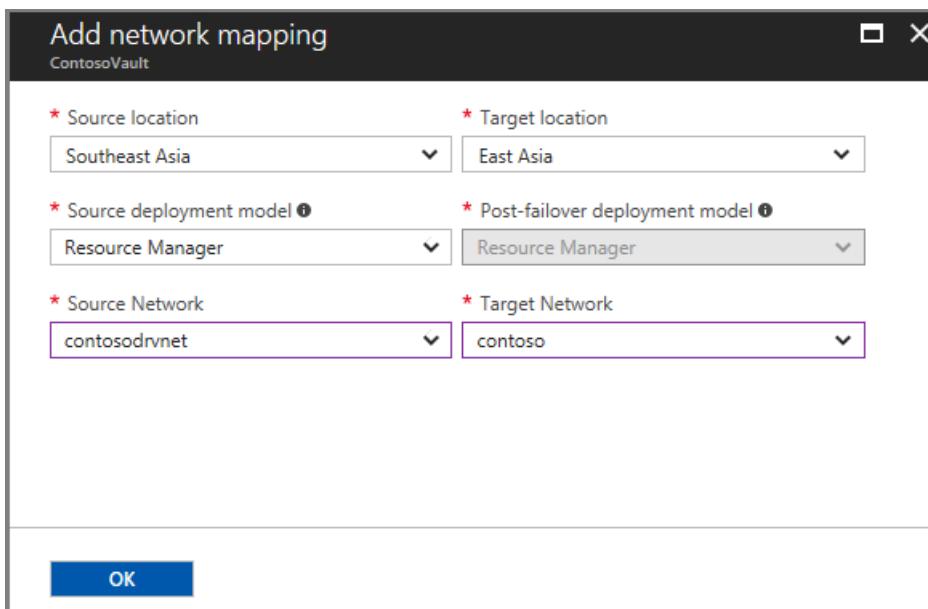
In the following example, the virtual machine is running in the East Asia region. The virtual machine is being replicated to the Southeast Asia region.

To create a network mapping from the East Asia region to the Southeast Asia region, select the location of the source network and the location of the target network. Then, select **OK**.



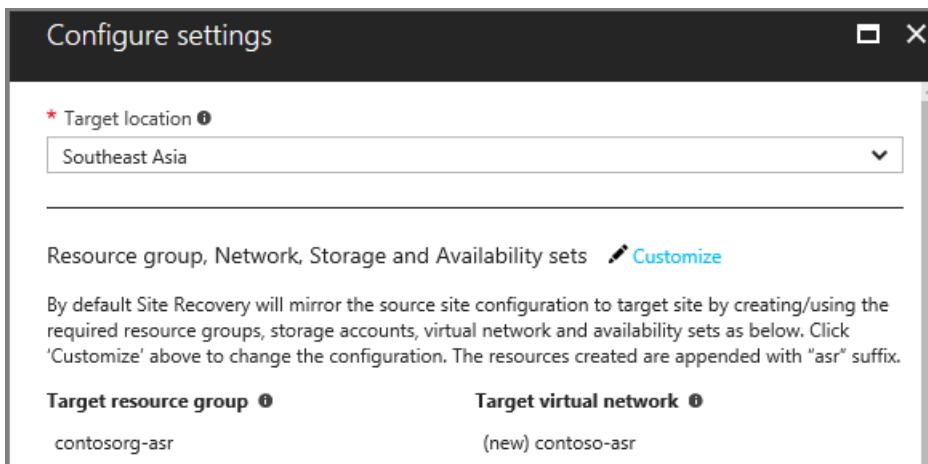
The dialog box is titled 'Add network mapping' and is associated with 'ContosoVault'. It contains four pairs of dropdown menus for 'Source location' (East Asia) and 'Target location' (Southeast Asia), 'Source deployment model' (Resource Manager) and 'Post-failover deployment model' (Resource Manager), 'Source Network' (contoso) and 'Target Network' (contosodrvnet). At the bottom is a blue 'OK' button.

Repeat the preceding process to create a network mapping from the Southeast Asia region to the East Asia region.

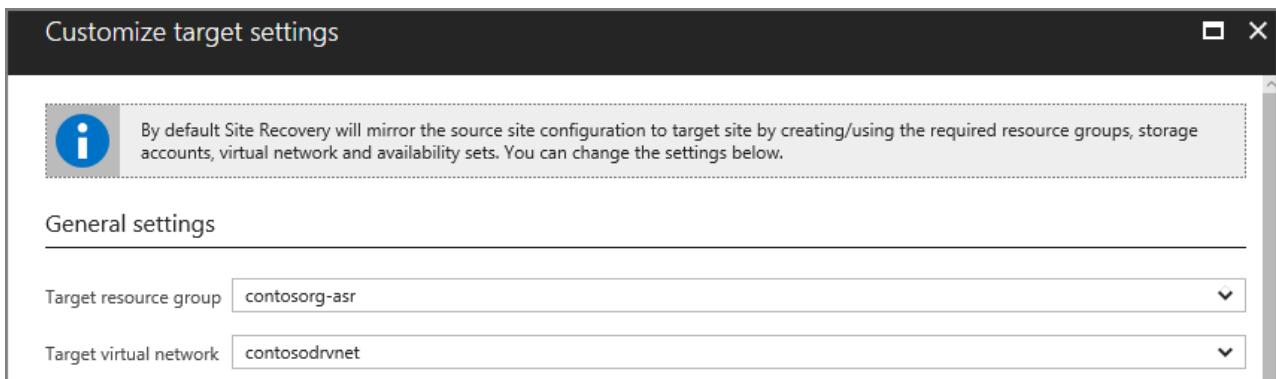


Map a network when you enable replication

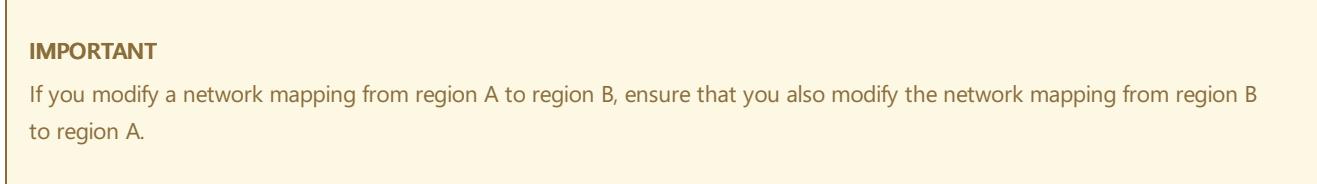
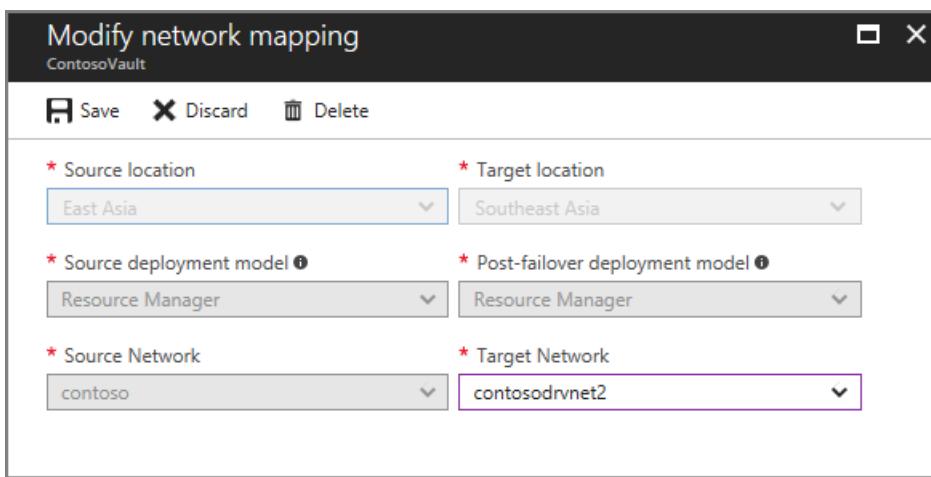
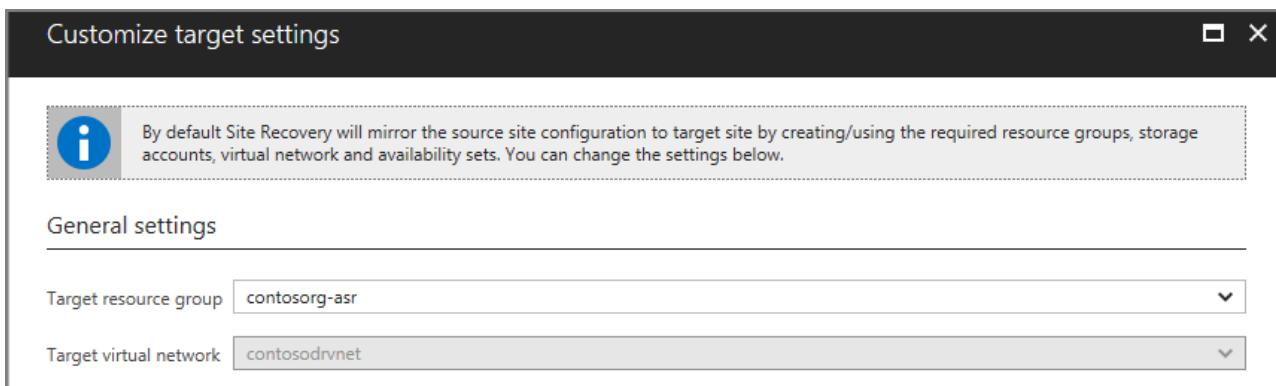
When you replicate a virtual machine from one Azure region to another region for the first time, if no network mapping exists, you can set the target network when you set up replication. Based on this setting, Azure Site Recovery creates network mappings from the source region to the target region, and from the target region to the source region.



By default, Site Recovery creates a network in the target region that is identical to the source network. Site Recovery creates a network by adding **-asr** as a suffix to the name of the source network. To choose a network that has already been created, select **Customize**.



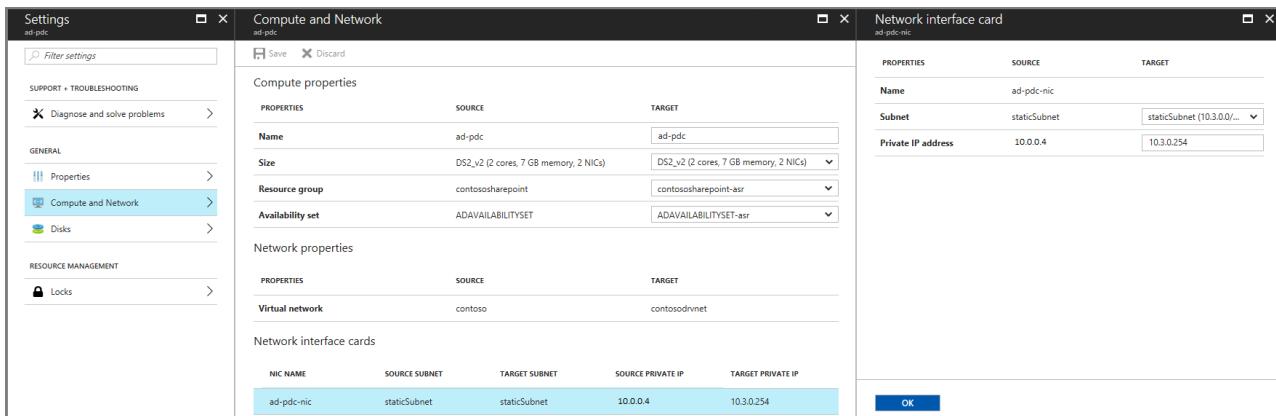
If network mapping has already occurred, you can't change the target virtual network when you enable replication. In this case, to change the target virtual network, modify the existing network mapping.



Subnet selection

The subnet of the target virtual machine is selected based on the name of the subnet of the source virtual machine. If a subnet that has the same name as the source virtual machine is available in the target network, that subnet is set for the target virtual machine. If a subnet with the same name doesn't exist in the target network, the alphabetically first subnet is set as the target subnet.

To modify the subnet, go to the **Compute and Network** settings for the virtual machine.



IP address

The IP address for each network interface of the target virtual machine is set as described in the following sections.

DHCP

If the network interface of the source virtual machine uses DHCP, the network interface of the target virtual machine is also set to use DHCP.

Static IP address

If the network interface of the source virtual machine uses a static IP address, the network interface of the target virtual machine is also set to use a static IP address. The following sections describe how a static IP address is set.

IP assignment behavior during Failover

1. Same address space

If the source subnet and the target subnet have the same address space, the IP address of the network interface of the source virtual machine is set as the target IP address. If the same IP address is not available, the next available IP address is set as the target IP address.

2. Different address spaces

If the source subnet and the target subnet have different address spaces, the next available IP address in the target subnet is set as the target IP address.

IP assignment behavior during Test Failover

1. If the target network chosen is the production vNet

- The recovery IP (Target IP) will be a static IP but it **will not be the same IP address** as reserved for Failover.
- The assigned IP address will be the next available IP from the end of the subnet address range.
- For e.g., if Source VM static IP is configured to be: 10.0.0.19 and Test Failover was attempted with the configured production network: **dr-PROD-nw**, with subnet range as 10.0.0.0/24.
The failed-over VM would be assigned with - The next available IP from the end of the subnet address range that is: 10.0.0.254

Note: The terminology **production vNet** is referred to the 'Target network' mapped during the disaster recovery configuration.

2. If the target network chosen is not the production vNet but has the same subnet range as production network

- The recovery IP (Target IP) will be a static IP with the **same IP address** (i.e., configured static IP address) as reserved for Failover. Provided the same IP address is available.
- If the configured static IP is already assigned to some other VM/device, then the recovery IP will be the next available IP from the end of the subnet address range.
- For e.g., if Source VM static IP is configured to be: 10.0.0.19 and Test Failover was attempted with a test network: **dr-NON-PROD-nw**, with same subnet range as production network - 10.0.0.0/24.
The failed-over VM would be assigned with following static IP
 - configured static IP: 10.0.0.19 if IP is available.
 - Next available IP: 10.0.0.254 if the IP address 10.0.0.19 is already in use.

To modify the target IP on each network interface, go to the **Compute and Network** settings for the virtual machine.

As a best practice it is always suggested to choose a test network to perform Test Failover.

Next steps

- Review [networking guidance for replicating Azure virtual machines](#).

IP address retention for Azure virtual machine failover

7/9/2018 • 7 minutes to read • [Edit Online](#)

Azure Site Recovery enables disaster recovery for Azure VMs. When failing over from one Azure region to another, customers often require retention of their IP configurations. Site Recovery, by default, mimics source virtual network and subnet structure when creating these resources on the target region. For Azure VMs configured with static private IP addresses, Site Recovery also makes a best effort attempt to provision the same private IP on the target VM, if that IP is not already blocked by an Azure resource or a replicated VM.

For simple applications, the above default configuration is all that is needed. For more complex enterprise applications, customers may need to provision additional networking resources to ensure post-failover connectivity with other components of their infrastructure. This article explains the networking requirements for failing over Azure VMs from one region to another while retaining VM IP addresses.

Azure-to-Azure connectivity

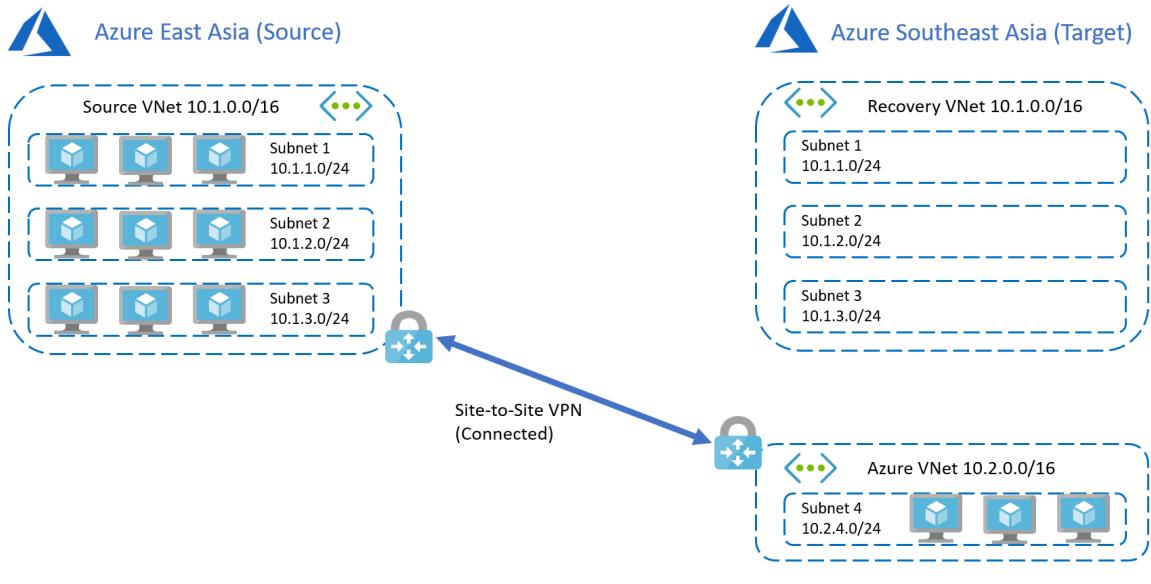
For the first scenario, we consider **Company A** that has all its application infrastructure running in Azure. For business continuity and compliance reasons, **Company A** decides to use Azure Site Recovery to protect its applications.

Given the requirement of IP retention (such as for application bindings), Company A has the same virtual network and subnet structure on the target region. To further reduce recovery time objective (RTO), **Company A** utilizes replica nodes for SQL Always ON, domain controllers, etc. and these replica nodes are placed in a different virtual network on the target region. Using a different address space for the replica nodes enables **Company A** to establish VPN site-to-site connectivity between source and target regions, which would otherwise not be possible if the same address space is used at both ends.

Here's what the network architecture looks like before failover:

- Application VMs are hosted in Azure East Asia, utilizing an Azure virtual network with address space 10.1.0.0/16. This virtual network is named **Source VNet**.
- Application workloads are split across three subnets – 10.1.1.0/24, 10.1.2.0/24, 10.1.3.0/24, respectively named **Subnet 1, Subnet 2, Subnet 3**.
- Azure Southeast Asia is the target region and has a recovery virtual network that mimics the address space and subnet configuration on source. This virtual network is named **Recovery VNet**.
- Replica nodes such as those needed for Always On, domain controller, etc. are placed in a virtual network with address space 10.2.0.0/16 inside Subnet 4 with address 10.2.4.0/24. The virtual network is named **Azure VNet** and is on Azure Southeast Asia.
- **Source VNet** and **Azure VNet** are connected through VPN site-to-site connectivity.
- **Recovery VNet** is not connected with any other virtual network.
- **Company A** assigns/verifies target IP address for replicated items. For this example, target IP is the same as source IP for each VM.

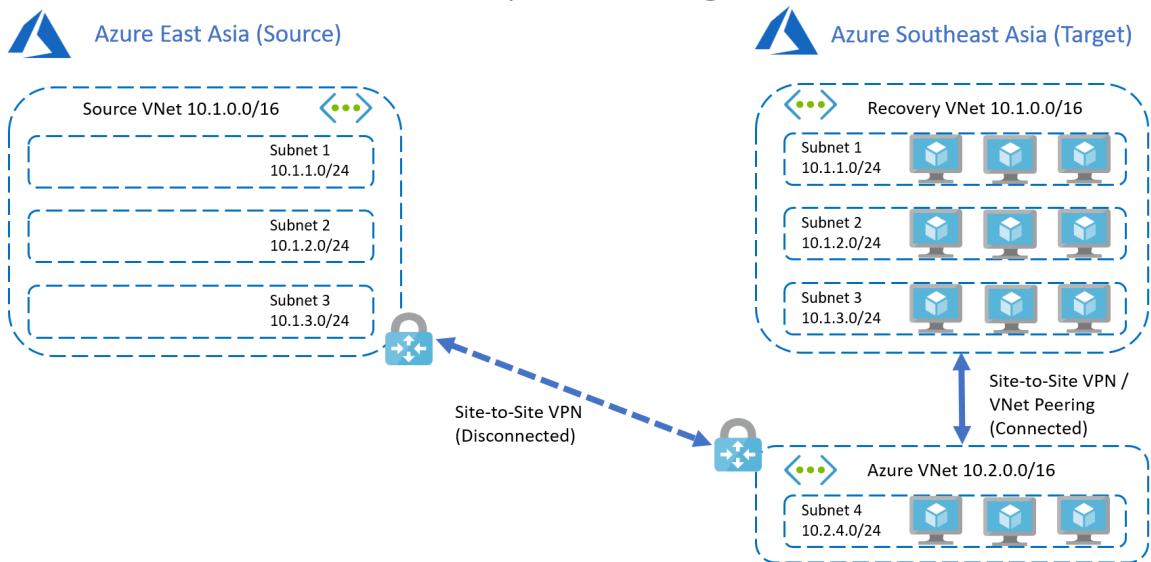
Azure to Azure connectivity – Before failover



Full region failover

In the event of a regional outage, **Company A** can recover its entire deployment quickly and easily using Azure Site Recovery's powerful [recovery plans](#). Having already set the target IP address for each VM prior to failover, **Company A** can orchestrate failover and automate connection establishment between Recovery VNet and Azure Vnet as shown in the below diagram.

Azure to Azure connectivity – Full region failover



Depending on application requirements, connections between the two VNets on the target region can be established before, during (as an intermediate step) or after failover. Use [recovery plans](#) to add scripts and define the failover order.

Company A also has the choice of using VNet peering or Site-to-Site VPN to establish connectivity between Recovery VNet and Azure VNet. VNet peering does not use a VPN gateway and has different constraints. Additionally, [VNet peering pricing](#) is calculated differently than [VNet-to-VNet VPN Gateway pricing](#). For failovers, it is generally advisable to mimic source connectivity, including connection type, to minimize unpredictable incidents arising out of network changes.

Isolated application failover

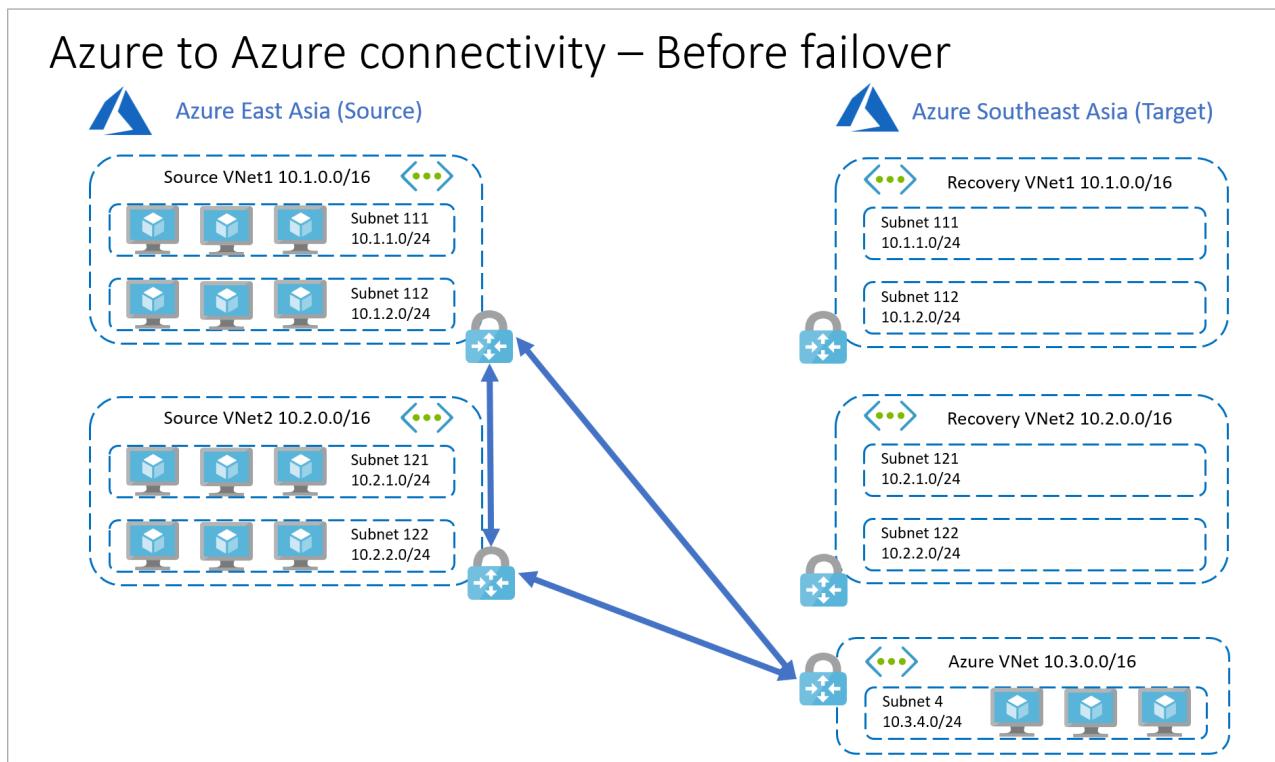
Under certain conditions users might need to failover parts of their application infrastructure. One such example is failing over a specific application or tier that is housed within a dedicated subnet. While a subnet failover with IP retention is possible, it is not advisable for most situations, as it substantially increases connectivity inconsistencies. You will also lose subnet connectivity to other subnets within the same Azure virtual network.

A better way to account for subnet-level application failover requirements is to use different target IP addresses for failover (if connectivity is required to other subnets on source virtual network) or isolate each application in its own dedicated virtual network on source. With the latter approach you can establish inter-network connectivity on the source and emulate the same when failing over to the target region.

To architect individual applications for resiliency, it is advised to house an application in its own dedicated virtual network and establish connectivity between these virtual networks as required. This allows for isolated application failover while retaining original private IP addresses.

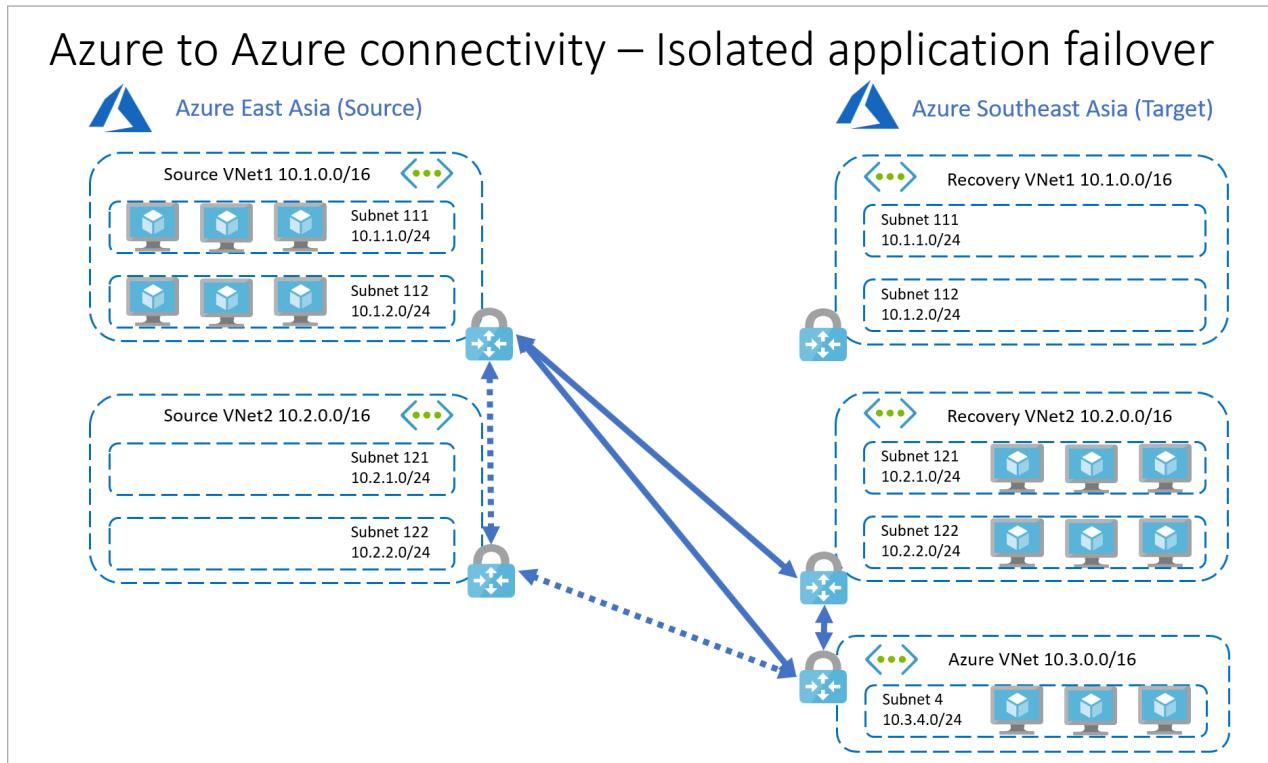
The pre-failover configuration then looks as follows:

- Application VMs are hosted in Azure East Asia, utilizing an Azure virtual network with address space 10.1.0.0/16 for the first application and 10.2.0.0/16 for the second application. The virtual networks are named **Source VNet1** and **Source VNet2** for the first and second application, respectively.
- Each VNet is further split into two subnets each.
- Azure Southeast Asia is the target region and has recovery virtual networks Recovery VNet1 and Recovery VNet2.
- Replica nodes such as those needed for Always On, domain controller, etc. are placed in a virtual network with address space 10.3.0.0/16 inside **Subnet 4** with address 10.3.4.0/24. The virtual network is called Azure VNet and is on Azure Southeast Asia.
- **Source VNet1** and **Azure VNet** are connected through VPN site-to-site connectivity. Similarly, **Source VNet2** and **Azure VNet** are also connected through VPN site-to-site connectivity.
- **Source VNet1** and **Source VNet2** are also connected through S2S VPN in this example. Since the two VNets are in the same region, VNet peering can also be used instead of S2S VPN.
- **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.



In the event of a disaster situation that affects only one application (in this example housed in Source VNet2), Company A can recover the affected application as follows:

- VPN connections between **Source VNet1** and **Source VNet2**, and between **Source VNet2** and **Azure VNet** are disconnected.
- VPN connections are established between **Source VNet1** and **Recovery VNet2**, and between **Recovery VNet2** and **Azure VNet**.
- VMs from **Source VNet2** are failed over to **Recovery VNet2**.



The above isolated failover 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.

Further considerations

VPN Gateways utilize public IP addresses and gateway hops to establish connections. If you do not want to use public IP, and/or want to avoid extra hops, you can use Azure [Virtual Network peering](#) to peer virtual networks across [supported Azure regions](#).

On-premises-to-Azure connectivity

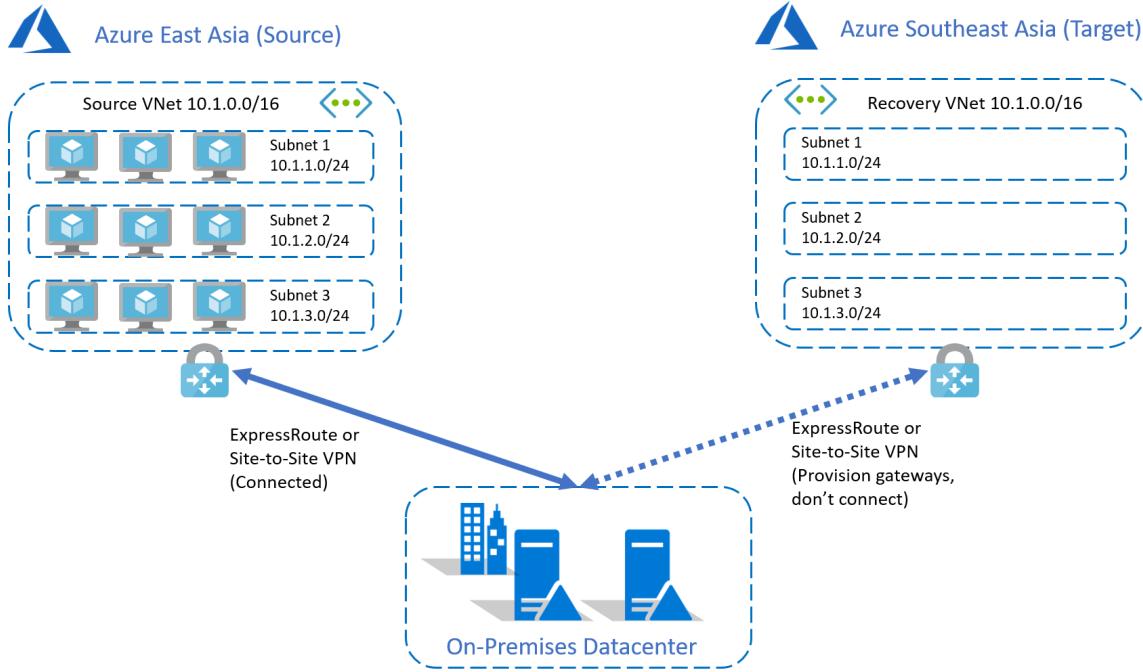
For the second scenario, we consider **Company B** that has a part of its application infrastructure running on Azure and the remainder running on-premises. For business continuity and compliance reasons, **Company B** decides to use Azure Site Recovery to protect its applications running in Azure.

Here's what the network architecture looks like before failover:

- Application VMs are hosted in Azure East Asia, utilizing an Azure virtual network with address space 10.1.0.0/16. This virtual network is named **Source VNet**.
- Application workloads are split across three subnets – 10.1.1.0/24, 10.1.2.0/24, 10.1.3.0/24, respectively named **Subnet 1**, **Subnet 2**, **Subnet 3**.
- Azure Southeast Asia is the target region and has a recovery virtual network that mimics the address space and subnet configuration on source. This virtual network is named **Recovery VNet**.
- VMs in Azure East Asia are connected to on-premises datacenter through ExpressRoute or Site-to-Site VPN.

- To reduce recovery time objective (RTO), Company B provisions gateways on Recovery VNet in Azure Southeast Asia prior to failover.
- **Company B** assigns/verifies target IP address for replicated items. For this example, target IP is the same as source IP for each VM

On-premises to Azure connectivity – Before failover

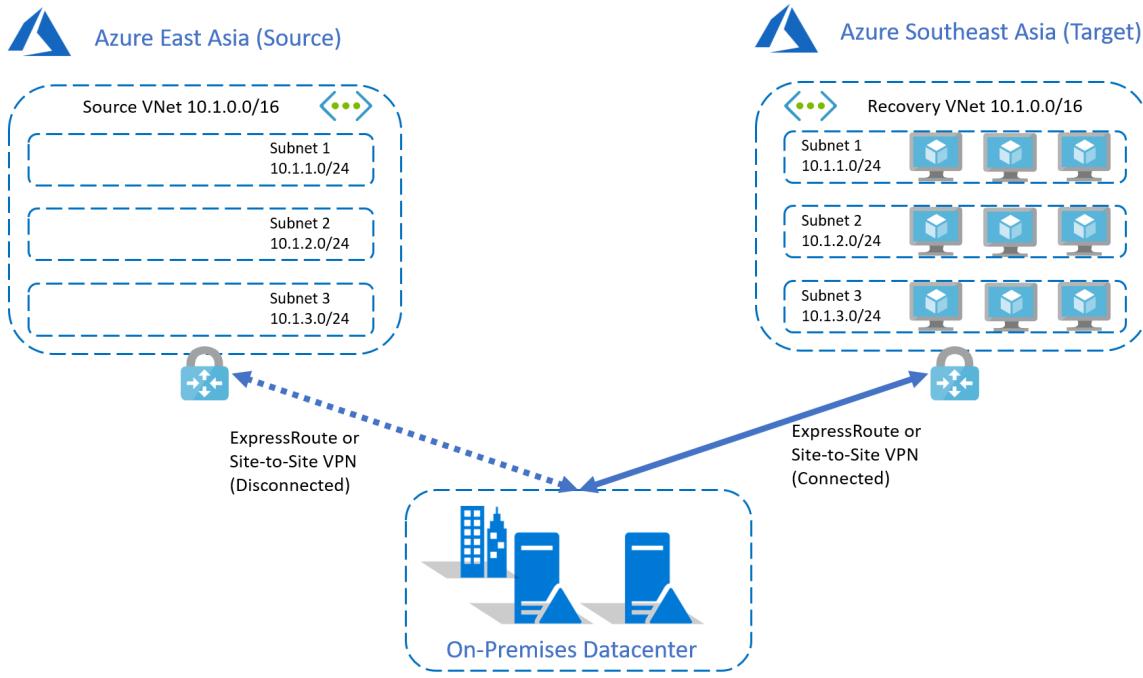


Full region failover

In the event of a regional outage, **Company B** can recover its entire deployment quickly and easily using Azure Site Recovery's powerful [recovery plans](#). Having already set the target IP address for each VM prior to failover, **Company B** can orchestrate failover and automate connection establishment between Recovery VNet and on-premises datacenter as shown in the below diagram.

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 also reconfigured to point to the target region and gateways post failover.

On-premises to Azure connectivity – Full region failover



Subnet failover

Unlike the Azure-to-Azure scenario described for **Company A**, a subnet-level failover is not possible in this case for **Company B**. This is because the address space on source and recovery virtual networks is the same and the original source to on-premises connection is active.

To achieve application resiliency, it is recommended that each application is housed in its own dedicated Azure virtual network. Applications can then be failed over in isolation and the required on-premises to source connections can be routed to the target region as described above.

Next steps

- Learn more about [recovery plans](#).

Using ExpressRoute with Azure virtual machine disaster recovery

7/9/2018 • 9 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. This article describes how you can use ExpressRoute with Site Recovery for disaster recovery of Azure virtual machines.

Prerequisites

Before you begin, ensure that you understand:

- ExpressRoute circuits
- ExpressRoute routing domains
- Azure virtual machine replication architecture
- [Setting up replication](#) for Azure virtual machines
- [Failing over](#) Azure virtual machines

ExpressRoute and Azure virtual machine replication

When protecting Azure virtual machines with Site Recovery, replication data is sent to an Azure Storage account or replica Managed Disk on the target Azure region depending on whether your Azure virtual machines use [Azure Managed Disks](#). 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.

For Azure VM disaster recovery, as replication data does not leave the Azure boundary, ExpressRoute is not required for replication. After virtual machines fail over to the target Azure region, you can access them using [private peering](#).

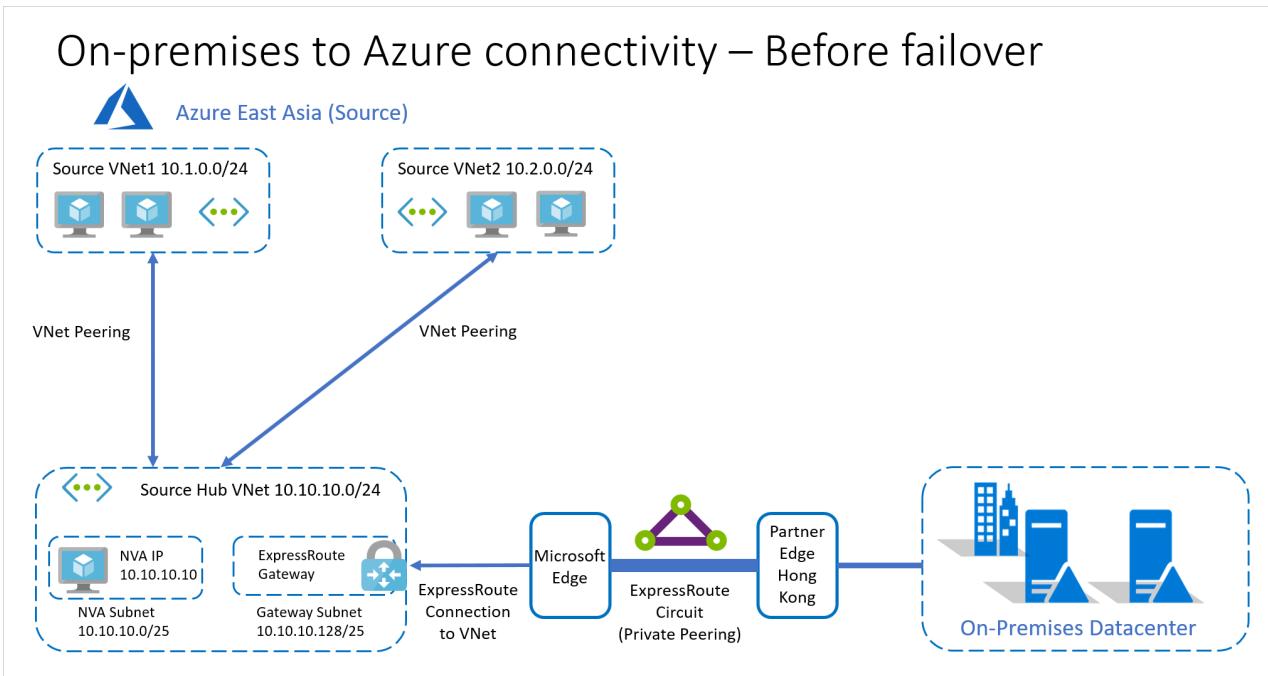
Replicating Azure deployments

An earlier [article](#), described a simple setup with one Azure virtual network connected to customer on-premises datacenter through ExpressRoute. Typical enterprise deployments have workloads split across multiple Azure virtual networks and a central connectivity hub establishes external connectivity, both to the Internet and to on-premises deployments.

This example describes a hub and spoke topology, which is common in enterprise deployments:

- The deployment is in the **Azure East Asia** region and the on-premises datacenter has an ExpressRoute circuit connection through a partner edge in Hong Kong.
- Applications are deployed across two spoke virtual networks – **Source VNet1** with address space 10.1.0.0/24 and **Source VNet2** with address space 10.2.0.0/24.
- The hub virtual network, **Source Hub VNet**, with address space 10.10.10.0/24 acts as the gatekeeper. All communication across subnets goes through the hub.
- The hub virtual network has two subnets – **NVA Subnet** with address space 10.10.10.0/25 and **Gateway Subnet** with address space 10.10.10.128/25.
- The **NVA subnet** has a network virtual appliance with IP address 10.10.10.10.
- The **Gateway Subnet** has an ExpressRoute gateway connected to an ExpressRoute connection that routes to customer on-premises datacenter through a Private Peering routing domain.

- Each spoke virtual network is connected to the hub virtual network and all routing within this network topology is controlled through Azure Route Tables (UDR). All outbound traffic from one VNet to the other VNet, or to the on-premises datacenter is routed through the NVA.



Hub and spoke peering

The spoke to hub peering has the following configuration:

- Allow virtual network address: Enabled
- Allow forwarded traffic: Enabled
- Allow gateway transit: Disabled
- Use remove gateways: Enabled

Configuration

Allow virtual network access Disabled Enabled

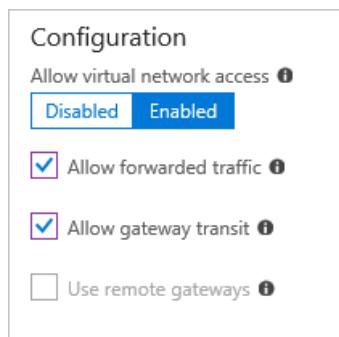
Allow forwarded traffic ?

Allow gateway transit ?

Use remote gateways ?

The hub to spoke peering has the following configuration:

- Allow virtual network address: Enabled
- Allow forwarded traffic: Enabled
- Allow gateway transit: Enabled
- Use remove gateways: Disabled



Enabling replication for the deployment

For the above setup, first [set up disaster recovery](#) for every virtual machine using Site Recovery. 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 replicate route tables, virtual network gateways, virtual network gateway connections, virtual network peering, or any other networking resources or connections. These and other resources not part of the [replication process](#) need to be created during or before failover and connected to the relevant resources. You can use Azure Site Recovery's powerful [recovery plans](#) to automate creating and connecting additional resources using automation scripts.

By default, the replication traffic does not leave the Azure boundary. Typically, NVA deployments also define a default route (0.0.0.0/0) that forces outbound Internet traffic to flow through the NVA. In this case, the appliance might get throttled if all the replication traffic passes through the NVA. The same also applies when using default routes for routing all Azure VM traffic to on-premises deployments. We recommend [creating a virtual network service endpoint](#) in your virtual network for "Storage" so that the replication traffic does not leave Azure boundary.

Failover models with ExpressRoute

When Azure virtual machines are failed over to a different region, the existing ExpressRoute connection to the source virtual network is not automatically transferred to the target virtual network on the recovery region. A new connection is required to connect ExpressRoute to the target virtual network.

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 need to enable ExpressRoute Premium if you're using a single ExpressRoute circuit for source and target region connectivity. For more details, check [ExpressRoute locations](#) and [ExpressRoute pricing](#).

Two ExpressRoute circuits in two different ExpressRoute peering locations

- This configuration is useful if you want to insure against failure of the primary ExpressRoute circuit and against large-scale regional disasters, which could also impact ExpressRoute peering locations and disrupt your primary ExpressRoute circuit.
- Normally the circuit connected to the production environment is used as the primary circuit and the secondary circuit is a failsafe and typically of lower bandwidth. The bandwidth of the secondary can be increased in a disaster event, when the secondary must take over as the primary.
- With this configuration you can establish connections from your secondary ExpressRoute circuit to the target virtual network post failover or have the connections established and ready for a disaster declaration, reducing your overall recovery time. With simultaneous connections to both primary and target region virtual networks, ensure that your on-premises routing uses the secondary circuit and connection only after failover.
- The source and target virtual networks for VMs protected with Site Recovery can have the same or different IP addresses at failover per your requirement. In both cases, the secondary connections can be established prior to failover.

Two ExpressRoute circuits in the same ExpressRoute peering location

- With this configuration, you can insure against failure of the primary ExpressRoute circuit, but not against large-scale regional disasters, which could impact ExpressRoute peering locations. With the latter, both the primary and secondary circuits can get impacted.
- The other conditions for IP addresses and connections remain the same as those in the earlier case. You can have simultaneous connections from on-premises datacenter to source virtual network with the primary circuit and to the target virtual network with the secondary circuit. With simultaneous connections to both primary and target region virtual networks, ensure that your on-premises routing uses the secondary circuit and connection only after failover.
- You can't connect both circuits to the same virtual network when circuits are created at the same peering location.

Single ExpressRoute circuit

- This configuration does not insure against a large-scale regional disaster, which could impact the ExpressRoute peering location.
- With a single ExpressRoute circuit, you can't connect source and target virtual networks simultaneously to circuit if the same IP address space is used on the target region.
- When the same IP address space is used on the target region, the source side connection should be disconnected, and the target side connection established thereafter. This connection change can be scripted as part of a recovery plan.
- In a regional failure, if the primary region is inaccessible, the disconnect operation could fail. Such an outage could impact connection creation to the target region when same IP address space is used on target virtual network.
- If connection creation succeeds on target and primary region recovers later, you can face packet drops if two simultaneous connections attempt to connect to the same address space. To prevent packet drops, the primary connection should be terminated immediately. Post failback of virtual machines to the primary region, the primary connection can again be established after disconnecting the secondary connection.
- If different address space is used on the target virtual network, then you can simultaneously connect to the source and target virtual networks from the same ExpressRoute circuit.

Recovering Azure deployments

Consider the failover model with two different ExpressRoute circuits in two different peering locations, and retention of private IP addresses for the protected Azure virtual machines. The target recovery region is Azure SouthEast Asia and a secondary ExpressRoute circuit connection is established through a partner edge in Singapore.

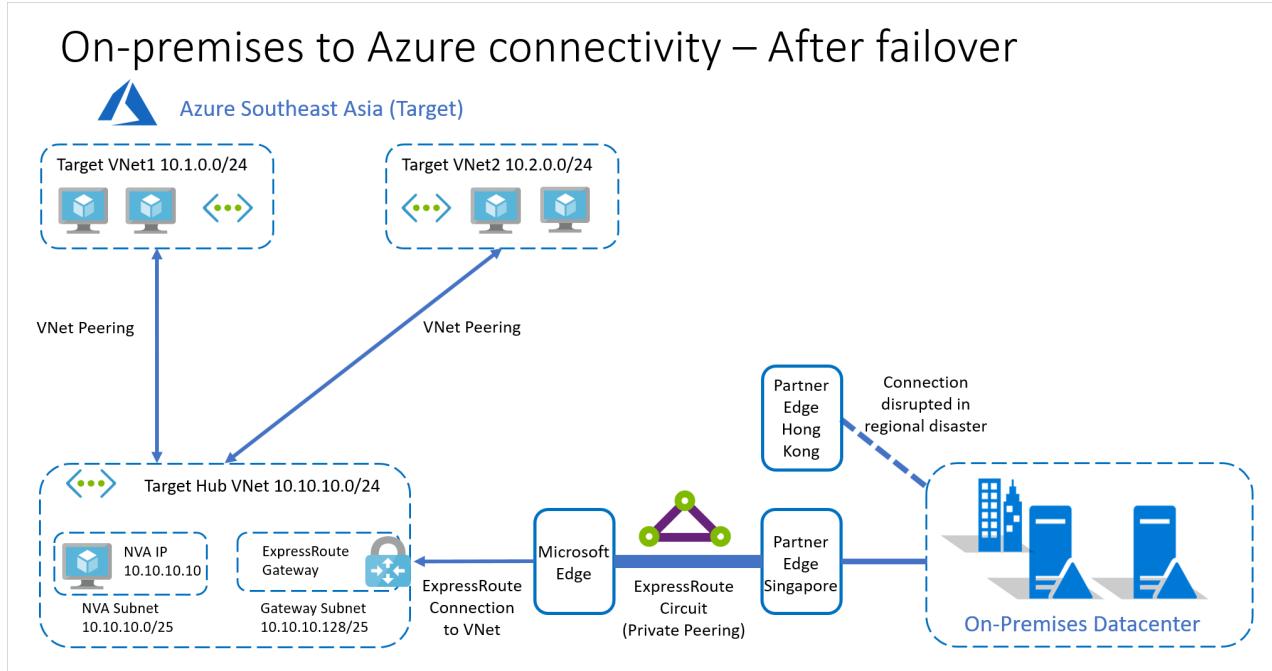
To automate recovery of the entire deployment, in addition to replicating virtual machines and virtual networks, other relevant networking resources and connections must also be created. For the earlier hub and spoke network topology the following additional steps need to be taken during or after the [failover](#) operation:

- Create the Azure ExpressRoute Gateway in the target region hub virtual network. The ExpressRoute Gateway is required to connect the target hub virtual network to the ExpressRoute circuit.
- Create the virtual network connection from the target hub virtual network to the target ExpressRoute circuit.
- 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.
- 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.

Post the recovery of the virtual machines and completion of the other connectivity steps, the recovery

environment looks as follows:



A simple topology example for Azure VM disaster recovery with single ExpressRoute circuit, with same IP on target virtual machines, is detailed [here](#).

Recovery Time Objective (RTO) considerations

To reduce the overall recovery time for your deployment, we recommend provisioning and deploying the additional target region [networking components](#) such as virtual network gateways beforehand. A small downtime is associated with deploying additional resources, and this downtime can impact the overall recovery time, if not accounted for during planning.

We recommend running regular [disaster recovery drills](#) for protected deployments. A drill validates your replication strategy without data loss or downtime and doesn't affect your production environment. Running a drill also avoids last-minute configuration issues that can adversely impact recovery time objective. We recommend using a separate Azure VM network for the test failover, instead of the default network that was set up when you enabled replication.

If you're using a single ExpressRoute circuit, we recommend using a different IP address space for the target virtual network to avoid connection establishment issues during regional disasters. If using different IP addresses is not feasible for your recovered production environment, the disaster recovery drill test failover should be done on a separate test network with different IP addresses as you can't connect two virtual networks with overlapping IP address space to the same ExpressRoute circuit.

Next steps

- Learn more about [ExpressRoute circuits](#).
- Learn more about [ExpressRoute routing domains](#).
- Learn more about [ExpressRoute locations](#).
- Learn more about [recovery plans](#) to automate application failover.

Set up disaster recovery for Azure VMs after migration to Azure

7/23/2018 • 2 minutes to read • [Edit Online](#)

Use this article after you've [migrated on-premises machines to Azure VMs](#) using the [Site Recovery](#) service. This article helps you to prepare the Azure VMs for setting up disaster recovery to a secondary Azure region, using Site Recovery.

Before you start

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.

Install the Azure VM agent

The Azure [VM agent](#) must be installed on the VM, so that the Site Recovery can replicate it.

1. To install the VM agent on VMs running Windows, download and run the [agent installer](#). You need admin privileges on the VM to complete the installation.
2. To install the VM agent on VMs running Linux, install the latest [Linux agent](#). You need administrator privileges to complete the installation. We recommend you install from your distribution repository. We don't recommend installing the Linux VM agent directly from GitHub.

Validate the installation on Windows VMs

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.

Migration from VMware VMs or physical servers

If you migrate on-premises VMware VMs (or physical servers) to Azure, note that:

- You only need to install the Azure VM agent if the Mobility service installed on the migrated machine is v9.6 or earlier.
- On Windows VMs running version 9.7.0.0 of the Mobility service onwards, the service installer installs the latest available Azure VM agent. When you migrate, these VMs already meet the agent installation prerequisite for any VM extension, including the Site Recovery extension.
- You need to manually uninstall the Mobility service from the Azure VM, using one of the following methods.
Restart the VM before you configure replication.
 - 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
```

Next steps

[Quickly replicate](#) an Azure VM to a secondary region.

Set up disaster recovery for Azure virtual machines using Azure PowerShell

7/9/2018 • 14 minutes to read • [Edit Online](#)

In this article, you see how to setup 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.
- Failover 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 replicate Azure virtual machines that use managed disks.
- 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.

Prerequisites

Before you start:

- Make sure that you understand the [scenario architecture and components](#).
- Review the [support requirements](#) for all components.
- You have version 5.7.0 or greater of the AzureRm PowerShell module. If you need to install or upgrade Azure PowerShell, follow this [Guide to install and configure Azure PowerShell](#).

Log in to your Microsoft Azure subscription

Log in to your Azure subscription using the `Connect-AzureRmAccount` cmdlet

```
Connect-AzureRmAccount
```

Select your Azure subscription. Use the `Get-AzureRmSubscription` cmdlet to get the list of Azure subscriptions you have access to. Select the Azure subscription to work with using the `Select-AzureRmSubscription` cmdlet.

```
Select-AzureRmSubscription -SubscriptionId "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
```

Get details of the virtual machine(s) to be replicated

In the example in this article, a virtual machine in the East US region will be replicated to and recovered in the West US 2 region. The virtual machine being replicated is a virtual machine with 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-AzureRmVM -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 disks of the virtual machine. 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-AzureRmResourceGroup -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 the example below 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-AzureRmRecoveryServicesVault -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

TIP

The Azure Site Recovery PowerShell module (AzureRm.RecoveryServices.SiteRecovery module) comes with easy to use aliases for most cmdlets. The cmdlets in the module take the form <Operation>-AzureRmRecoveryServicesAsr<Object> and have equivalent aliases that take the form <Operation>-ASR<Object>. This article uses the cmdlet aliases for ease of reading.

Set the vault context for use in the PowerShell session. To do this, download the vault settings file to, and import the downloaded file in the PowerShell session to set the vault context.

Once set, subsequent Azure Site Recovery operations in the PowerShell session are performed in the context of the selected vault.

```
#Download the vault settings file for the vault.
$Vaultsettingsfile = Get-AzureRmRecoveryServicesVaultSettingsFile -Vault $vault -SiteRecovery -Path
C:\users\user\Documents\

#Import the downloaded vault settings file to set the vault context for the PowerShell session.
Import-AzureRmRecoveryServicesAsrVaultSettingsFile -Path $Vaultsettingsfile.FilePath
```

ResourceName	ResourceGroupName	ResourceNamespace	ResouceType
a2aDemoRecoveryVault	a2ademorecoveryrg	Microsoft.RecoveryServices.Vaults	

```
#Delete the downloaded vault settings file
Remove-Item -Path $Vaultsettingsfile.FilePath
```

Prepare the vault to start replicating Azure virtual machines

1. 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 the fabric object 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.

NOTE

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. Use the job tracking object to get the latest status for the job (Get-ASRJob), and to monitor the status of the operation.

```
#Create Primary ASR fabric
$tempASRJob = New-ASRFabric -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-ASRJob -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-AsrFabric -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.

2. Create a Site Recovery fabric object to represent the recovery region

The recovery fabric object represents the recovery Azure location. Virtual machines will be replicated to and recovered to (in the event of a failover) 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-ASRFabric -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-ASRJob -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-AsrFabric -Name "A2Ademo-WestUS"
```

3. 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-AzureRmRecoveryServicesAsrProtectionContainer -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-ASRJob -Job $TempASRJob
}

Write-Output $TempASRJob.State

$PrimaryProtContainer = Get-ASRProtectionContainer -Fabric $PrimaryFabric -Name "A2AEastUSProtectionContainer"

```

4. 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-AzureRmRecoveryServicesAsrProtectionContainer -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-ASRJob -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-ASRProtectionContainer -Fabric $RecoveryFabric -Name
"A2AWestUSProtectionContainer"

```

5. Create a replication policy

```

#Create replication policy
$TempASRJob = New-ASRPolicy -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-ASRJob -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-ASRPolicy -Name "A2APolicy"

```

6. 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-ASRProtectionContainerMapping -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-ASRJob -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-ASRProtectionContainerMapping -ProtectionContainer $PrimaryProtContainer -Name
"A2APrimaryToRecovery"

```

7. Create a protection container mapping for failback (reverse replication after a failover)

After a failover, when you are ready to bring the failed over virtual machine back to the original Azure region, you failback. To failback, 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 failback) between the Recovery and Primary Protection Containers
with the Replication policy
$tempASRJob = New-ASRProtectionContainerMapping -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-ASRJob -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 cache storage account(s) and target storage account(s)

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 need not) 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-AzureRmStorageAccount -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(s) 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-AzureRmStorageAccount -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 failover 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 failover to

```
#Create a Recovery Network in the recovery region
$WestUSRecoveryVnet = New-AzureRmVirtualNetwork -Name "a2arecoveryvnet" -ResourceGroupName
"a2ademorecoveryrg" -Location 'West US 2' -AddressPrefix "10.0.0.0/16"

Add-AzureRmVirtualNetworkSubnetConfig -Name "default" -VirtualNetwork $WestUSRecoveryVnet -
AddressPrefix "10.0.0.0/20" | Set-AzureRmVirtualNetwork

$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-AzureRmNetworkInterface -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-ASRNetworkMapping -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-ASRJob -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 (failback)

```

#create an ASR network mapping for failback between the recovery Azure virtual network and the primary
Azure virtual network
$tempASRJob = New-ASRNetworkMapping -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-ASRJob -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.

```

#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-AzureRmRecoveryServicesAsrAzureToAzureDiskReplicationConfig -VhdUri
$OSDiskVhdURI.Uri -LogStorageAccountId $EastUSCacheStorageAccount.Id -RecoveryAzureStorageAccountId
$WestUSTargetStorageAccount.Id

#Disk replication configuration for data disk
$DataDisk1ReplicationConfig = New-AzureRmRecoveryServicesAsrAzureToAzureDiskReplicationConfig -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-AzureRmResourceGroup -Name "a2ademozurerg" -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-ASRReplicationProtectedItem -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-ASRJob -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.

Once 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-ASRReplicationProtectedItem -ProtectionContainer $PrimaryProtContainer | Select FriendlyName, ProtectionState, ReplicationHealth
```

FriendlyName	ProtectionState	ReplicationHealth
AzureDemoVM	Protected	Normal

Perform a test failover, validate, and cleanup test failover

Once 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-AzureRmVirtualNetwork -Name "a2aTFOvnet" -ResourceGroupName "a2ademorecoveryrg" -Location 'West US 2' -AddressPrefix "10.3.0.0/16"

Add-AzureRmVirtualNetworkSubnetConfig -Name "default" -VirtualNetwork $TFOVnet -AddressPrefix "10.3.0.0/20" |
Set-AzureRmVirtualNetwork

$TFONetwork= $TFOVnet.Id
```

Perform test failover.

```
$ReplicationProtectedItem = Get-ASRReplicationProtectedItem -FriendlyName "AzureDemoVM" -ProtectionContainer
$PrimaryProtContainer

$TFOJob = Start-ASRTTestFailoverJob -ReplicationProtectedItem $ReplicationProtectedItem -AzureVMNetworkId
$TFONetwork -Direction PrimaryToRecovery
```

Wait for the test failover operation to complete.

```
Get-ASRJob -Job $TFOJob
```

```
Name : 3dcb043e-3c6d-4e0e-a42e-8d4245668547
ID : /Subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxx/resourceGroups/a2ademorecoveryrg/providers/Microsoft.RecoveryServices/vaults/a2aDemoR
ecovreVault/replicationJobs/3dcb043e-3c6d-4e0e-a42e-8d4245668547
Type : Microsoft.RecoveryServices/vaults/replicationJobs
JobType : TestFailover
DisplayName : Test failover
ClientRequestId : 1ef8515b-b130-4452-a44d-91aaf071931c 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 : {}
```

Once 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-ASRTTestFailoverCleanupJob -ReplicationProtectedItem $ReplicationProtectedItem

Get-ASRJob -Job $Job_TFOCleanup | Select State
```

```
State
-----
Succeeded
```

Failover to Azure

Failover the virtual machine to a specific recovery point.

```
$RecoveryPoints = Get-ASRRecoveryPoint -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 failover job
$Job_Failover = Start-ASRUnplannedFailoverJob -ReplicationProtectedItem $ReplicationProtectedItem -Direction
PrimaryToRecovery -RecoveryPoint $RecoveryPoints[-1]

do {
    $Job_Failover = Get-ASRJob -Job $Job_Failover;
    sleep 30;
} while (($Job_Failover.State -eq "InProgress") -or ($JobFailover.State -eq "NotStarted"))

$Job_Failover.State
```

```
Succeeded
```

Once failed over successfully, you can commit the failover operation.

```
$CommitFailoverJob = Start-ASRCommitFailoverJob -ReplicationProtectedItem $ReplicationProtectedItem

Get-ASRJob -Job $CommitFailoverJob
```

```
Name : 58afc2b7-5cfe-4da9-83b2-6df358c6e4ff
ID : /Subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxx/resourceGroups/a2ademozurecoveryrg/providers/Microsoft.RecoveryServices/vaults/a2aDemoR
ecovreVault/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 : {}
```

After a failover, when you are ready to go back to the original region, start reverse replication for the replication protected item using the `Update-AzureRmRecoveryServicesAsrProtectionDirection` cmdlet.

Next steps

View the [Azure Site Recovery PowerShell reference](#) to learn how you can perform other tasks such as creating

Recovery Plans and testing failover of Recovery plans through PowerShell.

Replicate Azure virtual machines to another Azure region

7/9/2018 • 3 minutes to read • [Edit Online](#)

This article describes how to enable replication of Azure VMs, from one Azure region to another.

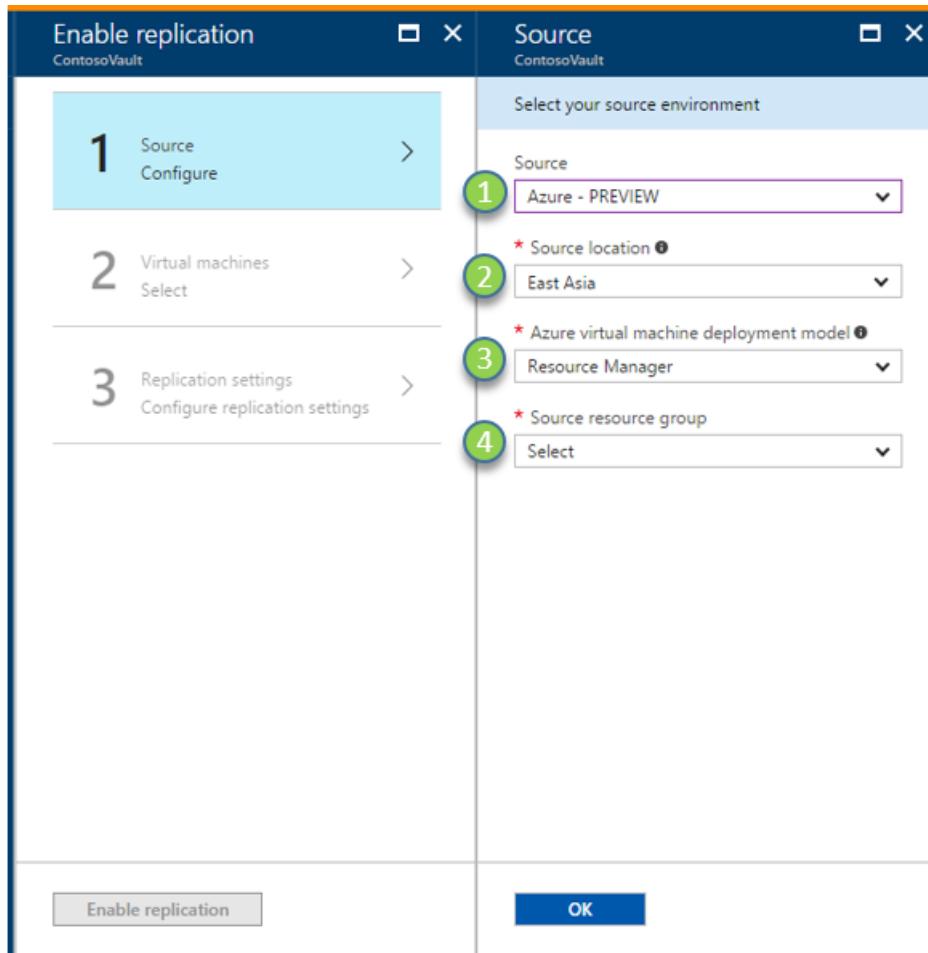
Prerequisites

This article assumes that you've already set up Site Recovery for this scenario, as described in the [Azure to Azure tutorial](#). Make sure that you've prepared the prerequisites, and created the Recovery Services vault.

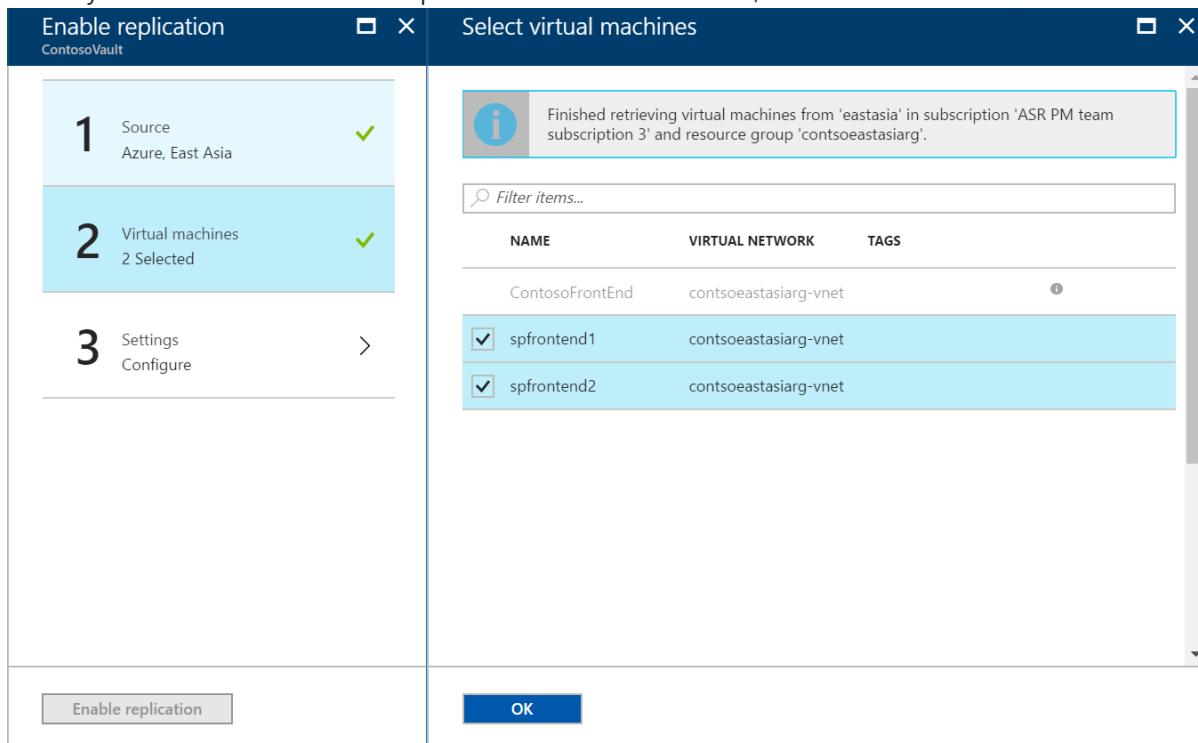
Enable replication

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 virtual machines. For this illustration, the source location is 'East Asia'
 - **Deployment model:** Azure deployment model of the source machines.
 - **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**.

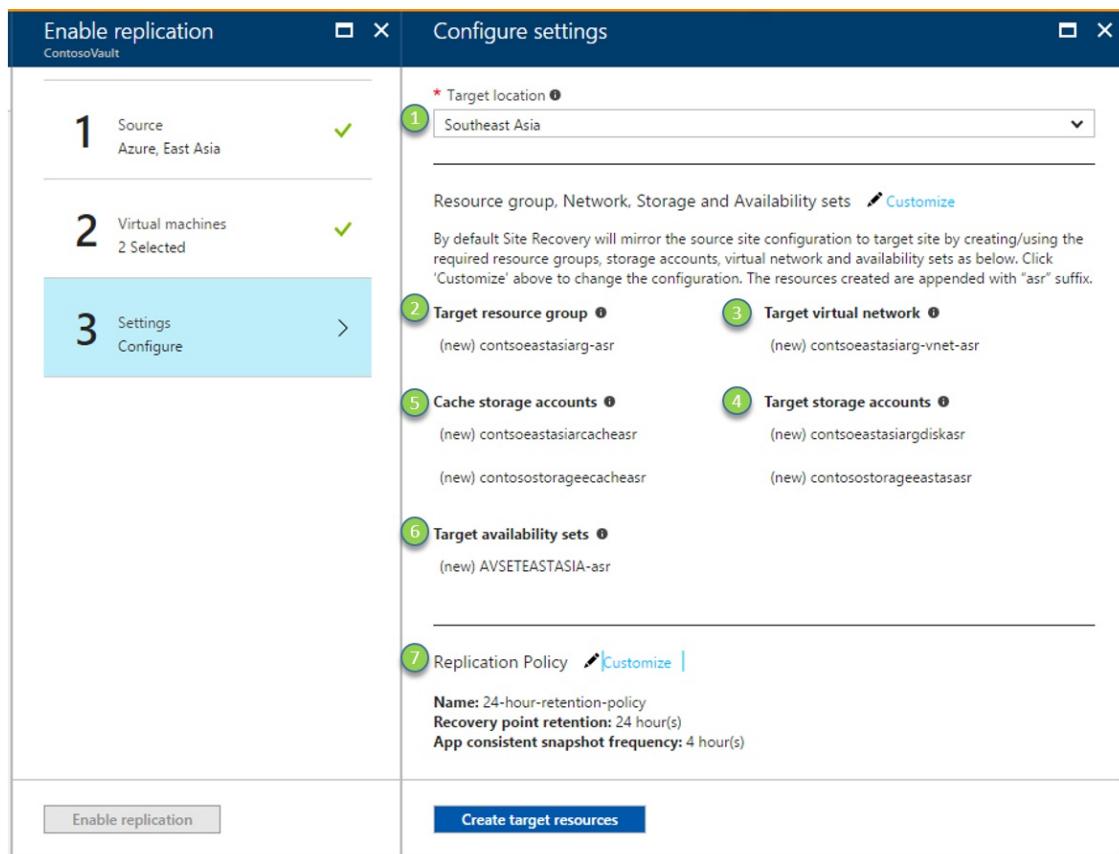


4. In **Settings**, you can optionally configure target site settings:

- **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 resource group:** The resource group to which all your replicated virtual machines belong. By

default Azure Site Recovery creates a new resource group in the target region with name having "asr" suffix. In case resource group created by Azure Site Recovery already exists, it is reused. You can also choose to customize it as shown in the section below. The location of the target resource group can be any Azure region except the region in which the source virtual machines are hosted.

- **Target Virtual Network:** By default, Site Recovery creates a new virtual network in the target region with name having "asr" suffix. This is mapped to your source network, and used for any future protection. [Learn more](#) about network mapping.
- **Target Storage accounts (If your source VM does not 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 (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 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.
- **Availability set:** By default, Azure Site Recovery creates a new availability set in the target region with name having "asr" suffix. In case availability set created by Azure Site Recovery already exists, it is reused.
- **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 '60 minutes' for app consistent snapshot frequency.

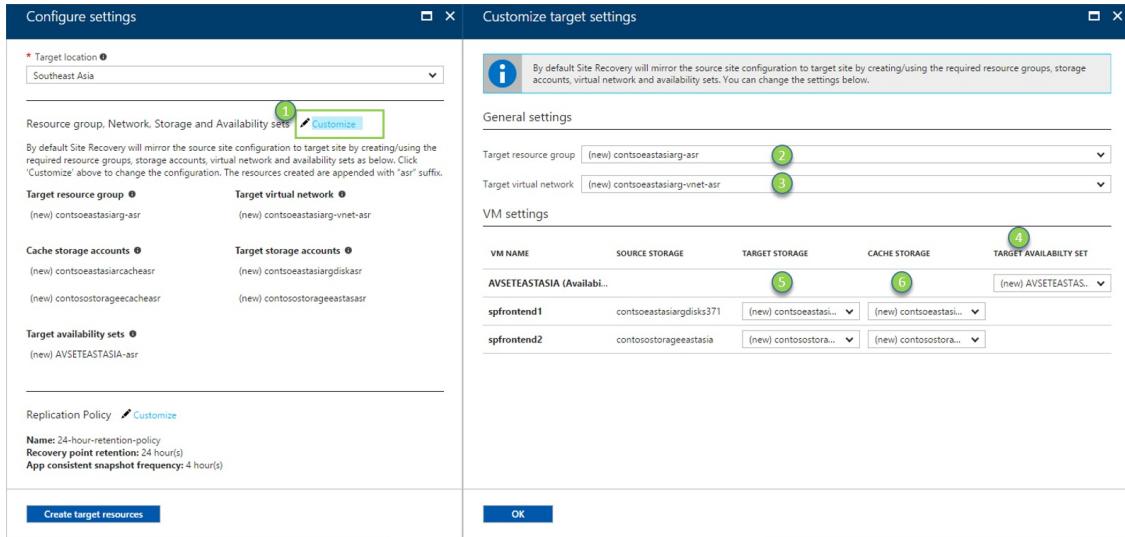


Customize target resources

You can modify the default target settings used by Site Recovery.

1. 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.



2. Click **Create target resource > Enable Replication**.

3. 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.

Reprotect failed over Azure VMs to the primary region

7/9/2018 • 3 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 fail back the VMs to the primary region, you need to do the following:

- Reprotect the VMs in the secondary region, so that they start to replicate to the primary region.
- After reprottection completes and the VMs are replicating, you can fail them over from the secondary to primary region.

WARNING

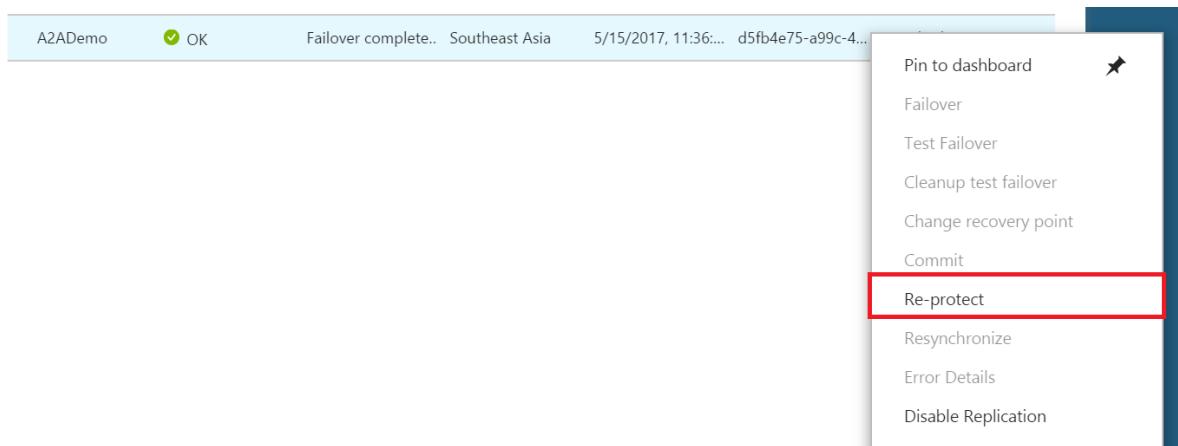
If you've [migrated](#) machines from the primary to the secondary region, moved the VM to another resource group, or deleted the Azure VM, you can't reprotect the VM, or fail it back.

Prerequisites

1. The VM failover from the primary to secondary region must be committed.
2. 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 are created as part of the reprottection process.
3. The reprottection job seeds the target site with the latest data. After that 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 does not 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 primary region
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 required. If you have 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 required components are created as part of reprotect. If they already exist, they are reused.
2. The target side VM is turned off if it's running.
3. The target side VM disk is copied by Site Recovery into a container, as a seed blob.
4. The target side VM is then deleted.
5. The seed blob is used by the current source side (secondary) VM to replicate. This ensures that only deltas are replicated.
6. Major changes between the source disk and the seed blob are synchronized. This can take some time to complete.
7. After the reprotect job completes, the delta replication begins, and creates a recovery point in line with the replication policy.
8. After the reprotect job succeeds, the VM enters a protected state.

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 VM in the primary region, with some small downtime. We recommend you choose a time accordingly, and that you run a test failover but initiating a full failover to the primary site. [Learn more](#) about failover.

Troubleshoot Azure-to-Azure VM replication issues

8/9/2018 • 10 minutes to read • [Edit Online](#)

This article describes the common issues in Azure Site Recovery when replicating and recovering Azure virtual machines from one region to another region and explains how to troubleshoot them. For more information about supported configurations, see the [support matrix for replicating Azure VMs](#).

Azure resource quota issues (error code 150097)

Your subscription should be enabled to create Azure VMs in the target region that you plan to use as your disaster recovery region. Also, your subscription should have sufficient quota enabled to create VMs of specific size. By default, Site Recovery picks the same size for the target VM as the source VM. If the matching size isn't available, the closest possible size is picked automatically. If there's no matching size that supports source VM configuration, this error message appears:

Error code	Possible causes	Recommendation
150097 Message: Replication couldn't be enabled for the virtual machine VmName.	<ul style="list-style-type: none">- Your subscription ID might not be enabled to create any VMs in the target region location.- Your subscription ID might not be enabled or doesn't have sufficient quota to create specific VM sizes in the target region location.- A suitable target VM size that matches the source VM NIC count (2) isn't found for the subscription ID in the target region location.	Contact Azure billing support to enable VM creation for the required VM sizes in the target location for your subscription. After it's enabled, retry the failed operation.

Fix the problem

You can contact [Azure billing support](#) to enable your subscription to create VMs of required sizes in the target location.

If the target location has a capacity constraint, disable replication and enable it to a different location where your subscription has sufficient quota to create VMs of the required sizes.

Trusted root certificates (error code 151066)

If all the latest trusted root certificates aren't present on the VM, your "enable replication" job might fail. Without the certificates, the authentication and authorization of Site Recovery service calls from the VM fail. The error message for the failed "enable replication" Site Recovery job appears:

Error code	Possible cause	Recommendations
------------	----------------	-----------------

ERROR CODE	POSSIBLE CAUSE	RECOMMENDATIONS
151066 Message: Site Recovery configuration failed.	The required trusted root certificates used for authorization and authentication aren't present on the machine.	<ul style="list-style-type: none"> - For a VM running the Windows operating system, ensure that the trusted root certificates are present on the machine. For information, see Configure trusted roots and disallowed certificates. - For a VM running the Linux operating system, follow the guidance for trusted root certificates published by the Linux operating system version distributor.

Fix the problem

Windows

Install all the latest Windows updates on the VM so that all the trusted root certificates are present on the machine. 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.

Follow the typical Windows update management or certificate update management process in your organization to get all the latest root certificates and the updated certificate revocation list on the VMs.

To verify that the issue is resolved, go to login.microsoftonline.com from a browser in your VM.

Linux

Follow the guidance provided by your Linux distributor to get the latest trusted root certificates and the latest certificate revocation list on the VM.

Because SuSE Linux uses 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 if the Symantec root CA cert is present.

```
# ls VeriSign_Class_3_Public_Primary_Certification_Authority_G5.pem
```

4. If the Symantec root CA cert is not found, run the following command to download the file. Check for any errors and follow recommended action 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 if the Baltimore root CA cert is present.

```
# ls Baltimore_CyberTrust_Root.pem
```

6. If the Baltimore root CA cert is not found, download the certificate.

```
# wget http://www.digicert.com/CACerts/BaltimoreCyberTrustRoot.crt.pem -O Baltimore_CyberTrust_Root.pem
```

7. Check if the DigiCert_Global_Root_CA cert 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 rehash script to update the certificate subject hashes for the newly downloaded certificates.

```
# c_rehash
```

10. Check if the subject hashes as symlinks are created for the certificates.

- Command

```
# ls -l | grep Baltimore
```

- Output

```
lrwxrwxrwx 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 lrwxrwxrwx 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

```
lrwxrwxrwx 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
```

11. 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
```

12. Create a copy of the file Baltimore_CyberTrust_Root.pem with filename 653b494a.0

```
# cp Baltimore_CyberTrust_Root.pem 653b494a.0
```

13. Create a copy of the file DigiCert_Global_Root_CA.pem with filename 3513523f.0

```
# cp DigiCert_Global_Root_CA.pem 3513523f.0
```

14. Check if 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 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.

Issue 1: Failed to register Azure virtual machine with Site Recovery (151037)

- **Possible cause**

- You're using NSG to control outbound access on the VM and the required IP ranges aren't whitelisted for outbound access.
- You're using third-party firewall tools and the required IP ranges/URLs are not whitelisted.

- **Resolution**

- If you're using firewall proxy to control outbound network connectivity on the VM, ensure that the prerequisite URLs or datacenter IP ranges are whitelisted. For information, see [firewall proxy guidance](#).
- If you're using NSG rules to control outbound network connectivity on the VM, ensure that the prerequisite datacenter IP ranges are whitelisted. For information, see [network security group guidance](#).
- To whitelist [the required URLs](#) or the [required IP ranges](#), follow the steps in the [networking guidance document](#).

Issue 2: Site Recovery configuration failed (151072)

- **Possible cause**

- Connection cannot be established to Site Recovery service endpoints

- **Resolution**

- If you're using firewall proxy to control outbound network connectivity on the VM, ensure that the prerequisite URLs or datacenter IP ranges are whitelisted. For information, see [firewall proxy guidance](#).
- If you're using NSG rules to control outbound network connectivity on the VM, ensure that the prerequisite datacenter IP ranges are whitelisted. For information, see [network security group guidance](#).
- To whitelist [the required URLs](#) or the [required IP ranges](#), follow the steps in the [networking guidance document](#).

Issue 3: A2A replication failed when the network traffic goes through on-premise proxy server (151072)

- **Possible cause**

- The custom proxy settings are invalid and ASR 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 ASR Mobility Service, then 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. ASR Mobility Service agent supports only **un-authenticated proxies**.

Fix the problem

To whitelist [the required URLs](#) or the [required IP ranges](#), follow the steps in the [networking guidance document](#).

Disk not found in the machine (error code 150039)

A new disk attached to the VM must be initialized.

Error code	Possible causes	Recommendations
150039 Message: 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.	- A new data disk was attached to the VM but it wasn't initialized. - The data disk inside the VM is not correctly reporting the LUN value at which the disk was attached to the VM.	Ensure that the data disks are initialized, and then retry the operation. For Windows: Attach and initialize a new disk . For Linux: Initialize a new data disk in Linux .

Fix the problem

Ensure that the data disks have been initialized, and then retry the operation:

- For Windows: [Attach and initialize a new disk](#).
- For Linux: [add a new data disk in Linux](#).

If the problem persists, contact support.

Unable to see the Azure VM for selection in "enable replication"

Cause 1: Resource group and source Virtual machine are in different location

Azure Site Recovery currently mandated that source region resource group and virtual machines should be in same location. If that is not the case then you would not be able to find the virtual machine during the time of protection.

Cause 2: Resource group is not part of selected subscription

You might not be able to find the resource group at the time of protection if it is not part of the given subscription. Make sure that the resource group belongs to the subscription which is being used.

Cause 3: Stale Configuration

If you don't see the VM you want to enable for replication, it might be because of a stale Site Recovery configuration left on the Azure VM. The stale configuration could be left on an Azure VM in the following cases:

- You enabled replication for the Azure VM by using Site Recovery and then deleted the Site Recovery vault without explicitly disabling replication on the VM.
- You enabled replication for the Azure VM by using Site Recovery and then deleted the resource group containing the Site Recovery vault without explicitly disabling replication on the VM.

Fix the problem

You can use [Remove stale ASR configuration script](#) and remove the stale Site Recovery configuration on the Azure VM. You should be able to see the VM after removing the stale configuration.

Unable to select Virtual machine for protection

Cause 1: Virtual machine has some extension installed in a failed or unresponsive state

Go to Virtual machines > Setting > Extensions and check if there are any extensions in a failed state. Uninstall the failed extension and retry protecting the virtual machine.

Cause 2: VM's provisioning state is not valid

VM's provisioning state is not valid (error code 150019)

To enable replication on the VM, the provisioning state should be **Succeeded**. You can check the VM state by

following the steps below.

1. Select the **Resource Explorer** from **All Services** in Azure portal.
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 virtual machine
5. Check the **provisioningState** field in Instance view on right hand side.

Fix the problem

- If **provisioningState** is **Failed**, contact support with details to troubleshoot.
- If **provisioningState** is **Updating**, another extension could be getting deployed. Check if there are any ongoing operations on the VM, wait for them to complete and retry the failed Site Recovery **Enable replication** job.

Unable to select Target virtual network - network selection tab is grayed out.

Cause 1: If your VM is attached to a network that is 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 target resource group, then by default network selection drop down will be disabled.

	SOURCE	TARGET
VM resource group	[REDACTED]	[REDACTED] <input type="button" value="..."/>
Availability set	[REDACTED]-ASR	[REDACTED] <input type="button" value="..."/>
Virtual network	vnet-asr	[REDACTED] vnet-asr-asr <input type="button" value="..."/>

Cause 2: If you previously protected the VM using Azure Site Recovery and disabled the replication.

- Disabling replication of a VM does not delete the Network Mapping. It has to be deleted from the recovery service vault where the VM was protected.
Navigate to recovery service vault > Site Recovery Infrastructure > Network mapping.

- Target network configured during the disaster recovery setup can be changed after the initial set up, after the VM is protected.

- Note that changing network mapping affects all protected VMs that use that specific network mapping.

COM+/Volume Shadow Copy service error (error code 151025)

ERROR CODE	POSSIBLE CAUSES	RECOMMENDATIONS
151025 Message: Site recovery extension failed to install	- 'COM+ System Application' service disabled. - 'Volume Shadow Copy' service is disabled.	Set 'COM+ System Application' and 'Volume Shadow Copy' services to automatic or manual start up mode.

Fix the problem

You can open 'Services' console and ensure the 'COM+ System Application' and 'Volume Shadow Copy' are not set to 'Disabled' for 'Startup Type'.

Next steps

[Replicate Azure virtual machines](#)

Troubleshoot Azure Site Recovery extension failures: Issues with the agent or extension

7/9/2018 • 4 minutes to read • [Edit Online](#)

This article provides troubleshooting steps that can help you resolve Azure Site Recovery errors related to 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 install an extension on the virtual machine as a part of enable protection job. Any of the following conditions might prevent the protection from being triggered and job to fail. Complete the following troubleshooting steps, and then retry your operation:

Cause 1: The agent is installed in the VM, but it's unresponsive (for Windows VMs)

Cause 2: The agent installed in the VM is out of date (for Linux VMs)

Cause 3: 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"

Cause 1: The agent is installed in the VM, but it's unresponsive (for Windows VMs)

Cause 2: The agent installed in the VM is out of date (for Linux VMs)

Cause 3: 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 occur if the Azure guest agent in the virtual machine is not in the ready state. You can check the status of Azure guest agent in [Azure portal](#). Go to the virtual machine you are trying to protect and check the status in "VM > Settings > Properties > Agent status". Most of the time the status of the agent become ready after rebooting the virtual machine. However, if reboot is not a possible option or you are still facing the issue, then complete the following troubleshooting steps.

Cause 1: The agent is installed in the VM, but it's unresponsive (for Windows VMs)

Cause 2: 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 occur when the agent version on the Linux machine is old. Please complete the following troubleshooting step.

Cause 1: 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. Re-installing 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). Try to restart the "Windows Azure Guest Agent service".
2. If the Windows Azure Guest Agent service isn't visible in services, in Control Panel, go to **Programs and Features** to determine whether the Windows Guest Agent service is installed.
3. If the Windows Azure Guest Agent appears in **Programs and Features**, uninstall the Windows Guest Agent.
4. Download and install the [latest version of the agent MSI](#). You must have Administrator rights to complete the installation.
5. Verify that the Windows Azure Guest Agent services appears in services.
6. Restart the protection job.

Also, verify that [Microsoft .NET 4.5 is installed](#) in the VM. .NET 4.5 is required 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 do not recommend downloading the agent code 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. 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 auto restart agent](#).

4. Enable protection of the virtual machine.

The Site Recovery extension fails to update or load

If extensions status is "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](#), and then run the protection.

Completing these steps causes the extension to be reinstalled during the protection.

Automatic update of the Mobility Service in Azure to Azure replication

7/9/2018 • 3 minutes to read • [Edit Online](#)

Azure Site Recovery has a monthly release cadence where enhancements to existing features or new ones are added, and known issues if any are fixed. This would mean that to remain current with the service, you need to plan for deployment of these patches, monthly. In order to avoid the overhead associated with the upgrade, users can instead choose to allow Site Recovery to manage updates of the components. As detailed in the [architecture reference](#) for Azure to Azure disaster recovery, Mobility Service gets installed on all Azure virtual machines for which replication is enabled while replicating virtual machines from one Azure region to another. Once you enable automatic update, the Mobility service extension gets updated with every new release. This document details the following:

- How does automatic update work?
- Enable automatic updates
- Common issues & troubleshooting

How does automatic update work

Once you allow Site Recovery to manage updates, a global runbook (which is used by Azure services) is deployed via an automation account, which is created in the same subscription as the vault. One automation account is used for a specific vault. The runbook checks for each VM in a vault for which auto-updates are turned ON and initiates an upgrade of the Mobility Service extension if a newer version is available. The default schedule of the runbook recurs daily at 12:00 AM as per the time zone of the replicated virtual machine's geo. The runbook schedule can also be modified via the automation account by the user, if necessary.

NOTE

Enabling automatic updates doesn't require a reboot of your Azure VMs, and doesn't affect on-going replication.

NOTE

Billing for jobs used by automation account is based on the number of job run time minutes used in the month and by default 500 minutes are included as free units for an automation account. The execution of the job daily amounts from a **few seconds to about a minute** and will be **covered in the free credits**.

FREE UNITS INCLUDED (PER MONTH)** PRICE Job run time 500 minutes ₹0.14/minute

Enable automatic updates

You can choose to allow Site Recovery to manage updates in the following ways:-

- [As part of the enable replication step](#)
- [Toggle the extension update settings inside the vault](#)

As part of the enable replication step:

When you enable replication for a virtual machine either starting [from the virtual machine view](#), or [from the recovery services vault](#), you will get an option to choose to either allow Site Recovery to manage updates for the

Site Recovery extension or to manually manage the same.

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	(new) MercuryPMDemo-asr
Availability set	(new) ADAVAILABILITYSET-asr
Virtual network	(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.

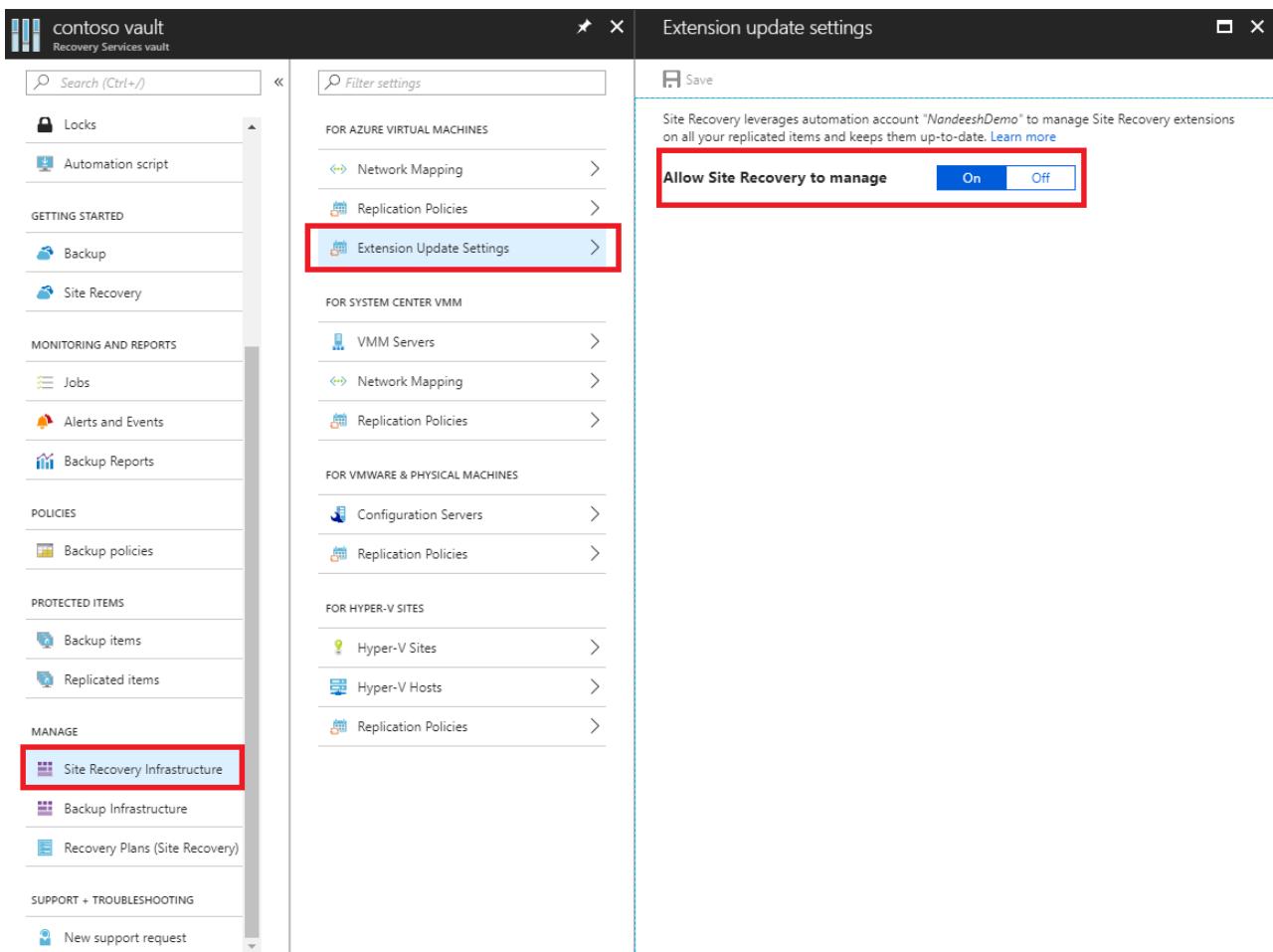
Extension settings [\[-\] Hide details](#)

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, navigate to **Manage-> Site Recovery Infrastructure**
2. Under **For Azure virtual Machines-> Extension Update Settings**, click the toggle to choose whether you want to allow *ASR to manage updates* or *manage manually*. Click **Save**.



IMPORTANT

When you choose *Allow ASR to manage*, the setting is applied to all virtual machines in the corresponding vault.

NOTE

Both the options will notify you of the automation account that is used for managing the updates. If you are enabling this feature for the first time in a vault, a new automation account will be created. All subsequent enable replications in the same vault will use the previously created one.

Common issues & troubleshooting

If there is an issue with the automatic updates, you'll be notified of the same under 'Configuration issues' in the vault dashboard.

In case you tried to enable automatic updates and it failed, refer below for troubleshooting.

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: Ensure that the logged in account is assigned the 'Contributor' and retry the operation. Refer to [this](#) document for further information on assigning the right permissions.

Once automatic updates are turned ON, most of the issues can be healed by the Site Recovery service and requires you to click on the '**Repair**' button.

The screenshot shows the 'Extension update settings' page for the 'ContosoVault - Site Recovery Infrastructure' resource. The left sidebar lists various management options. The main pane displays settings for different machine types. A specific section for 'Extension Update Settings' under 'FOR AZURE VIRTUAL MACHINES' is highlighted with a red box around a message: 'Auto update settings is un-healthy' with a 'Repair' button.

In case the repair button isn't available, refer to the error message displayed under extension settings pane.

- **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](#).

Manage virtual machine network interfaces for on-premises to Azure replication

7/9/2018 • 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.

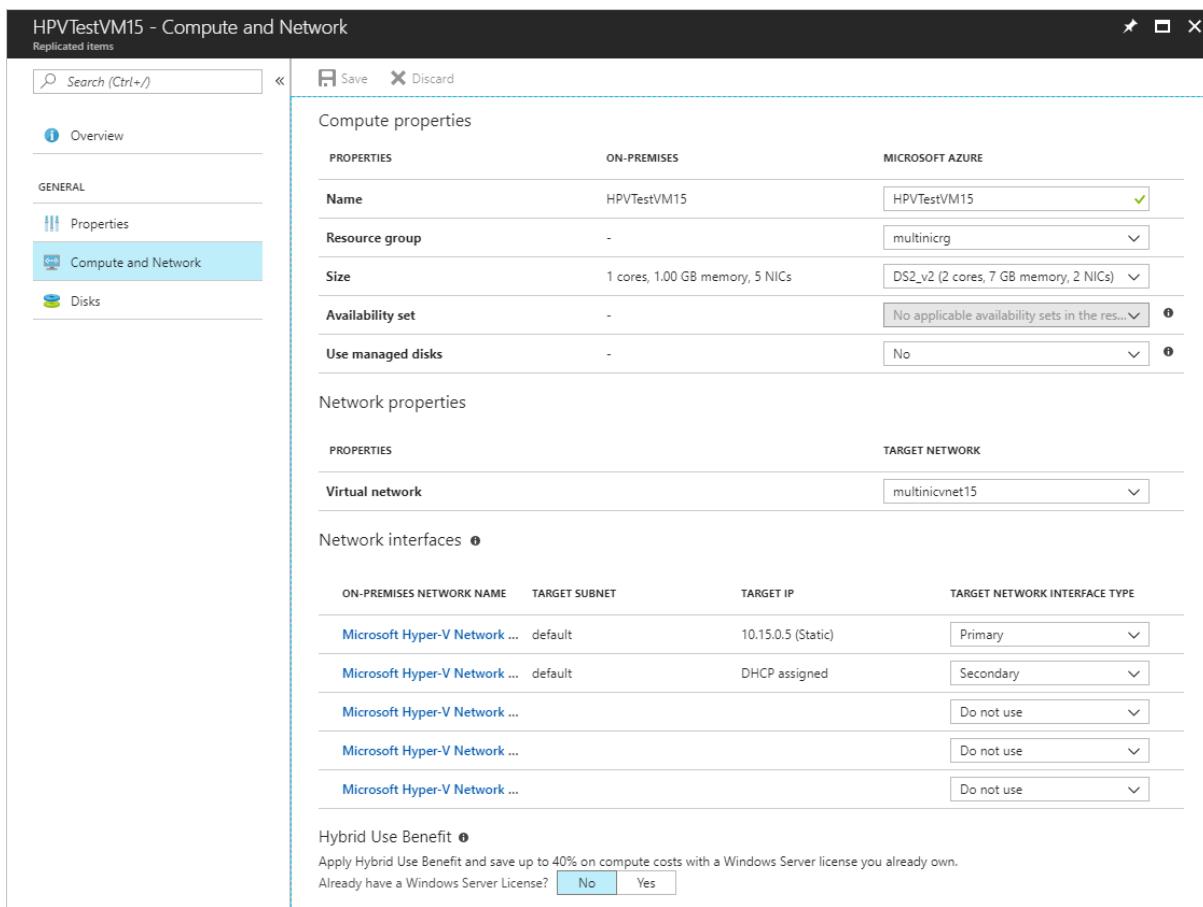
In an on-premises environment, virtual machines or servers can have multiple network interfaces for different networks within the environment. Different networks are typically used for performing specific operations such as upgrades, maintenance, and internet access. When you're migrating or failover 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.

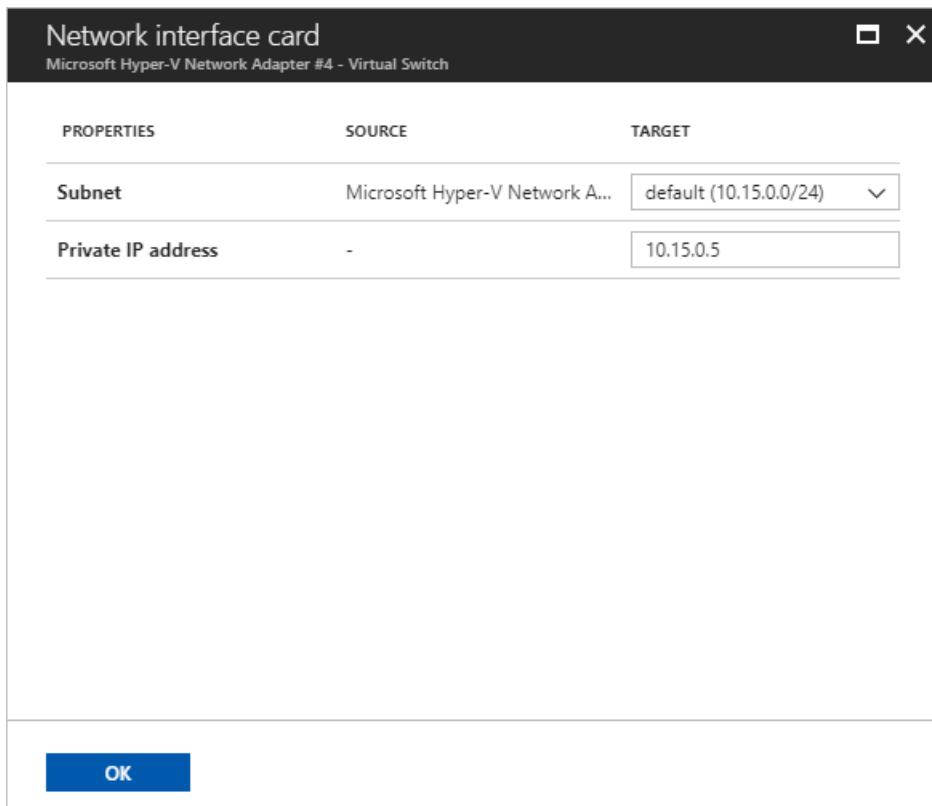
- A **Primary** network interface is required for failover.
- All other selected network interfaces, if any, are **Secondary** network interfaces.
- Select **Do not use** to exclude a network interface from creation at failover.

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.

Set up IP addressing to connect after failover to Azure

7/9/2018 • 3 minutes to read • [Edit Online](#)

This article explains the networking requirements for connecting to Azure VMs, after using the [Azure Site Recovery](#) service for replication and failover to Azure.

In this article you'll learn about:

- The connection methods you can use
- How to use a different IP address for replicated Azure VMs
- How to retain IP addresses for Azure VMs after failover

Connecting to replica VMs

When planning your replication and failover strategy, one of the key questions is how to connect to the Azure VM after failover. There are a couple of choices when designing your network strategy for replica Azure VMs:

- **Use different IP address:** You can select to use a different IP address range for the replicated Azure VM network. In this scenario the VM gets a new IP address after failover, and a DNS update is required.
- **Retain same IP address:** You might want to use the same IP address range as that in your primary on-premises site, for the Azure network after failover. Keeping the same IP addresses simplifies the recovery by reducing network related issues after failover. However, when you're replicating to Azure, you will need to update routes with the new location of the IP addresses after failover.

Retaining IP addresses

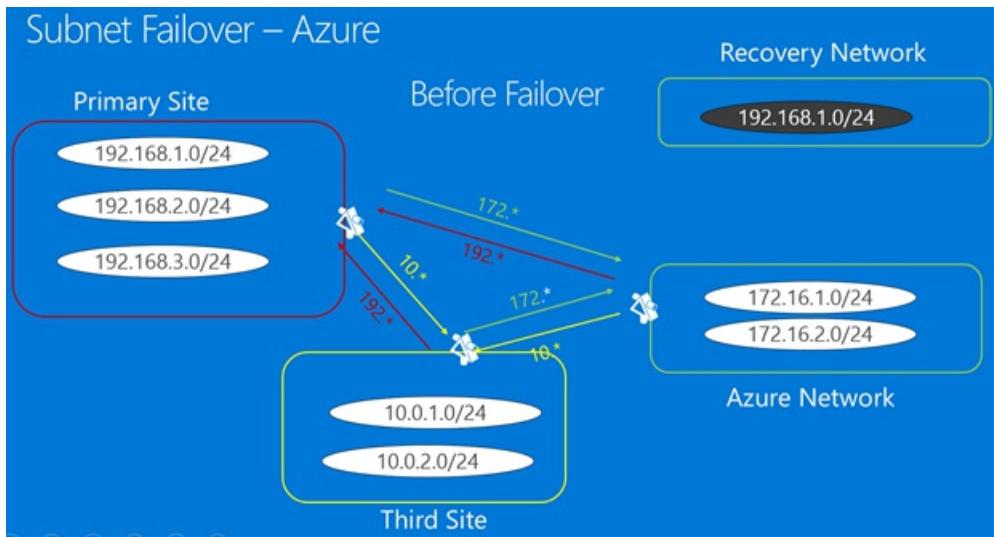
Site Recovery provides the capability to retain fixed IP addresses when failing over to Azure, with a subnet failover.

- With subnet failover, a specific subnet is present at Site 1 or Site 2, but never at both sites simultaneously.
- In order to maintain the IP address space in the event of a failover, you programmatically arrange for the router infrastructure to move the subnets from one site to another.
- During failover, the subnets move with the associated protected VMs. The main drawback is that in the event of a failure, you have to move the whole subnet.

Failover example

Let's look at an example for failover to Azure using a fictitious company, Woodgrove Bank.

- Woodgrove Bank hosts their business apps in an on-premises site. They host their mobile apps on Azure.
- There's VPN site-to-site connectivity between their on-premises edge network and the Azure virtual network. Because of the VPN connection, the virtual network in Azure appears as an extension of the on-premises network.
- Woodgrove wants to replicate on-premises workloads to Azure with Site Recovery.
 - Woodgrove has apps which depend on hard-coded IP addresses, so they need to retain IP addresses for the apps, after failover to Azure.
 - Resources running in Azure use the IP address range 172.16.1.0/24, 172.16.2.0/24.

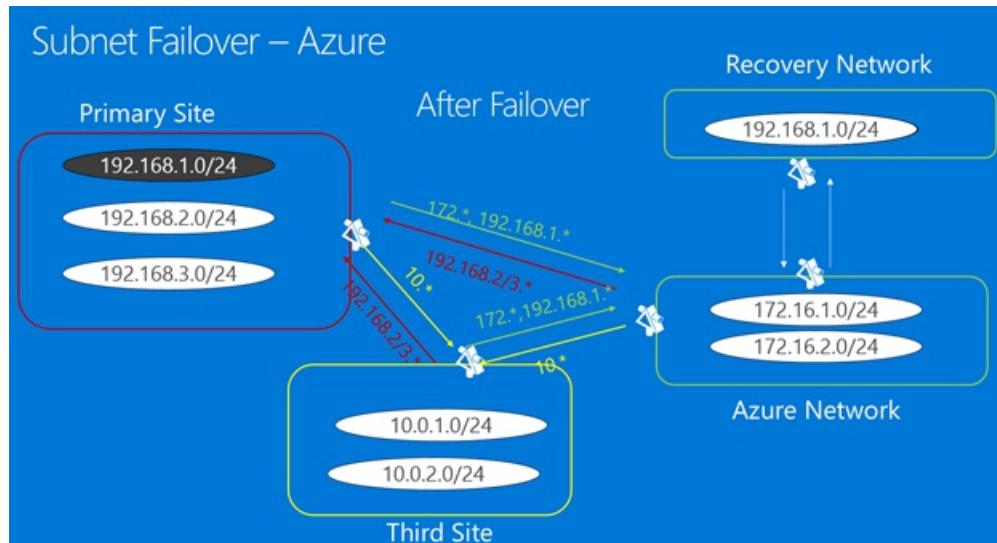


Infrastructure before failover

For Woodgrove to be able to replicate its VMs to Azure while retaining the IP addresses, here's what the company needs to do:

1. Create Azure virtual network in which the Azure VMs will be created after failover of on-premises machines. It should be an extension of the on-premises network, so that applications can fail over seamlessly.
2. Before failover, in Site Recovery, they assign the same IP address in the machine properties. After failover, Site Recovery assigns this address to the Azure VM.
3. After failover runs and the Azure VMs are created with the same IP address, they connect to the network using a [Vnet to Vnet connection](#). This action can be scripted.
4. They need to modify routes, to reflect that 192.168.1.0/24 has now moved to Azure.

Infrastructure after failover



Site-to-site connection

In addition to the vnet-to-vnet connection, after failover, Woodgrove can set up site-to-site VPN connectivity:

- When you set up a site-to-site connection, in the Azure network you can only route traffic to the on-premises location (local-network) if the IP address range is different from the on-premises IP address range. This is because Azure doesn't support stretched subnets. So, if you have subnet 192.168.1.0/24 on-premises, you can't add a local-network 192.168.1.0/24 in the Azure network. This is expected because Azure doesn't know that there are no active VMs in the subnet, and that the subnet is being created for disaster recovery only.
- To be able to correctly route network traffic out of an Azure network, the subnets in the network and the local-network mustn't conflict.

Assigning new IP addresses

This [blog post](#) explains how to set up the Azure networking infrastructure when you don't need to retain IP addresses after failover. It starts with an application description, looks at how to set up networking on-premises and in Azure, and concludes with information about running failovers.

Next steps

[Run a failover](#)

Plan capacity and scaling for VMware replication with Azure Site Recovery

7/13/2018 • 8 minutes to read • [Edit Online](#)

Use this article to figure out planning for capacity and scaling, when replicating on-premises VMware VMs and physical servers to Azure with [Azure Site Recovery](#).

How do I start capacity planning?

Gather information about your replication environment by running the [Azure Site Recovery Deployment Planner](#) for VMware replication. [Learn more](#) about this tool. You'll gather information about compatible and incompatible VMs, disks per VM, and data churn per disk. The tool also covers network bandwidth requirements, and the Azure infrastructure needed for successful replication and test failover.

Capacity considerations

COMPONENT	DETAILS
Replication	<p>Maximum daily change rate: A protected machine can only use one process server, and a single process server can handle a daily change rate up to 2 TB. Thus 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 storage account can handle a maximum of 20,000 requests per second, and we recommend that you keep the number of input/output operations per second (IOPS) across a source machine to 20,000. For example, if you have a source machine with 5 disks, and each disk generates 120 IOPS (8K size) on the source machine, then it will be 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 should be able to handle the daily change rate capacity across all workloads running on protected machines, and needs sufficient bandwidth to continuously replicate data to Azure Storage.</p> <p>As a best practice, locate the configuration server on the same network and LAN segment as the machines you want to protect. It can be located on a different network, but machines you want to protect should have layer 3 network visibility to it.</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, and optimizes it with caching, compression, and encryption. Then it sends the data to Azure. The process server machine should 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 stored in the event of a network bottleneck or outage.</p>

Size recommendations for the configuration server

CPU	MEMORY	CACHE DISK SIZE	DATA CHANGE RATE	PROTECTED MACHINES
8 vCPUs (2 sockets * 4 cores @ 2.5 gigahertz [GHz])	16 GB	300 GB	500 GB or less	Replicate less than 100 machines.
12 vCPUs (2 sockets * 6 cores @ 2.5 GHz)	18 GB	600 GB	500 GB to 1 TB	Replicate between 100-150 machines.
16 vCPUs (2 sockets * 8 cores @ 2.5 GHz)	32 GB	1 TB	1 TB to 2 TB	Replicate between 150-200 machines.
Deploy another process server			> 2 TB	Deploy additional process servers if you're replicating more than 200 machines, or if the daily data change rate exceeds 2 TB.

Where:

- Each source machine is configured with 3 disks of 100 GB each.
- We used benchmarking storage of 8 SAS drives of 10 K RPM, with RAID 10, for cache disk measurements.

Size recommendations for the process server

If you need to protect more than 200 machines, or the daily change rate is greater than 2 TB, you can add process servers to handle the replication load. To scale out, you can:

- Increase the number of configuration servers. For example, you can protect up to 400 machines with two configuration servers.
- Add more process servers, and use these to handle traffic instead of (or in addition to) the configuration server.

The following table describes a scenario in which:

- You're not planning to use the configuration server as a process server.
- You've set up an additional process server.
- You've configured protected virtual machines to use the additional process server.

- Each protected source machine is configured with three disks of 100 GB each.

CONFIGURATION SERVER	ADDITIONAL PROCESS SERVER	CACHE DISK SIZE	DATA CHANGE RATE	PROTECTED MACHINES
8 vCPUs (2 sockets * 4 cores @ 2.5 GHz), 16 GB memory	4 vCPUs (2 sockets * 2 cores @ 2.5 GHz), 8 GB memory	300 GB	250 GB or less	Replicate 85 or fewer machines.
8 vCPUs (2 sockets * 4 cores @ 2.5 GHz), 16 GB memory	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), 18 GB memory	12 vCPUs (2 sockets * 6 cores @ 2.5 GHz) 24 GB memory	1 TB	1 TB to 2 TB	Replicate between 150-225 machines.

The way in which you scale your servers depends on your preference for a scale-up or scale-out model. You scale up by deploying a few high-end configuration and process servers, or scale out by deploying more servers with fewer resources. For example, if you need to protect 220 machines, you could do either of the following:

- Set up the configuration server with 12 vCPU, 18 GB of memory, and an additional process server with 12 vCPU, 24 GB of memory. Configure protected machines to use the additional process server only.
- Set up two configuration servers (2 x 8 vCPU, 16 GB RAM) and two additional process servers (1 x 8 vCPU and 4 vCPU x 1 to handle 135 + 85 [220] machines). Configure protected machines to use the additional process servers only.

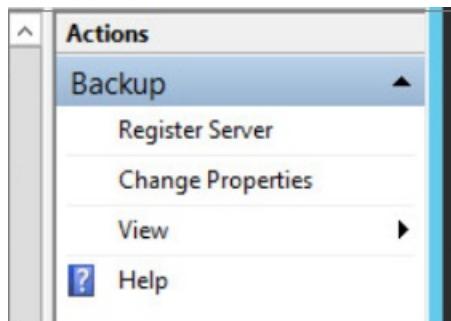
Control network bandwidth

After you've used the [the Deployment Planner tool](#) to calculate the bandwidth you need for replication (the initial replication and then delta), you can control the amount of bandwidth used for replication using a couple of options:

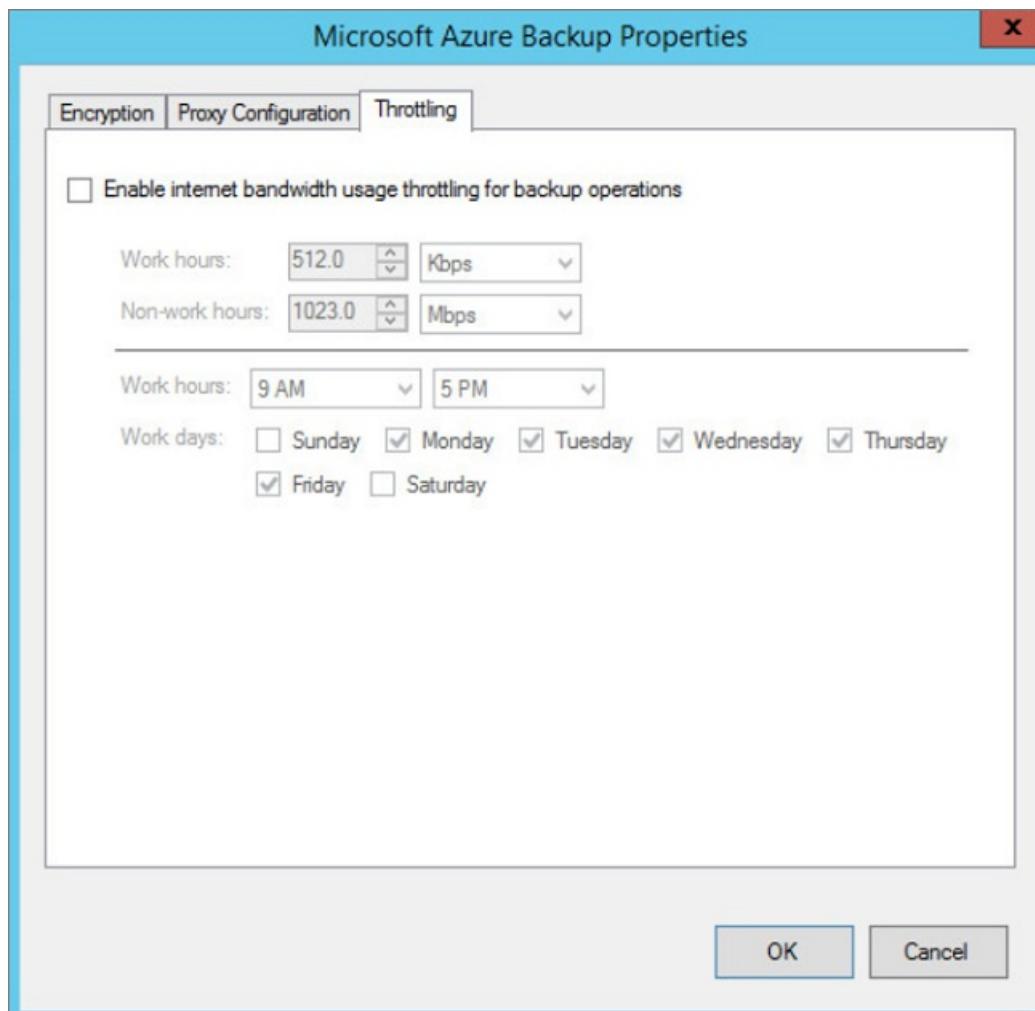
- Throttle bandwidth:** VMware traffic that replicates to Azure goes through a specific process server. You can throttle bandwidth on the machines running as process servers.
- Influence bandwidth:** You can influence the bandwidth used for replication by using a couple of registry keys:
 - The **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows 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 used for replication.
 - The **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Azure Backup\Replication\DownloadThreadsPerVM** specifies the number of threads used for data transfer during failback.

Throttle bandwidth

- Open the Azure Backup MMC snap-in on the machine acting 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\wabadmin.
- In the snap-in, click **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 1023 Mbps per second.



You can also use the [Set-OBMachineSetting](#) cmdlet to set throttling. Here's a sample:

```
$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.

Influence network bandwidth for a VM

1. In the VM's registry, navigate to **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Azure Backup\Replication**.
 - To influence the bandwidth traffic on a replicating disk, modify the value of **UploadThreadsPerVM**, or create the key if it doesn't exist.
 - To influence the bandwidth for fallback traffic from Azure, modify the value of

DownloadThreadsPerVM.

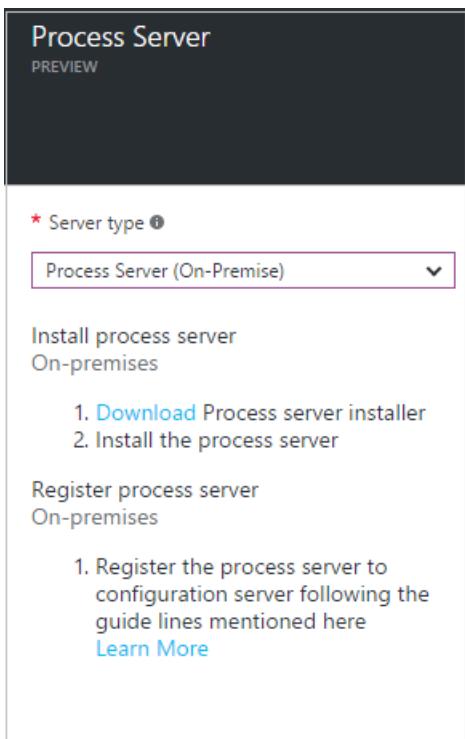
2. The default value is 4. In an “overprovisioned” network, these registry keys should be changed from the default values. The maximum is 32. Monitor traffic to optimize the value.

Deploy additional process servers

If you have to scale out your deployment beyond 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. Follow instructions given on [this article](#) to set up the process server. After setting up the server, you can migrate source machines to use it.

Migrate machines to use the new process server

1. In **Settings > Site Recovery servers**, click the configuration server, and then expand **Process servers**.



2. Right-click the process server currently in use, and click **Switch**.

3. In **Select target process server**, select the new process server you want to use, and then select the virtual machines that the server will handle. Click the information icon to get information about the server. To help you make load decisions, the average space that's needed to replicate each selected virtual machine to the new process server is displayed. Click the check mark to start replicating to the new process server.

Deploy additional master target servers

You will need additional master target server during the following scenarios

1. If you are trying to protect a Linux-based virtual machine.
2. If the master target server available on configuration server doesn't have access to the datastore of VM.
3. If the total number of disks on master target server (no. of local disks on server + disks to be protected) exceeds 60 disks.

To add a new master target server for **Linux-based virtual machine**, [click here](#).

For **Windows-based virtual machine**, follow the below given instructions.

1. Navigate to **Recovery Services Vault > Site Recovery Infrastructure > Configuration servers**.
2. Click on the required configuration server > **+Master Target Server**.

CS1
Configuration Server

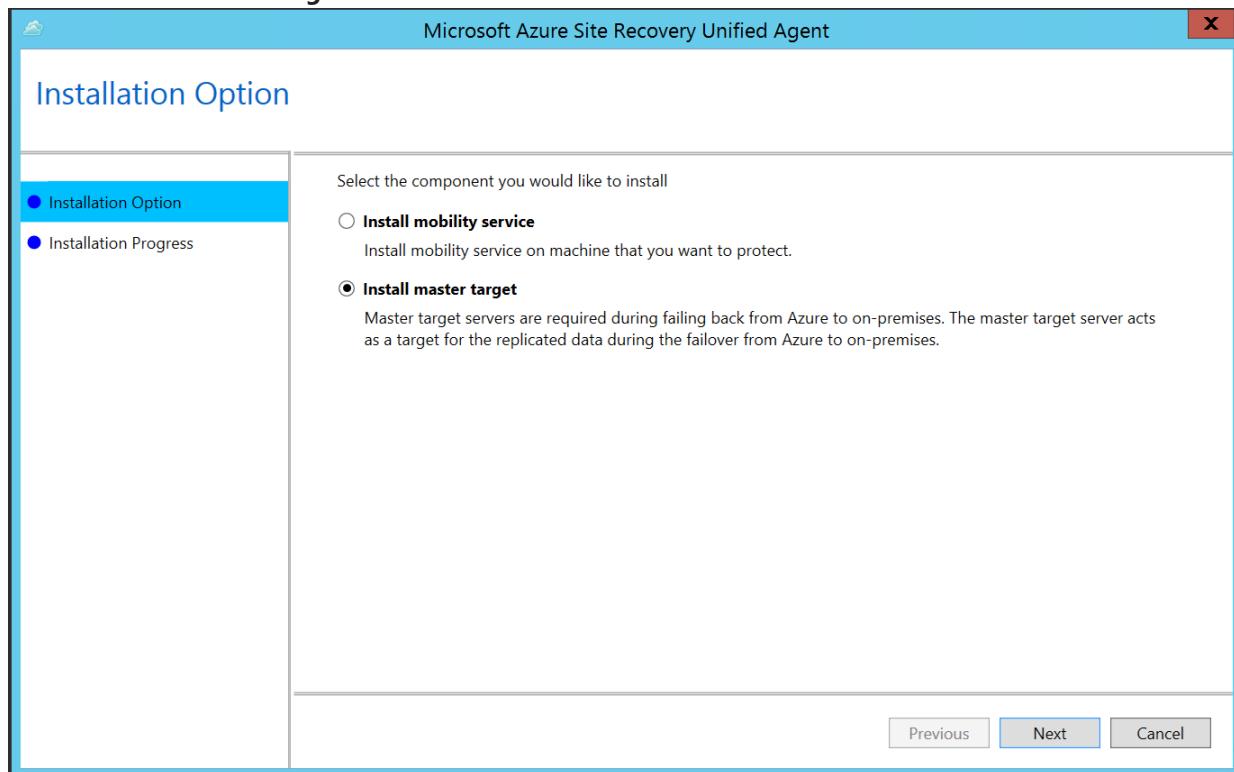
vCenter Process Server Master Target Server Refresh Server More

Essentials

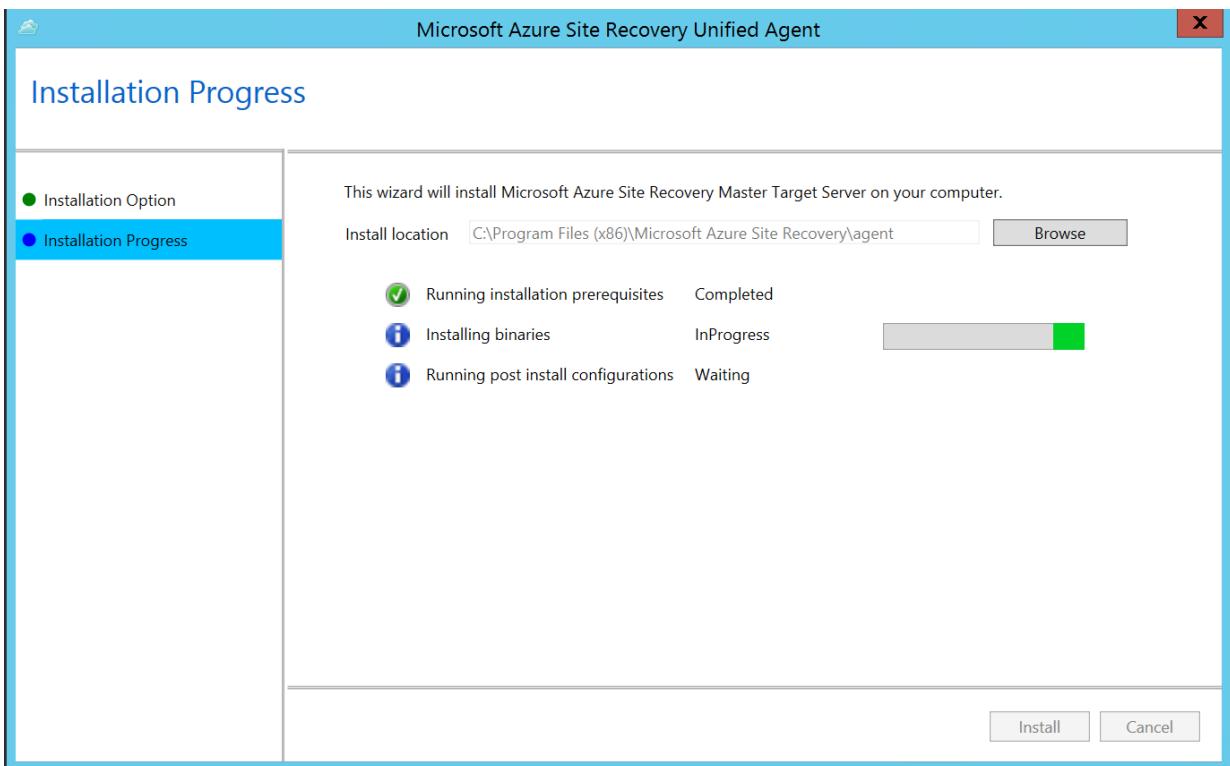
Recovery Services vault	Connection status
CS1	Connected
IP address	Last heartbeat at
[REDACTED]	6/26/2018 5:24:14 PM
Configuration Server version	Provider version
9.17.0.0	5.1.3400.0
Connected agents	Server ID
5	[REDACTED]
Protected items	
3	

3. Download the unified set-up and run it on the VM to set up master target server.

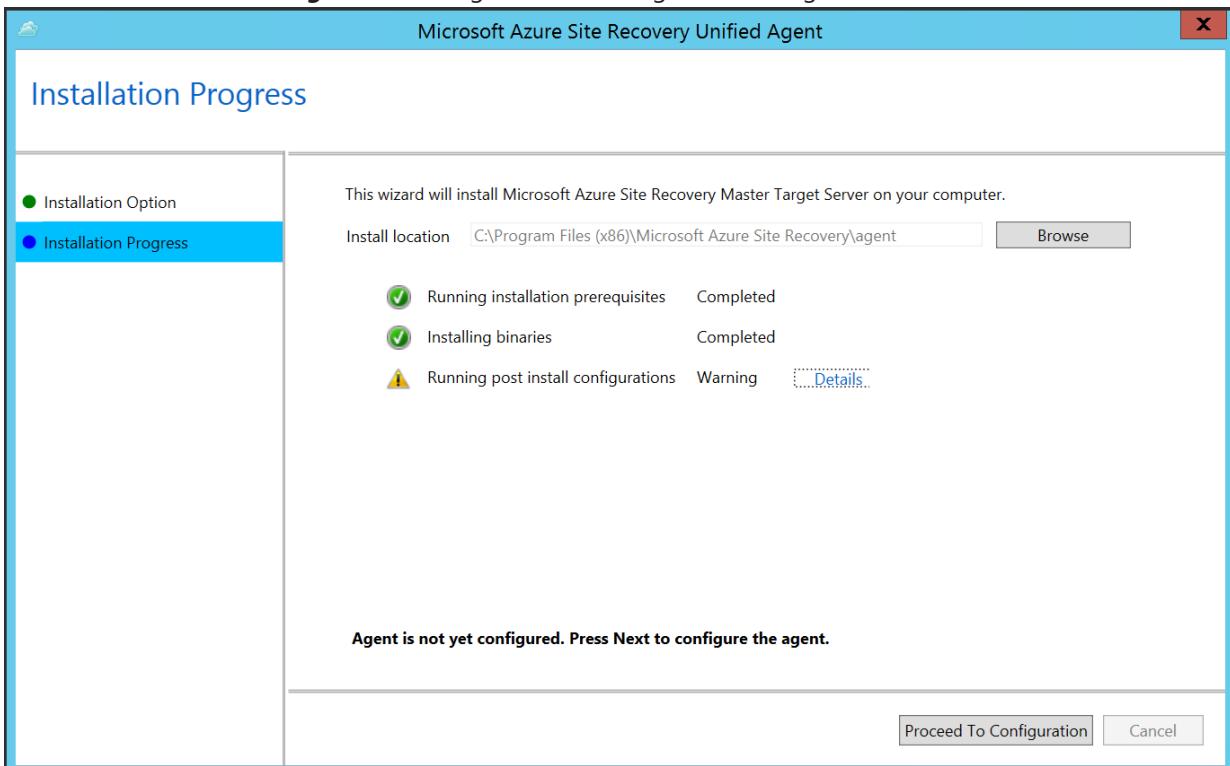
4. Choose **Install master target** > **Next**.



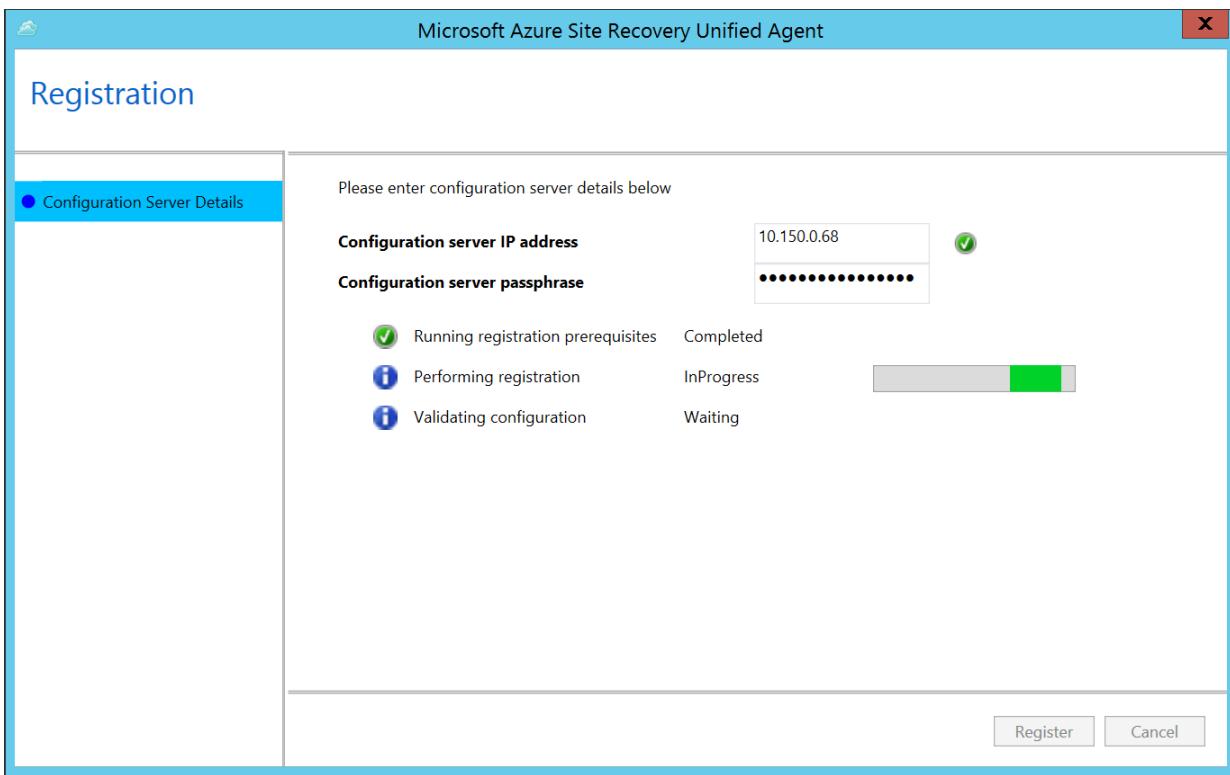
5. Choose default install location > click **Install**.



6. Click on **Proceed to Configuration** to register master target with configuration server.



7. Enter the IP address of configuration server & passphrase. [Click here](#) to learn how to generate passphrase.



8. Click **Register** and post registration click **Finish**.
9. Upon successful registration, this server is listed on portal under **Recovery Services Vault > Site Recovery Infrastructure > Configuration servers** > master target servers of relevant configuration server.

NOTE

You can also download the latest version of Master target server unified set-up for Windows [here](#).

Next steps

Download and run the [Azure Site Recovery Deployment Planner](#)

Azure Site Recovery Deployment Planner for VMware to Azure

7/9/2018 • 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 account) requirement for each VM
- Total number of standard and premium storage accounts to be set up for replication
- Storage-account naming suggestions, based on Storage guidance
- Storage account placement for all VMs
- 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 6.5, 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 should be set to 2 or high level • Allow 443 port: Site Recovery Deployment Planner uses this port to connect to the vCenter server/ESXi host
Report generation	A Windows PC or Windows Server with Excel 2013 or later
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

1. 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.
2. 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_v2.2.zip

E:\ASR Deployment Planner_v2.2\ASRDeploymentPlanner.exe

Update to the latest version of Deployment Planner

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 2.2. 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](#)

Run Azure Site Recovery deployment planner for VMware to Azure

7/9/2018 • 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 four 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.

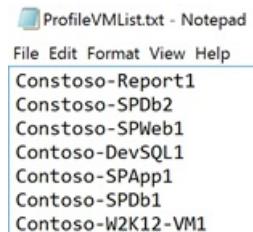
```
Add-PSSnapin VMware.VimAutomation.Core
```

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.



```
ProfileVMList.txt - Notepad
File Edit Format View Help
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 clouds.

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 upto 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 ASR 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  
Eby8vdM02xNOcqFlqUwJPL1mEt1CDXJ1OUzFT50uSRZ6IFsuFq2UVErCz4I6tq/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_.xlsm and placed in the specified directory.

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.
-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.

PARAMETER NAME	DESCRIPTION
-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.
-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 for your specific target Azure region in the specified currency.

PARAMETER NAME	DESCRIPTION
-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 configurd to profile and generate report upto 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

```
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 Mbps	To meet RPO 90% of the time: 570 Mbps	To meet RPO 100% of the time: 704 Mbps
-------------------------------	---------------------------------------	--

Required Azure Storage Accounts Total: 3

Standard	Premium
1	2

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

Recommendation: Use ExpressRoute

Recommended VM placement plan

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

Date	Peak RPO per day
01-Nov	15
02-Nov	12
03-Nov	18
04-Nov	15
05-Nov	8
06-Nov	10
07-Nov	18
08-Nov	8
09-Nov	10
10-Nov	12

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**

Bandwidth in Mbps	Number of VMs per batch
200	7
350	7
400	7
450	7
510	7
630	7
704	7
800	7

Cost estimation: Target region - WestUS2

Show per Month

Total DR Cost per Month In US Dollar (\$) **\$8,868**

Cost by components

- 2,675, 30%
- 1,507, 17%

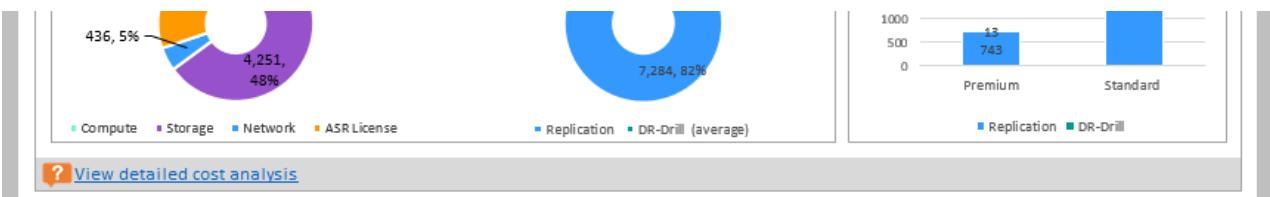
Cost by states

- 1,584, 18%

Azure Storage Cost per Month

US Dollar (\$)

Cost	Value
3,330	Low
65	High



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	(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 clouds.

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 -VMListFile
E:\vCenter1_ProfiledData\ProfileVMList1.txt -StorageAccountName asrspfarm1 -StorageAccountKey
by8vdM02xN0cqFlqUwJPLlmEt1CDXJ10UzFT50uSRZ6IFsuFq2UVErCz4I6tq/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.](#)

Azure Site Recovery deployment planner report

7/9/2018 • 19 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.

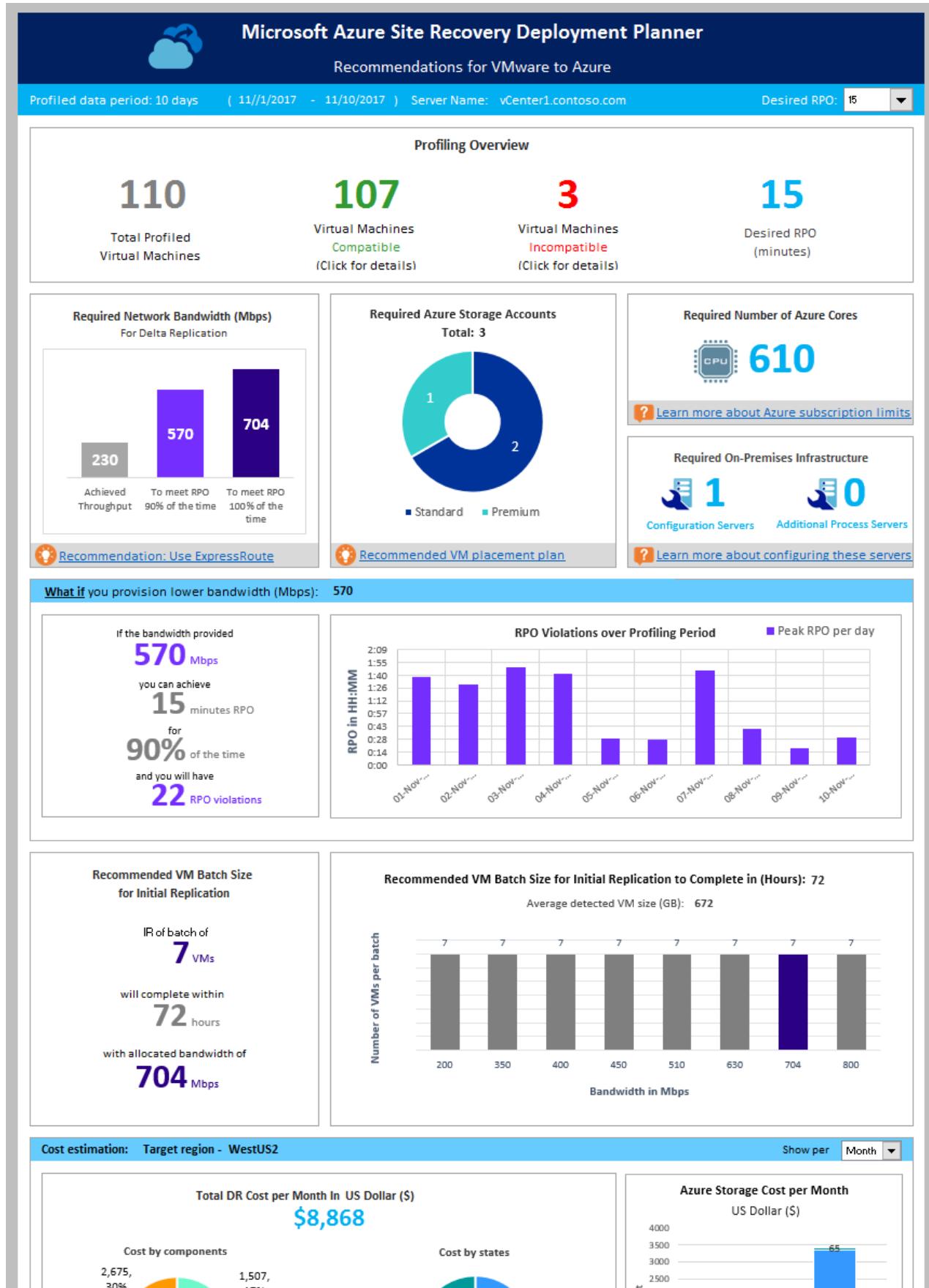
Desired RPO (minutes): Either the default recovery point objective or the value passed for the 'DesiredRPO' parameter at the time of report generation to estimate required bandwidth.

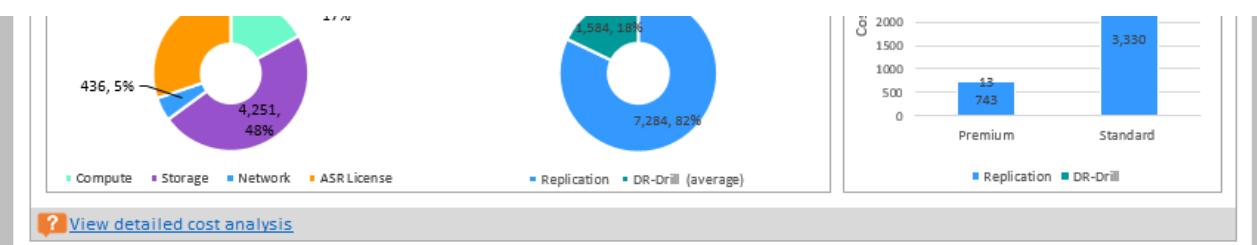
Desired bandwidth (Mbps): The value that you have passed for the 'Bandwidth' parameter at the time of report generation to estimate achievable RPO.

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:





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 ... [+](#)

Profiled data

Microsoft Azure Site Recovery Deployment Planner

Recommendations for VMware to Azure

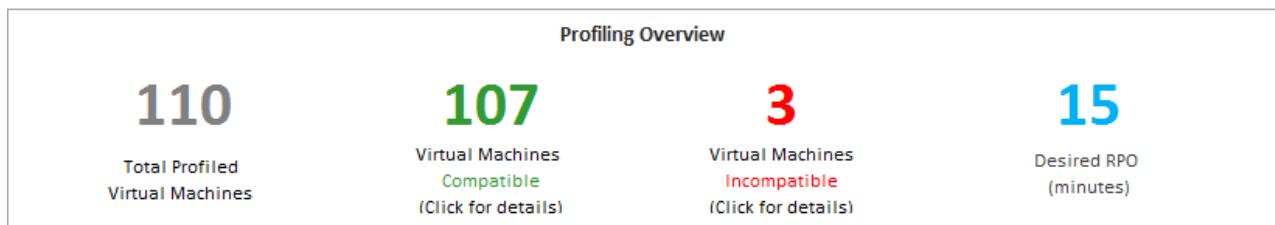
Profiled data period: 10 days (11/1/2017 - 11/10/2017) Server Name: vCenter1.contoso.com Desired RPO: 15

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



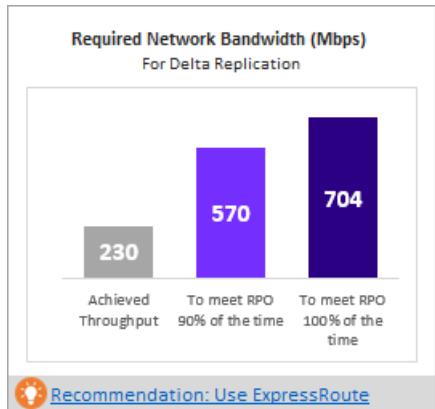
Total Profiled Virtual Machines: The total number of VMs whose profiled data is available. If the VMListFile has names of any VMs which were not profiled, those VMs are not considered in the report generation and are excluded from the total profiled VMs count.

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:

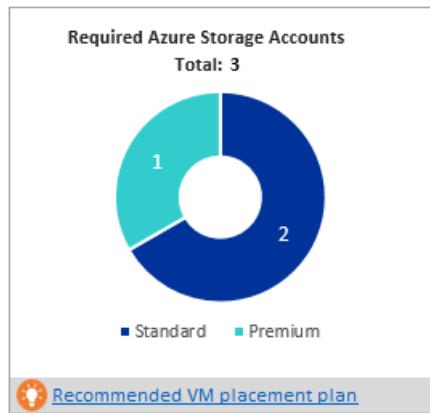
1. Check to see whether there is any network Quality of Service (QoS) that is limiting Site Recovery throughput.
2. Check to see whether your Site Recovery vault is in the nearest physically supported Microsoft Azure region to minimize network latency.
3. Check your local storage characteristics to determine 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](#).

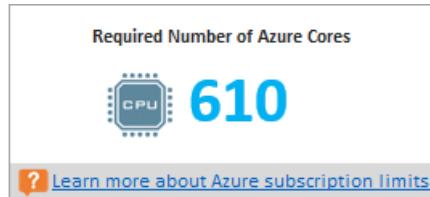
Required storage accounts

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.



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

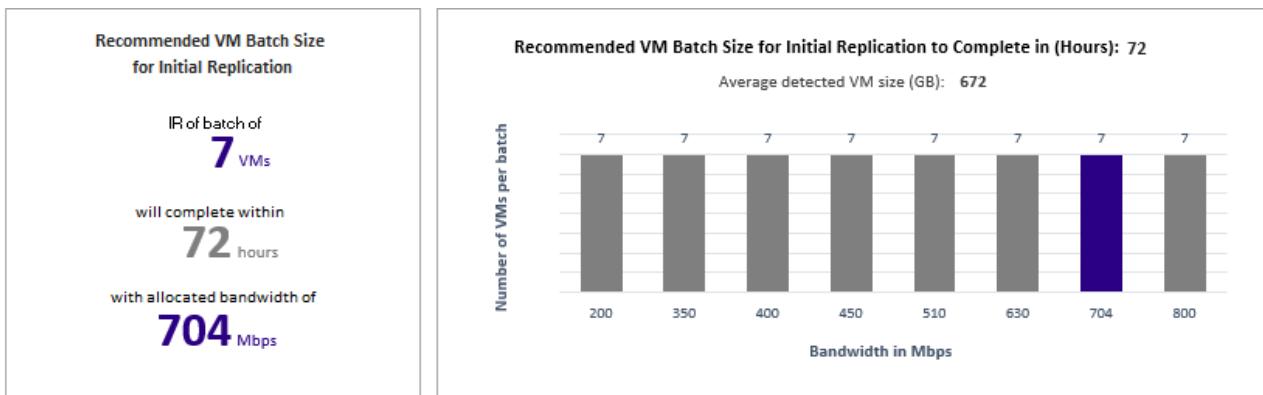


Recommended VM batch size for initial replication

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.

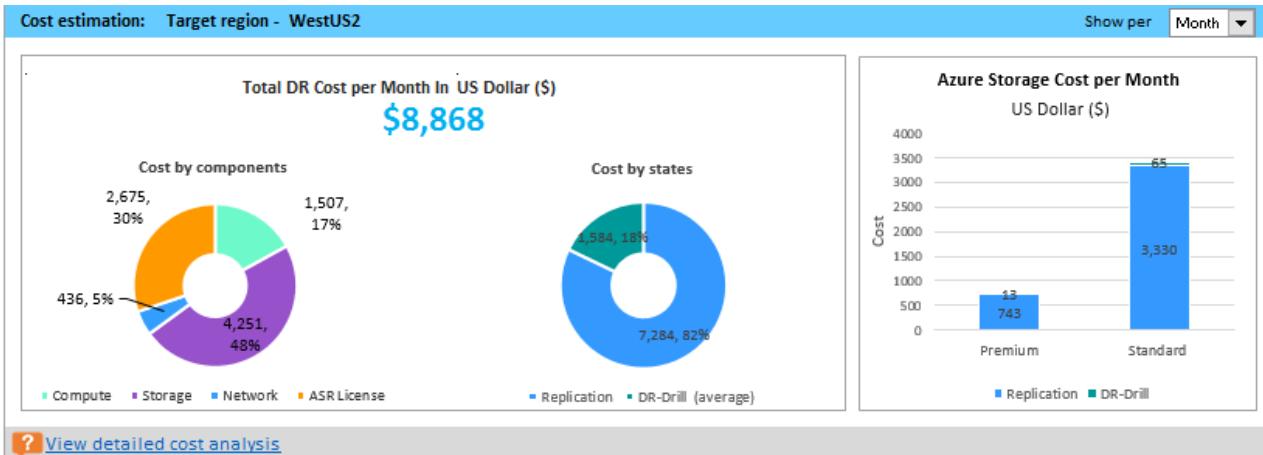
The graph here shows a range of bandwidth values and a calculated VM batch size count to complete initial replication in 72 hours, based on the average detected VM size across all the compatible VMs.

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.

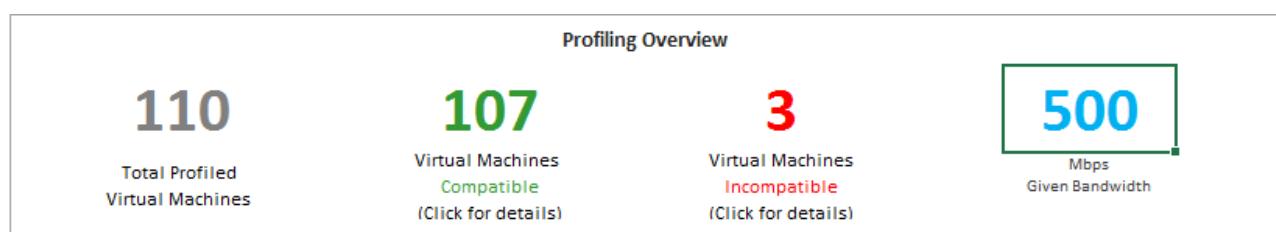
Azure storage cost per Month/Year It shows the total storage cost that will be incurred for premium and standard storage for replication and DR drill. You can view detailed cost analysis per VM in the [Cost Estimation](#) sheet.

Growth factor and percentile values used

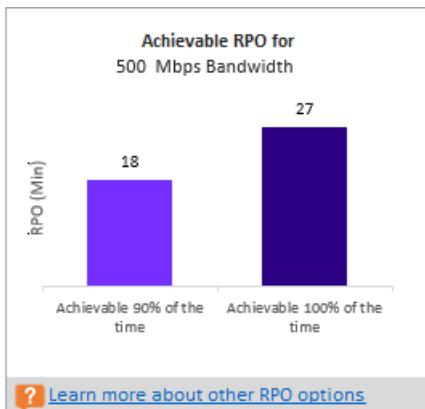
This section at the bottom of the sheet shows the percentile value used for all the performance counters of the profiled VMs (default is 95th percentile), and the growth factor (default is 30 percent) that's used in all the calculations.

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

Replication Storage Type	Suggested Prefix	Suggested Account Name	Log Storage Account Type	Suggested Prefix	Suggested Log Account Name	Placement Summary	VMs to Place
Standard	clk	clk<standard>	Standard	NA	NA	Total number of VMs: 103 Total read/write IOPS: 8482 Total write IOPS: 5292 Total provisioned size across all disks: 122.24 TB Total disks: 301 S4:10 S6:15 S10:50 S15:15 S20:200 S30:11	
Premium	cuz	cuz<premium>	Standard	m7y	m7y<standard2>	Total number of VMs: 4 Total read/write IOPS: 2885 Total write IOPS: 581 Total provisioned size across all disks: 5.76 TB Total disks: 9 P10:5 P15:2 P20:2 P30:3	
Managed disk considered for failover or test failover:							Yes
Total unmanaged disks across premium storage accounts for replication		Total premium managed disks created during failover and test failover					
Disk type	Total number of disks	Disk type	Total number of disks				
P10	5	P10	5				
P15	2	P15	2				
P20	2	P20	2				
P30	3	P30	3				
P40	0	P40	0				
P50	0	P50	0				
Total unmanaged disks across standard storage accounts for replication		Total standard managed disks created during failover and test failover					
Total number of disks	69024	S4	10				
Total disks size (GB)		S6	15				
		S10	50				
		S15	15				
		S20	200				
		S30	11				

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. It 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, 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	Suggested Prefix	Storage Account	Peak R/W IOPS (with Growth Factor)	Peak Data Churn (Mbps) (with Growth)	Number of Disks	Disk Size (GB)	Cores	Memory (MB)	NICs	Boot Type	OS Type
vm1.com)	Yes	Standard	c1k	c1v<standard>	6	0.04	Standard_A2	2	40	2	2048	1	BIOS
scsi0:0 Hard disk 1		\$4			6	0.04		30					
scsi0:1 Hard disk 2		\$4			0	0.00		10					
vm2.com)	Yes	Premium	cuz	cuz<premium>	60	8.85	Standard_D5s_v2	2	210	4	8192	1	BIOS
scsi0:0 Hard disk 1		P30			60	8.85		800					
scsi0:1 Hard disk 2		P20			0	0.00		300					
vm3.com)	Yes	Standard	c1k	c1v<standard>	95	0.97	Standard_A4	2	190	8	8192	1	BIOS
scsi0:0 Hard disk 1		\$15			95	0.97		150					
scsi0:1 Hard disk 2		\$6			0	0.00		40					
vm4.com)	Yes*	Standard	c1k	c1v<standard>	2	0.02	Standard_A1_v2	2	32	1	2048	1	BIOS
scsi0:0 Hard disk 1		\$4			2	0.02		30					
scsi0:1 Hard disk 2		\$4			0	0.00		2					

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 [Azure Premium Storage](#). 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.

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), 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
dc-01-01-00-00-00-00	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					
gwin-01-01-00-00-00-01.com	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					
scsi0:4 Hard disk 4	Not supported (Average effective write IOPS exceeds supported ASR (IOPS limit (840))	52	0.23		500					
scsi0:0 Hard disk 1		0	0.00		40					
lin-01-01-00-00-00-00	No	85	0.67	3	6500	2	1024	1	BIOS	Other Linux (64-bit)
scsi0:2 Hard disk 3	Not Supported (Disk size > 4095 GB)	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:

- Disk size is >4095 GB. Azure Storage currently does not support data disk sizes greater than 4095 GB.
 - OS disk is >2048 GB. Azure Storage currently does not support OS disk size greater than 2048 GB.
 - 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 10 MB/s for average I/O size for the disk.
 - Average data churn exceeds supported Site Recovery data churn limit of 25 MB/s for average I/O size for the VM (sum of all disks churn).
 - 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. Failback 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	10 MB/s	842 GB per disk

SOURCE DATA CHURN	MAXIMUM LIMIT
Average data churn per VM	25 MB/s
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](#).

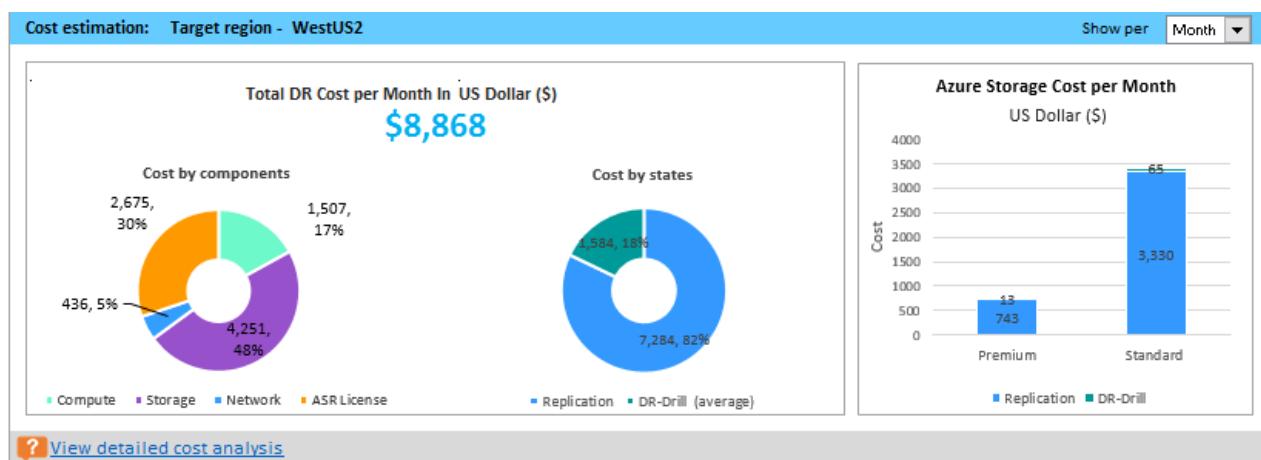
Cost estimation report of Azure Site Recovery deployment planner

7/9/2018 • 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.

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.

Microsoft Azure Site Recovery Deployment Planner

Cost estimation report

Subscription ID: 4d19f16b-3e00-4b89-a2ba-8645edf42fe5, Offer ID: MS-AZR-0003P

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)		Storage cost - Month (with discount)
Replication		DR-Drill	Replication	DR-Drill	Replication
Premium	\$34,025	\$3,847	\$34,025	\$3,847	\$2,835
Standard	\$40,073	\$3,290	\$40,073	\$3,290	\$3,339
Total	\$74,098	\$7,137	\$74,098	\$7,137	\$6,175
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		
Number of VMs		IaaS size	Using Managed disk	Yes	
Domain controller/DNS	0	Standard_D3	Currency		US Dollar (\$)
SQL Always On	0	Standard_D3	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:

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 / 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					
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)
START:INSERT A ROW BELOW TO ADD A NEW ENTRY							
colmagicsql1 (C01-CU-SV-EE001)	1	Standard_DS5_v2	Standard_DS5_v2	Premium	2949.00	4	Apply to all 7
coleciteweb05 (C01-CU-SV-EB003)	1	Standard_DS3_v2	Standard_DS3_v2	Premium	652.00	4	7
coleciteweb07 (C01-CU-SV-EB004)	1	Standard_A3	Standard_A3	Standard	652.00	4	7
colapiappsm02 (C01-CU-SV-EB004)	1	Standard_A2	Standard_A2	Standard	200.00	4	7
colsu1407 (C01-CU-SV-EB004)	1	Standard_A4	Standard_A4	Standard	300.00	4	7
colixtexssql (C01-CU-SV-EB004)	1	Standard_D5_v2	Standard_D5_v2	Standard	1194.00	4	7
colbimssql001 (C01-CU-SV-FR001)	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

Using managed disk: It specifies whether managed disk is being used at the time of DR drills. The default is yes. If you have set -UseManagedDisks to No, it uses the unmanaged disk price 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														
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 VMs, click on the Insert row button below to insert a new row between Start and End rows. 2. Click on 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														
Insert row		Re-calculate cost												
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 INSERT A ROW BELOW TO ADD A NEW ENTRY											\$0	\$0	\$0	
co1magrc01 (O1-CU-SV-F#001)	1	Standard_D5S_v2	Standard_D5S_v2	Premium	2949.00	4	Apply to all	Windows	LRS	Yes	\$5,862	\$4,954	\$608	
colecrwe001 (O1-CU-SV-E#003)	1	Standard_D5S_v2	Premium	652.00	4	7	Windows	LRS	Yes	\$1,577	\$1,095	\$181		
colecrwe002 (O1-CU-SV-E#004)	1	Standard_A3	Standard_A3	Standard	652.00	4	7	Windows	LRS	Yes	\$855	\$391	\$164	
colecrapp001 (O1-CU-SV-E#005)	1	Standard_A2	Standard_A2	Standard	200.00	4	7	Windows	LRS	Yes	\$441	\$210	\$24	
colecrapp002 (O1-CU-SV-E#006)	1	Standard_A4	Standard_A4	Standard	200.00	4	7	Windows	LRS	Yes	\$767	\$360	\$347	
colecrteq001 (O1-CU-SV-E#004)	1	Standard_D5_v2	Standard_D5_v2	Standard	1194.00	4	7	Windows	LRS	Yes	\$1,205	\$716	\$189	
colebmssrp001 (O1-CU-SV-E#001)	1	Standard_A4	Standard_A4	Standard	550.00	4	7	Windows	LRS	Yes	\$928	\$330	\$298	
colebmssrp002 (O1-CU-SV-E#004)	1	Standard_A2_v2	Standard_A2_v2	Standard	541.00	4	7	Windows	LRS	Yes	\$660	\$325	\$35	
colecrteq002 (O1-CU-SV-E#002)	1	Standard_A3	Standard_A3	Standard	200.00	4	7	Windows	LRS	Yes	\$586	\$360	\$164	
colecrteq003 (O1-CU-SV-E#004)	1	Standard_G5	Standard_G5	Standard	221.00	4	7	Windows	LRS	Yes	\$6,991	\$713	\$318	
colecrteq004 (O1-CU-SV-E#005)	1	Standard_G5	Standard_G5	Standard	200.00	4	7	Windows	LRS	Yes	\$5,291	\$210	\$281	
colecrteq005 (O1-CU-SV-E#006)	1	Standard_G5	Standard_G5	Standard	200.00	4	7	Windows	LRS	Yes	\$5,291	\$210	\$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)
 - 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 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 (руб)
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](#).

Set up additional process servers for scalability

8/9/2018 • 7 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 do this.

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.

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/Process server requirements

COMPONENT	REQUIREMENT
HARDWARE SETTINGS	
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

COMPONENT	REQUIREMENT
Free disk space (retention disk)	600 GB
SOFTWARE SETTINGS	
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 preexisting default website - No preexisting website/application listening on port 443 - Enable anonymous authentication - Enable FastCGI setting
NETWORK SETTINGS	
IP address type	Static
Internet access	The server needs access to these URLs (directly or via proxy): - *.accesscontrol.windows.net - *.backup.windowsazure.com - *.store.core.windows.net - *.blob.core.windows.net - *.hypervrecoverymanager.windowsazure.com - https://management.azure.com - *.services.visualstudio.com - time.nist.gov - time.windows.com OVF also needs access to the following URLs: - https://login.microsoftonline.com - https://secure.aadcdn.microsoftonline-p.com - https://login.live.com - https://auth.gfx.ms - https://graph.windows.net - https://login.windows.net - https://www.live.com - https://www.microsoft.com - https://dev.mysql.com/get/Downloads/MySQLInstaller/mysql-installer-community-5.7.20.0.msi

COMPONENT	REQUIREMENT
Ports	443 (Control channel orchestration) 9443 (Data transport)
NIC type	VMXNET3 (if the Configuration Server is a VMware VM)
SOFTWARE TO INSTALL	
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.

Configuration/Process server sizing requirements

CPU	MEMORY	CACHE DISK	DATA CHANGE RATE	REPLICATED MACHINES
8 vCPUs 2 sockets * 4 cores @ 2.5 GHz	16GB	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. Log on 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**.

The screenshot shows the Microsoft Azure Site Recovery Configuration Server interface. On the left, there's a sidebar with 'Essentials' expanded, showing details such as 'Recovery Services vault' (IgniteDemoVault), 'IP address' (10.10.20.66), 'Configuration Server version' (9.3.0.0), and 'Connected agents' (4). Below this is a table for 'Associated servers' with columns: NAME, STATUS, SERVER ROLE, VERSION, and LAST HEART BEAT. Three entries are listed: 'Process Ser...', 'vCenter Ser...', and 'Master Targ...'. Under 'Configuration Server health', there are two items: 'Processor queue' (0) and 'CPU utilization' (0 used). On the right, a modal window titled 'Add process server' is open. It has a step-by-step guide: 1. Download the Microsoft Azure Site Recovery Unified Setup, 2. Install additional Process Server to scale out your deployment. It also has sections for 'Install process server' (On-premises) and 'Register process server' (On-premises). A blue 'OK' button is at the bottom right of the modal.

- Click **Download the Microsoft Azure Site Recovery Unified Setup**. This downloads the latest version of the installation file.

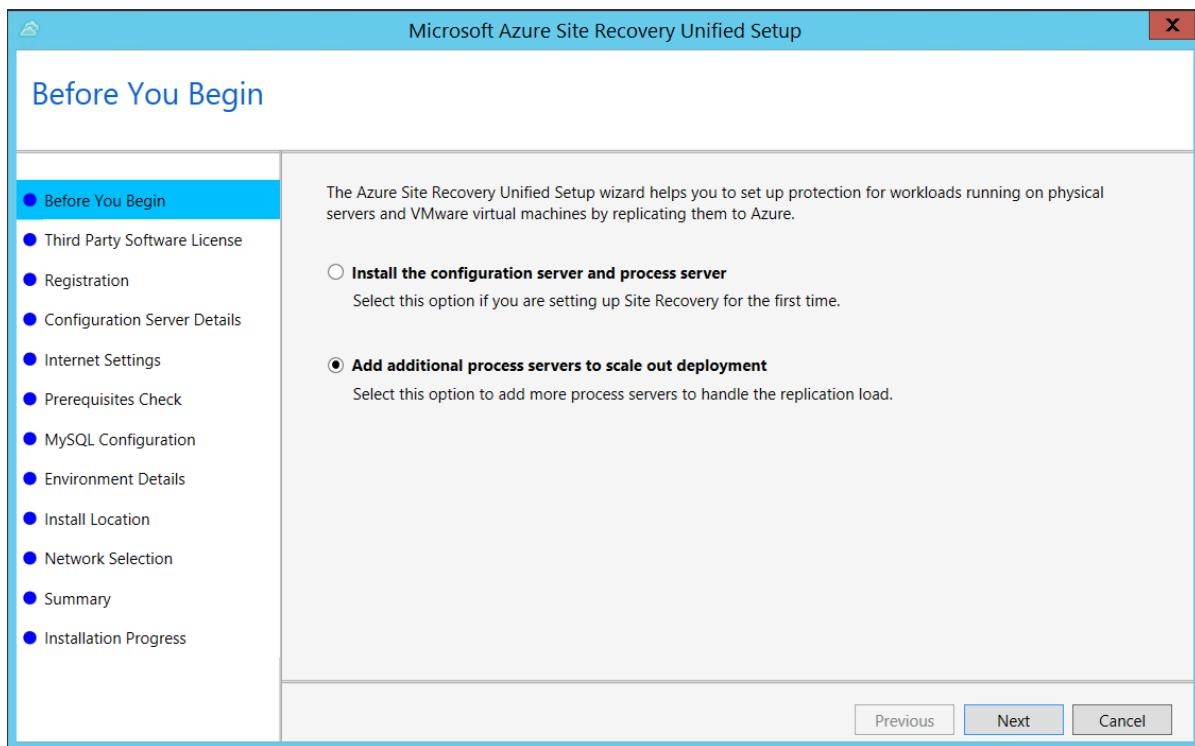
WARNING

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.

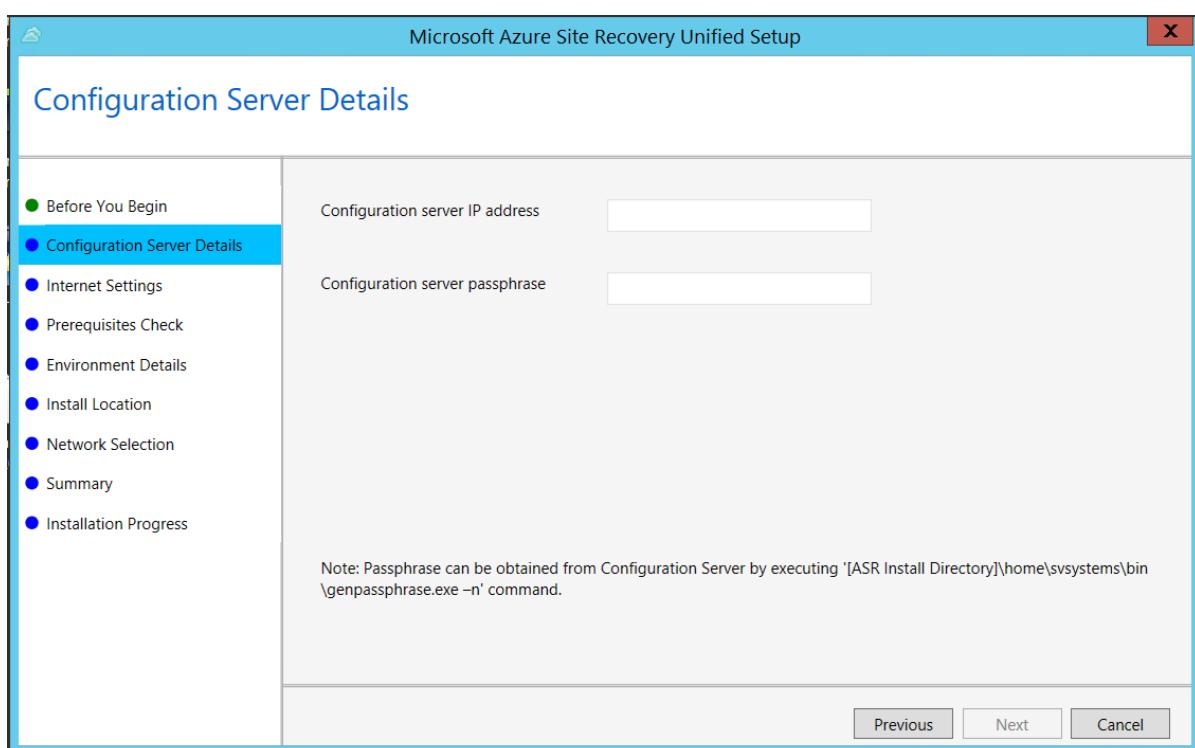
Install from the UI

Install as follows. After setting up the server, you migrate source machines to use it.

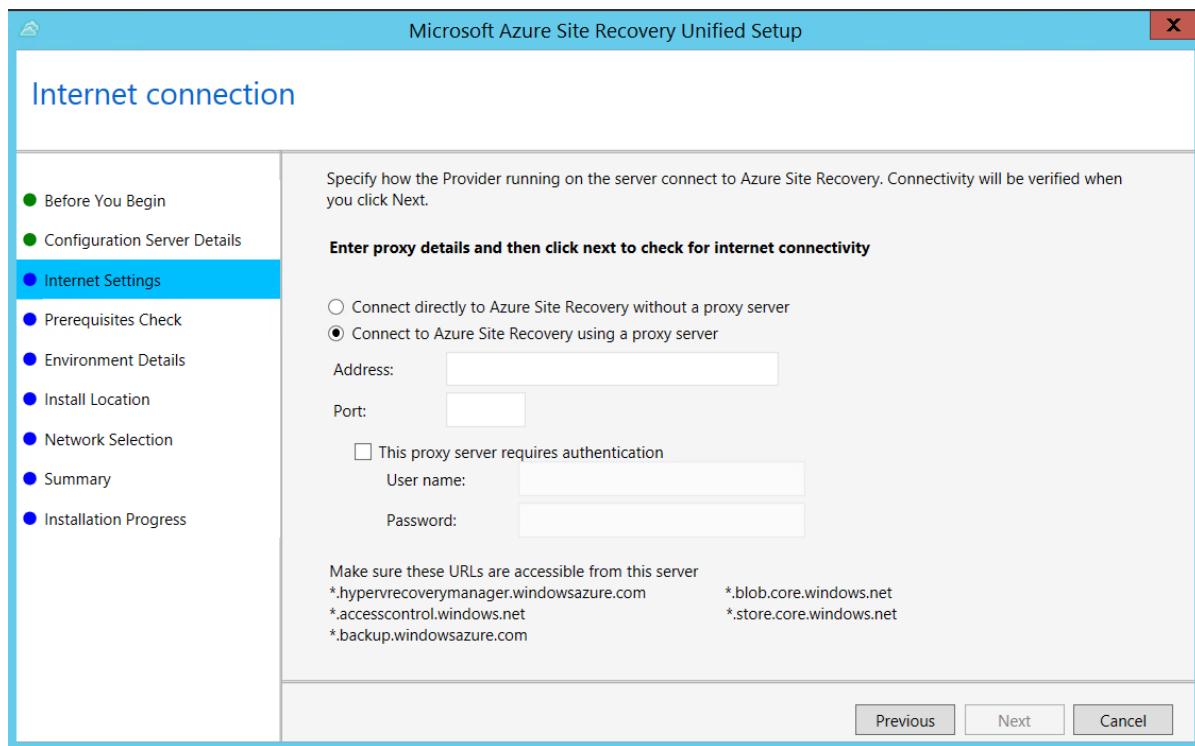
- Launch the Azure Site Recovery UnifiedSetup.exe
- In **Before you begin**, select **Add additional process servers to scale out deployment**.



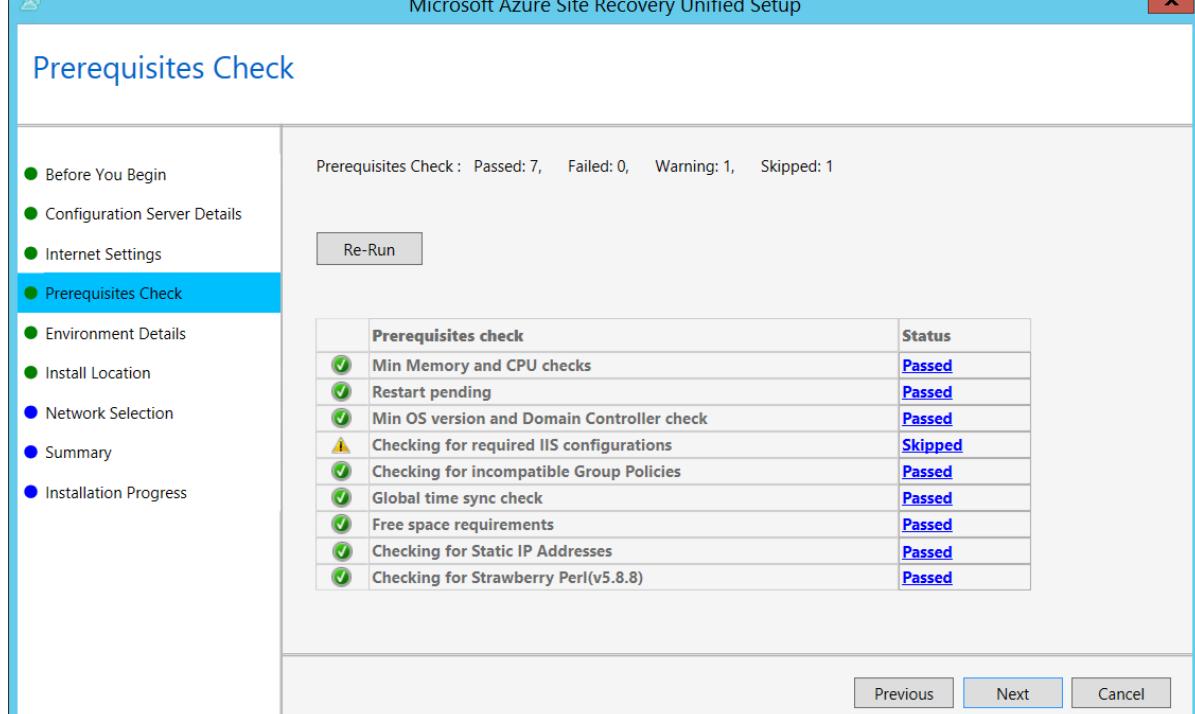
3. In **Configuration Server Details**, specify the IP address of the Configuration Server, and the passphrase.



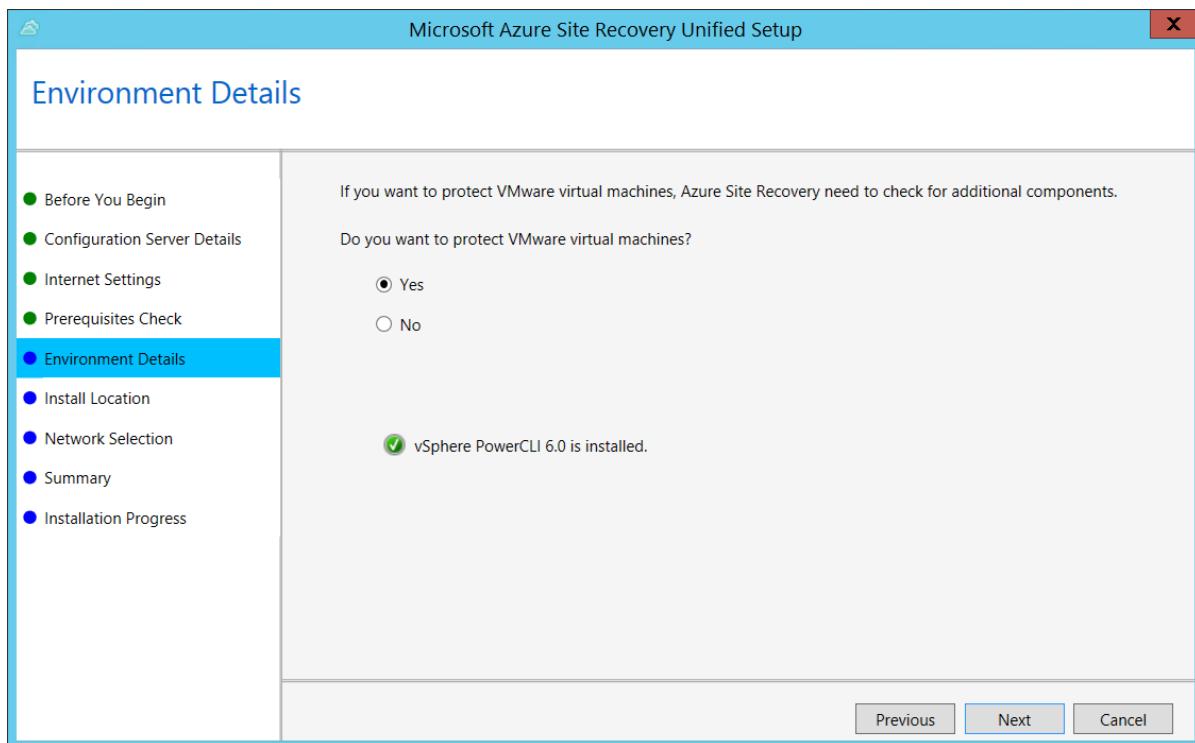
4. In **Internet Settings**, specify how the Provider running on the Configuration Server connects to Azure Site Recovery over the Internet.



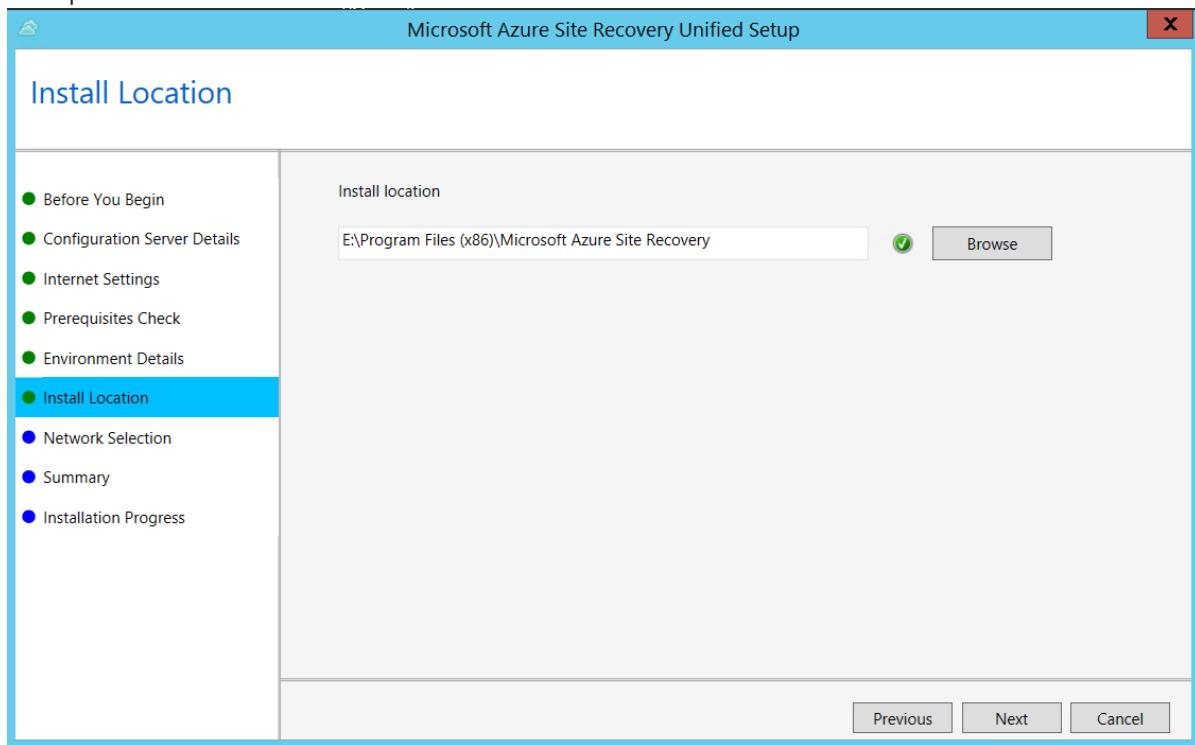
- If you want to connect with the proxy that's currently set up on the machine, select **Connect with existing proxy settings**.
 - If you want the Provider to connect directly, select **Connect directly without a proxy**.
 - If the existing proxy requires authentication, or if you want to use a custom 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.



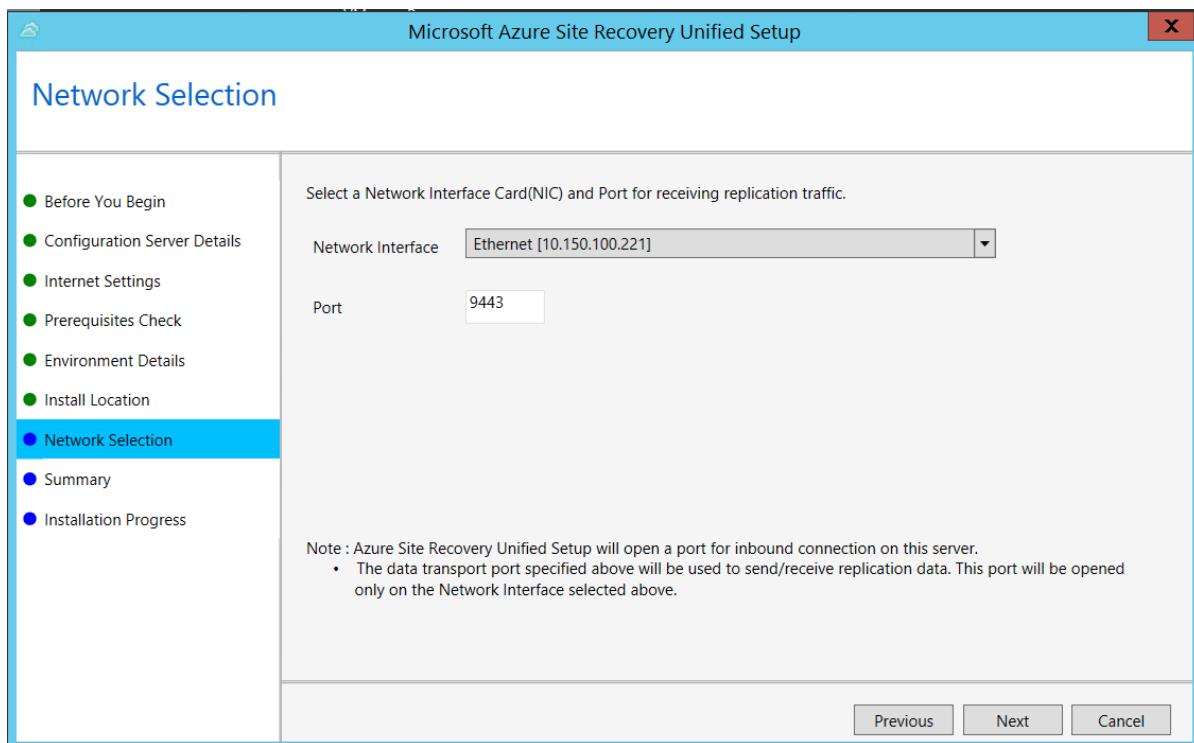
6. In **Environment Details**, select whether you're going to replicate VMware VMs. If you are, then setup checks that PowerCLI 6.0 is installed.



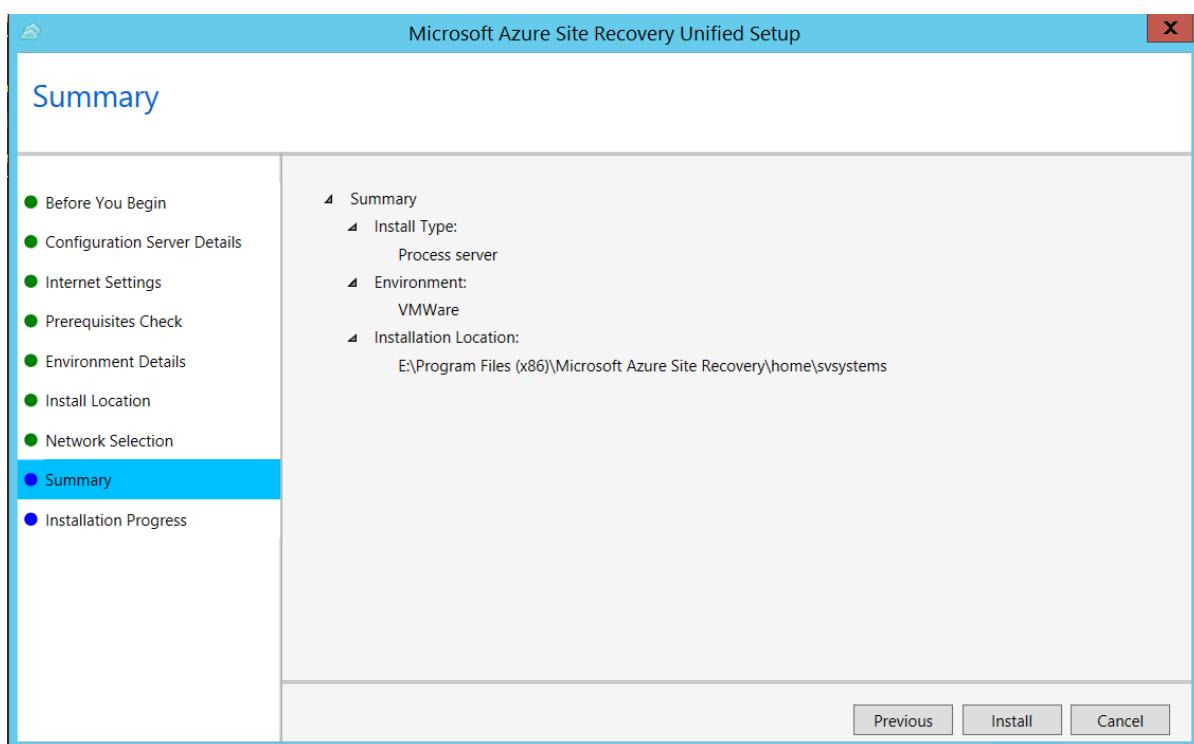
7. In **Install Location**, select where you want to install the binaries and store the cache. The drive you select must have at least 5 GB of disk space available, but we recommend a cache drive with at least 600 GB of free space.



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 /xC:\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](#)

Replicate and fail over VMware VMs to Azure with PowerShell

7/9/2018 • 12 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 data, and replicate the VMs.
- Perform a failover. Configure failover settings, perform a e settings for replicating virtual machines.

Prerequisites

Before you start:

- Make sure that you understand the [scenario architecture and components](#).
- Review the [support requirements](#) for all components.
- You have version 5.0.1 or greater of the AzureRm PowerShell 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-AzureRmAccount cmdlet:

```
Connect-AzureRmAccount
```

Select the Azure subscription you want to replicate your VMware virtual machines to. Use the Get-AzureRmSubscription cmdlet to get the list of Azure subscriptions you have access to. Select the Azure subscription to work with using the Select-AzureRmSubscription cmdlet.

```
Select-AzureRmSubscription -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-AzureRmResourceGroup -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 VMwareDRToAzurePs, and is created in the East Asia region and in the resource group created in the previous step.

```
New-AzureRmRecoveryServicesVault -Name "VMwareDRToAzurePs" -Location "East Asia" -ResourceGroupName "VMwareDRToAzurePs"
```

```
Name          : VMwareDRToAzurePs
ID           : /subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx/resourceGroups/VMwareDRToAzurePs/providers/Microsoft.RecoveryServices/vaults/VMwareDRToAzu
rePs
Type         : Microsoft.RecoveryServices/vaults
Location     : eastasia
ResourceGroupName : VMwareDRToAzurePs
SubscriptionId : xxxxxxxx-xxxx-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-AzureRmRecoveryServicesVault -Name "VMwareDRToAzurePS" -ResourceGroupName
"VMwareDRToAzurePS"

#Download vault registration key to the path C:\Work
Get-AzureRmRecoveryServicesVaultSettingsFile -SiteRecovery -Vault $Vault -Path "C:\Work\"
```

```
FilePath
-----
C:\Work\VMwareDRToAzurePs_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 (AzureRm.RecoveryServices.SiteRecovery module) comes with easy to use aliases for most cmdlets. The cmdlets in the module take the form <Operation>-AzureRmRecoveryServicesAsr<Object> and have equivalent aliases that take the form <Operation>-ASR<Object>. This article uses the cmdlet aliases for ease of reading.

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	ResouceType
VMwareDRToAzurePs	VMwareDRToAzurePs	Microsoft.RecoveryServices vaults	

As an alternative to the Set-ASRVaultContext cmdlet, one can also use the Import-AzureRmRecoveryServicesAsrVaultSettingsFile 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-AzureRmRecoveryServicesAsrVaultSettingsFile cmdlet. For example:

```
Get-AzureRmRecoveryServicesVaultSettingsFile -SiteRecovery -Vault $Vault -Path "C:\Work\"  
Import-AzureRmRecoveryServicesAsrVaultSettingsFile -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-ASRFabric  
$ASRFabrics.count
```

1

```
#Print details of the Configuration Server  
$ASRFabrics[0]
```

```

Name : 2c33d710a5ee6af753413e97f01e314fc75938ea4e9ac7bafb4a31f6804460d
FriendlyName : ConfigurationServer
ID : /Subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxx/resourceGroups/VMwareDRToAzurePs/providers/Microsoft.RecoveryServices/vaults/VMwareDRToAzurePs/replicationFabrics
                                         /2c33d710a5ee6af753413e97f01e314fc75938ea4e9ac7bafb4a31f6804460d
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-ASRPolicy -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-xxxx-
xxxxxxxxxxxx/resourceGroups/VMwareDRToAzurePs/providers/Microsoft.RecoveryServices/vaults/VMwareDRToAzu
rePs/replicationJobs/8d18e2d
                           9-479f-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-ASRPolicy -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-ASRProtectionContainer -Fabric $ASRFabrics[0]

#Get the replication policies to map by name.
$ReplicationPolicy = Get-ASRPolicy -Name "ReplicationPolicy"
$FallbackReplicationPolicy = Get-ASRPolicy -Name "ReplicationPolicy-Failback"

# Associate the replication policies to the protection container corresponding to the Configuration
Server.

$Job_AssociatePolicy = New-ASRProtectionContainerMapping -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-ASRProtectionContainerMapping -Name "FallbackPolicyAssociation" -
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-ASRVCenter -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/re
plicationJobs/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

In this step, the storage accounts to be used for replication are created. 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-AzureRmStorageAccount -ResourceGroupName "VMwareDRToAzurePs" -Name
"premiumstorageaccount1" -Location "East Asia" -SkuName Premium_LRS

$LogStorageAccount = New-AzureRmStorageAccount -ResourceGroupName "VMwareDRToAzurePs" -Name
"logstorageaccount1" -Location "East Asia" -SkuName Standard_LRS

$ReplicationStdStorageAccount= New-AzureRmStorageAccount -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. Additionally, a log storage is needed to protect virtual machines to a premium storage account.
- 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
Win2K12 VM1	ScaleOut-ProcessServer	premiumstorageaccount1	logstorageaccount1	ReplicationPolicy	Windows Account	VMwareDRToAzurePs	ASR-vnet	Subnet-1
CentOSVM1	ConfigurationServer	replicacionstdstorageaccount1	N/A	ReplicationPolicy	LinuxAccount	VMwareDRToAzurePs	ASR-vnet	Subnet-1
CentOSVM2	ConfigurationServer	replicacionstdstorageaccount1	N/A	ReplicationPolicy	LinuxAccount	VMwareDRToAzurePs	ASR-vnet	Subnet-1

```

#Get the target resource group to be used
$ResourceGroup = Get-AzureRmResourceGroup -Name "VMwareToAzureDrPs"

#Get the target virtual network to be used
$RecoveryVnet = Get-AzureRmVirtualNetwork -Name "ASR-vnet" -ResourceGroupName "asrrg"

#Get the protection container mapping for replication policy named ReplicationPolicy
$PolicyMap = Get-ASRProtectionContainerMapping -ProtectionContainer $ProtectionContainer | where
PolicyFriendlyName -eq "ReplicationPolicy"

#Get the protectable item corresponding to the virtual machine Win2K12VM1
$VM1 = Get-ASRProtectableItem -ProtectionContainer $ProtectionContainer -FriendlyName "Win2K12VM1"

# Enable replication for virtual machine Win2K12VM1
# 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-ASRReplicationProtectedItem -VMwareToAzure -ProtectableItem $VM1 -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 CentOSVM1
$VM2 = Get-ASRProtectableItem -ProtectionContainer $ProtectionContainer -FriendlyName "CentOSVM1"

# Enable replication for virtual machine CentOSVM1
$Job_EnableReplication2 = New-ASRReplicationProtectedItem -VMwareToAzure -ProtectableItem $VM2 -Name (New-
Guid).Guid -ProtectionContainerMapping $PolicyMap -RecoveryAzureStorageAccountId
$ReplicationStdStorageAccount.Id -ProcessServer $ProcessServers[1] -Account $AccountHandles[2] -
RecoveryResourceGroupId $ResourceGroup.ResourceId -RecoveryAzureNetworkId $RecoveryVnet.Id -
RecoveryAzureSubnetName "Subnet-1"

#Get the protectable item corresponding to the virtual machine CentOSVM2
$VM3 = Get-ASRProtectableItem -ProtectionContainer $ProtectionContainer -FriendlyName "CentOSVM2"

# Enable replication for virtual machine CentOSVM2
$Job_EnableReplication3 = New-ASRReplicationProtectedItem -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-ASRReplicationProtectedItem -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-ASRReplicationProtectedItem -FriendlyName "Win2K12VM1" -ProtectionContainer  
$ProtectionContainer  
  
Set-ASRReplicationProtectedItem -InputObject $ReplicatedVM1 -Size "Standard_DS11" -UseManagedDisk True
```

```
Name : cafa459c-44a7-45b0-9de9-3d925b0e7db9  
ID : /Subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-  
xxxxxxxxxxxx/resourceGroups/VMwareDRToAzurePs/providers/Microsoft.RecoveryServices/vaults/VMwareDRToAzurePs/re  
plicationJobs/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-AzureRmVirtualNetwork -Name "V2TestNetwork" -ResourceGroupName "asrg"  
  
#Start the test failover operation  
$TFOJob = Start-ASRTTestFailoverJob -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-ASRTTestFailoverCleanupJob -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-ASRRecoveryPoint -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-ASRUnplannedFailoverJob -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 on-premises physical servers

8/21/2018 • 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

[review the architecture](#) for this disaster recovery scenario.

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.
- The storage account can be standard or [premium](#).
- If you set up a premium account, you will also need an additional standard account for log data.

Prepare an account for Mobility service installation

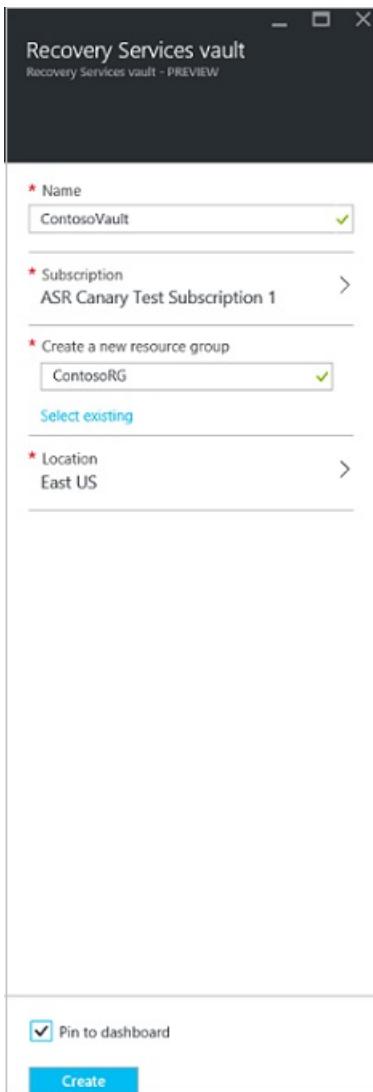
The Mobility service must be installed on each server you want to replicate. Site Recovery installs this service automatically when you enable replication for the server. To install automatically, you need to prepare an account that Site Recovery will use to access the server.

- 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

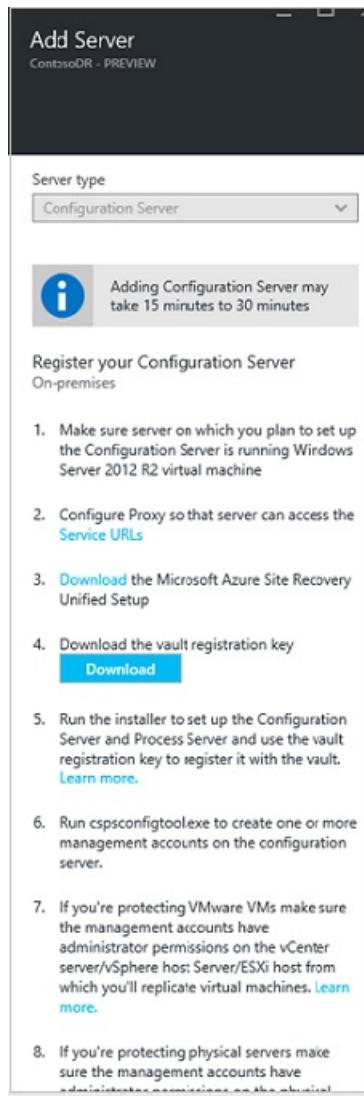
Select what to replicate, and to replicate it to.

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.



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 AD	login.microsoftonline.com	login.microsoftonline.us	Used for access control and identity management using AAD
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

NAME	COMMERCIAL URL	GOVERNMENT URL	DESCRIPTION
Telemetry (optional)	dc.services.visualstudio.com	dc.services.visualstudio.com	Used for telemetry

`time.nist.gov` and `time.windows.com` are used to check time synchronization between system and global time in all deployments.

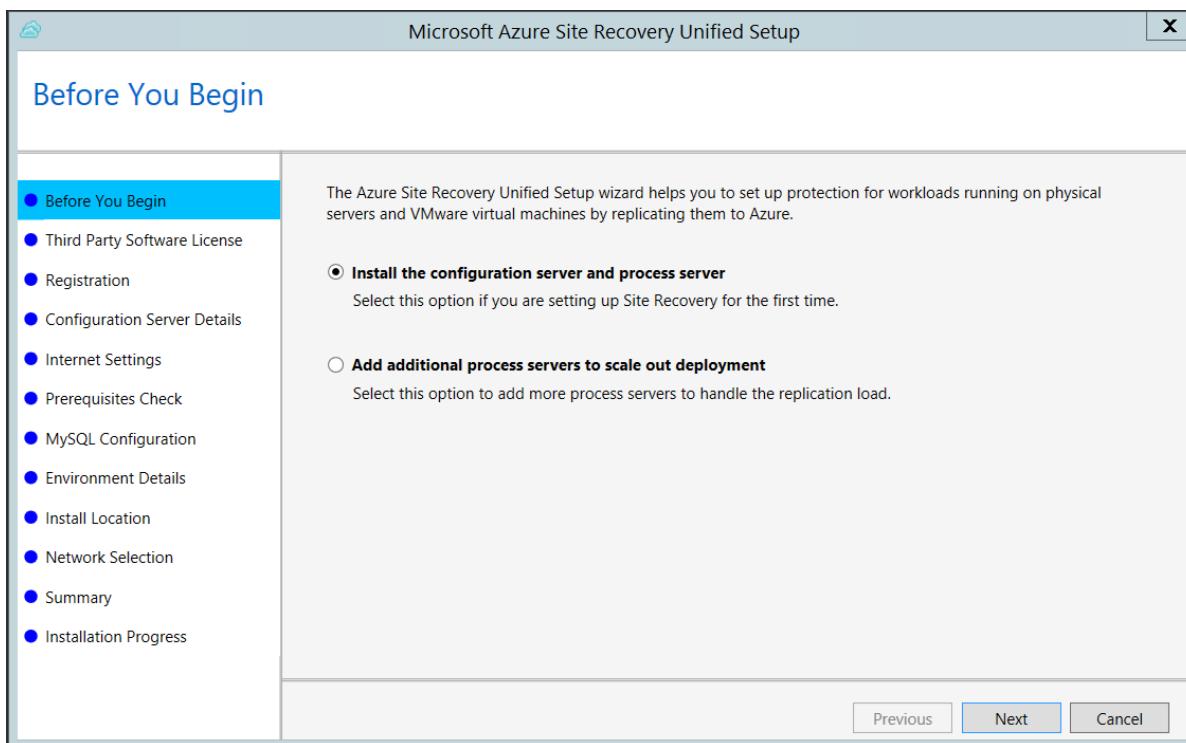
IP address-based firewall rules should allow communication to all of the Azure URLs that are listed above over HTTPS (443) port. To simplify and limit the IP Ranges, it is recommended that URL filtering be done.

- **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.

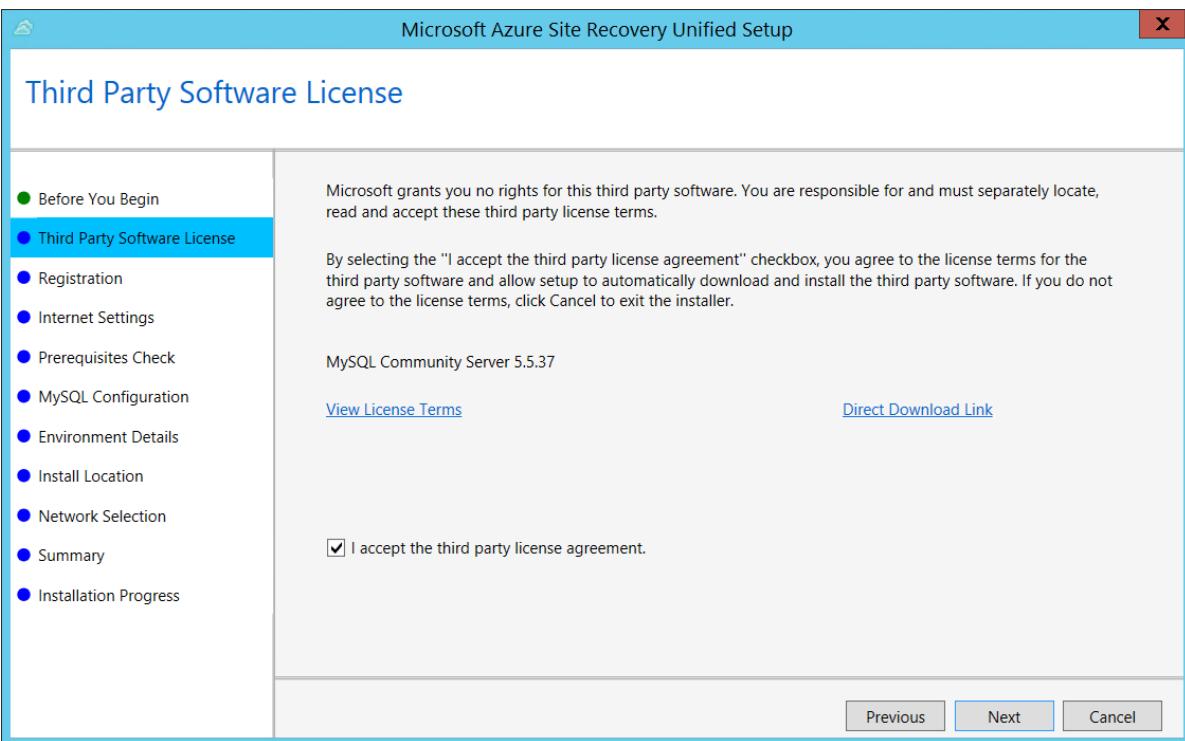
Run setup

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.

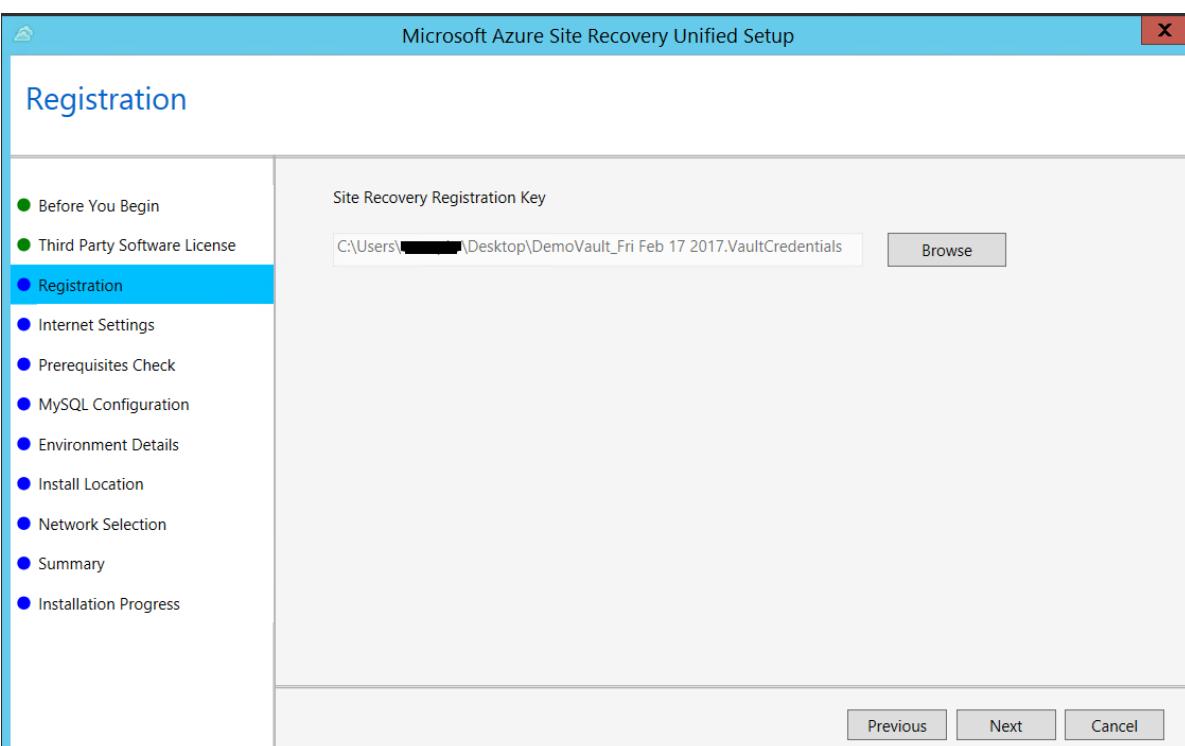
1. Run the Unified Setup installation file.
2. In **Before You Begin**, select **Install the configuration server and process server**.



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

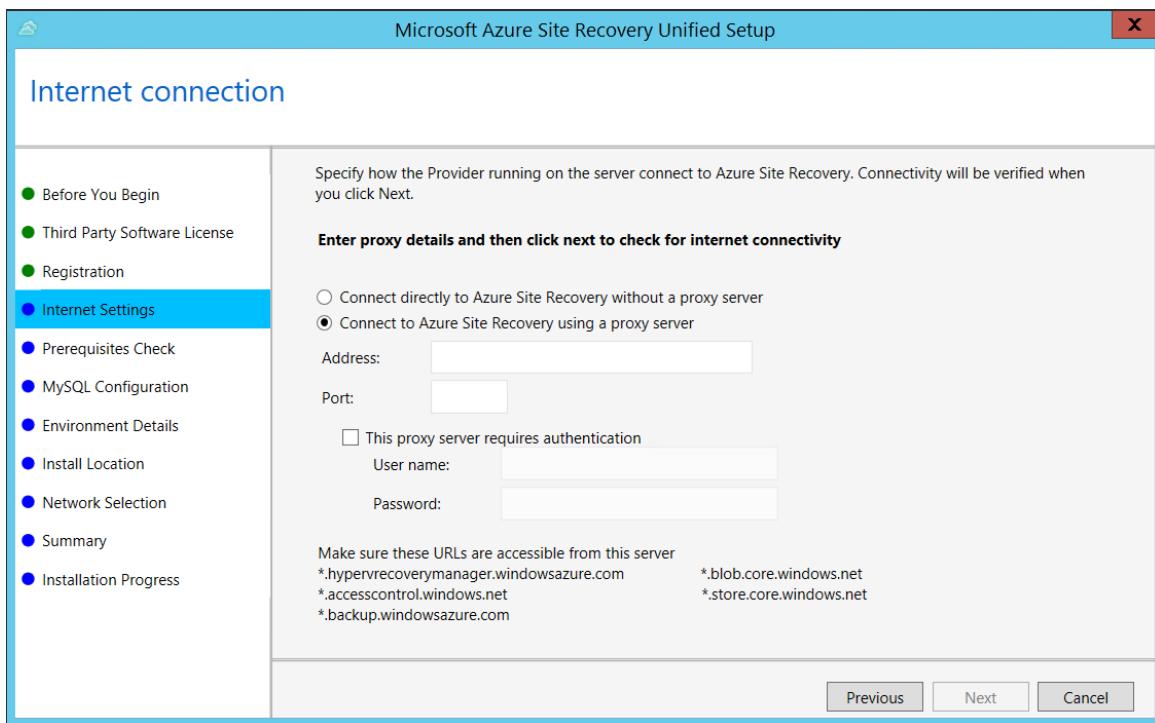


4. In **Registration**, select the registration key you downloaded from the vault.

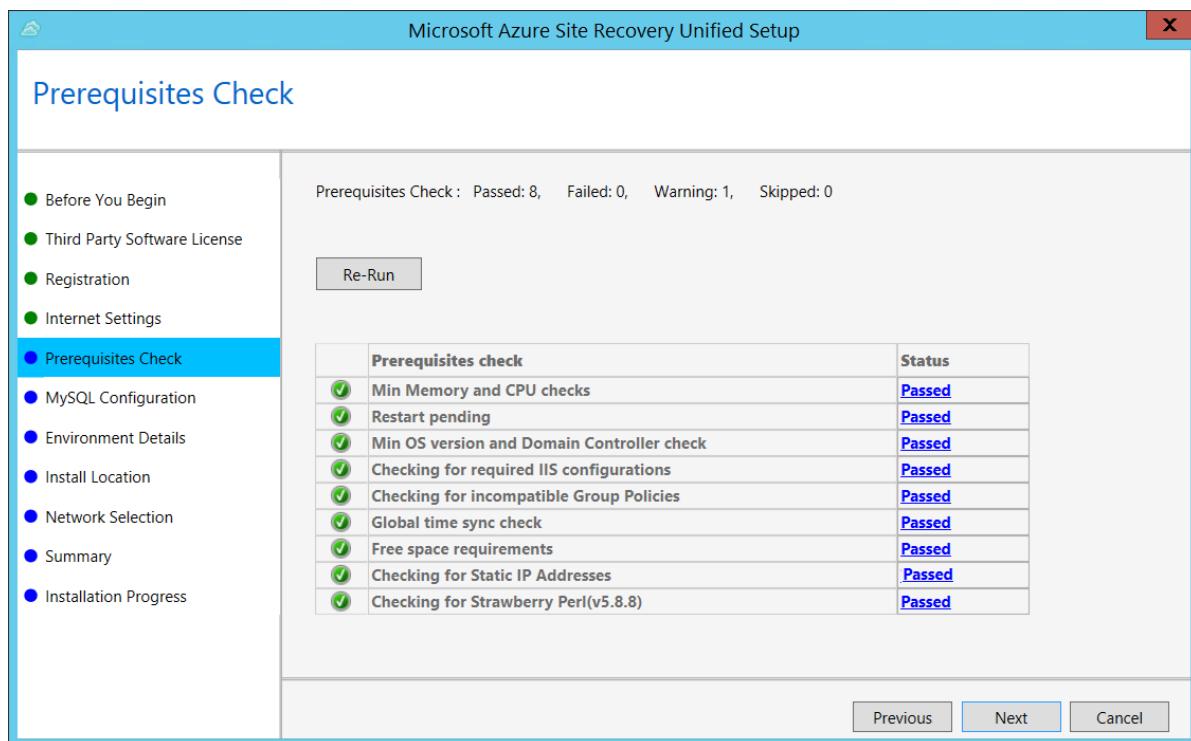


5. In **Internet Settings**, specify how the Provider running on the configuration server connects to Azure Site Recovery over the Internet. Make sure you've allowed the required URLs.

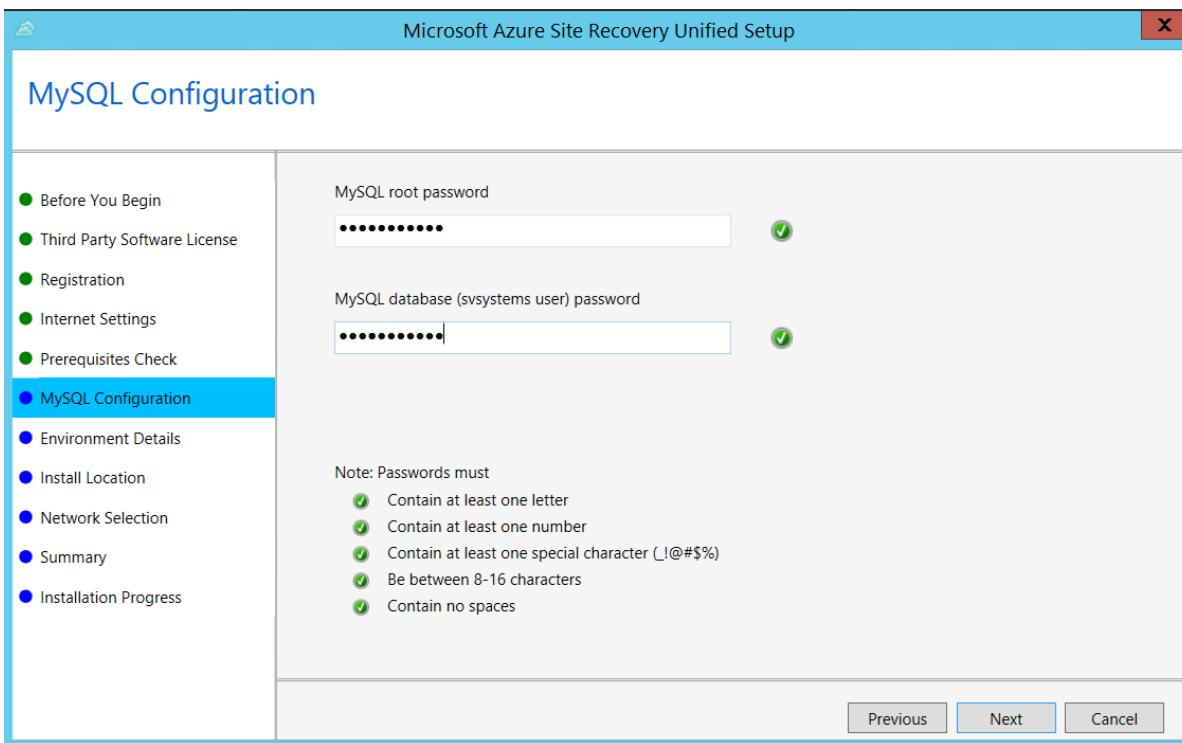
- If you want to connect with the proxy that's currently set up on the machine, select **Connect to Azure Site Recovery using a proxy server**.
- If you want the Provider to connect directly, select **Connect directly to Azure Site Recovery without a proxy server**.
- If the existing proxy requires authentication, 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.



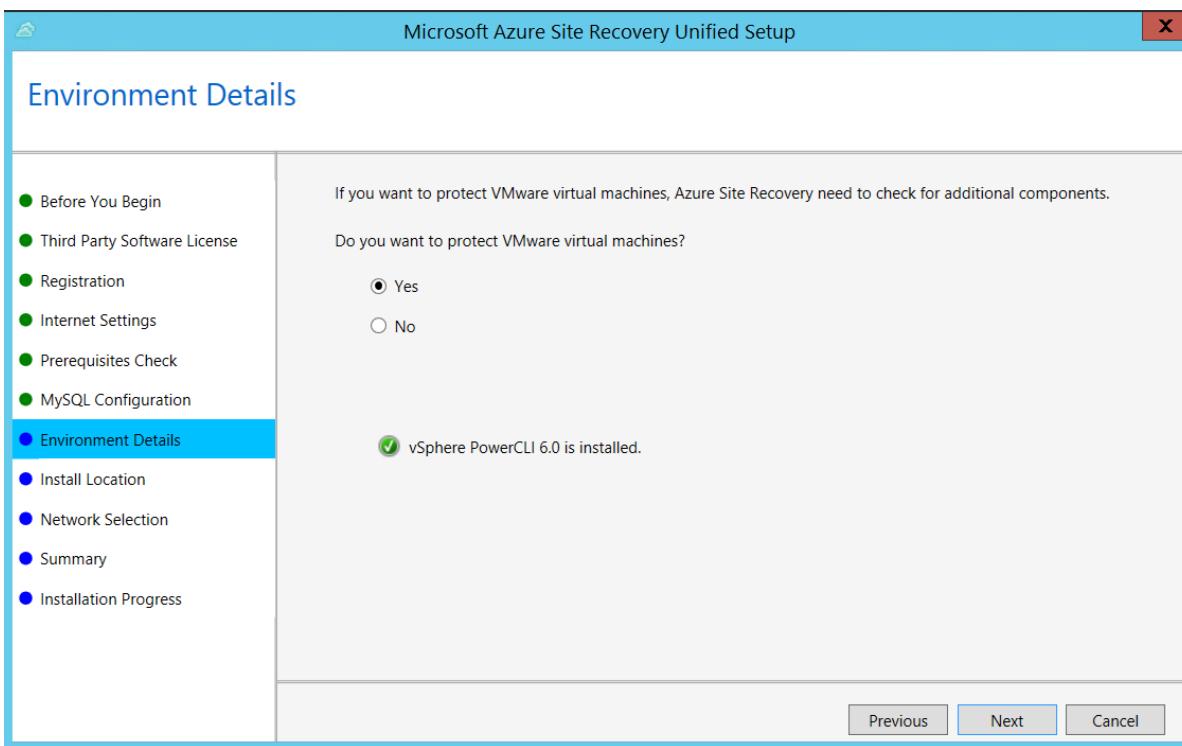
6. In **Prerequisites Check**, Setup runs a check to make sure that installation can run. If a warning appears about the **Global time sync check**, verify that the time on the system clock (**Date and Time** settings) is the same as the time zone.



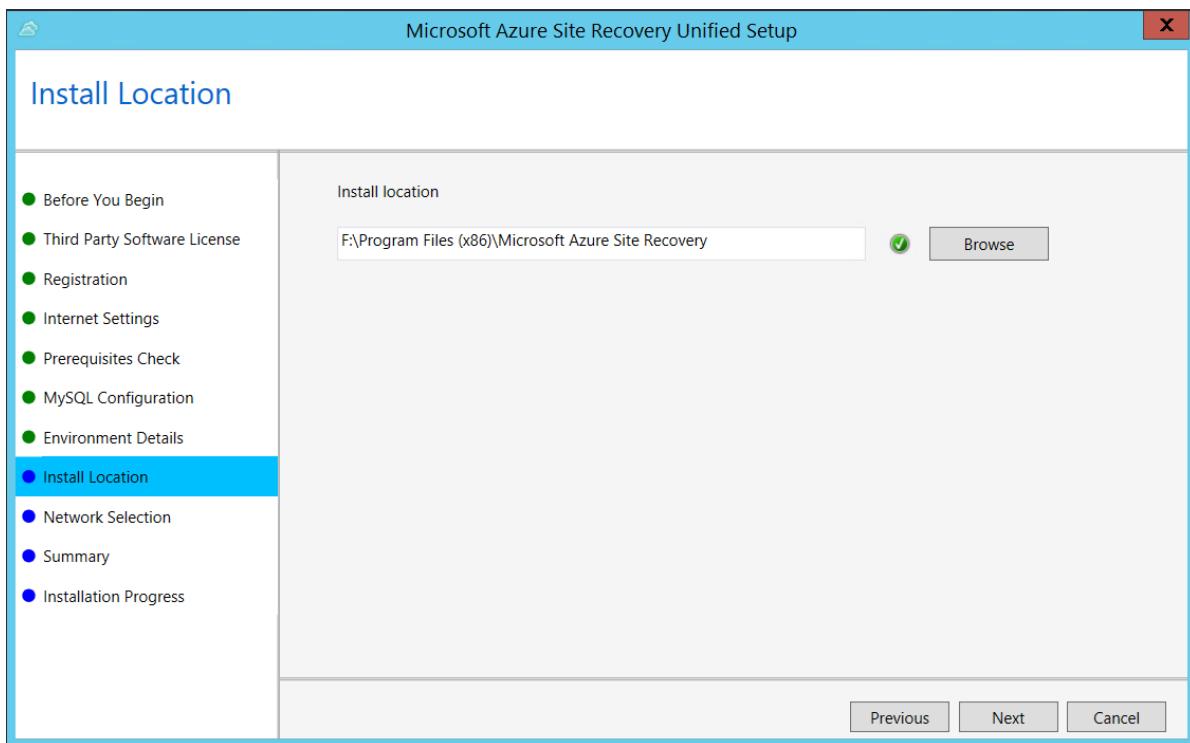
7. In **MySQL Configuration**, create credentials for logging on to the MySQL server instance that is installed.



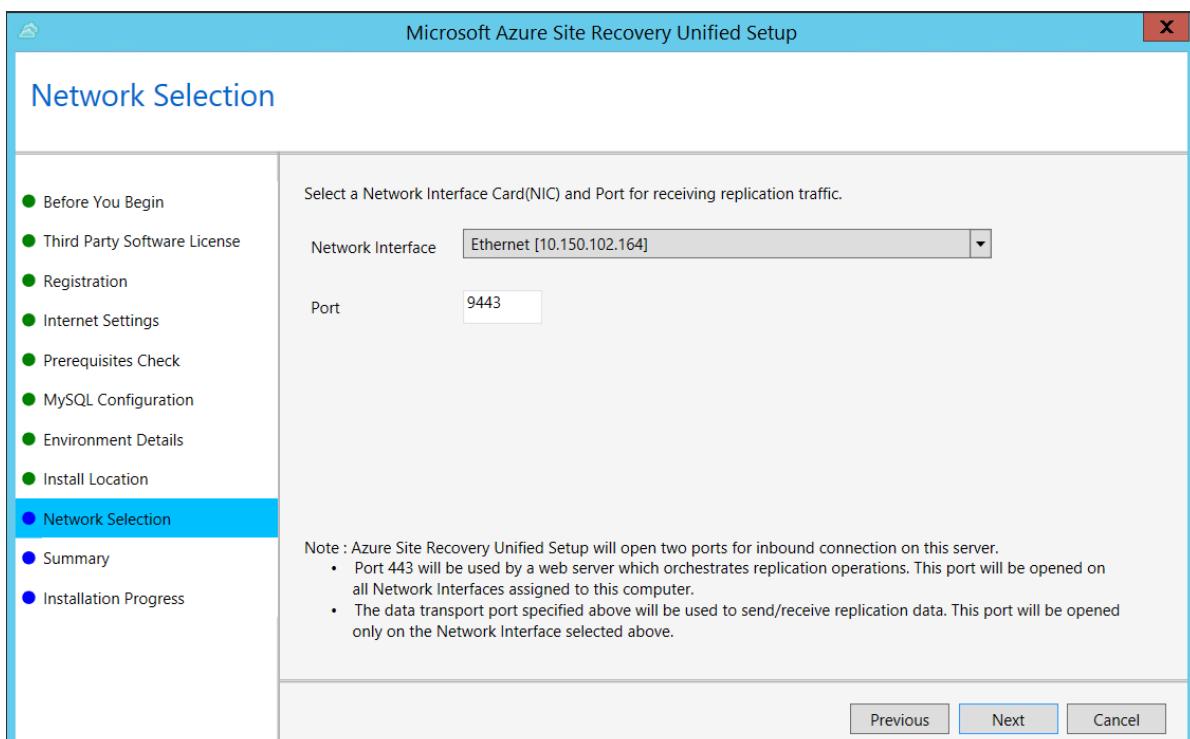
8. In **Environment Details**, select whether you're going to replicate VMware VMs. If you are, then Setup checks that PowerCLI 6.0 is installed.



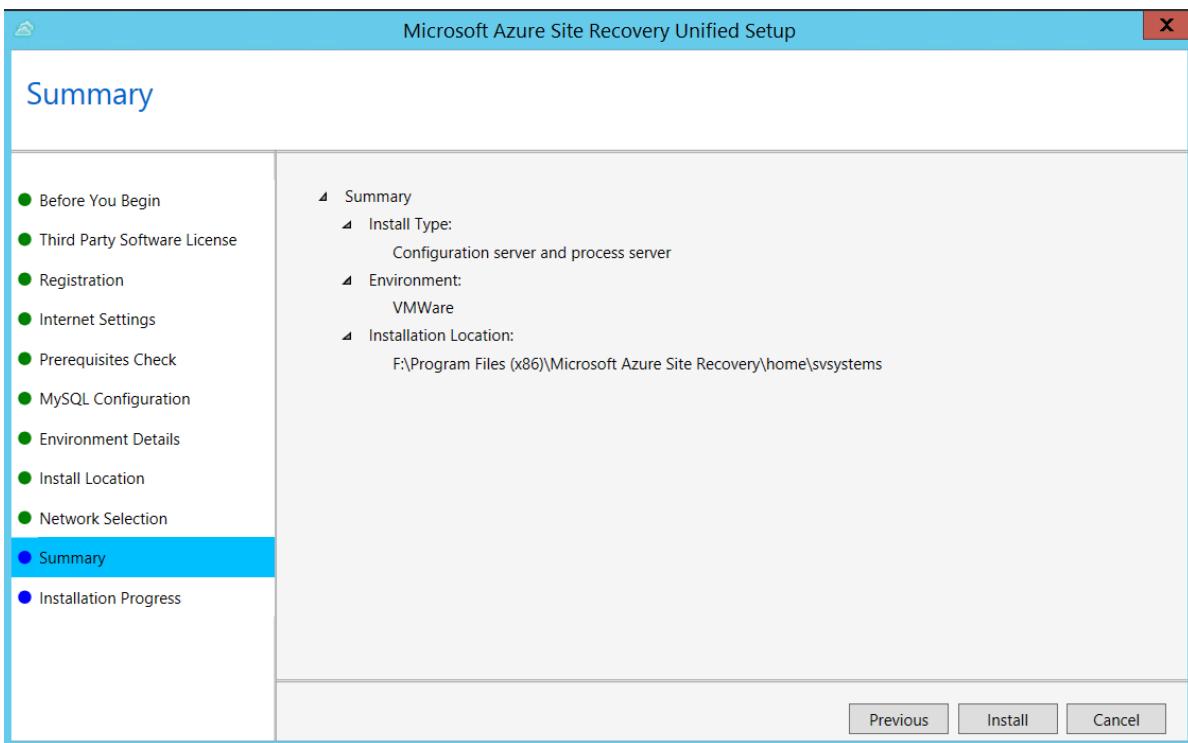
9. In **Install Location**, select where you want to install the binaries and store the cache. The drive you select must have at least 5 GB of disk space available, but we recommend a cache drive with at least 600 GB of free space.



10. In **Network Selection**, 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.



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.



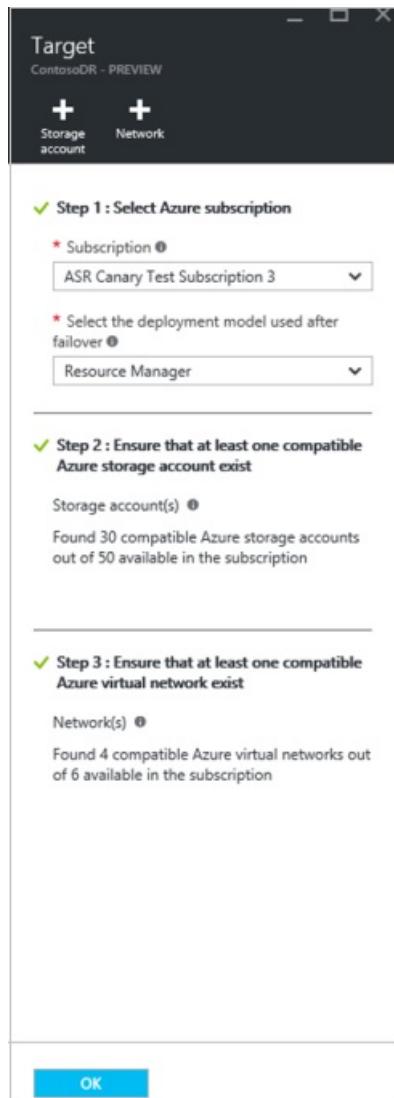
After registration finishes, the server is displayed on the **Settings > Servers** blade in the vault.

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

Set up the target environment

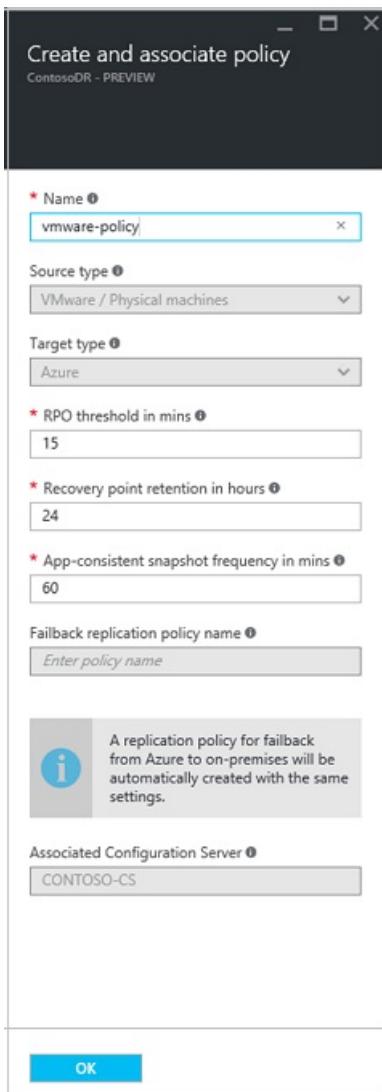
Select and verify target resources.

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 source environment for VMware to Azure replication

7/10/2018 • 3 minutes to read • [Edit Online](#)

This article describes how to set up your source on-premises environment, to replicate VMware VMs to Azure. It 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.

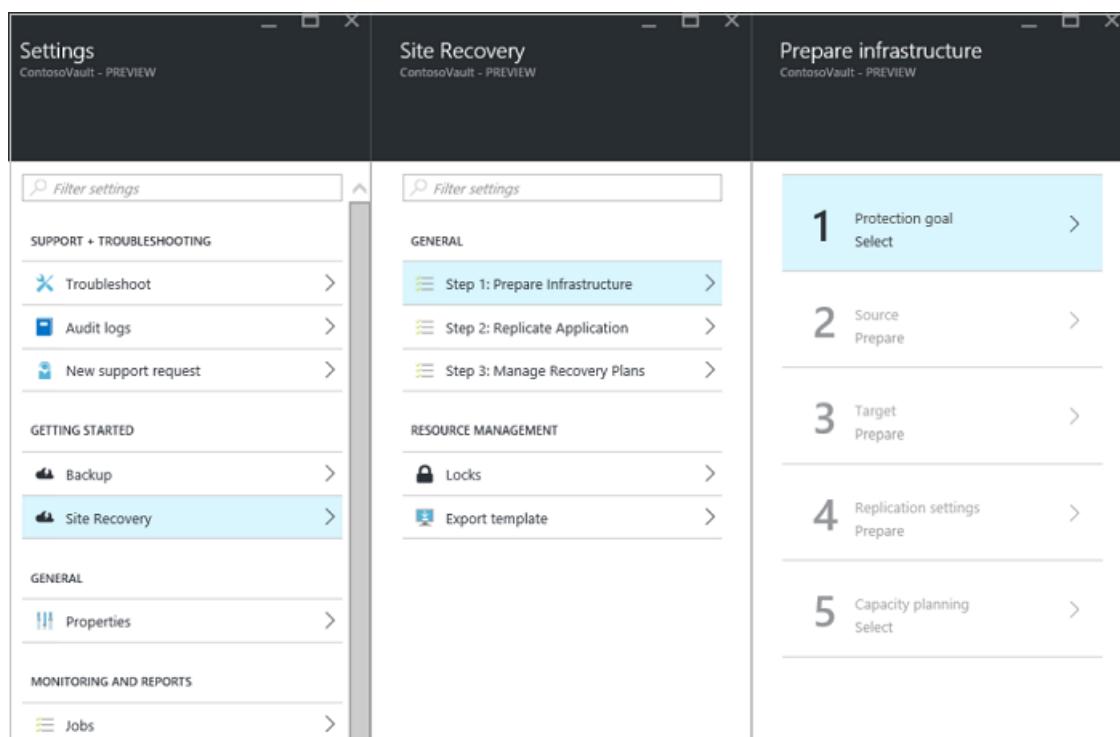
Prerequisites

The article assumes that you have already:

- [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 the Azure portal, go to the **Recovery Services** vault blade and select your vault.
2. On the resource menu of the vault, go to **Getting Started > Site Recovery > Step 1: Prepare Infrastructure > Protection goal**.



3. In **Protection goal**, select **To Azure**, and choose **Yes, with VMware vSphere Hypervisor**. Then click **OK**.

* Where do you want to replicate your machines to?

To Azure

* Are your machines virtualized?

Yes, with VMware vSphere Hypervisor

A screenshot of a configuration dialog box. It contains two dropdown menus. The top one is labeled "Where do you want to replicate your machines to?" and has "To Azure" selected. The bottom one is labeled "Are your machines virtualized?" and has "Yes, with VMware vSphere Hypervisor" selected. Both fields have red asterisks indicating they are required.

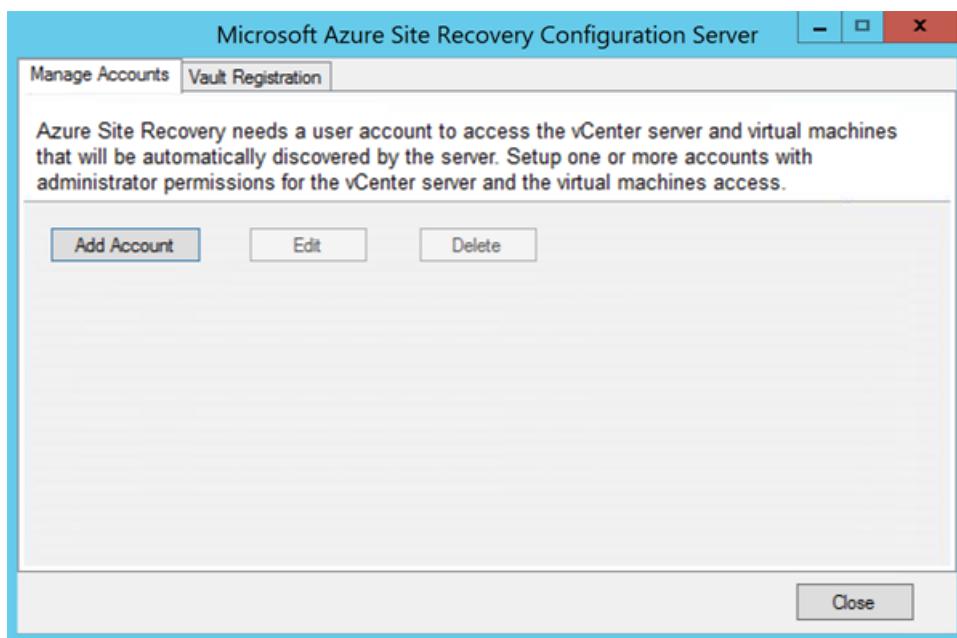
Set up the configuration server

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.

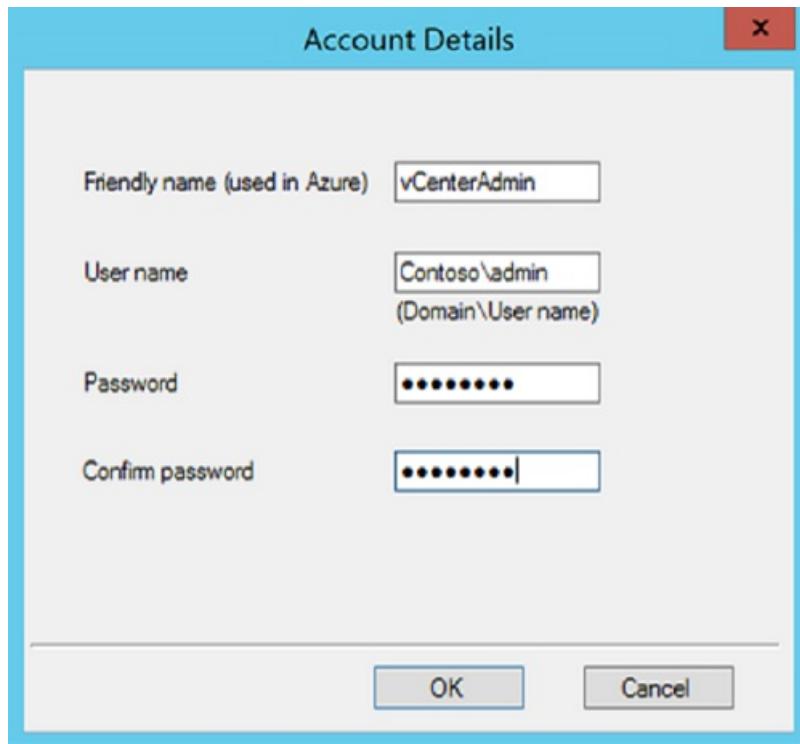
1. Learn about the [prerequisites](#) for configuration server deployment.
2. [Check capacity numbers](#) for deployment.
3. [Download](#) and [import](#) the OVA template to set up an on-premises VMware VM that runs the configuration server. The licence provided with the template is an evaluation licence and is valid for 180 days. Post this period, customer needs to activate the windows with a procured licence.
4. Turn on the VMware VM, and [register it](#) in the Recovery Services vault.

Add the VMware account for automatic discovery

1. On your configuration server, launch CSPSCfgtool.exe. It is available as a shortcut on the desktop and located in the *install location\home\svsystems\bin* folder.
2. Click **Manage Accounts > Add Account**.



3. In **Account Details**, add the account that will be used for automatic discovery.



NOTE

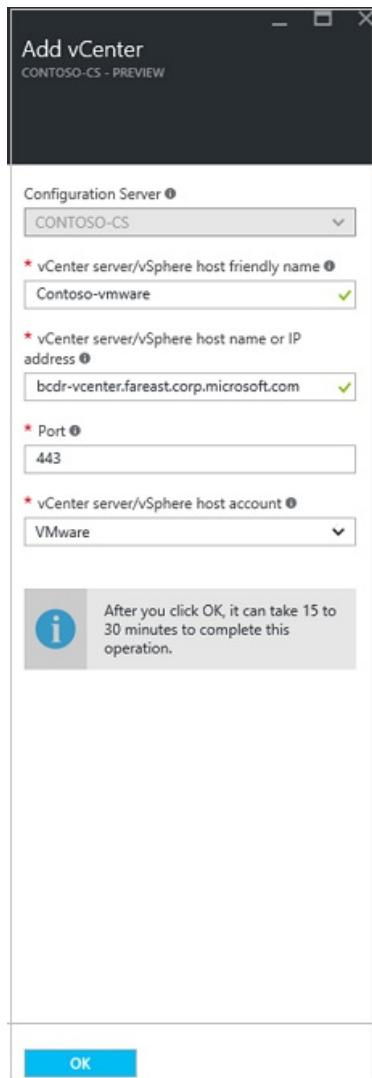
It can take 15 minutes or more for the account name to appear in the portal. To update immediately, click **Configuration Servers > server name > Refresh Server**.

Connect to the VMware server

To allow Azure Site Recovery to discover virtual machines running in your on-premises environment, you need to connect your VMware vCenter Server or vSphere ESXi hosts with Site Recovery.

Select **+vCenter** to start connecting a VMware vCenter server or a VMware vSphere ESXi host.

- In **Add vCenter**, specify a friendly name for the vSphere host or vCenter server, and then specify the IP address or FQDN of the server. Leave the port as 443 unless your VMware servers are configured to listen for requests on a different port. Select the account that is to connect to the VMware vCenter or vSphere ESXi server. Click **OK**.



NOTE

If you're adding the VMware vCenter server or VMware vSphere host with an account that doesn't have administrator privileges on the vCenter or host server, make sure that the account has these privileges enabled: Datacenter, Datastore, Folder, Host, Network, Resource, Virtual machine, and vSphere Distributed Switch. In addition, the VMware vCenter server needs the Storage views privilege enabled.

Common issues

Installation failures

SAMPLE ERROR MESSAGE	RECOMMENDED ACTION
ERROR Failed to load Accounts. Error: System.IO.IOException: Unable to read data from the transport connection when 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
<p>09:20:06:InnerException.Type: SrsRestApiClientLib.AcsException,InnerException. Message: ACS50008: SAML token is invalid. Trace ID: 1921ea5b-4723-4be7-8087-a75d3f9e1072 Correlation ID: 62fea7e6-2197-4be4-a2c0-71ceb7aa2d97> Timestamp: 2016-12-12 14:50:08Z</p>	<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>
<p>09:35:27 :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. Trace ID: e5ad1af1-2d39-4970-8eef-096e325c9950 Correlation ID: abe9deb8-3e64-464d-8375-36db9816427a Timestamp: 2016-05-19 01:35:39Z</p>	<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>
<p>06:28:45:Failed to create certificate 06:28:45:Setup cannot proceed. A certificate required to authenticate to Site Recovery cannot be created. Rerun Setup</p>	<p>Ensure you are running setup as a local administrator.</p>

Next steps

[Set up your target environment in Azure.](#)

Set up the source environment (physical server to Azure)

7/23/2018 • 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 disabled). [Learn more](#).

Configuration server minimum requirements

The following table lists the minimum hardware, software, and network requirements for a configuration server.

Configuration/Process server requirements

COMPONENT	REQUIREMENT
HARDWARE SETTINGS	
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 SETTINGS	
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

COMPONENT	REQUIREMENT
Group policies	<p>Don't enable these group policies:</p> <ul style="list-style-type: none"> - Prevent access to the command prompt. - Prevent access to registry editing tools. - Trust logic for file attachments. - Turn on Script Execution. <p>Learn more</p>
IIS	<ul style="list-style-type: none"> - No preexisting default website - No preexisting website/application listening on port 443 - Enable anonymous authentication - Enable FastCGI setting
NETWORK SETTINGS	
IP address type	Static
Internet access	<p>The server needs access to these URLs (directly or via proxy):</p> <ul style="list-style-type: none"> - *.accesscontrol.windows.net - *.backup.windowsazure.com - *.store.core.windows.net - *.blob.core.windows.net - *.hypervrecoverymanager.windowsazure.com - https://management.azure.com - *.services.visualstudio.com - time.nist.gov - time.windows.com <p>OVF also needs access to the following URLs:</p> <ul style="list-style-type: none"> - https://login.microsoftonline.com - https://secure.aadcdn.microsoftonline-p.com - https://login.live.com - https://auth.gfx.ms - https://graph.windows.net - https://login.windows.net - https://www.live.com - https://www.microsoft.com - https://dev.mysql.com/get/Downloads/MySQLInstaller/mysql-installer-community-5.7.20.0.msi
Ports	443 (Control channel orchestration) 9443 (Data transport)
NIC type	VMXNET3 (if the Configuration Server is a VMware VM)
SOFTWARE TO INSTALL	
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.

Configuration/Process server sizing requirements

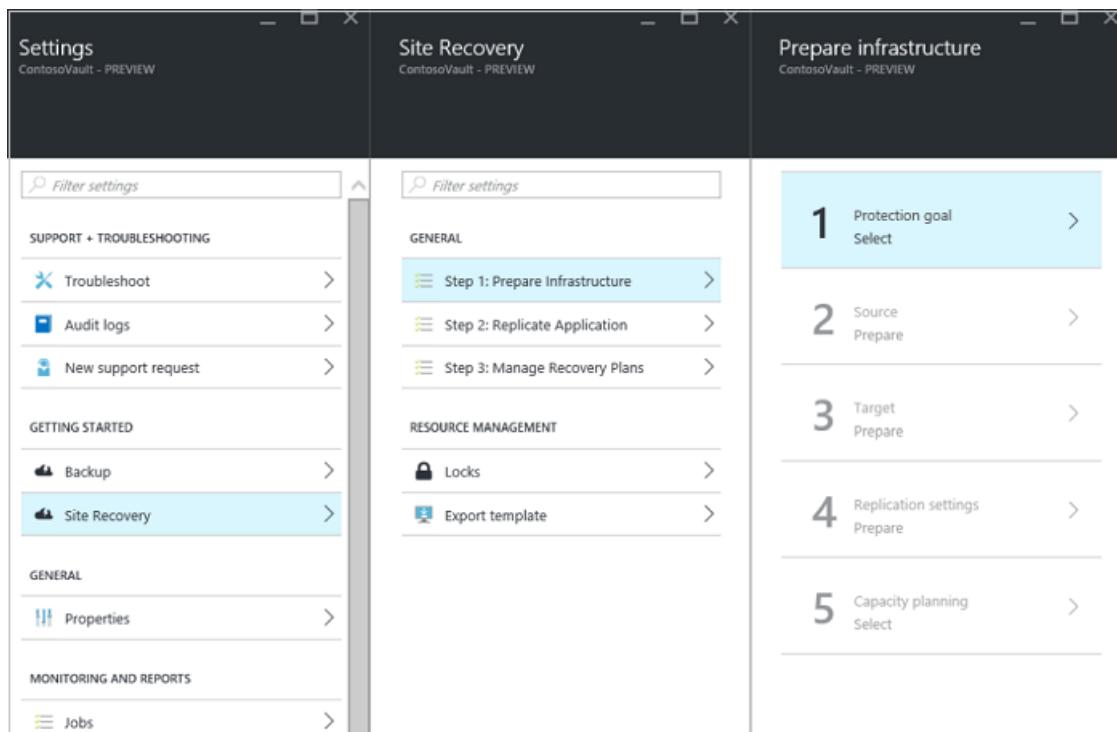
CPU	MEMORY	CACHE DISK	DATA CHANGE RATE	REPLICATED MACHINES
8 vCPUs 2 sockets * 4 cores @ 2.5 GHz	16GB	300 GB	500 GB or less	< 100 machines
12 vCPUs 2 socks * 6 cores @ 2.5 GHz	18 GB	600 GB	500 GB-1 TB	100 to 150 machines
16 vCPUs 2 socks * 8 cores @ 2.5 GHz	32 GB	1 TB	1-2 TB	150 -200 machines

NOTE

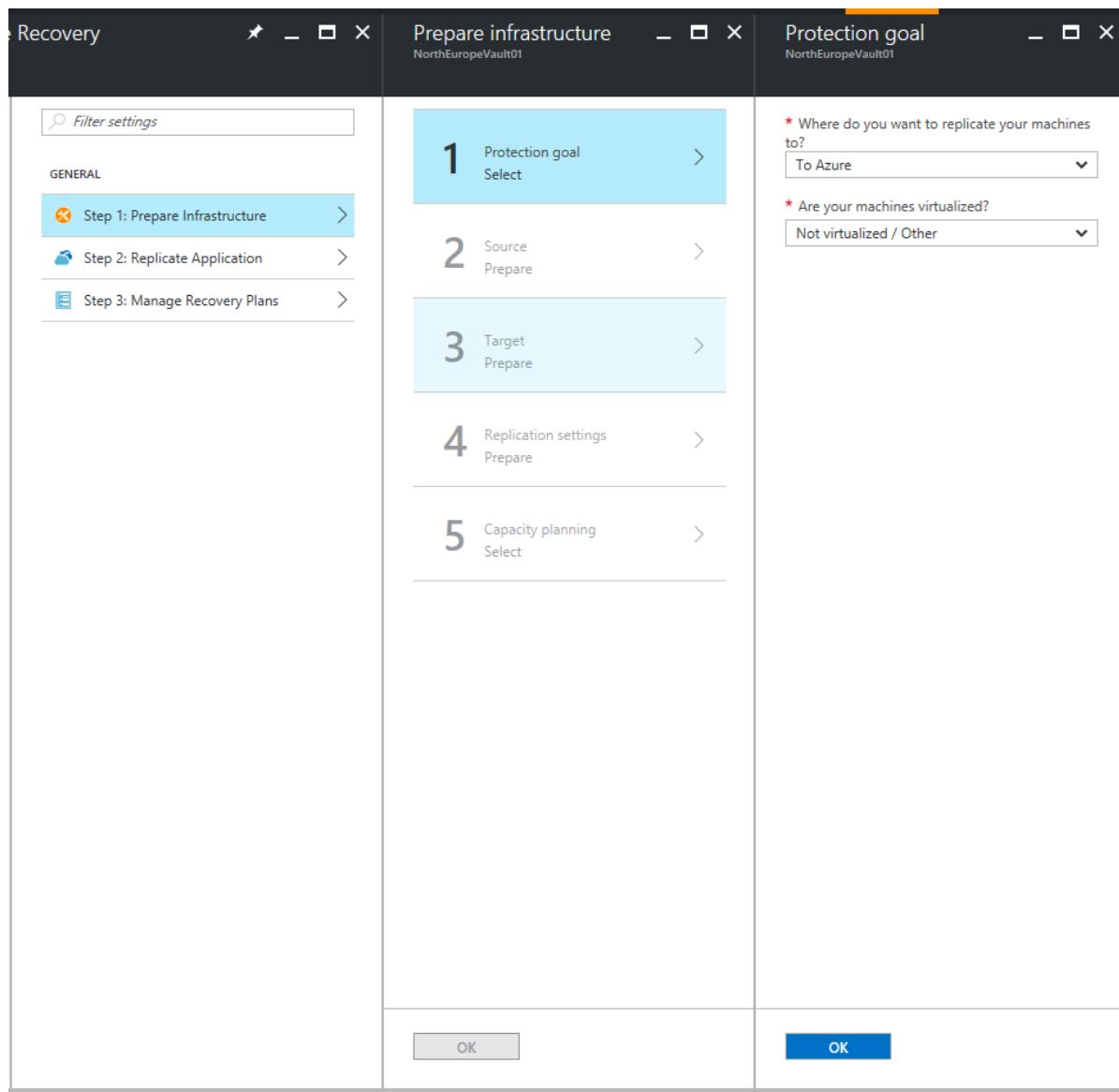
HTTPS-based proxy servers are not supported by the configuration server.

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.**

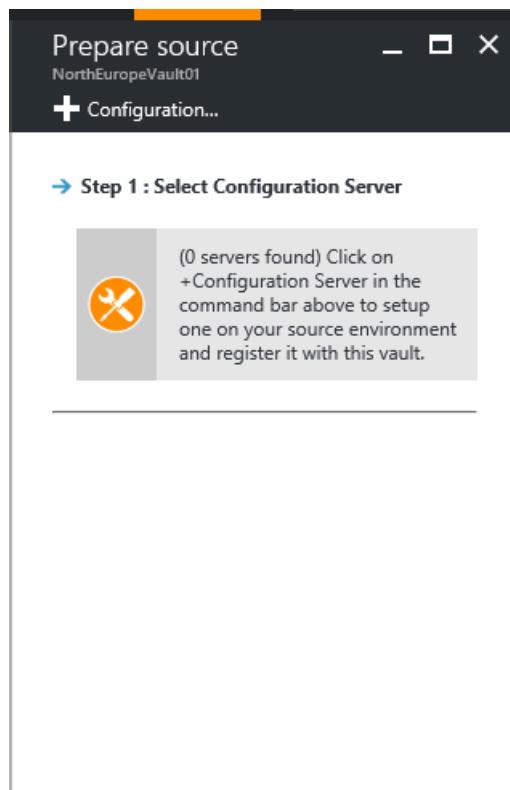


3. In **Protection goal**, select **To Azure** and **Not virtualized/Other**, and then click **OK**.

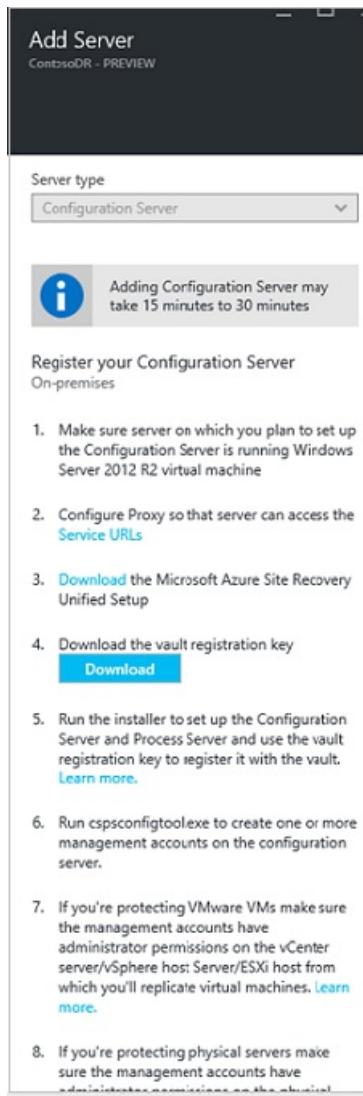


Set up the source environment

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.



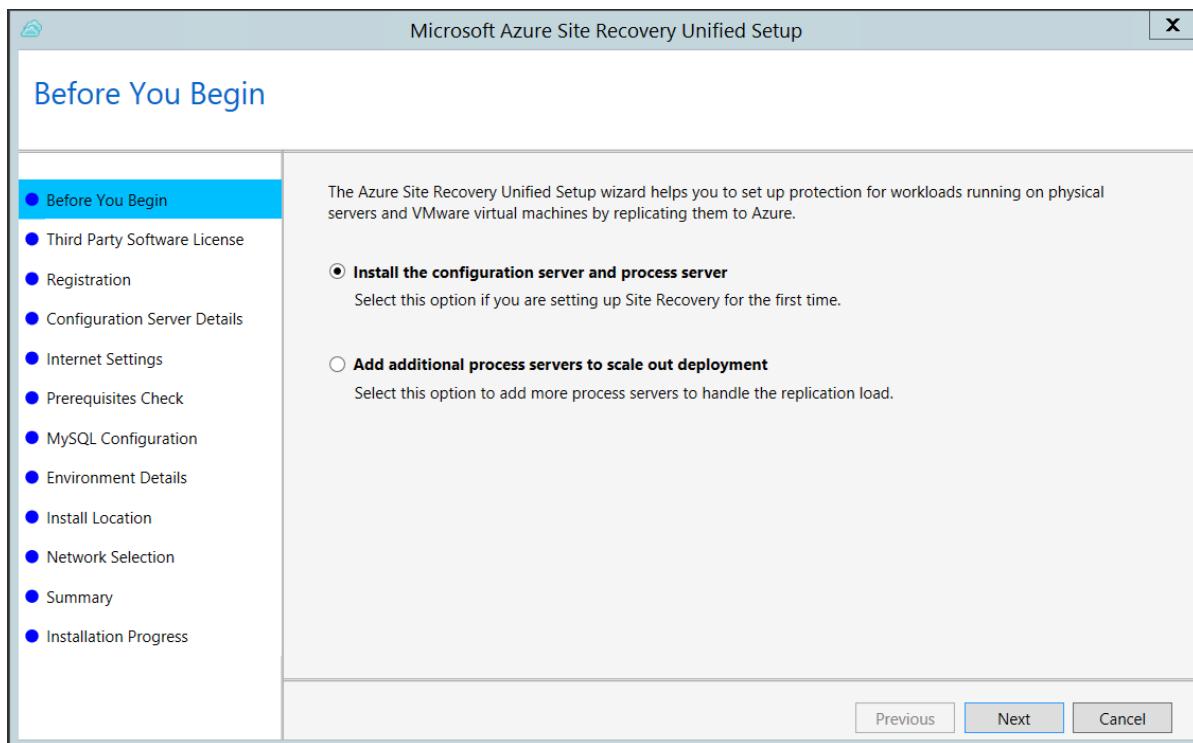
5. On the machine you're using as the configuration server, run **Azure Site Recovery Unified Setup** to install the configuration server, the process server, and the master target server.

Run Azure Site Recovery Unified Setup

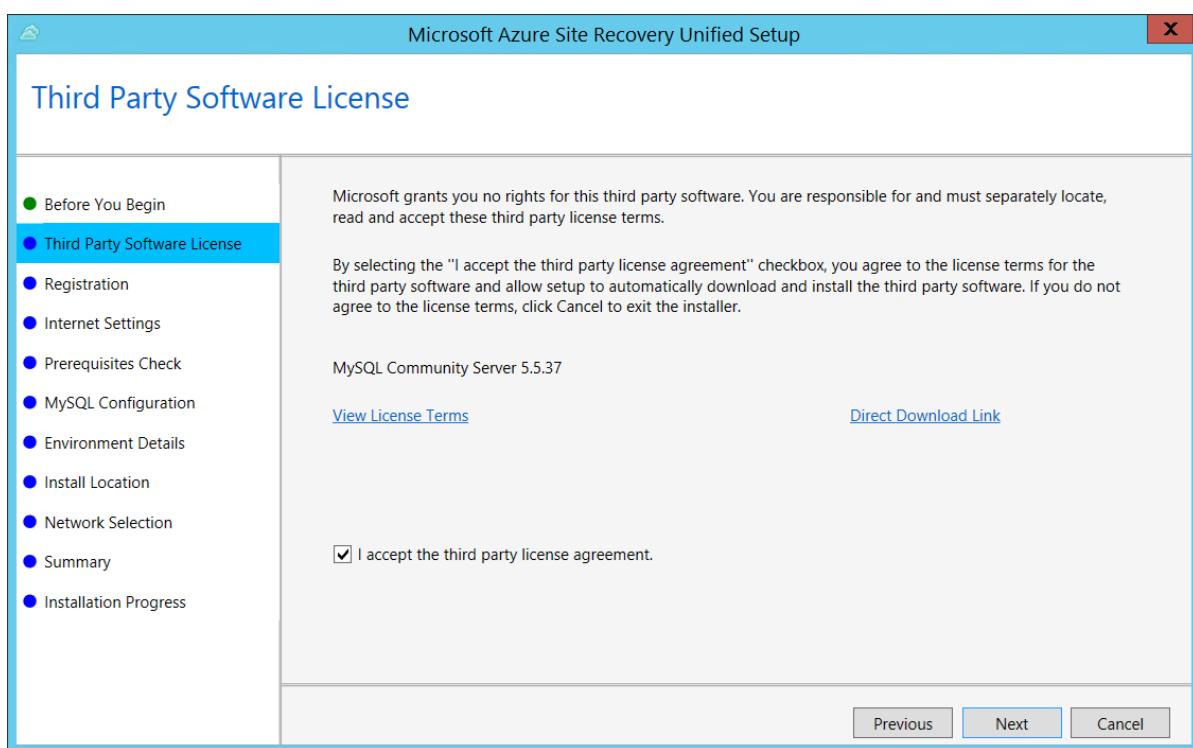
TIP

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.

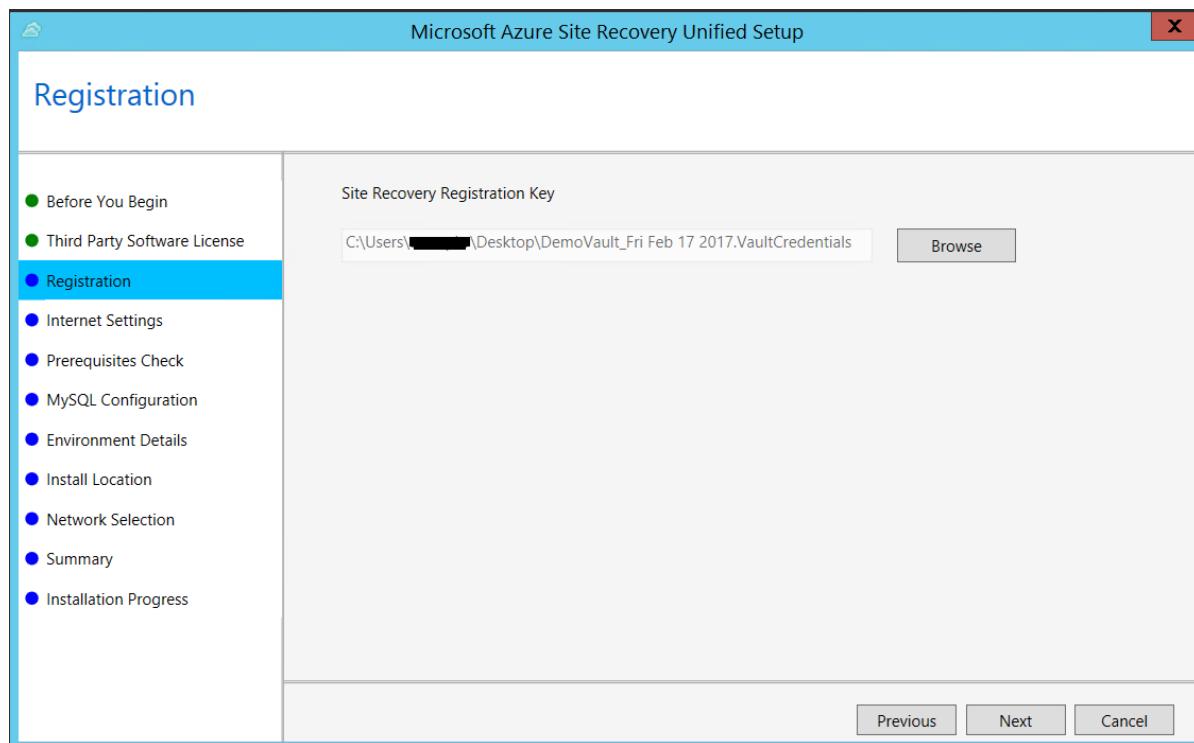
1. Run the Unified Setup installation file.
2. In **Before You Begin**, select **Install the configuration server and process server**.



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

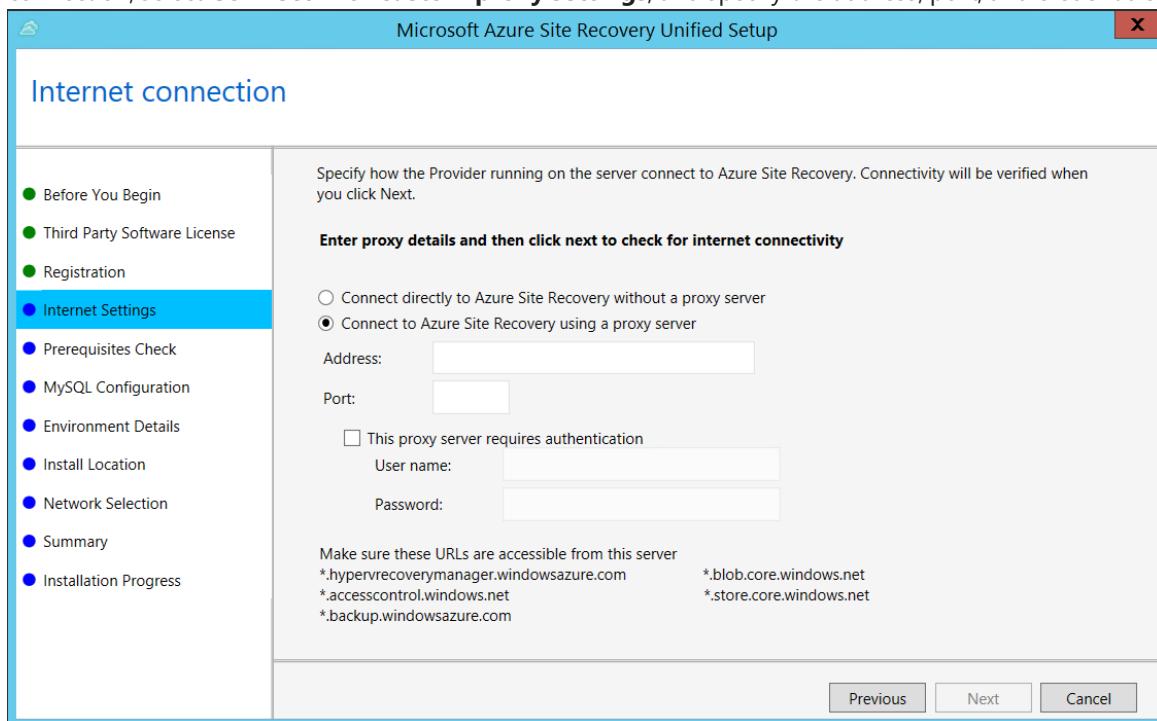


4. In **Registration**, select the registration key you downloaded from the vault.

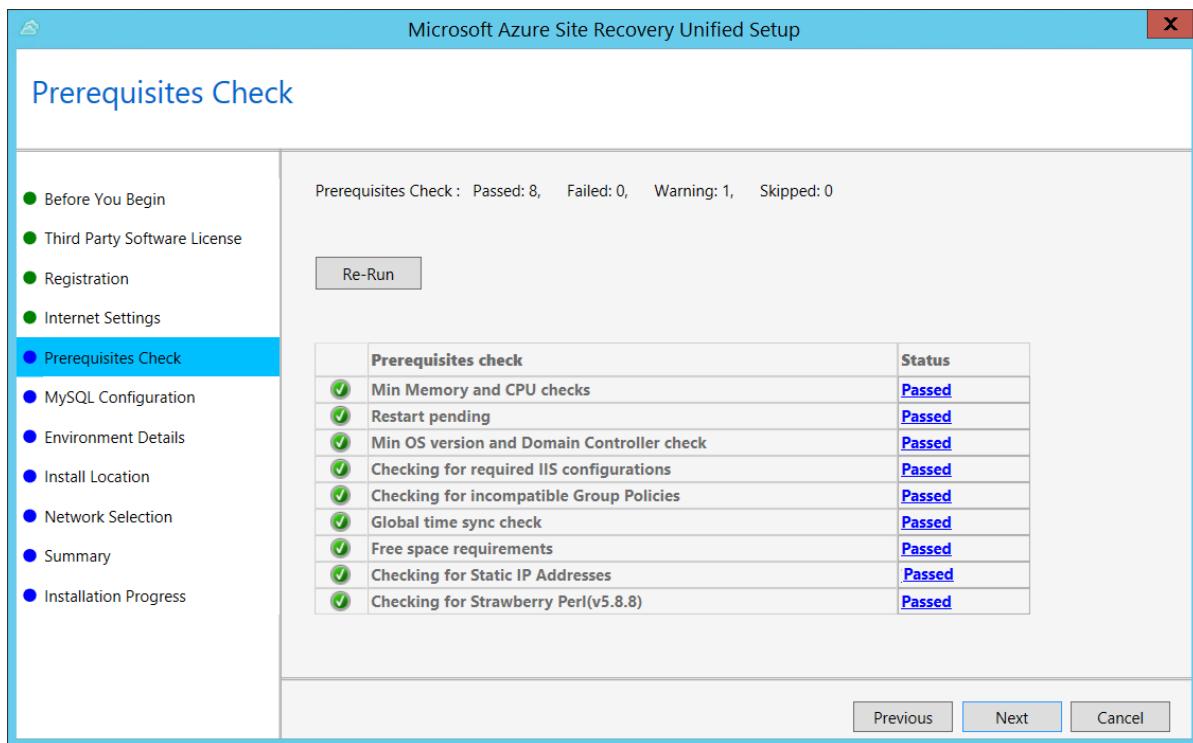


5. In **Internet Settings**, specify how the Provider running on the configuration server connects to Azure Site Recovery over the Internet. Make sure you've allowed the required URLs.

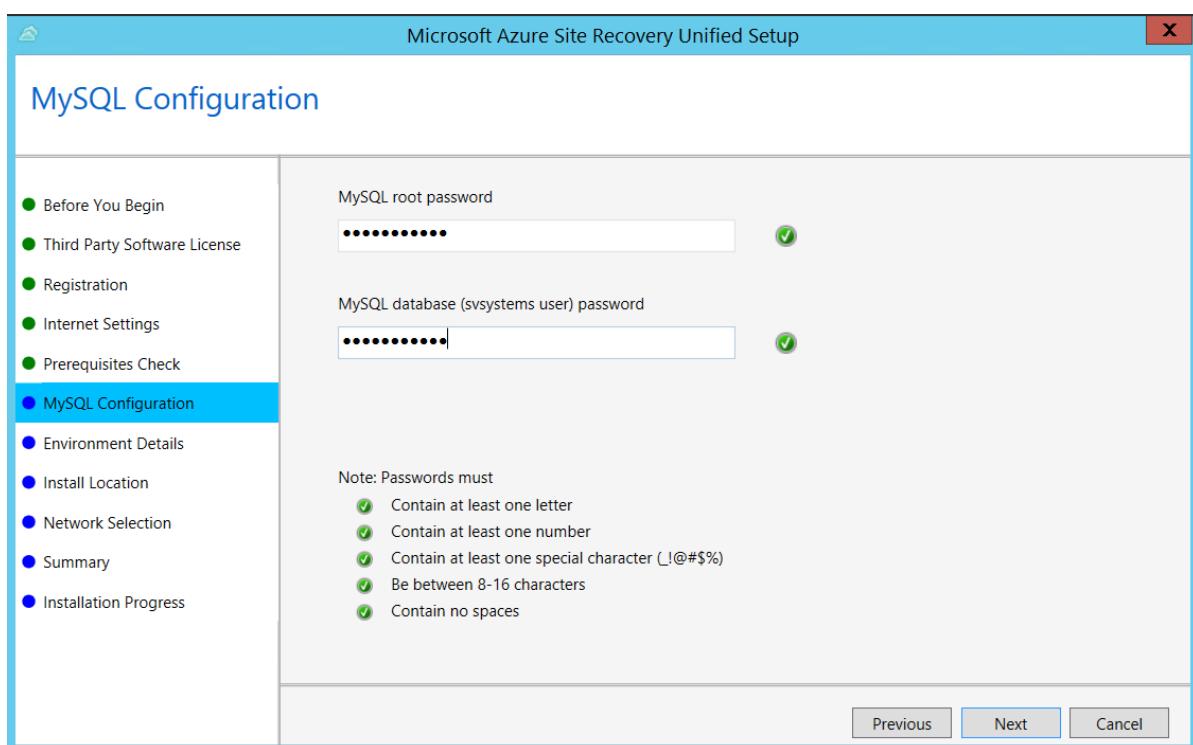
- If you want to connect with the proxy that's currently set up on the machine, select **Connect to Azure Site Recovery using a proxy server**.
- If you want the Provider to connect directly, select **Connect directly to Azure Site Recovery without a proxy server**.
- If the existing proxy requires authentication, 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.



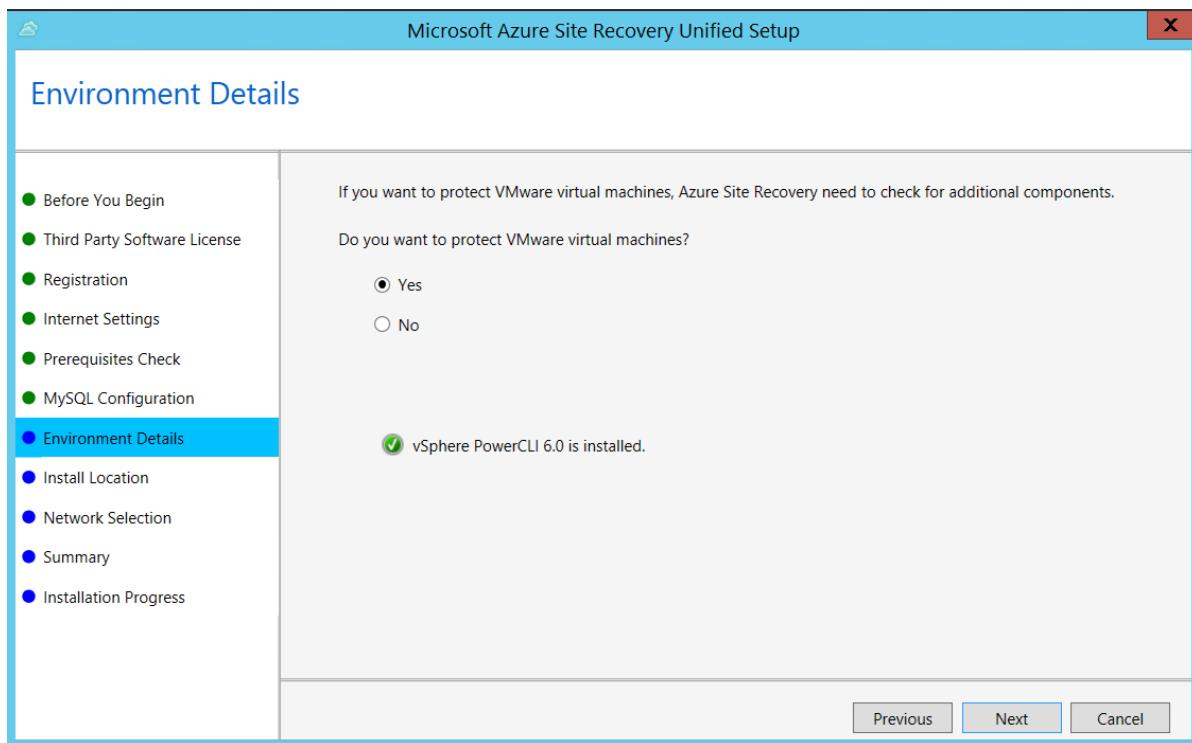
6. In **Prerequisites Check**, Setup runs a check to make sure that installation can run. If a warning appears about the **Global time sync check**, verify that the time on the system clock (**Date and Time** settings) is the same as the time zone.



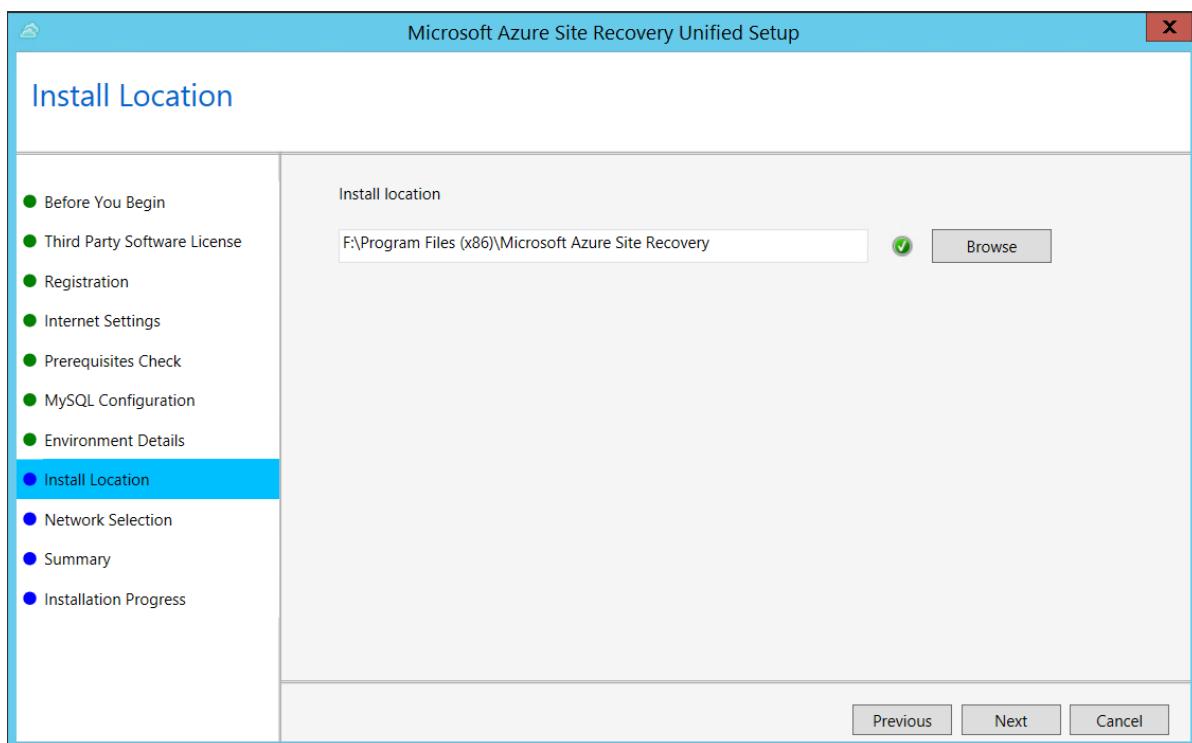
7. In **MySQL Configuration**, create credentials for logging on to the MySQL server instance that is installed.



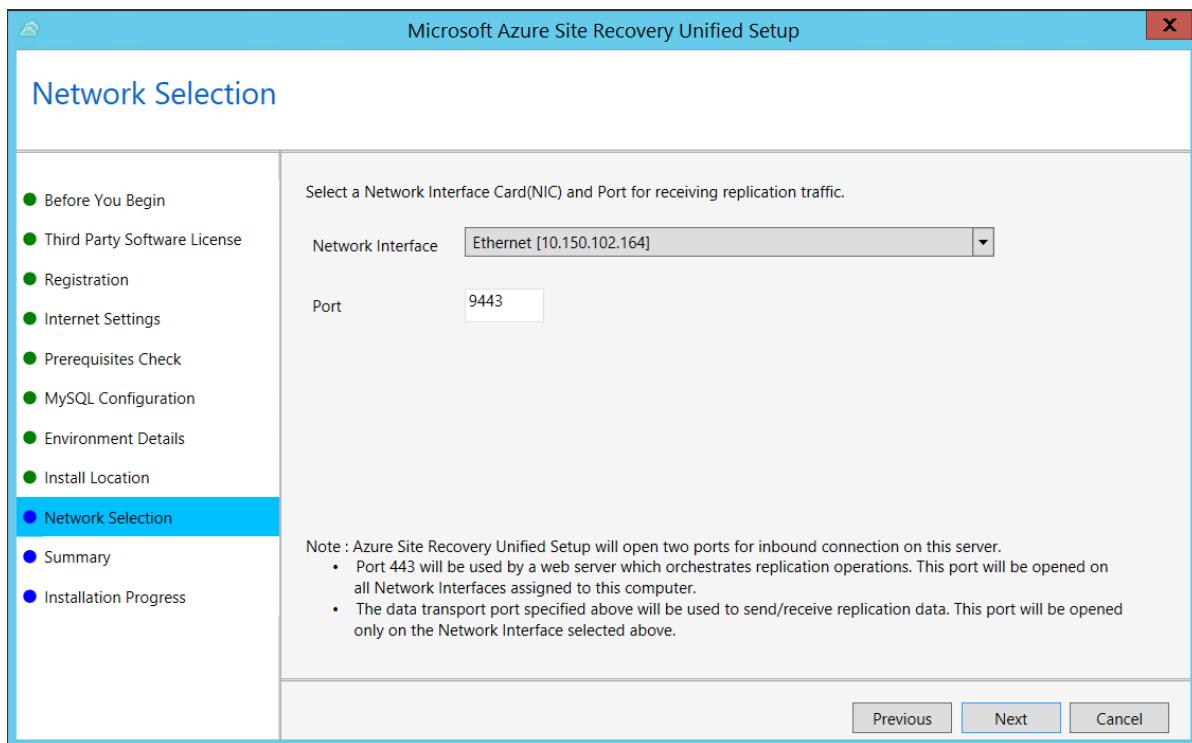
8. In **Environment Details**, select whether you're going to replicate VMware VMs. If you are, then Setup checks that PowerCLI 6.0 is installed.



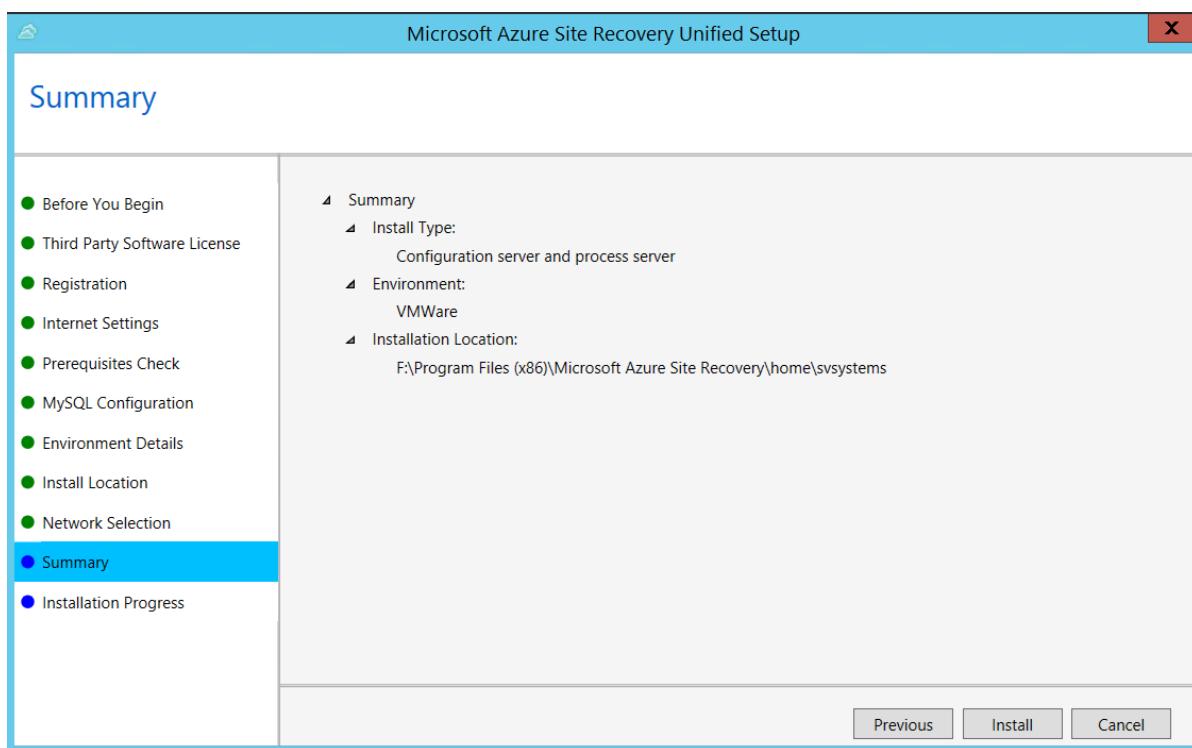
9. In **Install Location**, select where you want to install the binaries and store the cache. The drive you select must have at least 5 GB of disk space available, but we recommend a cache drive with at least 600 GB of free space.



10. In **Network Selection**, 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.



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: Unable to read data from the transport connection when 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
09:20:06: InnerException.Type: SrsRestApiClientLib.AcsException,InnerException. Message: ACS50008: SAML token is invalid. Trace ID: 1921ea5b-4723-4be7-8087-a75d3f9e1072 Correlation ID: 62fea7e6-2197-4be4-a2c0-71ceb7aa2d97> Timestamp: 2016-12-12 14:50:08Z	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.
09:35:27 : 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. Trace ID: e5ad1af1-2d39-4970-8eef-096e325c9950 Correlation ID: abe9deb8-3e64-464d-8375-36db9816427a Timestamp: 2016-05-19 01:35:39Z	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.
06:28:45:Failed to create certificate 06:28:45:Setup cannot proceed. A certificate required to authenticate to Site Recovery cannot be created. Rerun Setup	Ensure you are running setup as a local administrator.

Next steps

Next step involves [setting up your target environment](#) in Azure.

Deploy a configuration server

7/13/2018 • 9 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. [Follow this article](#) if you need to set up a configuration server for physical server replication.

TIP

You can learn about role of Configuration server as part of Azure Site Recovery architecture [here](#).

Deployment of configuration server through OVA template

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 OVA (Open Virtualization Application) template to set up the configuration server that complies with all the mandated requirements listed below.

Prerequisites

Minimum hardware requirements for a configuration server are summarized in the following table.

Configuration/Process server requirements

COMPONENT	REQUIREMENT
HARDWARE SETTINGS	
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 SETTINGS	
Operating system	Windows Server 2012 R2 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"> - Active Directory Domain Services - Internet Information Services - Hyper-V
Group policies	<p>Don't enable these group policies:</p> <ul style="list-style-type: none"> - Prevent access to the command prompt. - Prevent access to registry editing tools. - Trust logic for file attachments. - Turn on Script Execution. <p>Learn more</p>
IIS	<ul style="list-style-type: none"> - No preexisting default website - No preexisting website/application listening on port 443 - Enable anonymous authentication - Enable FastCGI setting
NETWORK SETTINGS	
IP address type	Static
Internet access	<p>The server needs access to these URLs (directly or via proxy):</p> <ul style="list-style-type: none"> - *.accesscontrol.windows.net - *.backup.windowsazure.com - *.store.core.windows.net - *.blob.core.windows.net - *.hypervrecoverymanager.windowsazure.com - https://management.azure.com - *.services.visualstudio.com - time.nist.gov - time.windows.com <p>OVF also needs access to the following URLs:</p> <ul style="list-style-type: none"> - https://login.microsoftonline.com - https://secure.aadcdn.microsoftonline-p.com - https://login.live.com - https://auth.gfx.ms - https://graph.windows.net - https://login.windows.net - https://www.live.com - https://www.microsoft.com - https://dev.mysql.com/get/Downloads/MySQLInstaller/mysql-installer-community-5.7.20.0.msi
Ports	443 (Control channel orchestration) 9443 (Data transport)
NIC type	VMXNET3 (if the Configuration Server is a VMware VM)
SOFTWARE TO INSTALL	
VMware vSphere PowerCLI	PowerCLI version 6.0 should be installed if the Configuration Server is running on a VMware VM.

COMPONENT	REQUIREMENT
MYSQL	MySQL should be installed. You can install manually, or Site Recovery can install it.

Configuration/Process server sizing requirements

CPU	MEMORY	CACHE DISK	DATA CHANGE RATE	REPLICATED MACHINES
8 vCPUs 2 sockets * 4 cores @ 2.5 GHz	16GB	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

Capacity planning

The sizing requirements for the configuration server depend on the potential data change rate. Use this table as a guide.

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	Replicate fewer than 100 machines.
12 vCPUs (2 sockets * 6 cores @ 2.5 GHz)	18 GB	600 GB	500 GB to 1 TB	Replicate 100-150 machines.
16 vCPUs (2 sockets * 8 cores @ 2.5 GHz)	32 GB	1 TB	1 TB to 2 TB	Replicate 150-200 machines.

If you're replicating more than one VMware VM, read [capacity planning considerations](#). Run the [Deployment planner tool](#) for VMWare replication.

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 Open Virtualization Application (OVA) template for the configuration server.

TIP

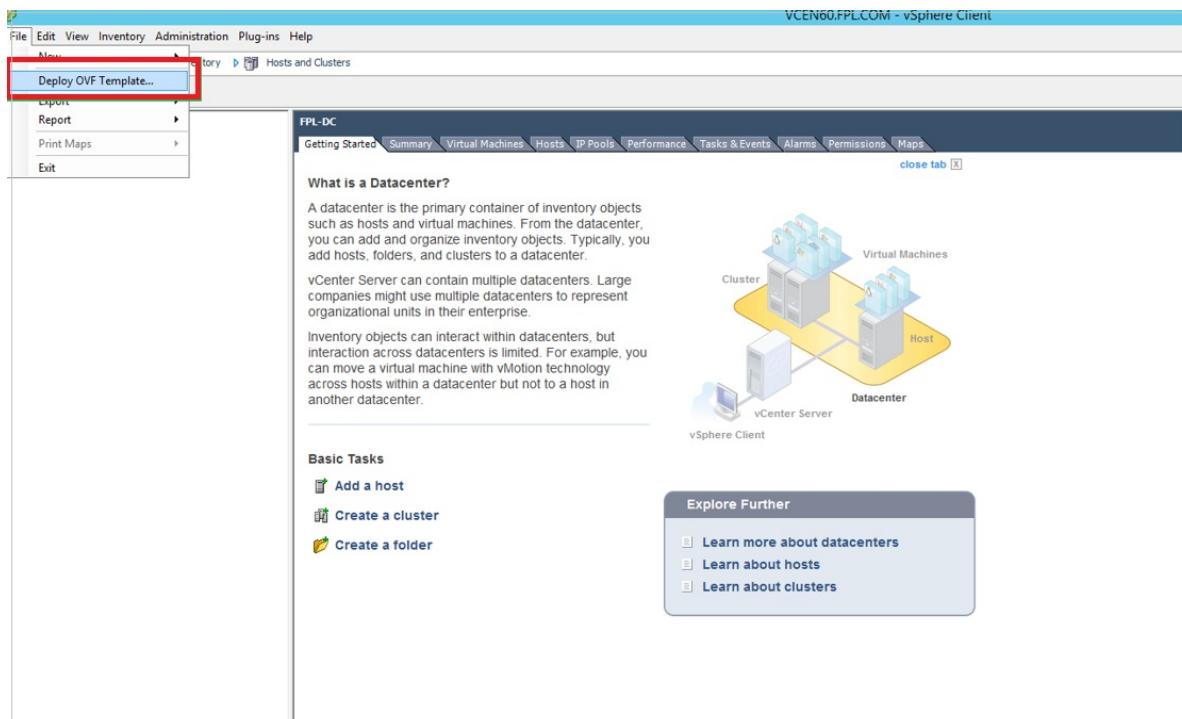
You can also download the latest version of the configuration server template directly from [Microsoft Download Center](#).

NOTE

The licence provided with OVA template is an evaluation licence valid for 180 days. Post this period, customer needs to activate the windows with a procured licence.

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. In **Select source**, enter the location of the downloaded OVF.
4. In **Review details**, select **Next**.
5. In **Select name and folder** and **Select configuration**, accept the default settings.
6. In **Select storage**, for best performance select **Thick Provision Eager Zeroed** in **Select virtual disk format**.
7. In the rest of the wizard pages, accept the default settings.
8. In **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.

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**. 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 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. The credentials must have access to the vault in which you want to register the configuration server.
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 few seconds.

Configure settings

1. In the configuration server management wizard, select **Setup connectivity**, and then select the NIC that the process server uses to receive replication traffic from VMs. Then select **Save**. You can't change this setting after it is configured.
2. In **Select Recovery Services vault**, sign in to Microsoft Azure, select your Azure subscription and the relevant resource group and vault.

NOTE

Once registered, there is no flexibility to change the recovery services vault.

3. In **Install third-party software**,

SCENARIO	STEPS TO FOLLOW
Can I download & install MySQL manually?	Yes. Download MySQL application & place it in the folder C:\Temp\ASRSetup , then install manually. Now, when you accept the terms > click on 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 > click on Download and install , the portal will use the installer added by you and installs the application. You can proceed to the next step post installation.
I would like to download & install MySQL through Azure Site Recovery	Accept the license agreement & click on Download and Install . Then you can proceed to the next step post installation.

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 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**, and then **Continue**. The credentials entered here are locally saved.

7. In **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.
8. Select **Finalize configuration** to complete registration.
9. After registration finishes, open Azure portal, verify that the configuration server and VMware server are listed on **Recovery Services Vault > Manage > Site Recovery Infrastructure > Configuration Servers**.

FAQ

1. Can I use the VM, where Configuration server is installed, for different purposes?

No, we recommend you to use the VM for sole purpose of configuration server. Ensure to follow all the specifications mentioned in the [previous section](#) for efficient management of disaster recovery.

2. Can I switch the vault already registered in the configuration server with a newly created vault?

No, once a vault is registered with configuration server, it cannot be changed.

3. Can I use the same configuration server for protecting both physical and virtual machines?

Yes, same configuration server can be used for replicating physical and virtual machines. However, physical machine can be failed back only to a VMware VM.

4. What is the purpose of a Configuration server and where is it used?

Refer to our Azure Site Recovery architecture [here](#) to learn more about configuration server and its functionalities.

5. Where can I find the latest version of Configuration server?

Refer to the article on steps to upgrade the configuration server [through portal](#). You can also directly download it from [Microsoft Download Center](#).

6. Where can I download the passphrase for configuration server?

Refer to [this article](#) to download the passphrase.

7. Where can I download vault registration keys?

In the **Recovery Services Vault, Manage > Site Recovery Infrastructure > Configuration Servers**. In Servers, select **Download registration key** to download the vault credentials file.

Upgrade the configuration server

To upgrade the configuration server to the latest version, read the steps given [here](#)

Troubleshoot deployment issues

Installation failures

SAMPLE ERROR MESSAGE	RECOMMENDED ACTION
ERROR Failed to load Accounts. Error: System.IO.IOException: Unable to read data from the transport connection when 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
<p>09:20:06:InnerException.Type: SrsRestApiClientLib.AcsException,InnerException. Message: ACS50008: SAML token is invalid. Trace ID: 1921ea5b-4723-4be7-8087-a75d3f9e1072 Correlation ID: 62fea7e6-2197-4be4-a2c0-71ceb7aa2d97> Timestamp: 2016-12-12 14:50:08Z</p>	<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>
<p>09:35:27 :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. Trace ID: e5ad1af1-2d39-4970-8eef-096e325c9950 Correlation ID: abe9deb8-3e64-464d-8375-36db9816427a Timestamp: 2016-05-19 01:35:39Z</p>	<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>
<p>06:28:45:Failed to create certificate 06:28:45:Setup cannot proceed. A certificate required to authenticate to Site Recovery cannot be created. Rerun Setup</p>	<p>Ensure you are running setup as a local administrator.</p>

Next steps

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

Prepare the target environment for VMware replication to Azure

7/9/2018 • 2 minutes to read • [Edit Online](#)

This article describes how to prepare your target Azure environment to start replicating VMware virtual machines to Azure.

Prerequisites

The article assumes:

- You have created a Recovery Services Vault to protect your VMware virtual machines. You can create a Recovery Services Vault from the [Azure portal](#).
- You have [setup your on-premises environment](#) to replicate VMware virtual machines 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. The left window is titled 'Prepare infrastructure' and the right window is titled 'Target'. Both windows belong to 'Contoso-RecoveryVault'.

Prepare infrastructure Window:

- Step 1:** Protection goal (VMware VMs/physical servers to...)
- Step 2:** Source (CONTOSO-CS2/Contoso-vCent...)
- Step 3:** Target (Prepared) - This step is highlighted with a blue background.
- Step 4:** Replication settings (Prepare)
- Step 5:** Capacity planning (Select)

Target Window:

- Step 1 : Select Azure subscription:**
 - Subscription: DR Hybrid Application Scenarios
 - Select the deployment model used after failover: Resource Manager
- Step 2 : Ensure that at least one compatible Azure storage account exist:**
 - Storage account(s): Found 9 compatible Azure storage accounts out of 122 available in the subscription.
- Step 3 : Ensure that at least one compatible Azure virtual network exist:**
 - Network(s): Found 3 compatible Azure virtual networks out of 59 available in the subscription.

Both windows have an 'OK' button at the bottom right.

1. **Subscription:** From the drop-down menu, select the Subscription that you want to replicate your virtual

machines to.

2. **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 compatible storage account and virtual network in the target subscription to replicate and failover your virtual machine to.

Once the validations complete successfully, click OK to go to the next step.

If you don't have a compatible Resource Manager storage account or virtual network, you can create one by clicking the **+ Storage Account** or **+ Network** buttons at the top of the page.

Next steps

[Configure replication settings.](#)

Prepare target (VMware to Azure)

7/9/2018 • 2 minutes to read • [Edit Online](#)

This article describes how to prepare your Azure environment to start replicating physical servers (x64) running Windows or Linux into Azure.

Prerequisites

The article assumes:

- You have created a Recovery Services Vault to protect your physical servers. You can create a Recovery Services Vault from the [Azure portal](#).
- You have [setup your on-premises environment](#) to replicate 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' on the left and 'Target' on the right.

Prepare infrastructure (Left Window):

- Header: Contoso-RecoveryVault
- Section: These are long running tasks done on premise.
 - 1 Protection goal: VMware VMs/physical servers t... (Green checkmark)
 - 2 Source: CONTOSO-CS2 (Green checkmark)
 - 3 Target Prepare (Blue box highlighting this step)
 - 4 Replication settings: Prepare
 - 5 Capacity planning: Select
- Buttons: OK

Target (Right Window):

- Header: Contoso-RecoveryVault
- Section: Step 1 : Select Azure subscription
 - * Subscription: DR Hybrid Application Scenarios (dropdown menu)
 - * Select the deployment model used after failover:
 - Resource Manager (selected)
- Section: Step 2 : Ensure that at least one compatible Azure storage account exist
 - Storage account(s):
 - Found 9 compatible Azure storage accounts out of 122 available in the subscription
- Section: Step 3 : Ensure that at least one compatible Azure virtual network exist
 - Network(s):
 - Found 3 compatible Azure virtual networks out of 59 available in the subscription
- Buttons: OK

1. **Subscription:** From the drop-down menu, select the Subscription that you want to replicate your physical servers to.
2. **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 compatible storage account and virtual network in the target subscription to replicate and failover your physical servers to.

Once the validations complete successfully, click OK to go to the next step.

If you don't have a compatible Resource Manager storage account or virtual network, you can create one by clicking the **+ Storage Account** or **+ Network** buttons at the top of the page.

Next steps

[Configure replication settings.](#)

Configure and manage replication policies for VMware replication

8/2/2018 • 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

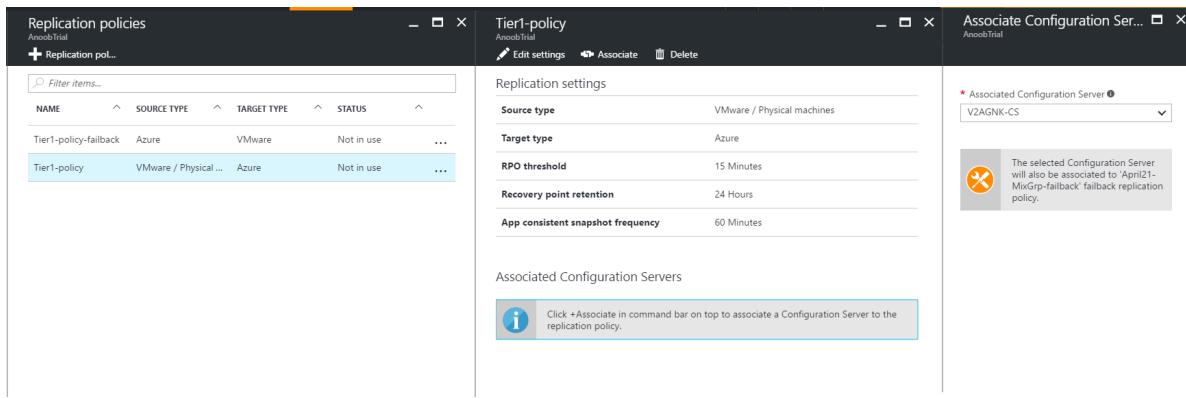
1. Select **Manage > Site Recovery Infrastructure**.
2. In **For VMware and Physical machines**, select **Replication policies**.
3. Click **+Replication policy**, and specify the policy name.
4. In **RPO threshold**, specify the RPO limit. Alerts are generated when continuous replication exceeds this 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**, specify how often (in minutes) recovery points that contain application-consistent snapshots will be created.
7. Click **OK**. The policy should be created in 30 to 60 seconds.

When you create a replication policy, a matching fallback replication policy is automatically created, with the suffix "fallback". 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.

Replication policies

AnoobTrial

+ Replication pol...

Filter items...

NAME	SOURCE TYPE	TARGET TYPE	STATUS	...
Tier1-policy-fallback	Azure	VMware	Not in use	...
Tier1-policy	VMware / Physical ...	Azure	Not in use	...

Tier1-policy

AnoobTrial

Edit settings Associate Delete

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	...

Disassociate or delete a replication policy

1. 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.
2. Click **OK**.

Exclude disks from replication for VMware to Azure scenario

7/9/2018 • 9 minutes to read • [Edit Online](#)

This article describes how to exclude disks when replicating VMware VMs to Azure. This exclusion can optimize the consumed replication bandwidth or optimize the target-side resources that such disks utilize. If you need information about excluding disks for Hyper-V, read [this article](#).

Prerequisites

By default, all disks on a machine are replicated. To exclude a disk from replication, you must manually install the Mobility service on the machine before you enable replication if you are replicating from VMware to Azure.

Why exclude disks from replication?

Excluding disks from replication is often necessary because:

- The data that's churned on the excluded disk is not important or doesn't need to be replicated.
- You want to save storage and network resources by not replicating this churn.

What are the typical scenarios?

You can identify specific examples of data churn that are great candidates for exclusion. Examples might 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 file can register a significant amount of churn. However, replicating this data from the primary site to Azure would be resource intensive. Thus, you can use the following steps to optimize replication of a virtual machine with a single virtual disk that has both the operating system and the paging file:

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.

Similarly, you can use the following steps to optimize a disk that has both the Microsoft SQL Server tempdb file and the system database file:

1. Keep the system database and tempdb on two different disks.
2. Exclude the tempdb disk from replication.

How to exclude disks from replication?

Follow the [Enable replication](#) workflow to protect a virtual machine from the Azure Site Recovery portal. In the fourth step of the workflow, use the **DISK TO REPLICATE** column to exclude disks from replication. By default, all disks are selected for replication. Clear the check box of disks that you want to exclude from replication, and then complete the steps to enable replication.

1 Source
EV2ACS3 ✓

2 Target
Azure ✓

3 Virtual machines
2 Selected ✓

4 Properties
Configure properties >

5 Replication settings
Configure replication settings >

NOTE

- You can only exclude disks on VMs that already have the Mobility service installed. You need to manually install the Mobility service, because the Mobility service is only installed using the push mechanism after replication is enabled.
- Only basic disks can be excluded from replication. You can't exclude operating system or dynamic disks.
- After you enable replication, you can't add or remove disks for replication. If you want to add or exclude a disk, you need to disable protection for the machine and then enable it again.
- If you exclude a disk that's needed for an application to operate, after failover to Azure, you'll need to create the disk manually in Azure so that the replicated application can run. Alternatively, you can integrate Azure automation into a recovery plan to create the disk during failover of the machine.
- Window virtual machine: Disks that you create manually in Azure are not failed back. For example, if you fail over three disks and create two disk directly in Azure Virtual Machines, only three disks that were failed over are failed back. You can't include disks that you created manually in failback or in reprotect from on-premises to Azure.
- Linux virtual machine: Disks that you create manually in Azure are failed back. For example, if you fail over three disks and create two disks directly in Azure Virtual Machines, all five will be failed back. You can't exclude disks that were created manually from failback.

End-to-end scenarios of exclude disks

Let's consider two scenarios to understand the exclude disk feature:

- SQL Server tempdb disk
- Paging file (pagefile.sys) disk

Example 1: Exclude the SQL Server tempdb disk

Let's consider a SQL Server virtual machine that has a tempdb that can be excluded.

The name of the virtual disk is SalesDB.

Disk on the source virtual machine are as follows:

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:\	SQL system database and User Database1

DISK NAME	GUEST OPERATING SYSTEM DISK#	DRIVE LETTER	DATA TYPE ON THE DISK
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)) Write down the folder path before failover.
DB-Disk4	Disk4	G:\	User Database2

Because data churn on two disks of the virtual machine is temporary, while you protect the SalesDB virtual machine, exclude Disk2 and Disk3 from replication. Azure Site Recovery will not replicate those disks. On failover, those disks will not be present on the failover virtual machine on Azure.

Disks on the Azure virtual machine after failover are as follows:

GUEST OPERATING SYSTEM DISK#	DRIVE LETTER	DATA TYPE ON THE DISK
DISK0	C:\	Operating system disk
Disk1	E:\	Temporary storage Azure adds this disk and assigns the first available drive letter.
Disk2	D:\	SQL system database and User Database1
Disk3	G:\	User Database2

Because Disk2 and Disk3 were excluded from the SalesDB virtual machine, E: is the first drive letter from the available list. Azure assigns E: to the temporary storage volume. For all the replicated disks, the drive letters remain the same.

Disk3, which was the SQL tempdb disk (tempdb folder path F:\MSSQL\Data), was excluded from replication. The disk is not available on the failover virtual machine. As a result, the SQL service is in a stopped state, and it needs the F:\MSSQL\Data path.

There are two ways to create this path:

- Add a new disk and assign tempdb folder path.
- Use an existing temporary storage disk for the tempdb folder path.

Add a new disk:

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 virtual machine with the same or more size as that of the source SQL tempdb disk (Disk3).
3. Sign in to the Azure virtual machine. From the disk management (diskmgmt.msc) console, initialize and format the newly added disk.
4. Assign the same drive letter that was used by the SQL tempdb disk (F:).
5. Create a tempdb folder on the F: volume (F:\MSSQL\Data).
6. Start the SQL service from the service console.

Use an existing temporary storage disk for the SQL tempdb folder path:

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
```

Refer to the following Azure guideline for temporary storage disk:

- [Using SSDs in Azure VMs to store SQL Server TempDB and Buffer Pool Extensions](#)
- [Performance best practices for SQL Server in Azure Virtual Machines](#)

Fallback (from Azure to an on-premises host)

Now let's understand the disks that are replicated when you fail over from Azure to your on-premises VMware. Disks that you create manually in Azure will not be replicated. For example, if you fail over three disks and create two directly in Azure Virtual Machines, only three disks that were failed over will be failed back. You can't include disks that were created manually in failback or in reprotect from on-premises to Azure. It also does not replicate the temporary storage disk to on-premises hosts.

Fallback to original location recovery

In the previous example, the Azure virtual machine disk configuration is as follows:

GUEST OPERATING SYSTEM DISK#	DRIVE LETTER	DATA TYPE ON THE DISK
DISK0	C:\	Operating system disk
Disk1	E:\	Temporary storage Azure adds this disk and assigns the first available drive letter.
Disk2	D:\	SQL system database and User Database1

GUEST OPERATING SYSTEM DISK#	DRIVE LETTER	DATA TYPE ON THE DISK
Disk3	G:\	User Database2

When failback is done to the original location, the failback virtual machine disk configuration does not have excluded disks. Disks that were excluded from VMware to Azure will not be available on the failback virtual machine.

After planned failover from Azure to on-premises VMware, disks on the VMWare virtual machine (original location) are as follows:

GUEST OPERATING SYSTEM DISK#	DRIVE LETTER	DATA TYPE ON THE DISK
DISK0	C:\	Operating system disk
Disk1	D:\	SQL system database and User Database1
Disk2	G:\	User Database2

Example 2: Exclude the paging file (pagefile.sys) disk

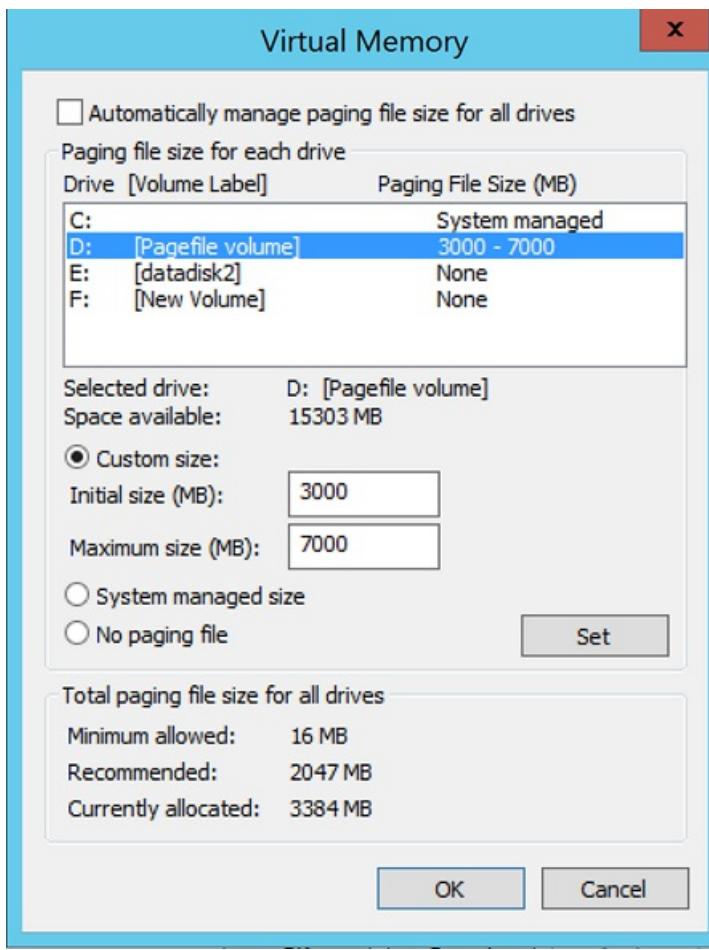
Let's consider a virtual machine that has a paging file disk that can be excluded. There are two cases.

Case 1: The paging file is configured on the D: drive

Here's the disk configuration:

DISK NAME	GUEST OPERATING SYSTEM DISK#	DRIVE LETTER	DATA TYPE ON THE DISK
DB-Disk0-OS	DISK0	C:\	Operating system disk
DB-Disk1 (Excluded the disk from the protection)	Disk1	D:\	pagefile.sys
DB-Disk2	Disk2	E:\	User data 1
DB-Disk3	Disk3	F:\	User data 2

Here are the paging file settings on the source virtual machine:

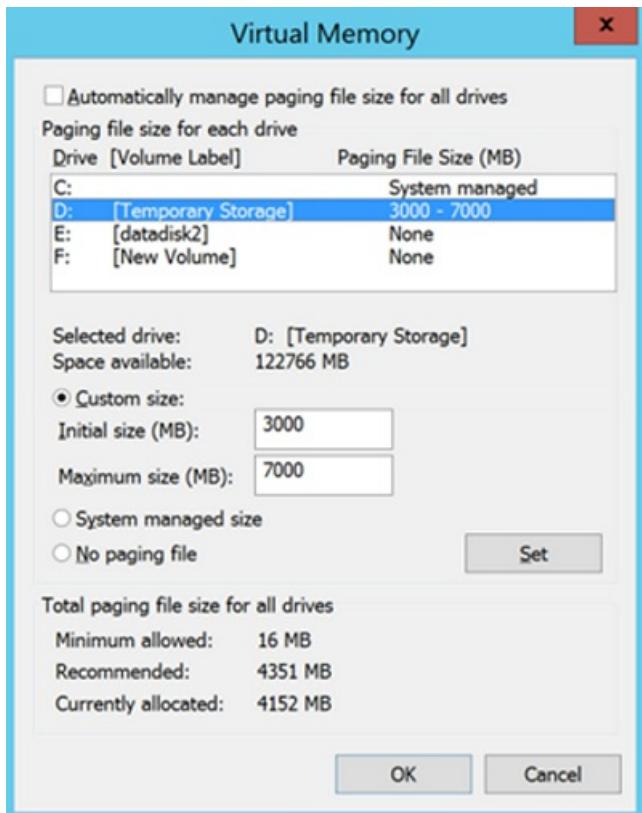


After failover of the virtual machine from VMware to Azure, disks on the Azure virtual machine are as follows:

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:\	Temporary storage pagefile.sys
DB-Disk2	Disk2	E:\	User data 1
DB-Disk3	Disk3	F:\	User data 2

Because Disk1 (D:) was excluded, D: is the first drive letter from the available list. Azure assigns D: to the temporary storage volume. Because D: is available on the Azure virtual machine, the paging file setting of the virtual machine remains the same.

Here are the paging file settings on the Azure virtual machine:

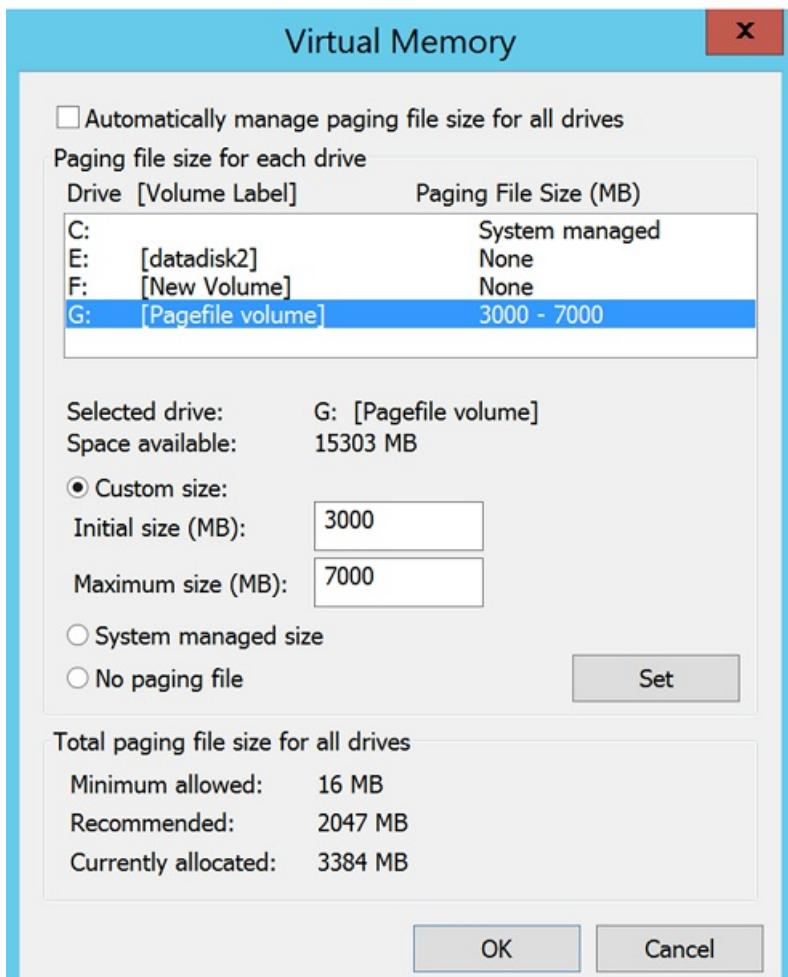


Case 2: The paging file is configured on another drive (other than D: drive)

Here's the source virtual machine disk configuration:

DISK NAME	GUEST OPERATING SYSTEM DISK#	DRIVE LETTER	DATA TYPE ON THE DISK
DB-Disk0-OS	DISK0	C:\	Operating system disk
DB-Disk1 (Excluded the disk from protection)	Disk1	G:\	pagefile.sys
DB-Disk2	Disk2	E:\	User data 1
DB-Disk3	Disk3	F:\	User data 2

Here are the paging file settings on the on-premises virtual machine:

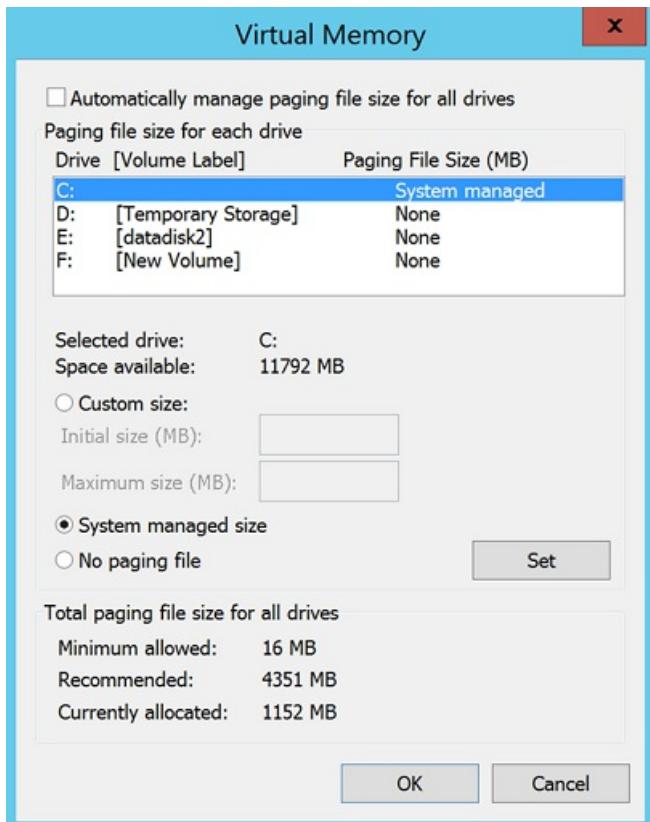


After failover of the virtual machine from VMware to Azure, disks on the Azure virtual machine are as follows:

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:\	Temporary storage pagefile.sys
DB-Disk2	Disk2	E:\	User data 1
DB-Disk3	Disk3	F:\	User data 2

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 is not available, the system will use the C: drive for the paging file.

Here are the paging file settings on the Azure virtual machine:



Next steps

After your deployment is set up and running, [learn more](#) about different types of failover.

Enable replication to Azure for VMware VMs

7/9/2018 • 7 minutes to read • [Edit Online](#)

This article describes how to enable replication of on-premises VMware VMs to Azure.

Prerequisites

This article assumes that you have:

1. [Set up on-premises source environment](#).
2. [Set up target environment in Azure](#).

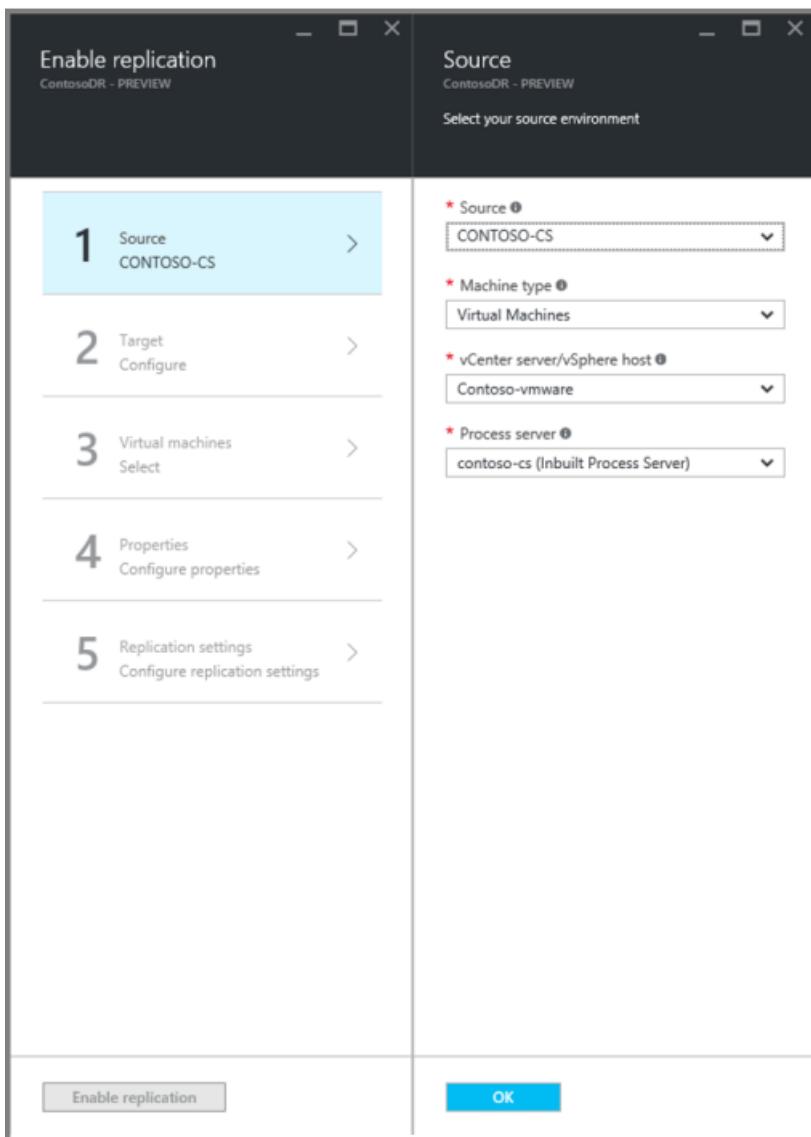
Before you start

When replicating VMware virtual machines:

- 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 might take 15 minutes or longer for them to appear in the Azure portal after discovery. Likewise, discovery can take 15 minutes or more when you add a new vCenter server or vSphere host.
- Environment changes on the virtual machine (such as VMware tools installation) can take 15 minutes or more to be updated in the portal.
- You can check the last discovered time for VMware VMs in the **Last Contact At** field for the vCenter server/vSphere host, on the **Configuration Servers** page.
- To add machines for replication without waiting for the scheduled discovery, highlight the configuration server (don't click it), and click the **Refresh** button.
- When you enable replication, if the machine is prepared, the process server automatically installs the Mobility Service on it.

Enable replication

1. Click **Step 2: Replicate application > Source**. After you've enabled replication for the first time, click **+Replicate** in the vault to enable replication for additional machines.
2. In the **Source** page > **Source**, select the configuration server.
3. In **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 machines.
5. Select the process server, which will be the name of the configuration server if you haven't created any additional process servers. Then click **OK**.

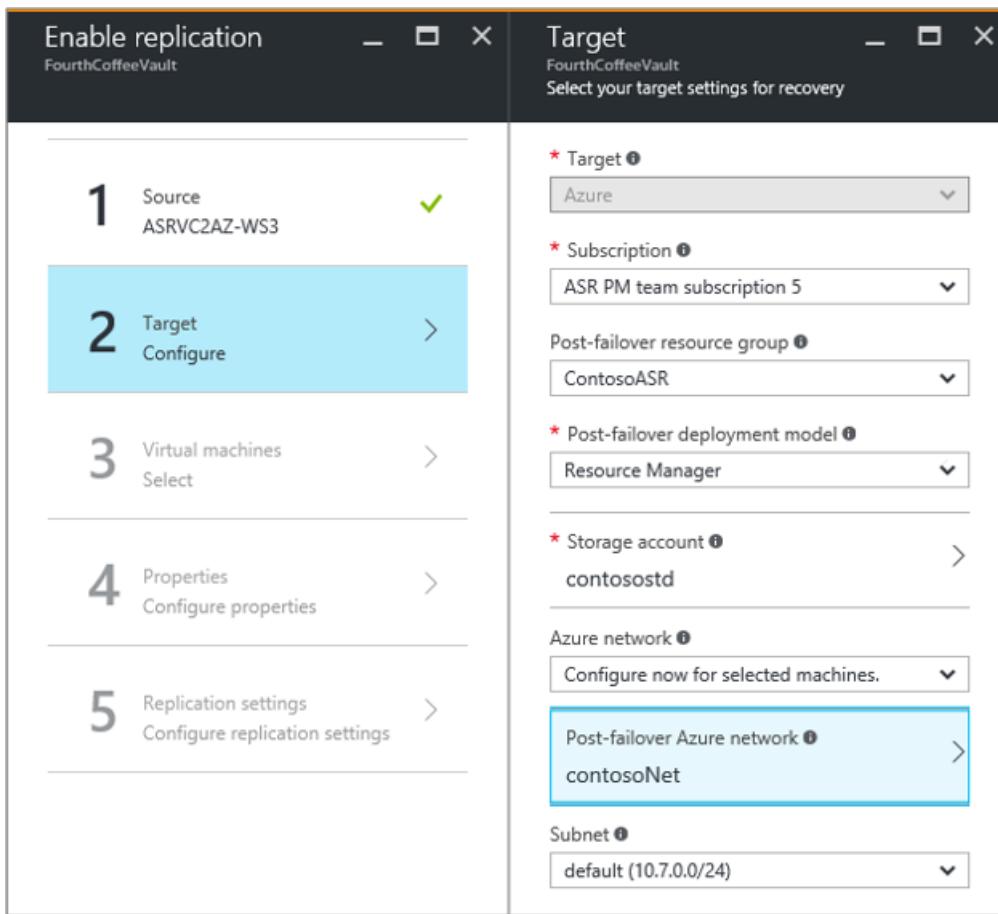


6. In **Target**, select the subscription and the resource group where you want to create the failed-over virtual machines. Choose the deployment model that you want to use in Azure for the failed-over virtual machines.
7. Select the Azure Storage account you want to use for replicating data.

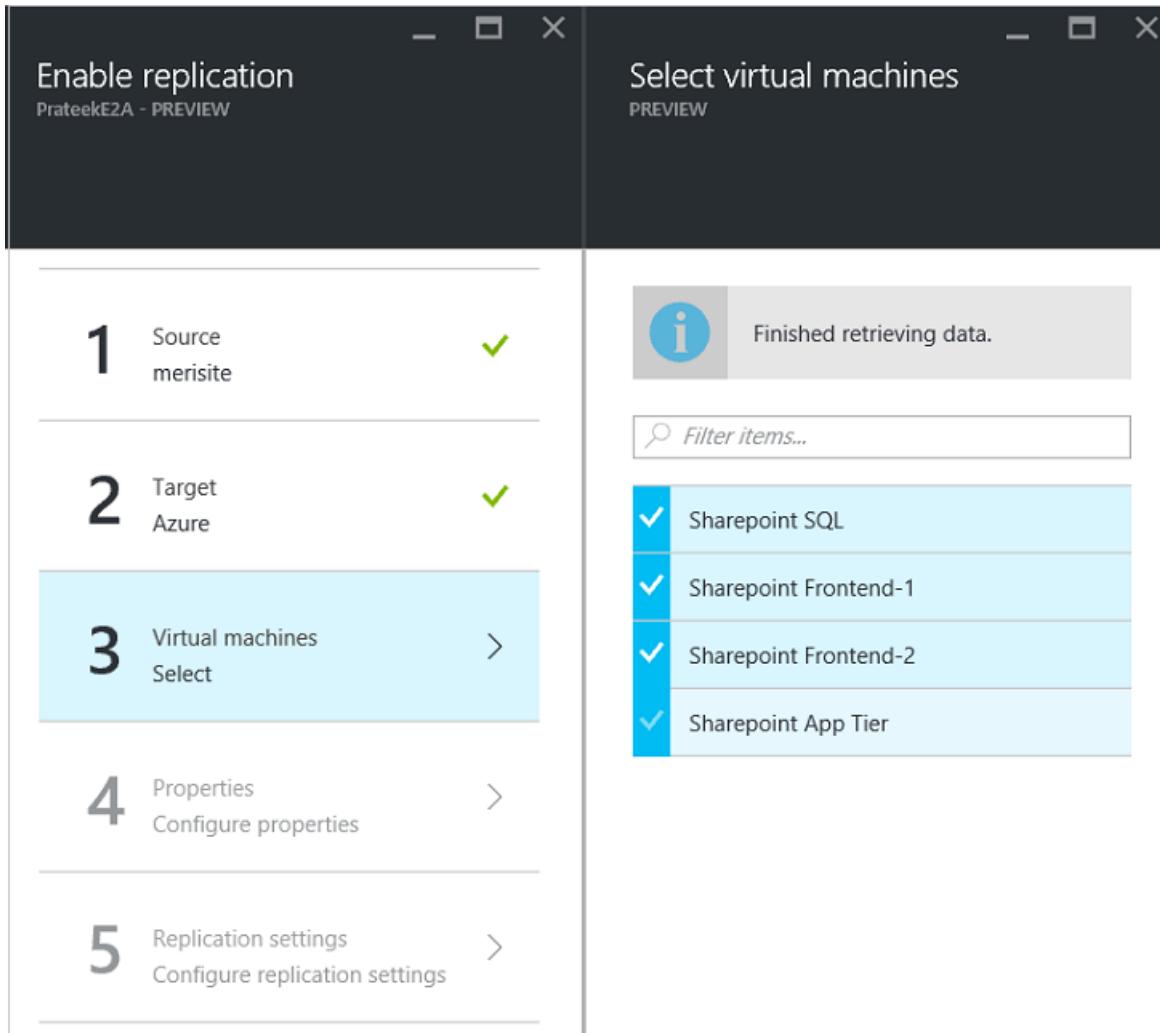
NOTE

- You can select a premium or standard storage account. If you select a premium account, you need to specify an additional standard storage account for ongoing replication logs. Accounts must be in the same region as the Recovery Services vault.
- If you want to use a different storage account, you can [create one](#). To create a storage account by using Resource Manager, click **Create new**.

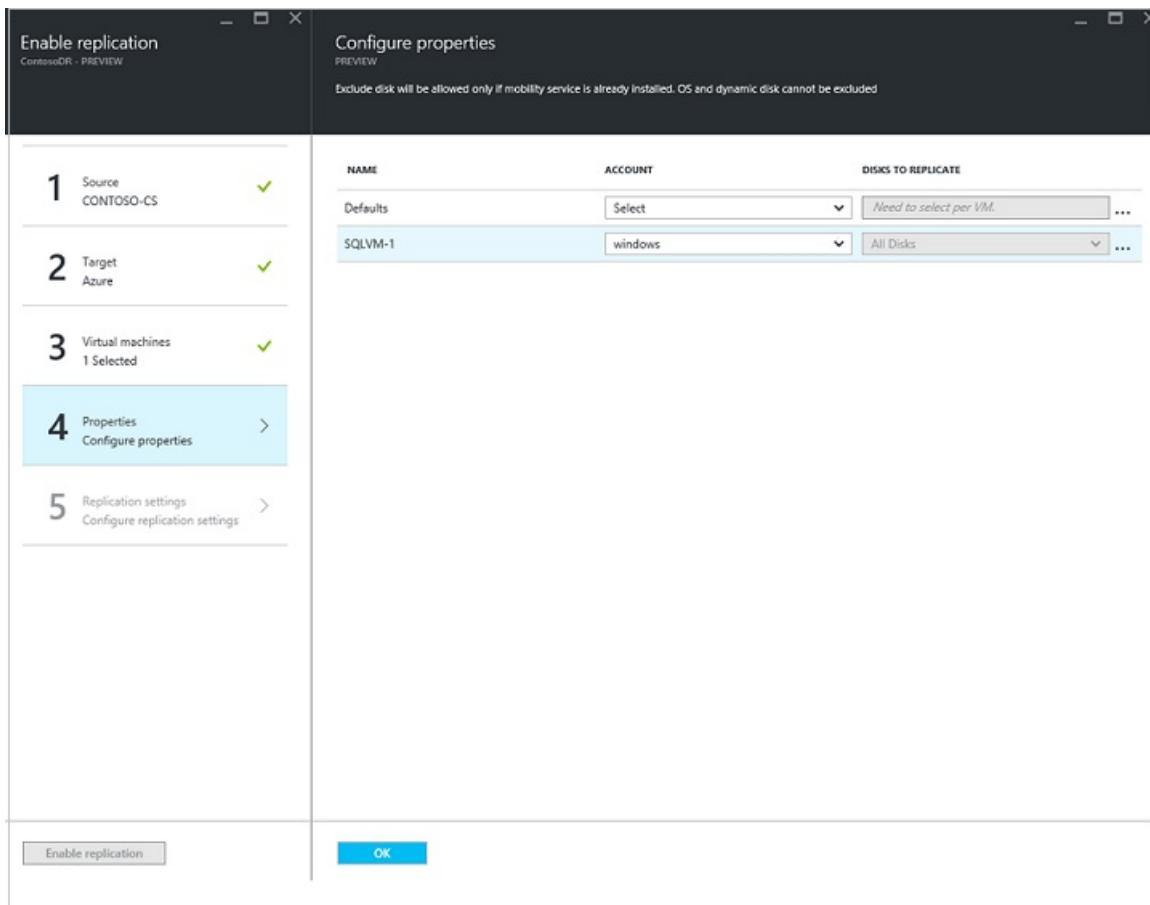
8. Select the Azure network and subnet to which Azure VMs will connect when they're spun up after failover. The network must be in the same region as the Recovery Services vault. Select **Configure now for selected machines** to apply the network setting to all machines you select for protection. Select **Configure later** to select the Azure network per machine. If you don't have a network, you need to [create one](#). To create a network by using Resource Manager, click **Create new**. Select a subnet if applicable, and then click **OK**.



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 click **OK**.



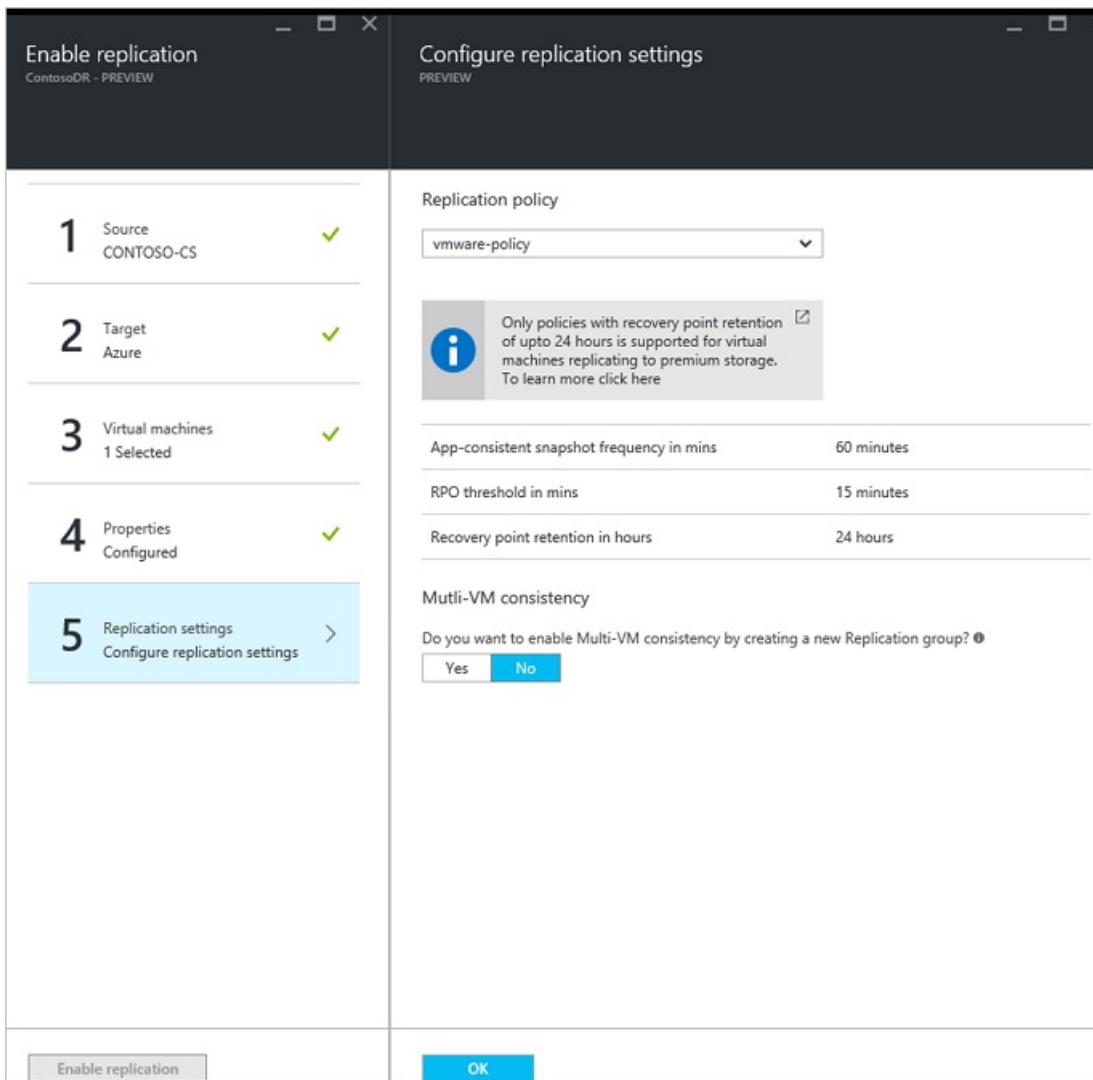
- In **Properties > Configure properties**, select the account used by the process server to automatically install the Mobility Service on the machine.
- By default, all disks are replicated. To exclude disks from replication, click **All Disks** and clear any disks you don't want to replicate. Then click **OK**. You can set additional properties later. [Learn more](#) about excluding disks.



- In **Replication settings > Configure replication settings**, verify that the correct replication policy is selected. You can modify replication policy settings in **Settings > Replication policies > (policy name) > Edit Settings**. Changes you apply to a policy also apply to replicating and new machines.
- Enable **Multi-VM consistency** if you want to gather machines into a replication group. Specify a name for the group, and then click **OK**.

NOTE

- Machines in a replication group replicate together and have shared crash-consistent and app-consistent recovery points when they fail over.
- Gather VMs and physical servers together so that they mirror your workloads. Enabling multi-VM consistency can impact workload performance. Use only if machines are running the same workload and you need consistency.



14. 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.

NOTE

If the machine is prepared for push installation, the Mobility Service component is installed when protection is enabled. After the component is installed on the machine, a protection job starts and fails. After the failure, you need to manually restart each machine. After the restart, the protection job begins again and initial replication occurs.

View and manage VM properties

Next, you verify the properties of the source machine. Remember that the Azure VM name needs to conform with [Azure virtual machine requirements](#).

1. Click **Settings > Replicated items >**, and then select the machine. The **Essentials** page shows information about machine 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 specify the Azure VM name and target size. Modify the name to comply with Azure requirements if necessary.

4. You can select a **resource group** from which a machine becomes part of a post failover. You can change this setting any time before failover. Post failover, if you migrate the machine to a different resource group, the protection settings for that machine break.
5. You can select an **availability set** if your machine needs to be part of a post failover. While you're selecting an availability set, keep in mind that:
 - Only availability sets belonging to the specified resource group are listed.
 - Machines with different virtual networks cannot be a part of the same availability set.
 - Only virtual machines of the same size can be a part of an availability set.
6. You can also view and add information about the target network, subnet, and IP address assigned to the Azure VM.
7. In **Disks**, you can see the operating system and data disks on the VM to be replicated.

Configure networks and IP addresses

- You can set the target IP address. If you don't provide an address, the failed-over 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, the same target IP address can be used for test failover.
- 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 has 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 is used. For example, if a source machine has two network adapters and the target machine size supports four, the target machine has two adapters. If the source machine has two adapters but the supported target size only supports one, then the target machine has only one adapter.
 - If the virtual machine has multiple network adapters, they all connect to the same network. Also, the first one 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 machines that are migrated to Azure, or to use Azure for disaster recovery. If you're eligible to use the Azure Hybrid Benefit, you can specify that the virtual machine assigned this benefit is the one Azure Site Recovery creates if there's a failover. To do this:

- Go to the Compute and Network properties section of the replicated virtual machine.
- Answer the question that asks if you have a Windows Server License that makes you eligible for Azure Hybrid Benefit.
- Select the check box to confirm that you have an eligible Windows Server license with Software Assurance, which you can use to apply the Azure Hybrid Benefit on the machine that will be created on failover.
- Save settings for the replicated machine.

Learn more about [Azure Hybrid Benefit](#).

Common issues

- Each disk should be less than 1 TB in size.
- The OS disk should be a basic disk and not a dynamic disk.
- For generation 2/UEFI-enabled virtual machines, the operating system family should be Windows and the boot disk should be less than 300 GB.

Next steps

After protection is complete and the machine has reached a protected state, you can try a [failover](#) to check whether your application comes up in Azure or not.

If you want to disable protection, learn how to [clean registration and protection settings](#).

Set up VMware replication in a multi-tenancy environment with the Cloud Solution Provider (CSP) program

7/9/2018 • 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 interface for creating a new customer. On the left sidebar, under 'New customer', there are tabs for 'Account info', 'Subscriptions', 'Review', and 'Confirmation'. Below these are links for 'Customers' and 'Programs'. The main content area is titled 'Account info' and contains fields for 'Company name' (ASRTest), 'Primary domain name' (.onmicrosoft.com), 'Address line 1' (1 Microsoft Way), 'Address line 2' (empty), 'City' (Redmond), 'State/Province' (Washington), 'ZIP/Postal code' (98052), '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

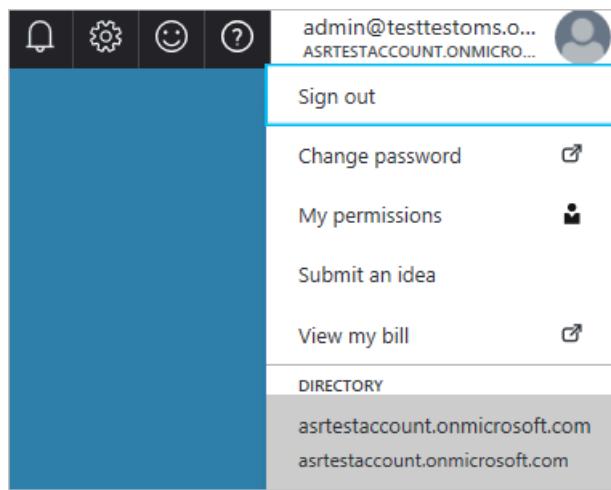
Current estimate Set a budget, and you'll be able to track the usage on the portal if your monthly spending will exceed it.
\$0.00 Apply

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.

Microsoft Partner Center

Programs How-to Support Find a Partner Dashboard

ASRTTest Subscriptions Export subscriptions

Subscriptions Customer insights

Users and licenses

Service management Account

← Customers

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 All resources (Azure portal)

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

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 **Add**, to add a user with the relevant access level. The users that were created through the CSP portal are automatically displayed on the page that opens after you click an access level.

Microsoft Azure - Access control (IAM)

Subscription

+ Add Roles

Search (Ctrl+)

Overview

Access control (IAM)

Diagnose and solve problems

SETTINGS

Programmatic deployment

Resource groups

Add access Microsoft Azure

Select 1 Select a role Owner ✓

2 Add users None selected >

Add users Owner + Invite

Select Search by name or email address

ASRTTest admin@asrttestaccount.onmicrosoft.com

- 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.

Install the Mobility service

8/6/2018 • 8 minutes to read • [Edit Online](#)

Azure Site Recovery Mobility Service is installed on VMware VMs and physical servers that you want to replicate to Azure. The service captures data writes on a computer and then forwards them to the process server. Deploy Mobility Service to every computer (VMware VM or physical server) that you want to replicate to Azure. You can deploy the Mobility Service on the servers and VMware VMs you want to protect using the following methods:

- [Install using software deployment tools like System Center Configuration Manager](#)
- [Install with Azure Automation and Desired State Configuration \(Automation DSC\)](#)
- [Install manually from the UI](#)
- [Install manually from a command prompt](#)
- [Install using the Site Recovery push installation](#)

IMPORTANT

Beginning with version 9.7.0.0, **on Windows VMs**, the Mobility Service installer also installs the latest available [Azure VM agent](#). When a computer fails over to Azure, the computer meets the agent installation prerequisite for using any VM extension.

On **Linux VMs**, WALinuxAgent has to be manually installed.

Prerequisites

Complete these prerequisite steps before you manually install Mobility Service on your server:

1. Sign in to your configuration server, and then open a command prompt window as an administrator.
2. Change the directory to the bin folder, and then create a passphrase file.

```
cd %ProgramData%\ASR\home\svsystems\bin  
genpassphrase.exe -v > MobSvc.passphrase
```

3. Store the passphrase file in a secure location. You use the file during Mobility Service installation.
4. Mobility Service installers for all supported operating systems are in the %ProgramData%\ASR\home\svsystems\pushinstallsvc\repository folder.

Mobility Service installer-to-operating system mapping

To see a list of Operating System versions with a compatible Mobility Service package refer to the list of [supported operating systems for VMware virtual machines and physical servers](#).

INSTALLER FILE TEMPLATE NAME	OPERATING SYSTEM
Microsoft-ASR_UA*Windows*release.exe	Windows Server 2008 R2 SP1 (64-bit) Windows Server 2012 (64-bit) Windows Server 2012 R2 (64-bit) Windows Server 2016 (64-bit)
Microsoft-ASR_UA*RHEL6-64*release.tar.gz	Red Hat Enterprise Linux (RHEL) 6.* (64-bit only) CentOS 6.* (64-bit only)

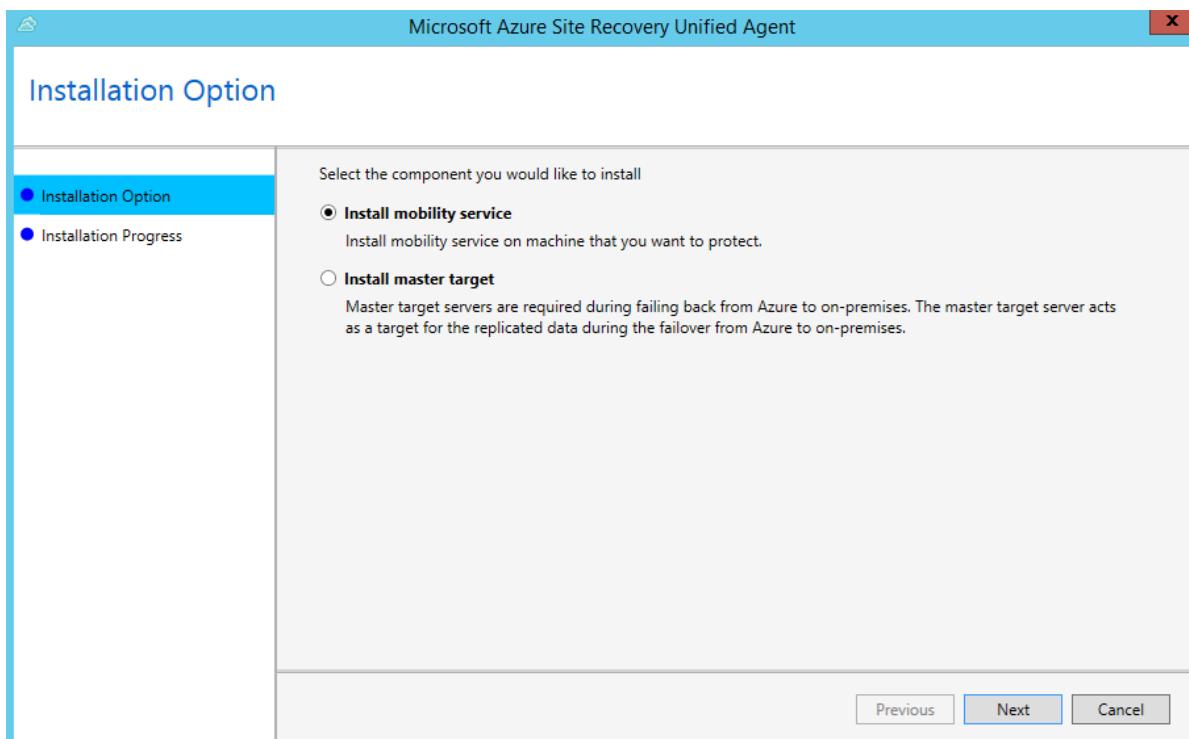
INSTALLER FILE TEMPLATE NAME	OPERATING SYSTEM
Microsoft-ASR_UA*RHEL7-64*release.tar.gz	Red Hat Enterprise Linux (RHEL) 7.* (64-bit only) CentOS 7.* (64-bit only)
Microsoft-ASR_UA*SLES12-64*release.tar.gz	SUSE Linux Enterprise Server 12 SP1,SP2,SP3 (64-bit only)
Microsoft-ASR_UA*SLES11-SP3-64*release.tar.gz	SUSE Linux Enterprise Server 11 SP3 (64-bit only)
Microsoft-ASR_UA*SLES11-SP4-64*release.tar.gz	SUSE Linux Enterprise Server 11 SP4 (64-bit only)
Microsoft-ASR_UA*OL6-64*release.tar.gz	Oracle Enterprise Linux 6.4, 6.5 (64-bit only)
Microsoft-ASR_UA*UBUNTU-14.04-64*release.tar.gz	Ubuntu Linux 14.04 (64-bit only)
Microsoft-ASR_UA*UBUNTU-16.04-64*release.tar.gz	Ubuntu Linux 16.04 LTS server (64-bit only)
Microsoft-ASR_UA*DEBIAN7-64*release.tar.gz	Debian 7 (64-bit only)
Microsoft-ASR_UA*DEBIAN8-64*release.tar.gz	Debian 8 (64-bit only)

Install Mobility Service manually by using the GUI

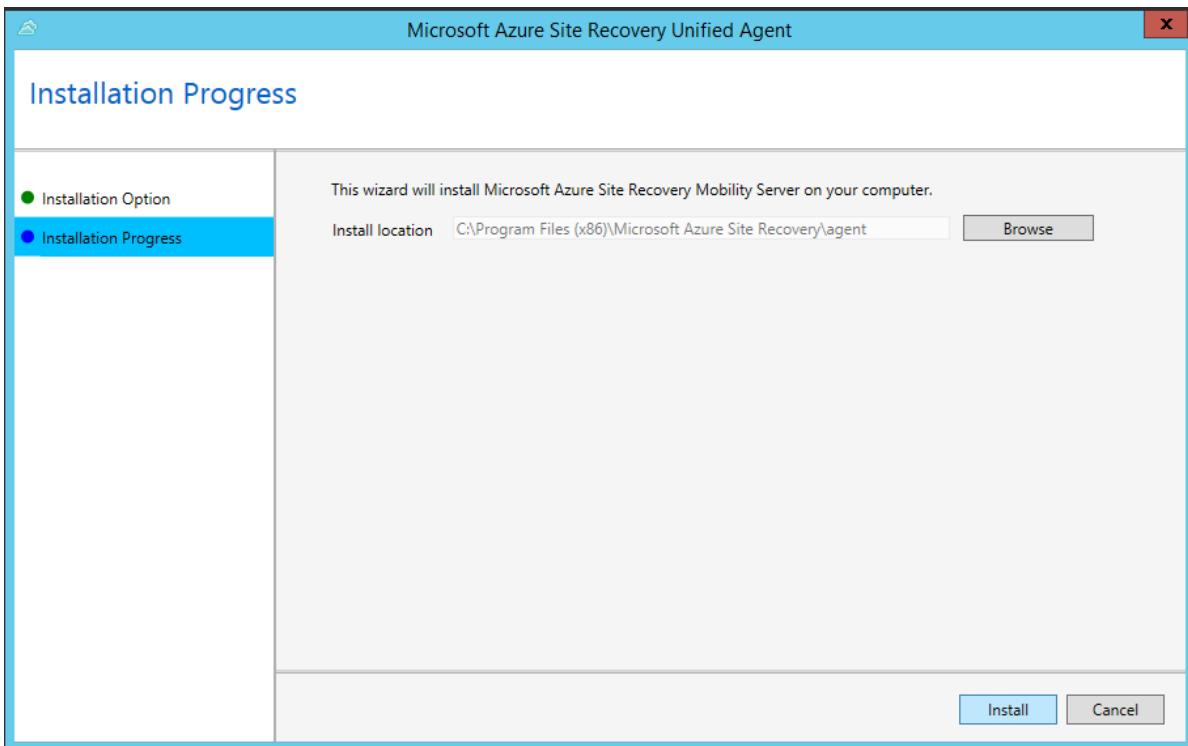
IMPORTANT

If you use a configuration server to replicate Azure IaaS virtual machines from one Azure subscription/region to another, use the command-line-based installation method.

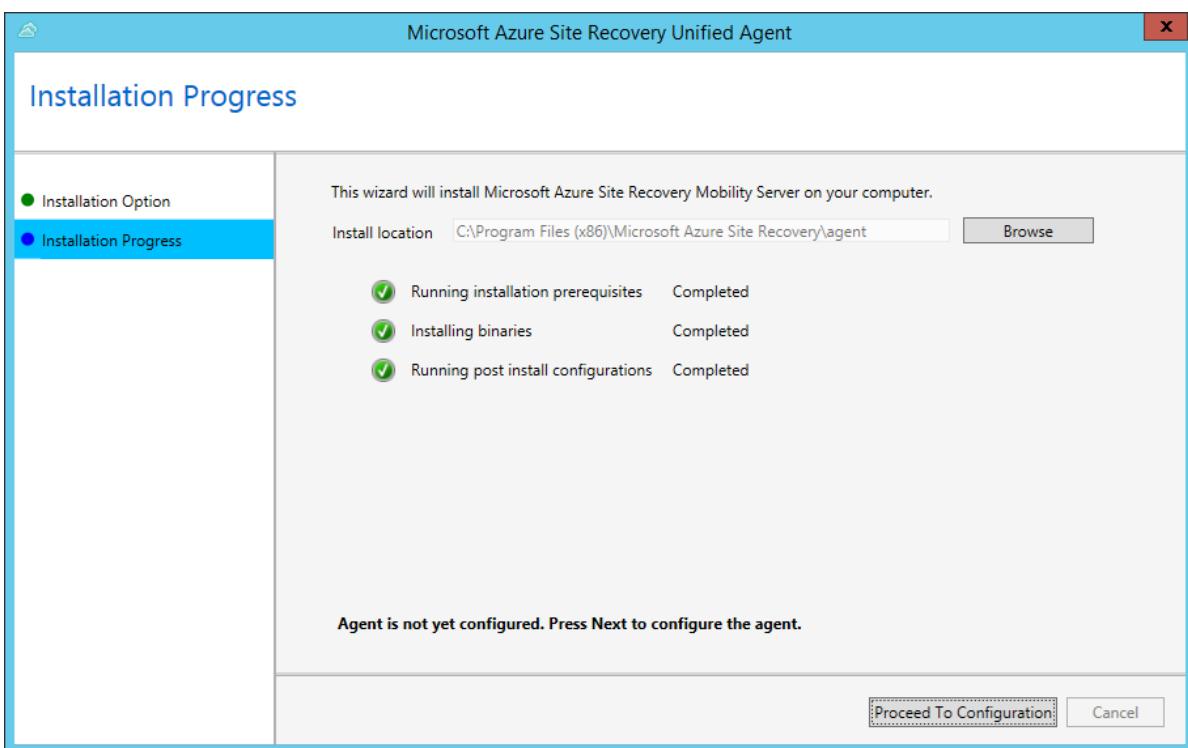
1. Copy the installation to the server, and then open the installer.
2. On **Installation Option**, select **Install mobility service**.



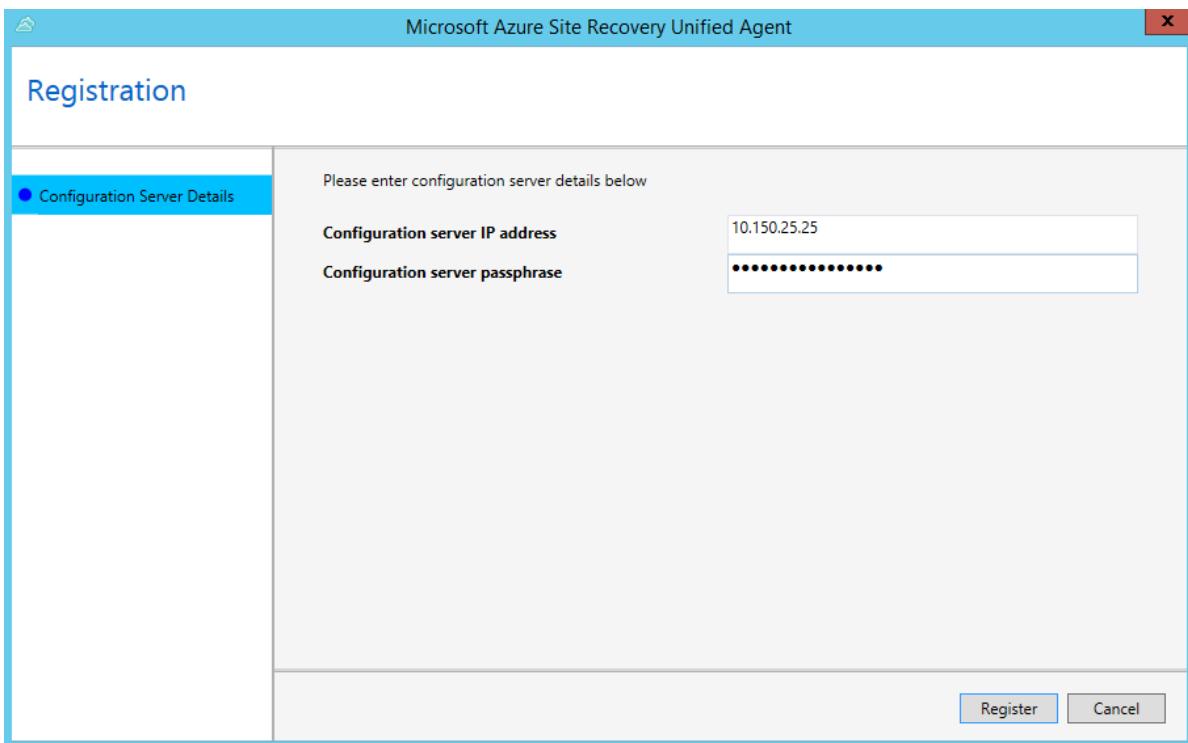
3. Select the installation location, and then select **Install** to start the installation procedure.



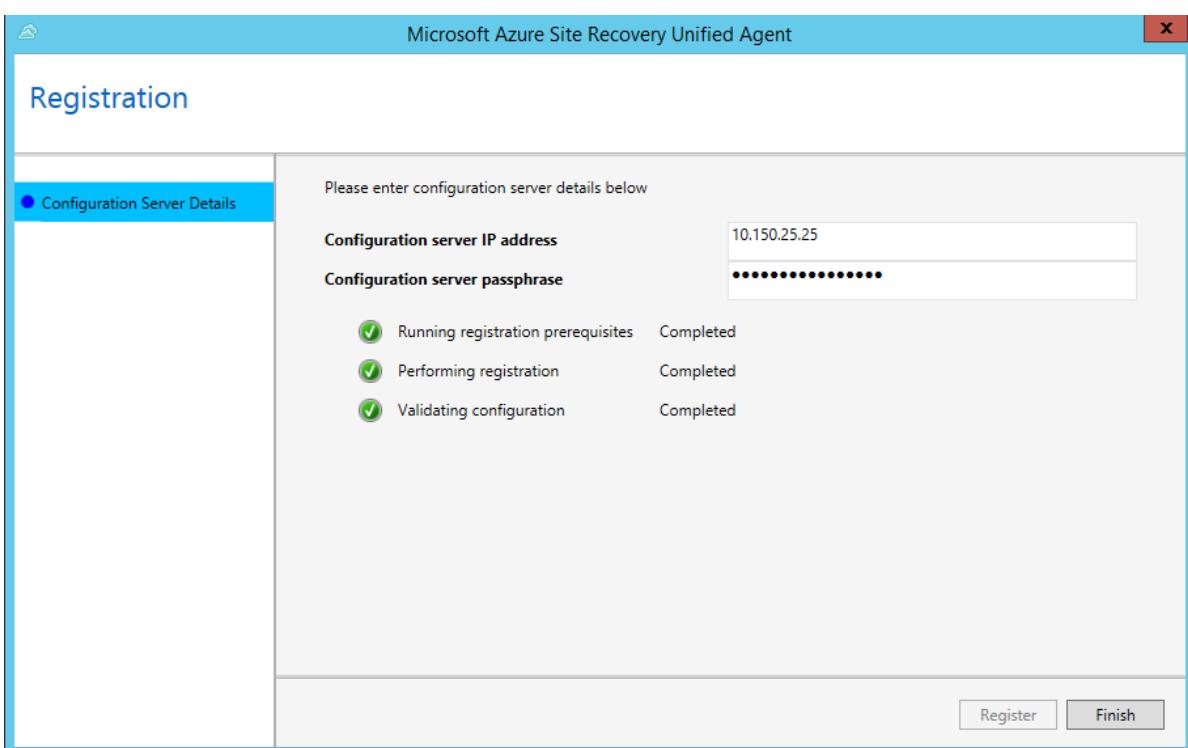
4. Use the **Installation Progress** page to monitor the installer's progress.



5. After the installation is finished, select **Proceed to Configuration** to register Mobility Service with your configuration server.



6. Select **Register** to finish the registration.



Install Mobility Service manually at a command prompt

Command-line installation on a Windows computer

1. Copy the installer to a local folder (for example, C:\Temp) on the server that you want to protect. Run the following commands as an administrator at a command prompt:

```
cd C:\Temp  
ren Microsoft-ASR_UA*Windows*release.exe MobilityServiceInstaller.exe  
MobilityServiceInstaller.exe /q /x:C:\Temp\Extracted  
cd C:\Temp\Extracted.
```

2. To install Mobility Service, run the following command:

```
UnifiedAgent.exe /Role "MS" /InstallLocation "C:\Program Files (x86)\Microsoft Azure Site Recovery"
/Platform "VmWare" /Silent
```

- Now the agent needs to be registered with the configuration server.

```
cd C:\Program Files (x86)\Microsoft Azure Site Recovery\agent
UnifiedAgentConfigurator.exe /CSEndPoint <CSIP> /PassphraseFilePath <PassphraseFilePath>
```

Mobility Service installer command-line arguments

Usage :
UnifiedAgent.exe /Role <MS|MT> /InstallLocation <Install Location> /Platform "VmWare" /Silent

PARAMETER	TYPE	DESCRIPTION	POSSIBLE VALUES
/Role	Mandatory	Specifies whether Mobility Service (MS) should be installed or MasterTarget (MT) should be installed.	MS MT
/InstallLocation	Optional	Location where Mobility Service is installed.	Any folder on the computer
/Platform	Mandatory	Specifies the platform on which Mobility Service is installed. - VMware : Use this value if you install Mobility Service on a VM running on <i>VMware vSphere ESXi hosts, Hyper-V hosts, and physical servers</i> . - Azure : Use this value if you install an agent on an Azure IaaS VM.	VMware Azure
/Silent	Optional	Specifies to run the installer in silent mode.	N/A

TIP

The setup logs can be found under %ProgramData%\ASRSetupLogs\ASRUnifiedAgentInstaller.log.

Mobility Service registration command-line arguments

Usage :
UnifiedAgentConfigurator.exe /CSEndPoint <CSIP> /PassphraseFilePath <PassphraseFilePath>

PARAMETER	TYPE	DESCRIPTION	POSSIBLE VALUES
/CSEndPoint	Mandatory	IP address of the configuration server	Any valid IP address

PARAMETER	TYPE	DESCRIPTION	POSSIBLE VALUES
/PassphraseFilePath	Mandatory	Location of the pass phrase	Any valid UNC or local file path

TIP

The Agent Configuration logs can be found under %ProgramData%\ASRSetupLogs\ASRUnifiedAgentConfigurator.log.

Command-line installation on a Linux computer

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 -xvzf Microsoft-ASR_UA*release.tar.gz
```

2. To install Mobility Service, run the following command:

```
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
```

Mobility Service installer command line

```
Usage:
./install -d <Install Location> -r <MS|MT> -v VmWare -q
```

PARAMETER	TYPE	DESCRIPTION	POSSIBLE VALUES
-r	Mandatory	Specifies whether Mobility Service (MS) should be installed or MasterTarget (MT) should be installed.	MS MT
-d	Optional	Location where Mobility Service is installed.	/usr/local/ASR

PARAMETER	TYPE	DESCRIPTION	POSSIBLE VALUES
-v	Mandatory	<p>Specifies the platform on which Mobility Service is installed.</p> <p>- VMware: Use this value if you install Mobility Service on a VM running on <i>VMware vSphere ESXi hosts, Hyper-V hosts, and physical servers</i>.</p> <p>- Azure: Use this value if you install an agent on an Azure IaaS VM.</p>	VMware Azure
-q	Optional	Specifies to run the installer in silent mode.	N/A

Mobility Service configuration command line

```
Usage:  
cd /usr/local/ASR/Vx/bin  
UnifiedAgentConfigurator.sh -i <CSIP> -P <PassphraseFilePath>
```

PARAMETER	TYPE	DESCRIPTION	POSSIBLE VALUES
-i	Mandatory	IP of the configuration server	Any valid IP Address
-P	Mandatory	Full file path for the file where the connection pass phrase is saved	Any valid folder

Install Mobility Service by push installation from Azure Site Recovery

You can do a push installation of Mobility Service by using Site Recovery. All target computers must meet the following prerequisites.

Prepare for a push installation on a Windows computer

1. Ensure that there's network connectivity between the Windows computer and the process 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.

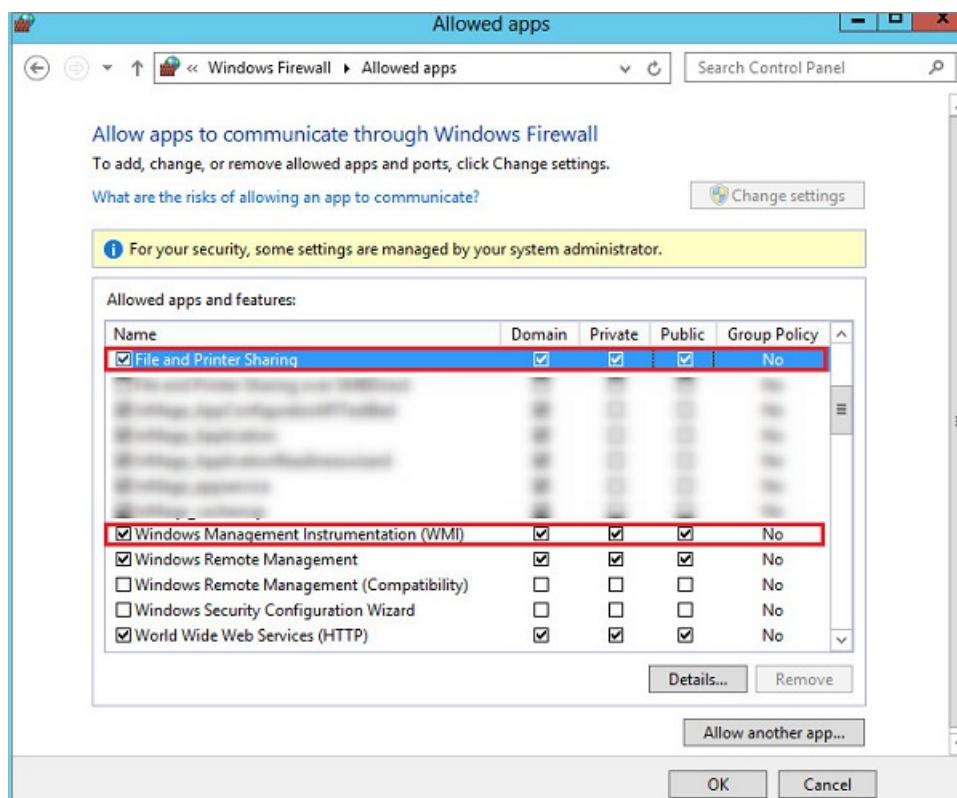
NOTE

If you don't use a domain account, 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 do this task 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 1
```

3. In Windows Firewall on the computer 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).



4. Add the account that you created in CSPSCfgtool. Follow these steps:

- a. Sign in to your configuration server.
- b. Open **cspscfgtool.exe**. It's available as a shortcut on the desktop and in the %ProgramData%\home\svsystems\bin folder.
- c. On the **Manage Accounts** tab, select **Add Account**.
- d. Add the account you created.
- e. Enter the credentials you use when you enable replication for a computer.

Prepare for a push installation on a Linux server

1. Ensure that there's network connectivity between the Linux computer 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. Follow these steps:
 - a. Sign in as **root**.
 - b. In the **/etc/ssh/sshd_config** file, find the line that begins with **PasswordAuthentication**.
 - c. Uncomment the line, and change the value to **yes**.
 - d. Find the line that begins with **Subsystem**, and uncomment the line.

```
# override default of no subsystems
Subsystem      sftp      /usr/libexec.openssh.sftp-server
```

- e. Restart the **sshd** service.
7. Add the account that you created in CSPSCfgtool. Follow these steps:
- a. Sign in to your configuration server.
 - b. Open **cspscfgtool.exe**. It's available as a shortcut on the desktop and in the %ProgramData%\home\svsystems\bin folder.
 - c. On the **Manage Accounts** tab, select **Add Account**.
 - d. Add the account you created.
 - d. Enter the credentials you use when you enable replication for a computer.

NOTE

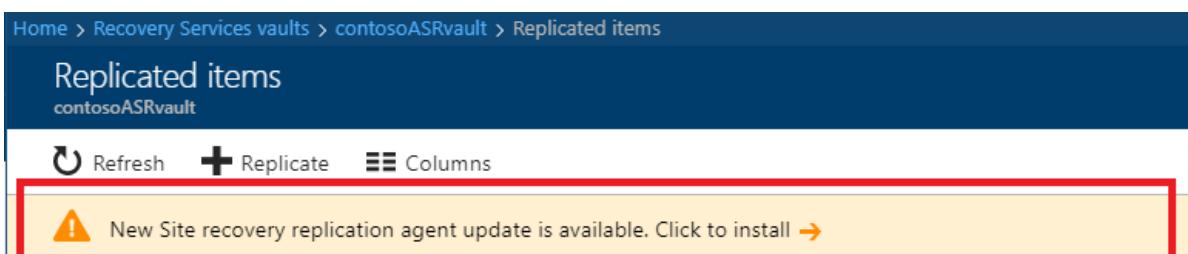
After Mobility Service is installed, in the Azure portal, select + **Replicate** to start protecting these VMs.

Update Mobility Service

WARNING

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 start updating Mobility Service on the protected servers.

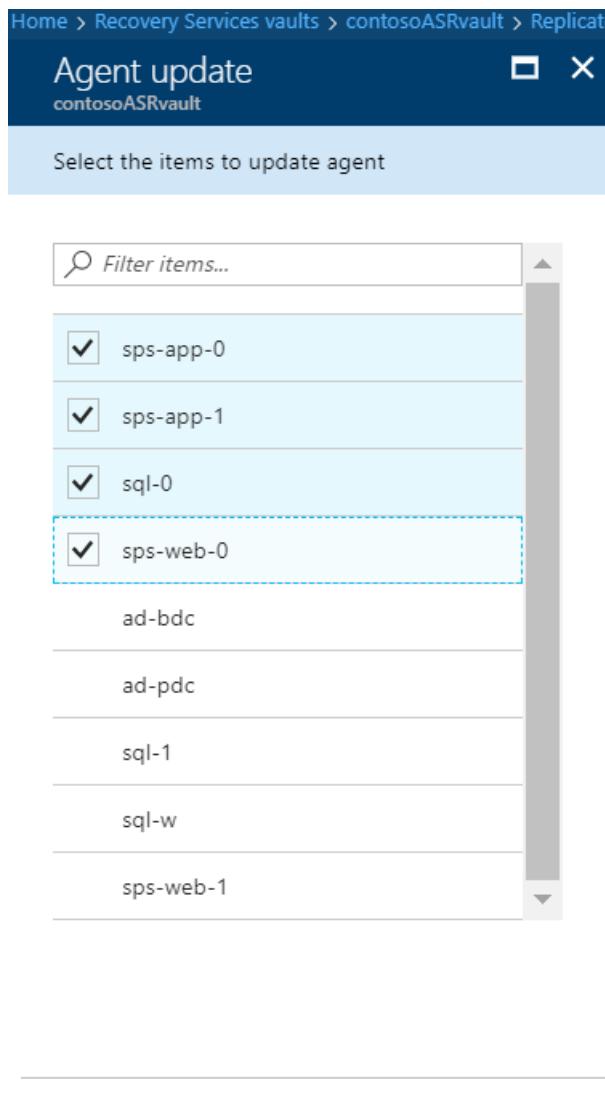
1. On the Azure portal, browse to the *name of your vault* > **Replicated items** view.
2. If the configuration server was already updated to the latest version, you see a notification that reads "New Site recovery replication agent update is available. Click to install."



Last refreshed at: 18/10/2017, 12:04:22 PM

NAME	HEALTH	STATUS
sps-app-0	Critical	Protected
sps-app-1	Critical	Protected
sql-0	Critical	Protected
sps-web-0	Critical	Protected

3. Select the notification to open the virtual machine selection page.
4. Select the virtual machines you want to upgrade mobility service on, and select **OK**.



The Update Mobility Service job starts for each of the selected virtual machines.

NOTE

[Read more](#) on how to update the password for the account used to install Mobility Service.

Uninstall Mobility Service on a Windows Server computer

Use one of the following methods to uninstall Mobility Service on a Windows Server computer.

Uninstall by using the GUI

1. In Control Panel, select **Programs**.
2. Select **Microsoft Azure Site Recovery Mobility Service/Master Target server**, and then select **Uninstall**.

Uninstall at a command prompt

1. Open a command prompt window as an administrator.
2. To uninstall Mobility Service, run the following command:

```
MsiExec.exe /qn /x {275197FC-14FD-4560-A5EB-38217F80CBD1} /L+*V  
"C:\ProgramData\ASRSetupLogs\UnifiedAgentMSIUninstall.log"
```

Uninstall Mobility Service on a Linux computer

1. On your Linux server, sign in as a **root** user.
2. In a terminal, go to /user/local/ASR.
3. To uninstall Mobility Service, run the following command:

```
uninstall.sh -Y
```

Automate Mobility Service installation with System Center Configuration Manager

7/10/2018 • 10 minutes to read • [Edit Online](#)

The Mobility service is installed on VMware VMs and physical servers that you want to replicate to Azure using [Azure Site Recovery](#)

This article provides you an example of how you can use System Center Configuration Manager to deploy the Azure Site Recovery Mobility Service on a VMware VM. Using a software deployment tool like Configuration Manager has the following advantages:

- Schedule fresh installations and upgrades during your planned maintenance window for software updates
- Scale deployment to hundreds of servers simultaneously

This article uses System Center Configuration Manager 2012 R2 to demonstrate the deployment activity. We assumes you are using version **9.9.4510.1** or higher of the Mobility service.

Alternately, you can automate Mobility Service installation with [Azure Automation DSC](#).

Prerequisites

1. A software deployment tool, like Configuration Manager, that's already deployed in your environment.
2. You should create two [device collections](#), one for all **Windows servers**, and another for all **Linux servers**, that you want to protect by using Site Recovery.
3. A configuration server that is already registered in the Recovery Services vault.
4. A secure network file share (SMB share) that can be accessed by the configuration manager machine.

Deploy on Windows machines

NOTE

This article assumes that the IP address of the configuration server is 192.168.3.121, and that the secure network file share is \\ContosoSecureFS\MobilityServiceInstallers.

Prepare for deployment

1. Create a folder on the network share, and name it **MobSvcWindows**.
2. Sign in to your configuration server, and open an administrative command prompt.
3. Run the following commands to generate a passphrase file:

```
cd %ProgramData%\ASR\home\svsystems\bin
```

```
genpassphrase.exe -v > MobSvc.passphrase
```

4. Copy the **MobSvc.passphrase** file into the **MobSvcWindows** folder on your network share.
5. Browse to the installer repository on the configuration server by running the following command:

```
cd %ProgramData%\ASR\home\svsystems\pushinstallsvc\repository
```
6. Copy the **Microsoft-ASR_UA_version_Windows_GA_date_Release.exe** to the **MobSvcWindows** folder on your network share.

7. Copy the following code, and save it as **install.bat** into the **MobSvcWindows** folder.

NOTE

Replace the [CSIP] placeholders in this script with the actual values of the IP address of your configuration server.

```
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

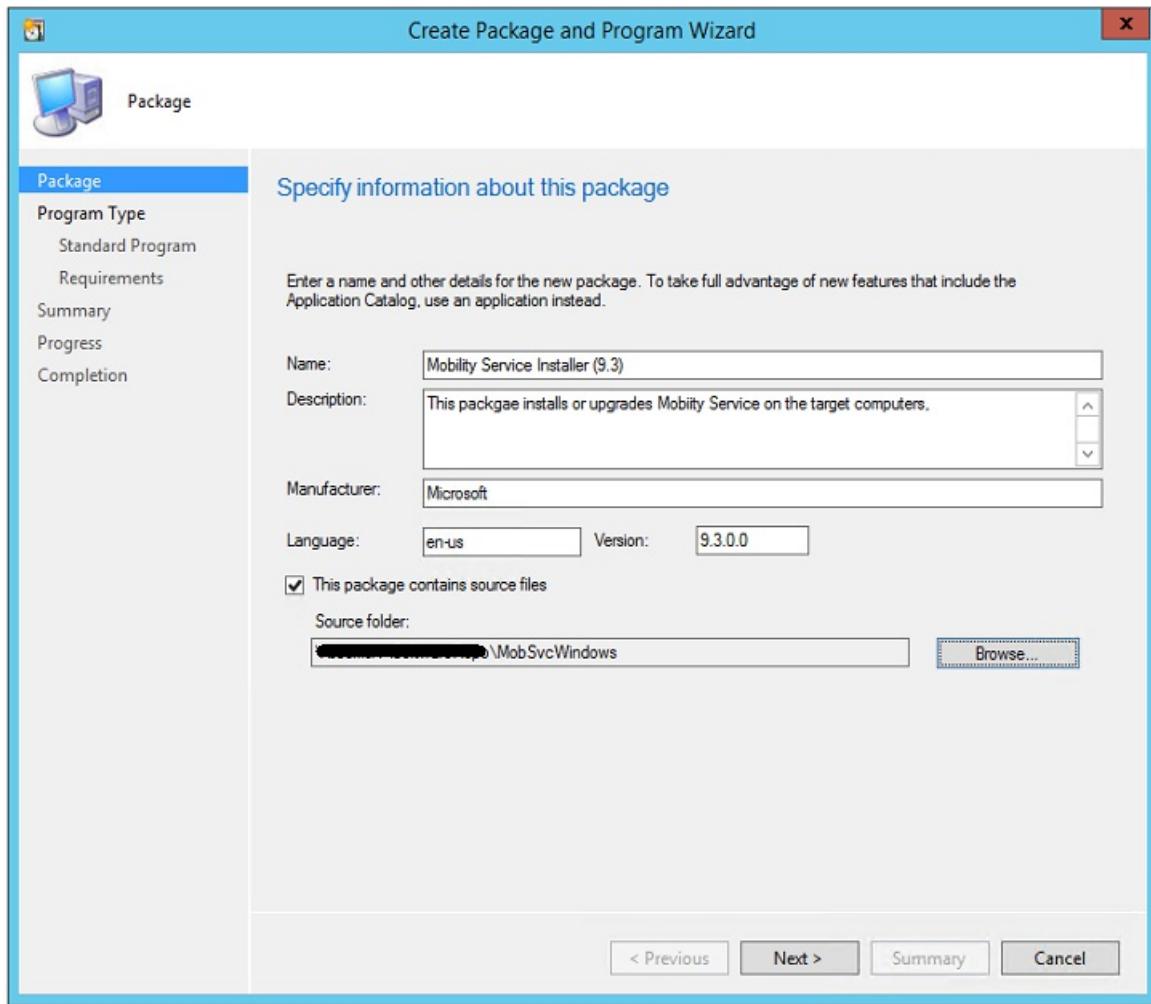
:UPGRADE
echo "Perform upgrade." >> C:\Temp\logfile.log
UnifiedAgent.exe /Platform "VmWare" /Silent
IF %ERRORLEVEL% EQU 0 (
    echo "Upgrade has succeeded." >> C:\Temp\logfile.log
) ELSE (
    echo "Upgrade has failed." >> C:\Temp\logfile.log
)
GOTO :ENDSCRIPT

:ENDSCRIPT
echo "End of script." >> C:\Temp\logfile.log

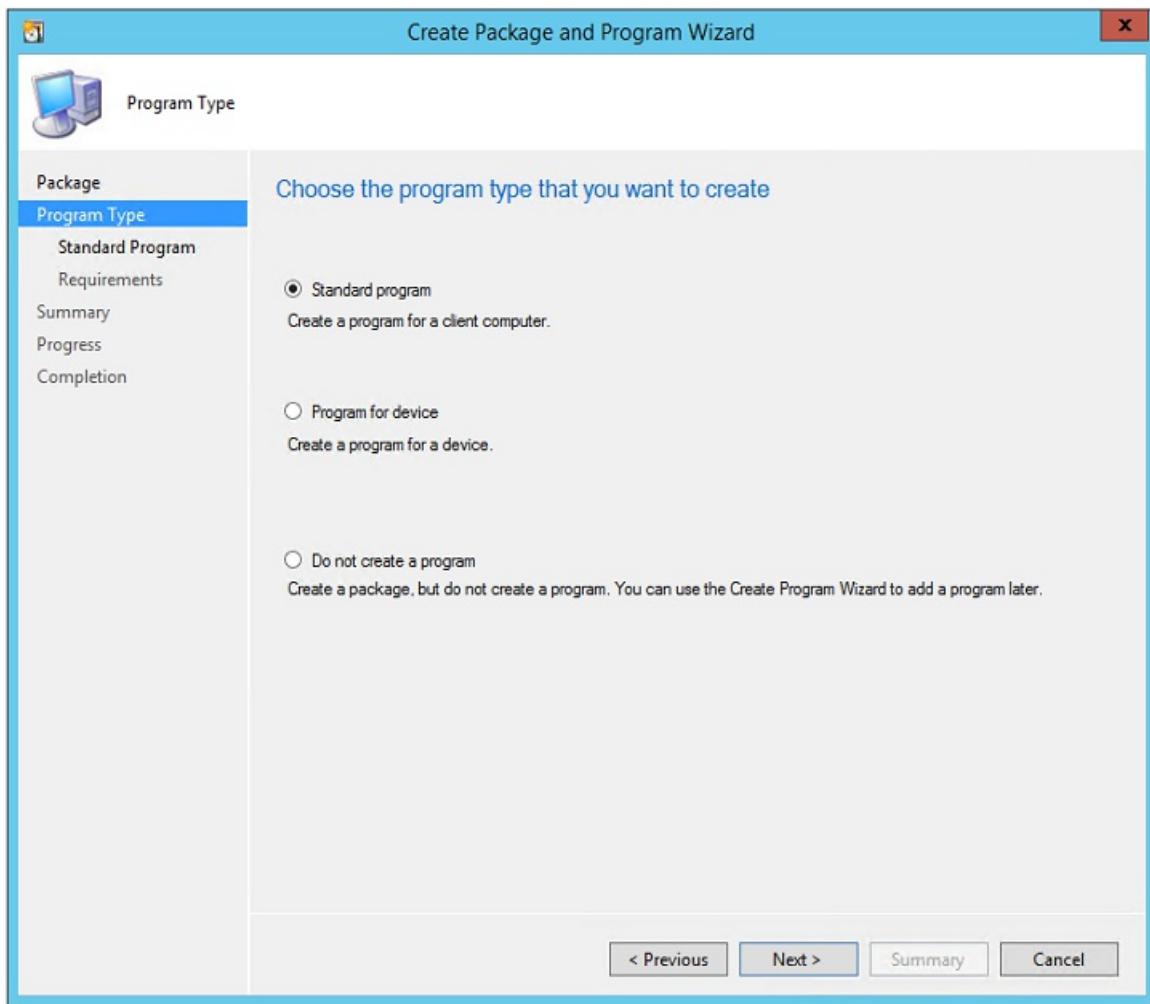
```

Create a package

1. Sign in to your Configuration Manager console.
2. Browse to **Software Library > Application Management > Packages**.
3. Right-click **Packages**, and select **Create Package**.
4. Provide values for the name, description, manufacturer, language, and version.
5. Select the **This package contains source files** check box.
6. Click **Browse**, and select the network share where the installer is stored
(\\ContosoSecureFS\MobilityServiceInstaller\MobSvcWindows).

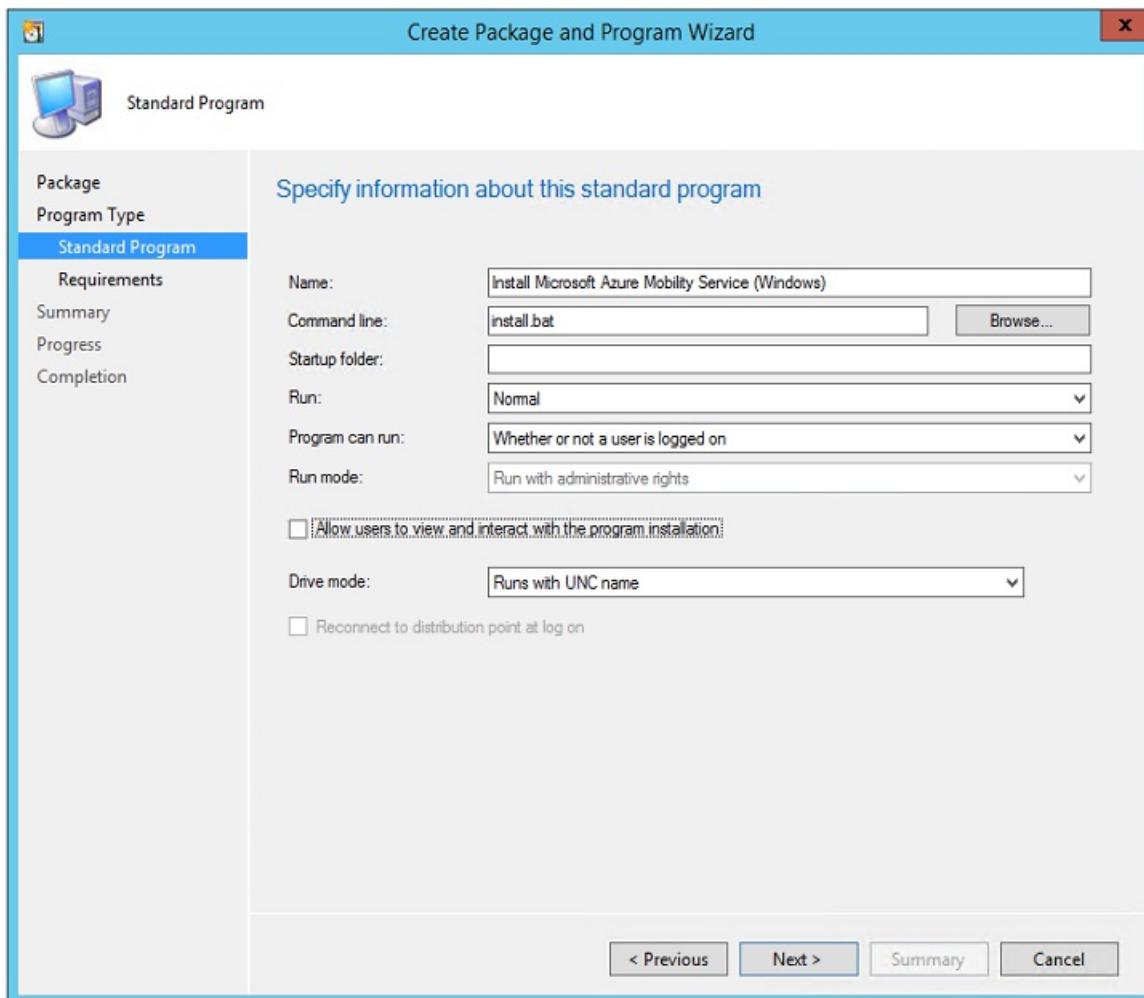


7. On the **Choose the program type that you want to create** page, select **Standard Program**, and click **Next**.

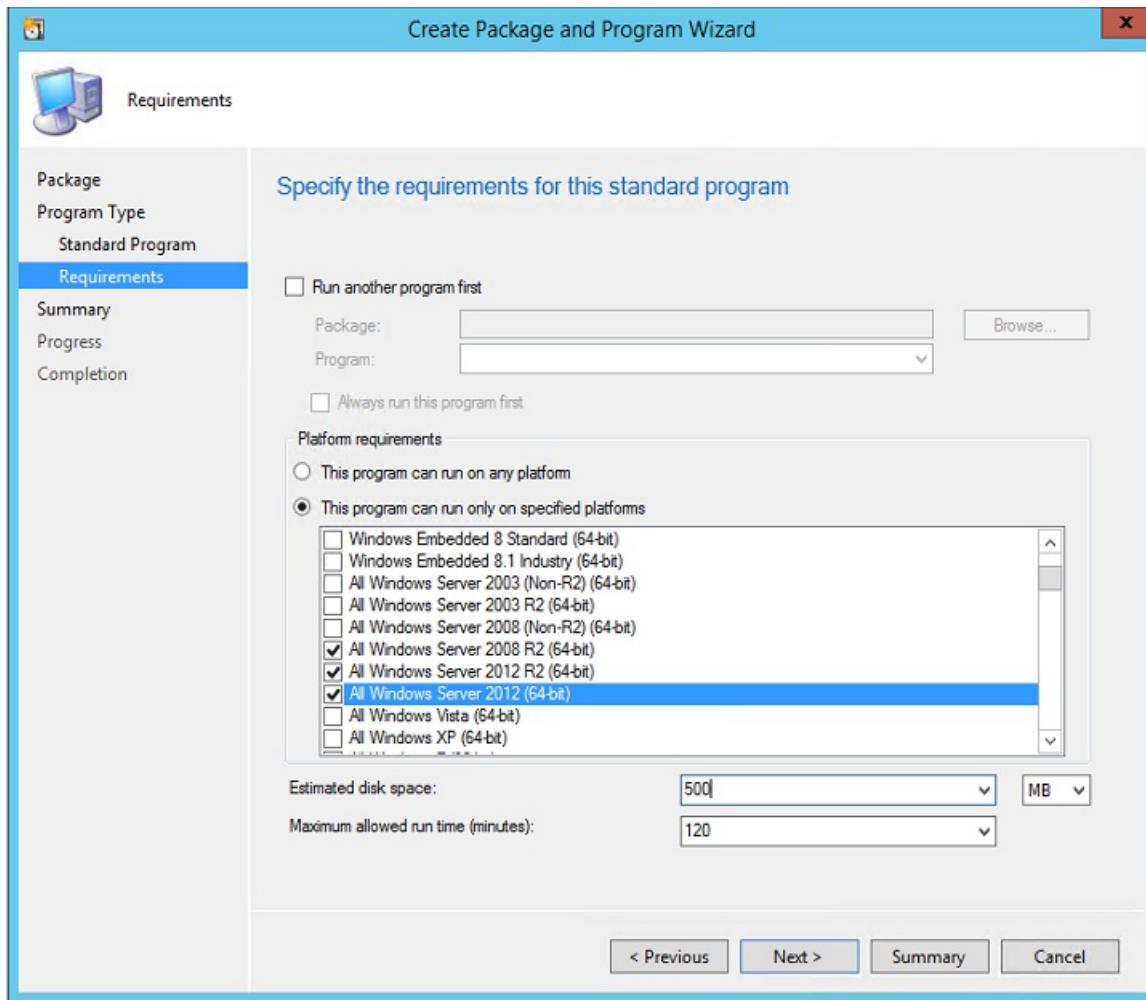


8. On the **Specify information about this standard program** page, provide the following inputs, and click **Next**. (The other inputs can use their default values.)

PARAMETER NAME	VALUE
Name	Install Microsoft Azure Mobility Service (Windows)
Command line	install.bat
Program can run	Whether or not a user is logged on



9. On the next page, select the target operating systems. Mobility Service can be installed only on Windows Server 2012 R2, Windows Server 2012, and Windows Server 2008 R2.



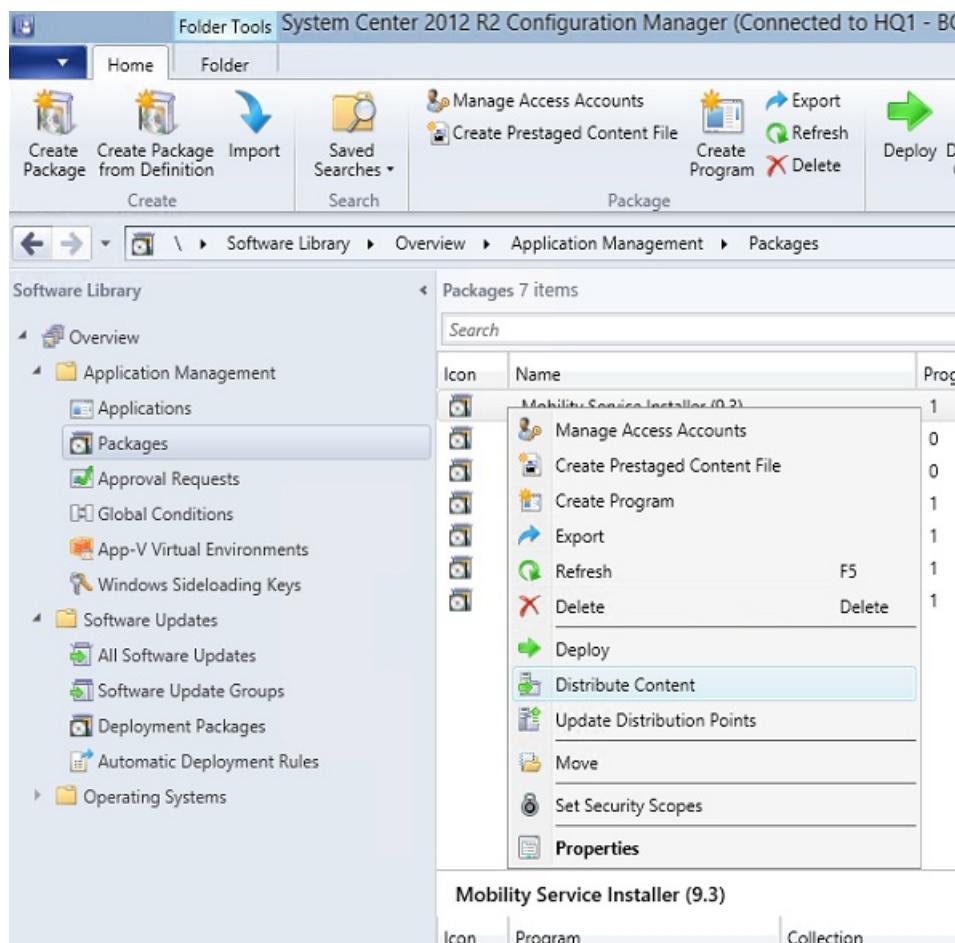
10. To complete the wizard, click **Next** twice.

NOTE

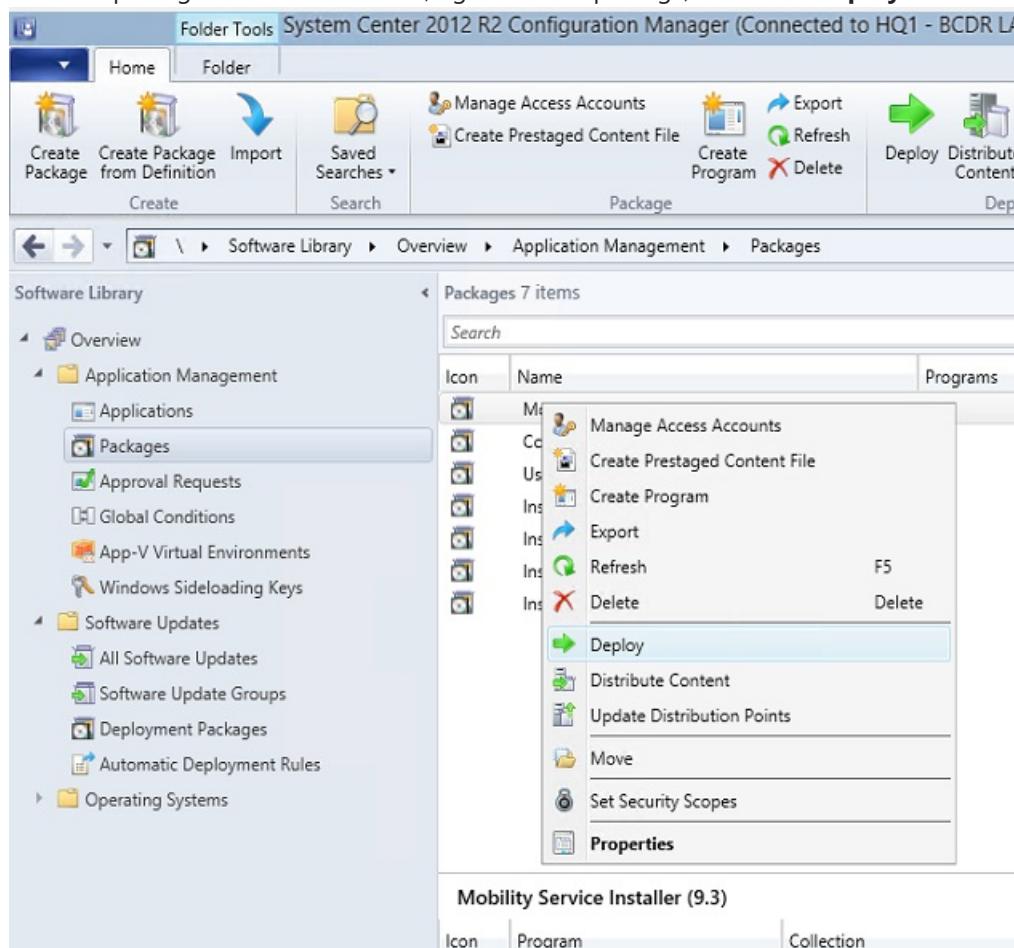
The script supports both new installations of Mobility Service agents and updates to agents that are already installed.

Deploy the package

- In the Configuration Manager console, right-click your package, and select **Distribute Content**.

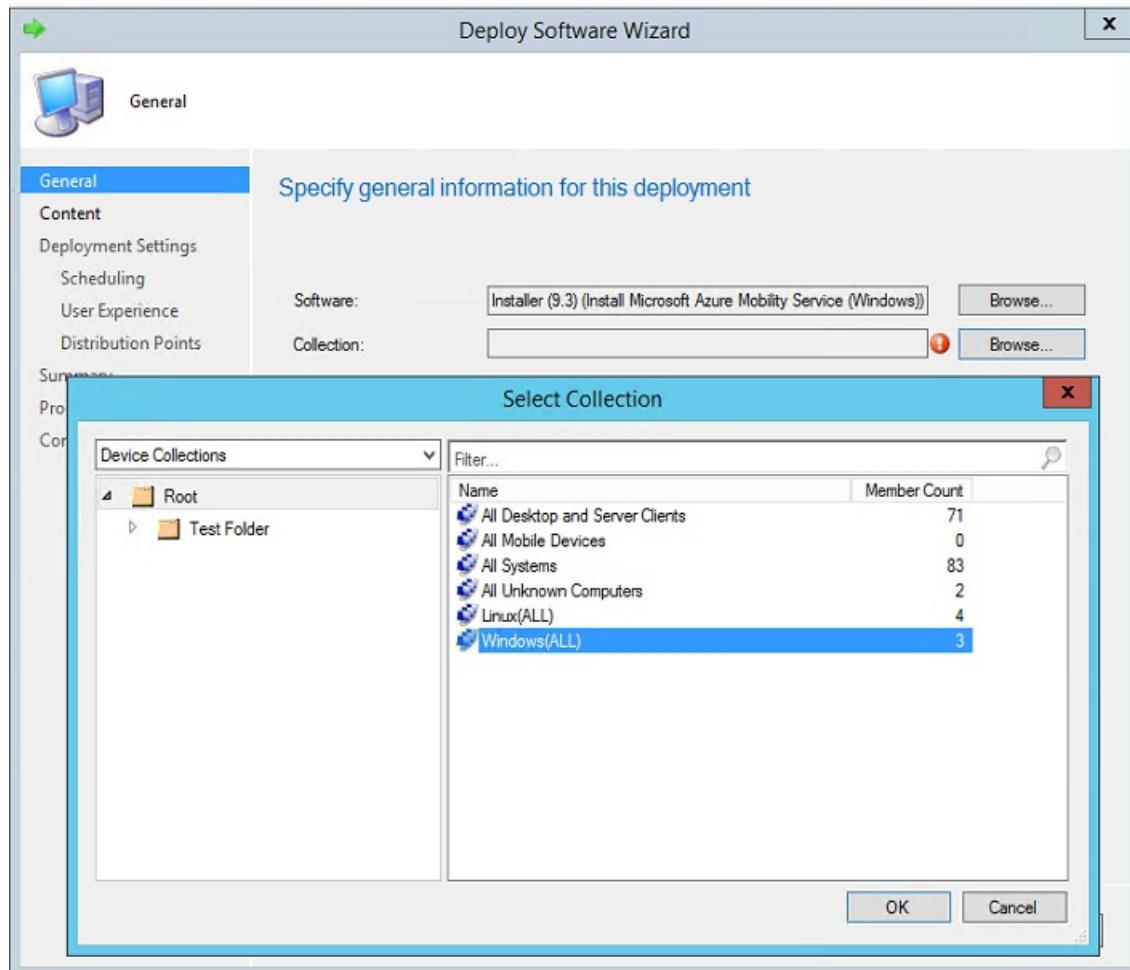


2. Select the **distribution points** on to which the packages should be copied.
3. Complete the wizard. The package then starts replicating to the specified distribution points.
4. After the package distribution is done, right-click the package, and select **Deploy**.

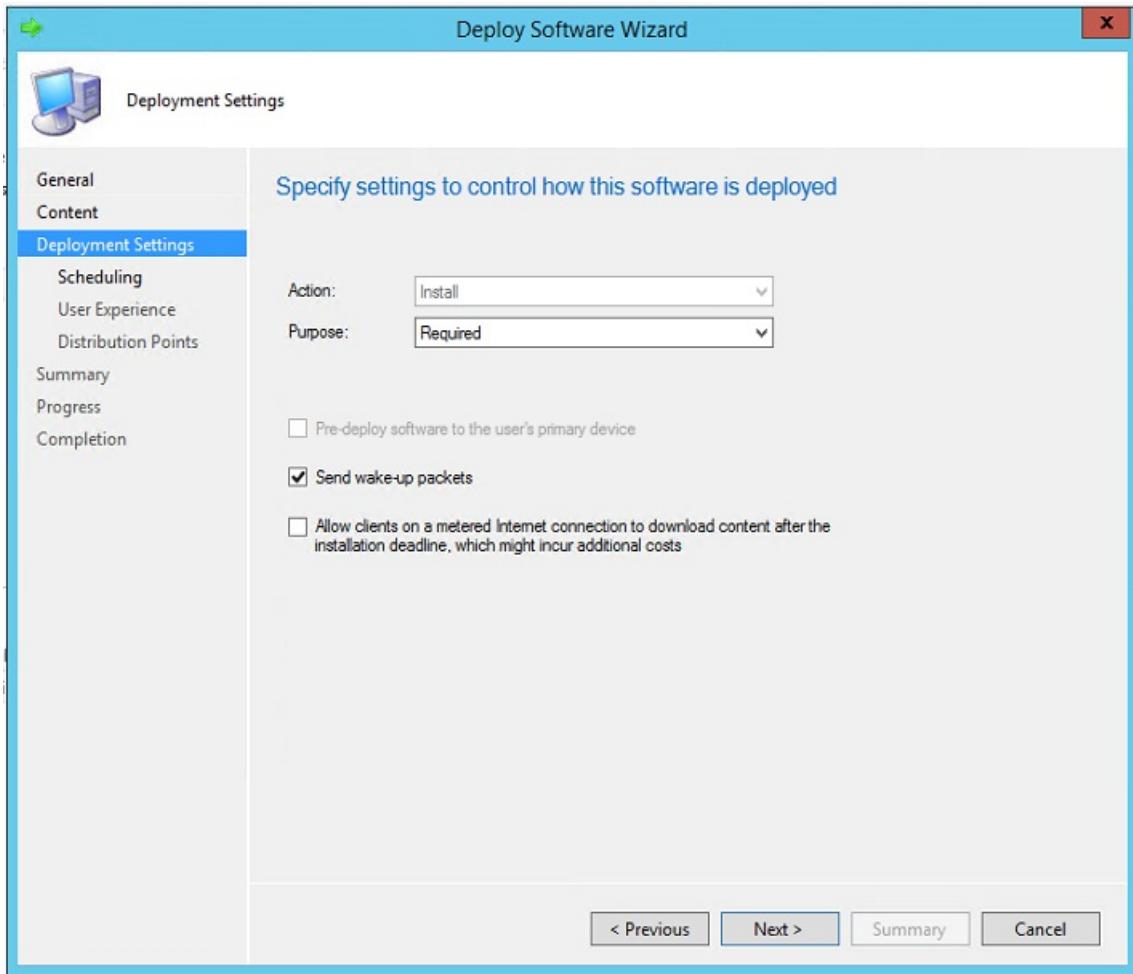


5. Select the Windows Server device collection you created in the prerequisites section as the target collection

for deployment.



6. On the **Specify the content destination** page, select your **Distribution Points**.
7. On the **Specify settings to control how this software is deployed** page, ensure that the purpose is **Required**.



8. On the **Specify the schedule for this deployment** page, specify a schedule. For more information, see [scheduling packages](#).
9. On the **Distribution Points** page, configure the properties according to the needs of your datacenter. Then complete the wizard.

TIP

To avoid unnecessary reboots, schedule the package installation during your monthly maintenance window or software updates window.

You can monitor the deployment progress by using the Configuration Manager console. Go to **Monitoring > Deployments > [your package name]**.

General		Completion Statistics	Related Objects
Software:	Install Mob Svc (9.3) - Windows (Install 9.3 (windows))	Total Asset Count: 3 (Last Update: 12/21/2016 11:23:49 PM) View Status	Collection Applications Content Status
Collection:	Windows(ALL)	 Success: 3 In Progress: 0 Error: 0 Requirements Not Met: 0 Unknown: 0	
Feature Type:	Program		
Purpose:	Required		
Date Created:	12/8/2016 1:57 AM		
Last Date Modified:	12/8/2016 1:57 AM		

Content Status	
 1 Targeted (Last Update: 12/8/2016 1:53 AM)	 Success: 1 In Progress: 0 Failed: 0 Unknown: 0
Activate Windows Go to System in Control Panel to activate Windows.	

Deploy on Linux machines

NOTE

This article assumes that the IP address of the configuration server is 192.168.3.121, and that the secure network file share is \\ContosoSecureFS\MobilityServiceInstallers.

Prepare for deployment

1. Create a folder on the network share, and name it as **MobSvcLinux**.
2. Sign in to your configuration server, and open an administrative command prompt.
3. Run the following commands to generate a passphrase file:

```
cd %ProgramData%\ASR\home\svsystems\bin
```

```
genpassphrase.exe -v > MobSvc.passphrase
```

4. Copy the **MobSvc.passphrase** file into the **MobSvcLinux** folder on your network share.
5. Browse to the installer repository on the configuration server by running the command:

```
cd %ProgramData%\ASR\home\svsystems\pushinstallsvc\repository
```

6. Copy the following files to the **MobSvcLinux** folder on your network share:

- Microsoft-ASR_UA*RHEL6-64*release.tar.gz
- Microsoft-ASR_UA*RHEL7-64*release.tar.gz
- Microsoft-ASR_UA*SLES11-SP3-64*release.tar.gz
- Microsoft-ASR_UA*SLES11-SP4-64*release.tar.gz
- Microsoft-ASR_UA*OL6-64*release.tar.gz
- Microsoft-ASR_UA*UBUNTU-14.04-64*release.tar.gz

7. Copy the following code, and save it as **install_linux.sh** into the **MobSvcLinux** folder.

NOTE

Replace the [CSIP] placeholders in this script with the actual values of the IP address of your configuration server.

```
#!/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"
        fi
    fi
fi
```

```

        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
            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
        elif [ -f /etc/lsb-release ] ; then
            if grep -q 'DISTRO_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
    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

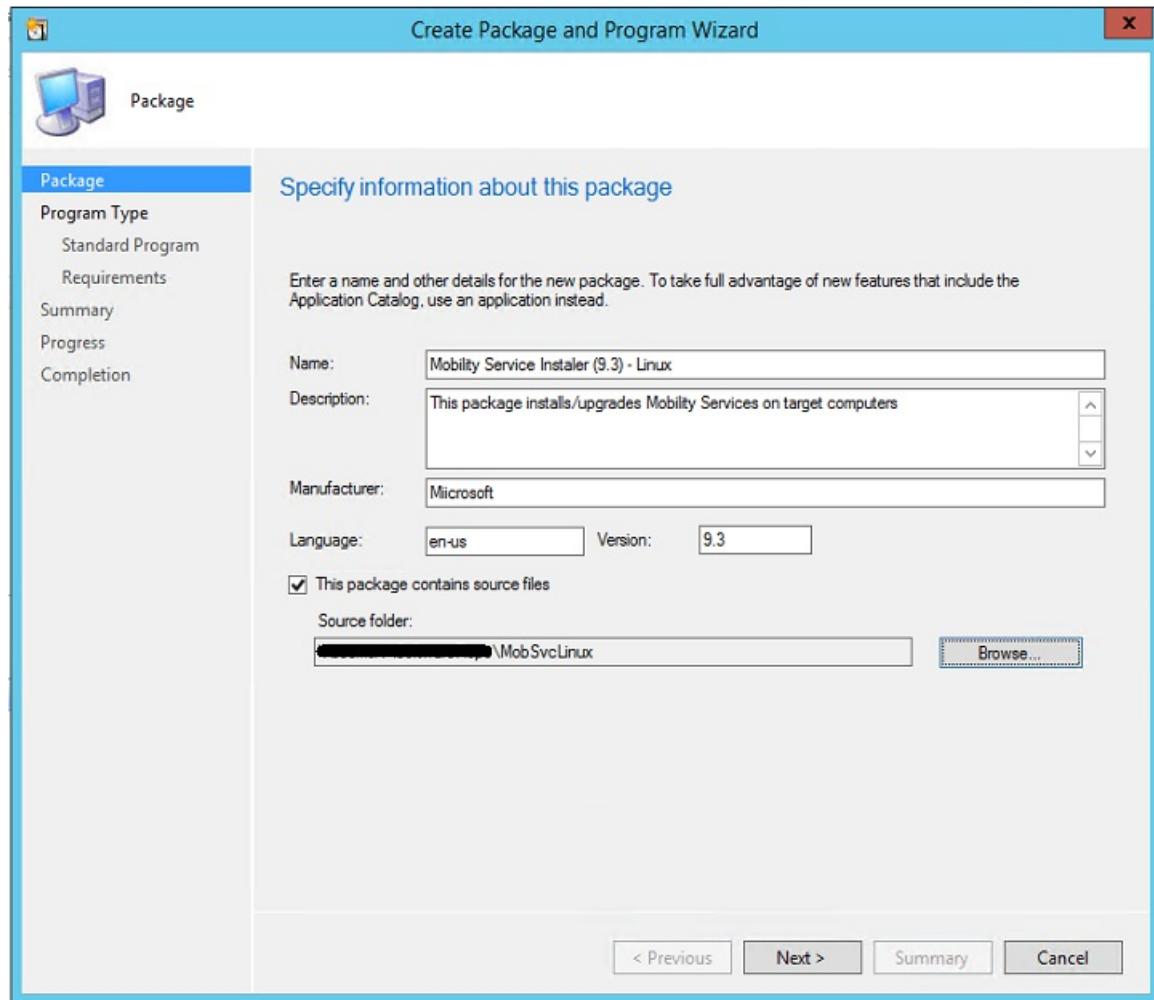
if [ -e ${VX_VERSION_FILE} ]; then
    echo "${VX_VERSION_FILE} exists. Checking for configuration status." >> /tmp/MobSvc/sccm.log
    agent_configuration=$(grep ^AGENT_CONFIGURATION_STATUS "${VX_VERSION_FILE}" | cut -d "=" -f2 | tr -d " ")
    echo "agent_configuration=$agent_configuration" >> /tmp/MobSvc/sccm.log
    if [ "$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

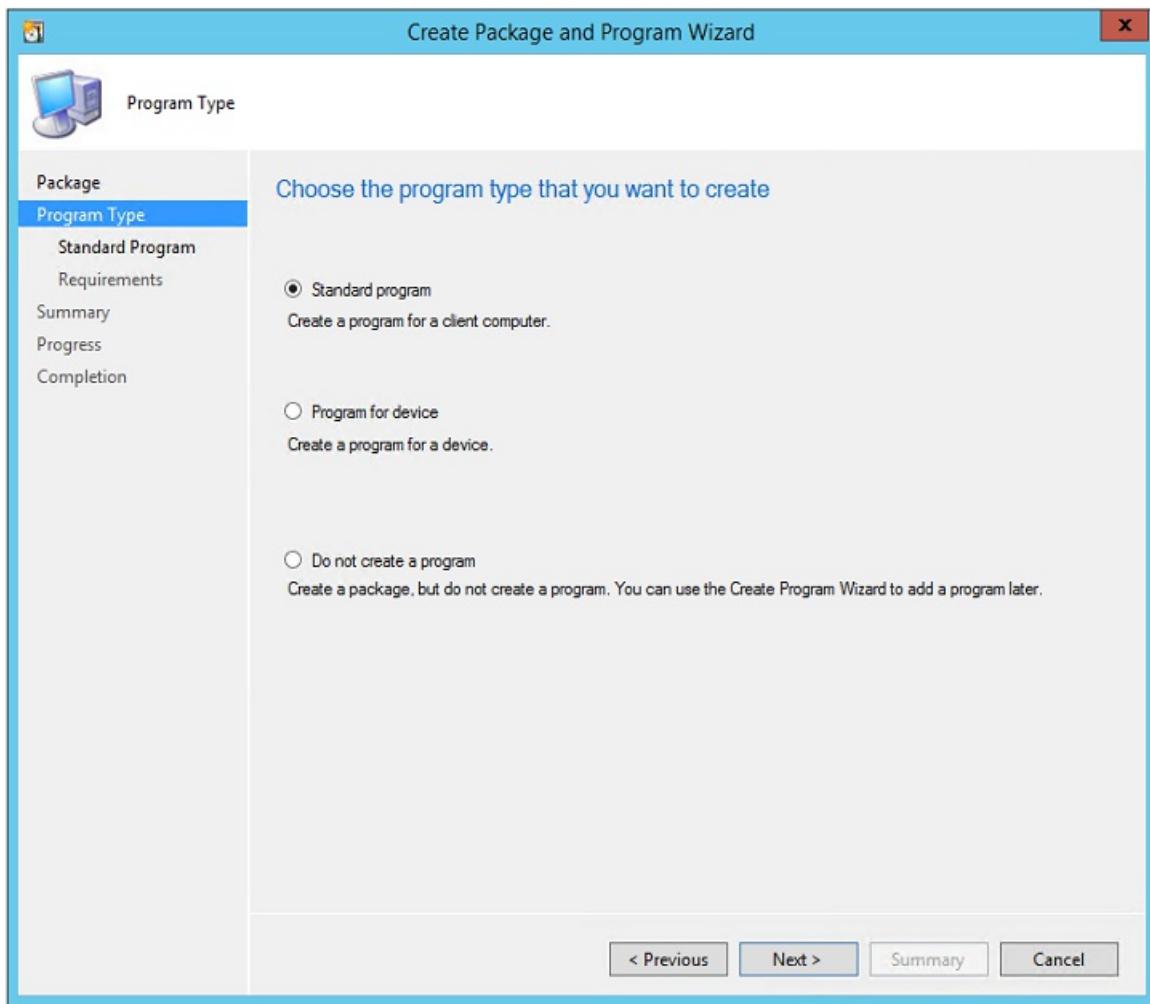
```

Create a package

1. Sign in to your Configuration Manager console.
2. Browse to **Software Library > Application Management > Packages**.
3. Right-click **Packages**, and select **Create Package**.
4. Provide values for the name, description, manufacturer, language, and version.
5. Select the **This package contains source files** check box.
6. Click **Browse**, and select the network share where the installer is stored
(\\ContosoSecureFS\MobilityService\Installer\MobSvcLinux).

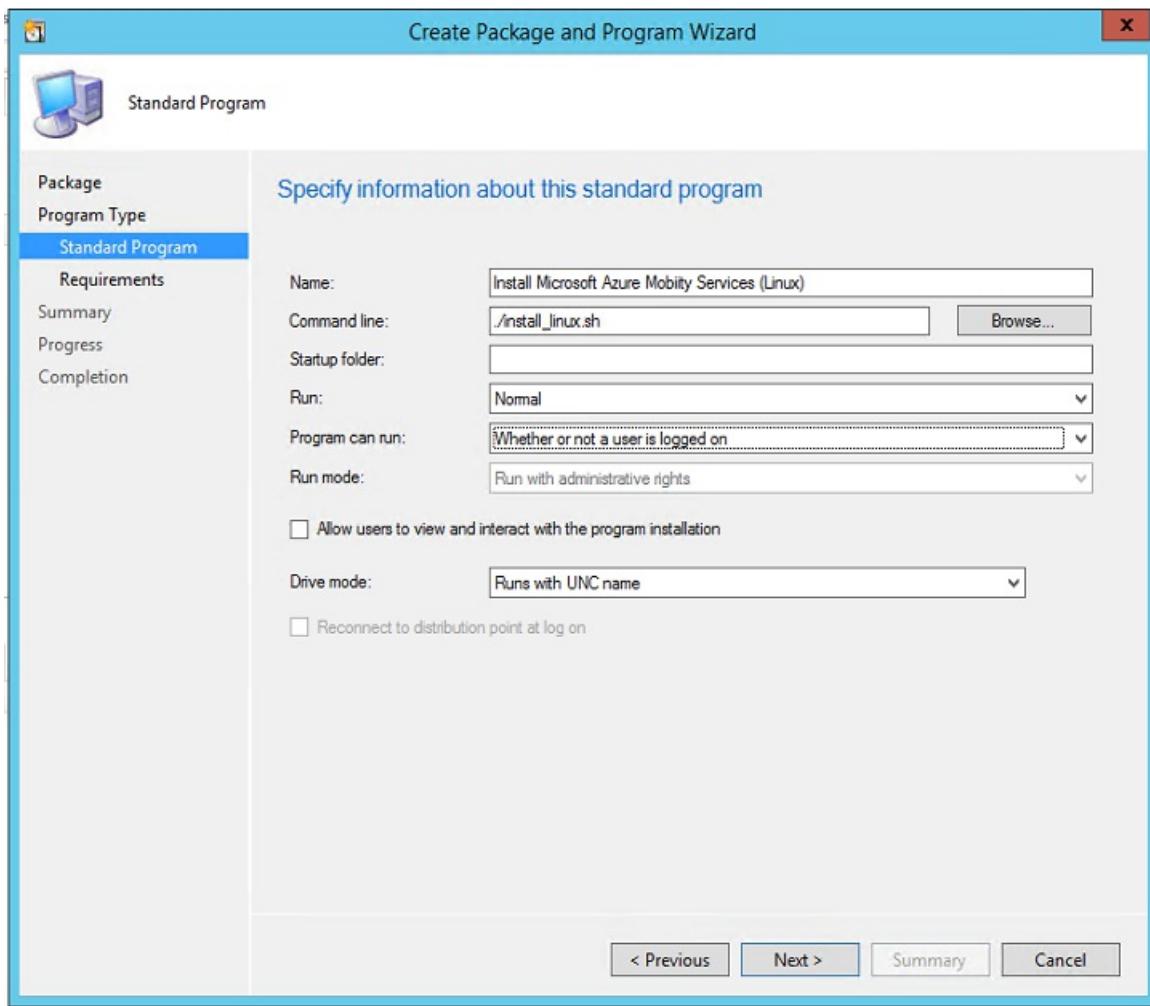


7. On the **Choose the program type that you want to create** page, select **Standard Program**, and click **Next**.

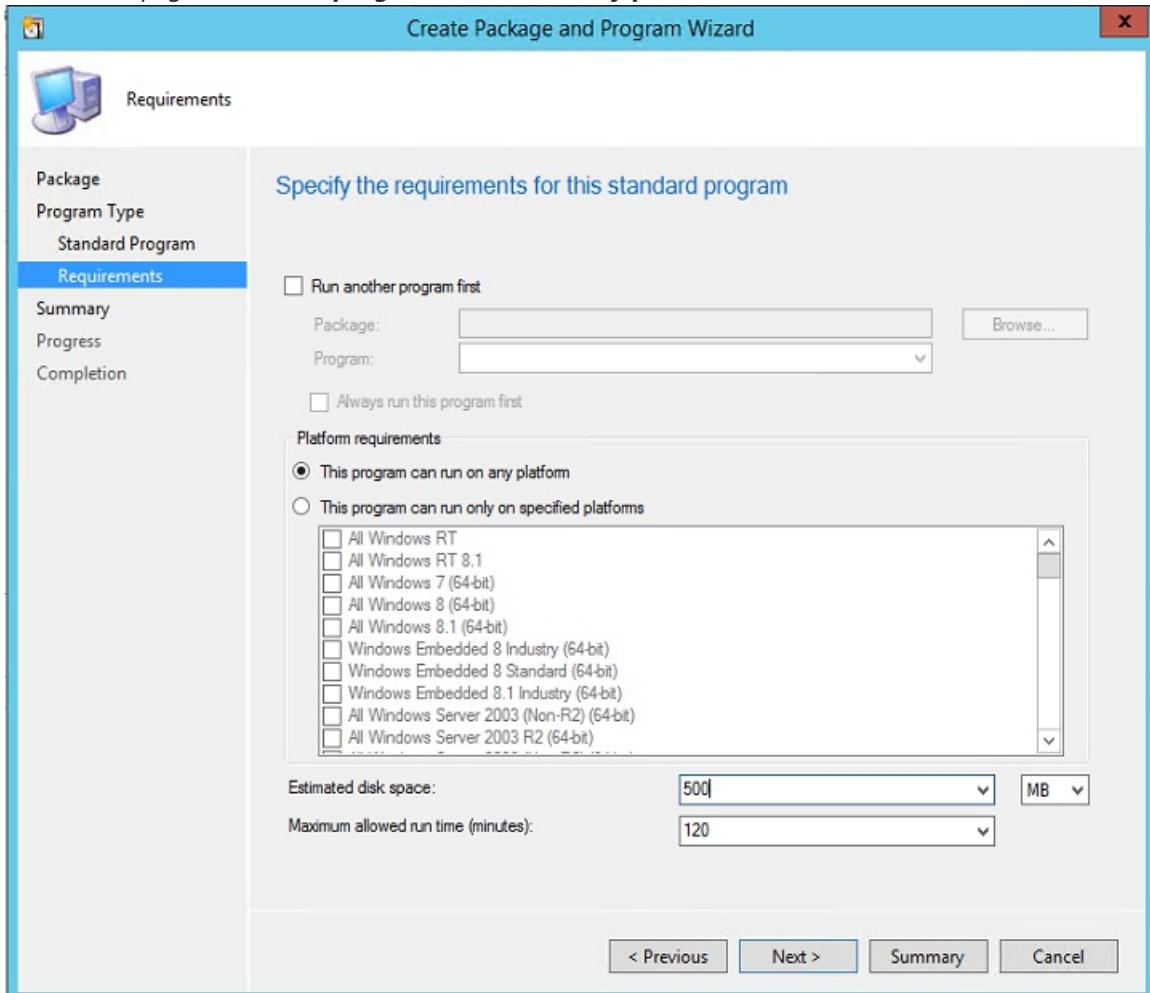


8. On the **Specify information about this standard program** page, provide the following inputs, and click **Next**. (The other inputs can use their default values.)

PARAMETER NAME	VALUE
Name	Install Microsoft Azure Mobility Service (Linux)
Command line	./install_linux.sh
Program can run	Whether or not a user is logged on



9. On the next page, select **This program can run on any platform**.



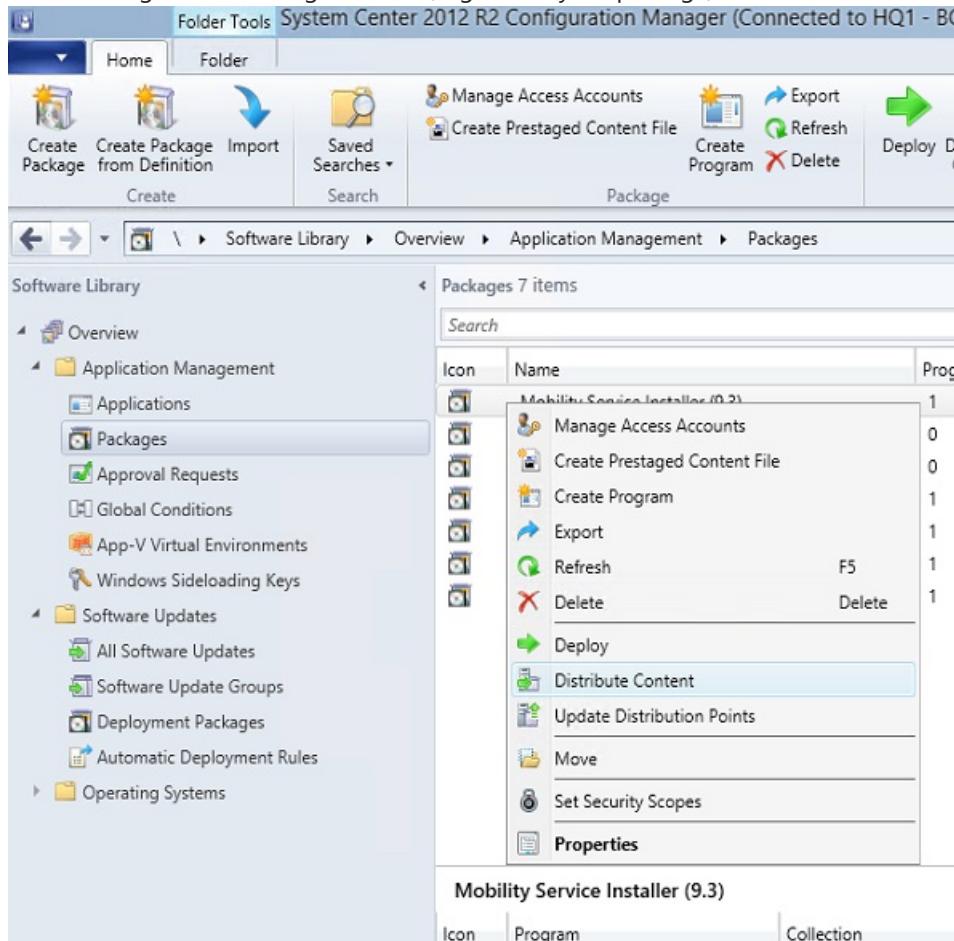
10. To complete the wizard, click **Next** twice.

NOTE

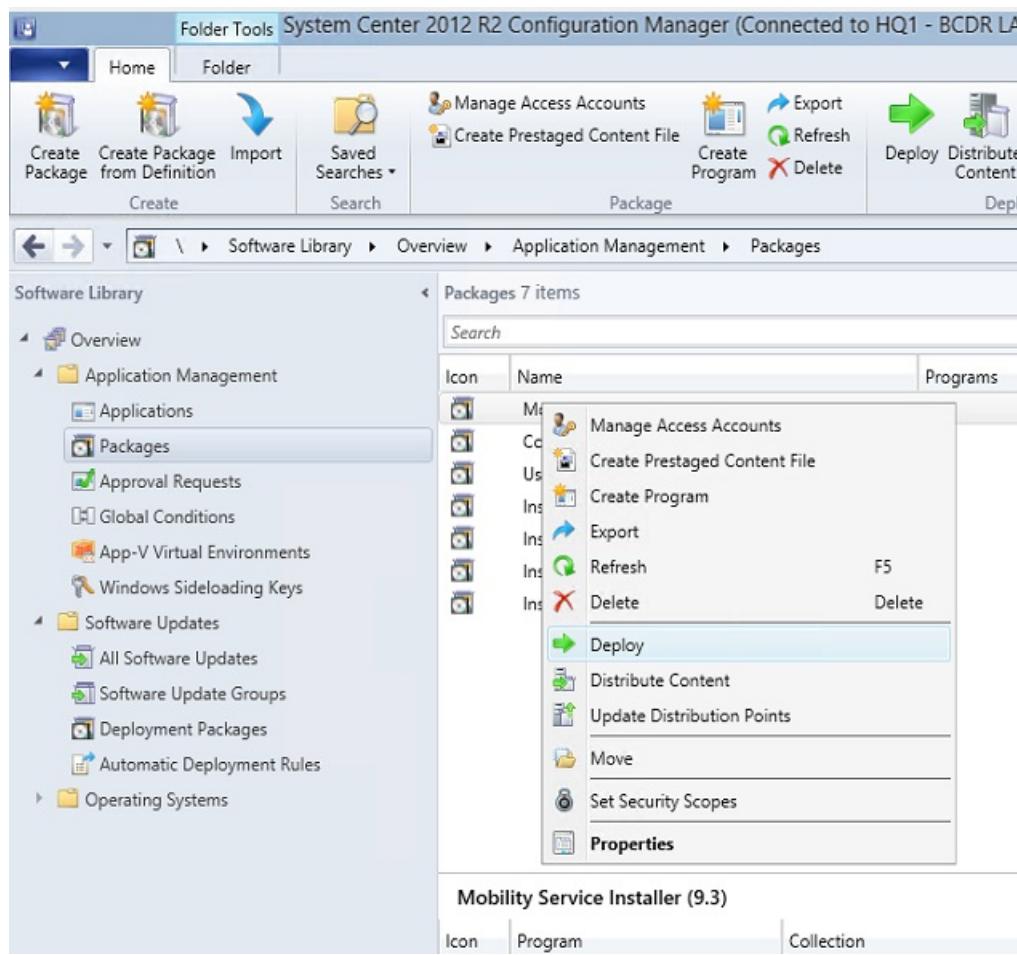
The script supports both new installations of Mobility Service agents and updates to agents that are already installed.

Deploy the package

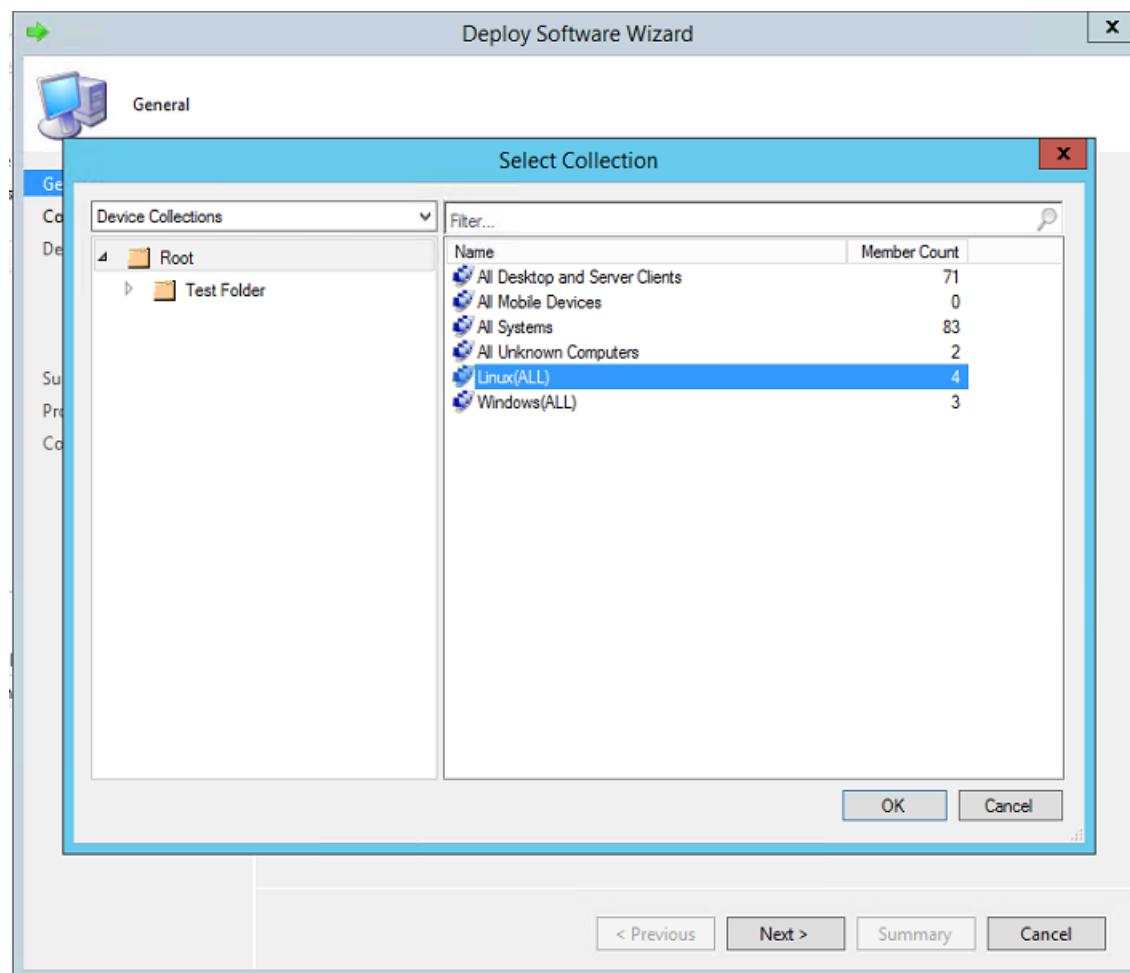
1. In the Configuration Manager console, right-click your package, and select **Distribute Content**.



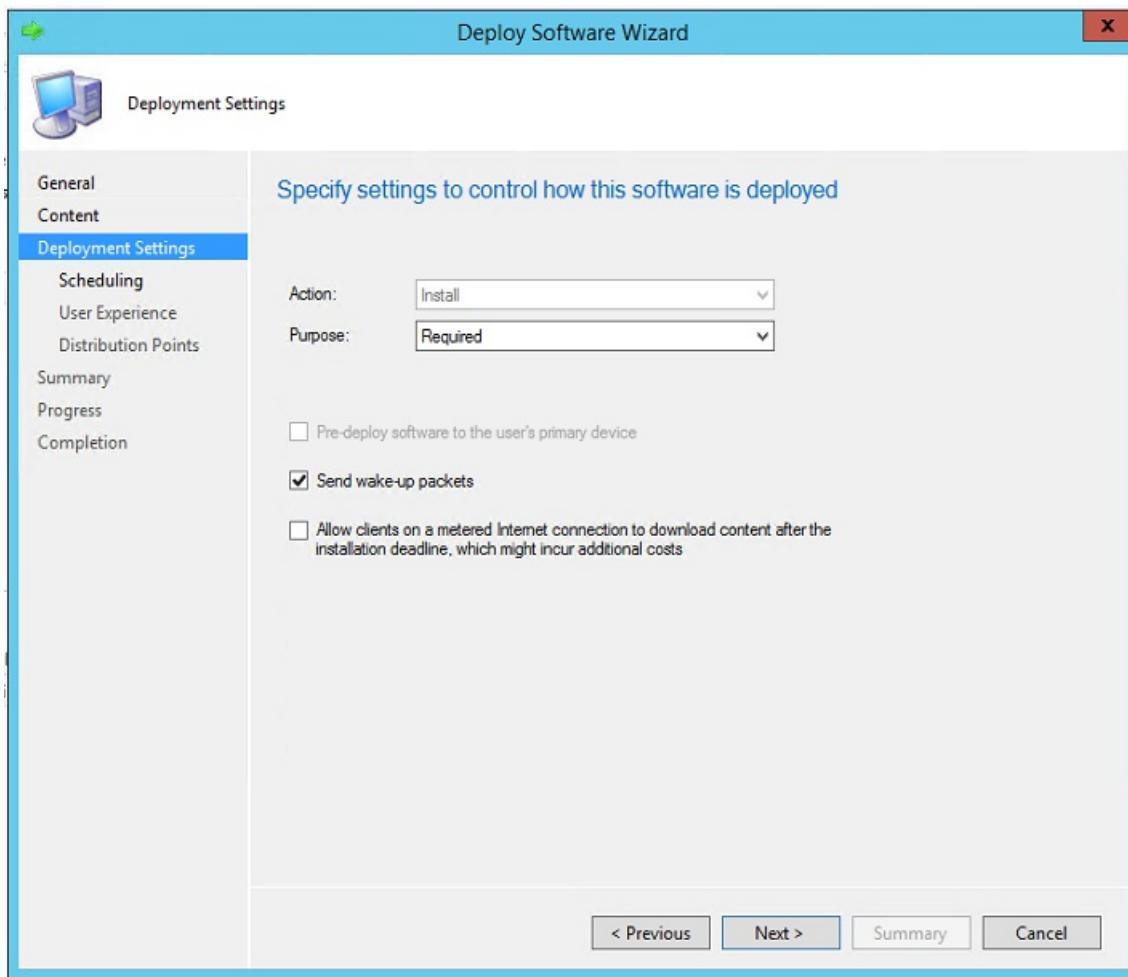
2. Select the **distribution points** on to which the packages should be copied.
3. Complete the wizard. The package then starts replicating to the specified distribution points.
4. After the package distribution is done, right-click the package, and select **Deploy**.



5. Select the Linux Server device collection you created in the prerequisites section as the target collection for deployment.



6. On the **Specify the content destination** page, select your **Distribution Points**.
7. On the **Specify settings to control how this software is deployed** page, ensure that the purpose is **Required**.



8. On the **Specify the schedule for this deployment** page, specify a schedule. For more information, see [scheduling packages](#).
9. On the **Distribution Points** page, configure the properties according to the needs of your datacenter. Then complete the wizard.

Mobility Service gets installed on the Linux Server Device Collection, according to the schedule you configured.

Uninstall the Mobility service

You can create Configuration Manager packages to uninstall Mobility Service. Use the following script to do so:

```
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

You are now ready to [enable protection](#) for your virtual machines.

Test failover to Azure in Site Recovery

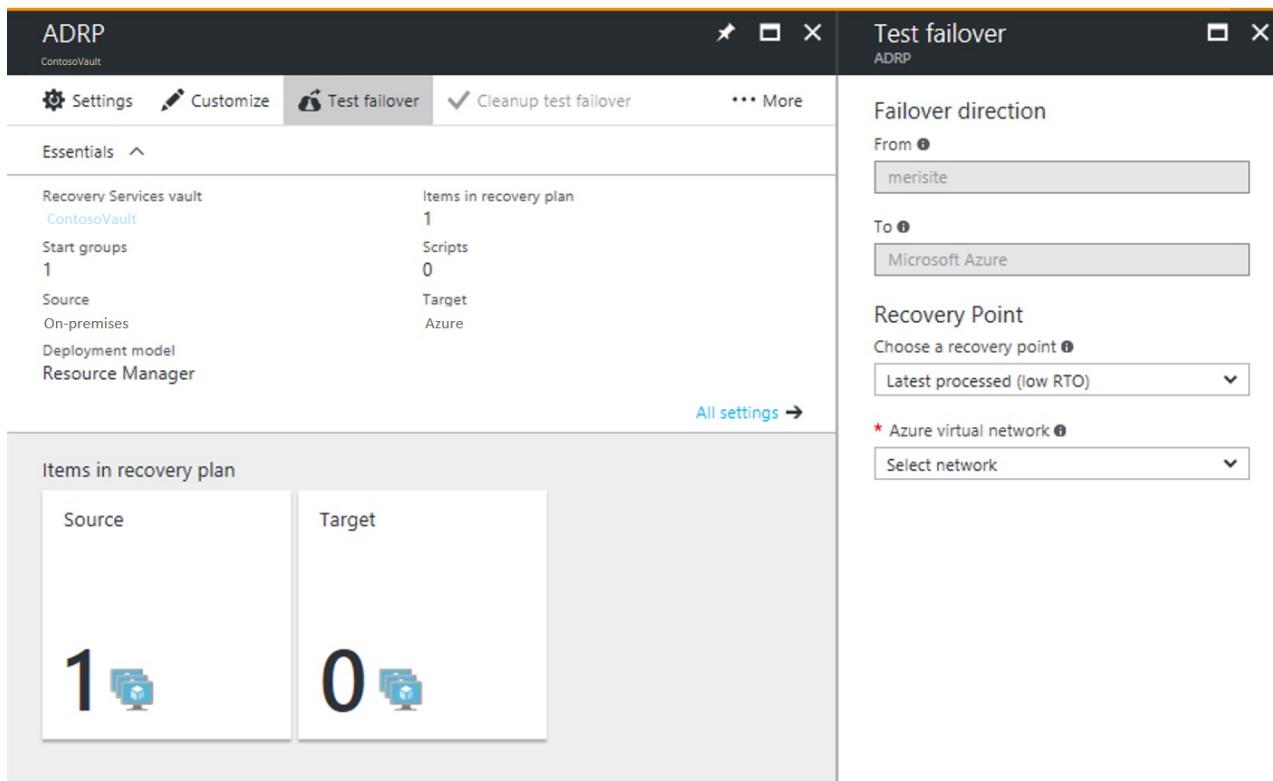
7/13/2018 • 6 minutes to read • [Edit Online](#)

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.



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 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 after failover, follow the requirements summarized in the table.

FAILOVER	LOCATION	ACTIONS
----------	----------	---------

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>

Next steps

After you've completed a disaster recovery drill, learn more about other types of [failover](#).

Create and customize recovery plans

7/24/2018 • 4 minutes to read • [Edit Online](#)

This article describes how to create and customize a recovery plan 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	Azure region	Azure region
VMware to Azure	Configuration server	Azure
Physical machines to Azure	Configuration server	Azure
Hyper-V managed by VMM to Azure	VMM display name	Azure
Hyper-V without VMM to Azure	Hyper-V site name	Azure
VMM to VMM	VMM friendly name	VMM display name

NOTE

A recovery plan can contain machines with the same source and target. VMware and Hyper-V VMs managed by VMM can't be in the same plan. VMware VMs and physical servers can be in the same plan, where the source is a configuration server.

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 `\MSSCVMM\Library\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 Azure Automation runbooks to recovery plans

8/6/2018 • 7 minutes to read • [Edit Online](#)

In this article, we describe how Azure Site Recovery integrates with Azure Automation to help you extend your recovery plans. Recovery plans can orchestrate recovery of VMs that are protected with Site Recovery. Recovery plans work both for replication to a secondary cloud, and for replication to Azure. Recovery plans also help make the recovery **consistently accurate, repeatable**, and **automated**. If you fail over your VMs to Azure, integration with Azure Automation extends your recovery plans. You can use it to execute runbooks, which offer powerful automation tasks.

If you are new to Azure Automation, you can [sign up](#) and [download sample scripts](#). For more information, and to learn how to orchestrate recovery to Azure by using [recovery plans](#), see [Azure Site Recovery](#).

In this article, we describe how you can integrate Azure Automation runbooks into your recovery plans. We use examples to automate basic tasks that previously required manual intervention. We also describe how to convert a multi-step recovery to a single-click recovery action.

Customize the recovery plan

1. Go to the **Site Recovery** recovery plan resource blade. For this example, the recovery plan has two VMs added to it, for recovery. To begin adding a runbook, click the **Customize** tab.

The screenshot shows the Azure Site Recovery recovery plan resource blade for a vault named 'IbizaAsrTest'. The 'Customize' tab is selected. The 'Essentials' section displays the following details:

Recovery Services vault	Items in recovery plan
IbizaAsrTest	2
Start groups	Scripts
2	0
Source	Target
CP-L2B18-X64-15.dratest.nttest.microsoft.c...	CP-L2B18-X64-15.dratest.nttest.microsoft.c...
Deployment model	-

Below this, the 'Items in recovery plan' section shows two items: 'Source' (2) and 'Target' (0). Each item is represented by a large number and a small icon of a computer monitor with a blue square on it.

2. Right-click **Group 1: Start**, and then select **Add post action**.

This recovery plan contains 2 machine(s).

STAGE NAME	DETAILS
All groups shutdown	2 machines in 2 groups.
▶ All groups failover	
▶ Group 1: Start	1 Machine
▶ Group 2: Start	1 Machine

3. Click **Choose a script**.
4. On the **Update action** blade, name the script **Hello World**.

Update action

* Name: Hello World

Failover to azure script

* Automation account name: RPTTestAutomationAccount1

* Runbook name: helloworld1

Failover to on-premise script

I want to use a script to failover from azure to on-premise.

5. Enter an Automation account name.

NOTE

The Automation account can be in any Azure region. The Automation account must be in the same subscription as the Azure Site Recovery vault.

6. In your Automation account, select a runbook. This runbook is the script that runs during the execution of the recovery plan, after the recovery of the first group.
7. To save the script, click **OK**. The script is added to **Group 1: Post-steps**.

The screenshot shows the SharepointRecovery application window. On the left, a list of stages is displayed:

STAGE NAME	DETAILS
All groups shutdown	2 machines in 2 groups.
▶ All groups failover	
▼ Group 1: Start	1 Machine
PrimaryOS1	Machine
▼ Group 1: Post-steps	1 Step
Script: Hello World	Script
▼ Group 2: Start	1 Machine
PrimaryOS2	Machine

On the right, a configuration panel titled "Update action" is shown for the selected "Script: Hello World" step. It includes fields for "Name" (Hello World), "Automation account name" (RPTTestAutomationAccount1), and "Runbook name" (helloworld1). A checkbox for "Failover to on-premise script" is present, with a note below it stating "I want to use a script to failover from azure to on-premise".

Considerations for adding a script

- For options to **delete a step** or **update the script**, right-click the script.
- A script can run on Azure during failover from an on-premises machine to Azure. It also can run on Azure as a primary-site script before shutdown, during failback from Azure to an on-premises machine.
- When a script runs, it injects a recovery plan context. 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"
    }
  }
}
```

The following table lists the name and description of each variable in the context.

VARIABLE NAME	DESCRIPTION
---------------	-------------

VARIABLE NAME	DESCRIPTION
RecoveryPlanName	The name of the plan being run. This variable helps you take different actions based on the recovery plan name. You also can reuse the script.
FailoverType	Specifies whether the failover is a test, planned, or unplanned.
FailoverDirection	Specifies whether recovery is to a primary or secondary site.
GroupID	Identifies the group number in the recovery plan when the plan is running.
VmMap	An array of all VMs in the group.
VMMMap key	A unique key (GUID) for each VM. It's the same as the Azure Virtual Machine Manager (VMM) ID of the VM, where applicable.
SubscriptionId	The Azure subscription ID in which the VM was created.
RoleName	The name of the Azure VM that's being recovered.
CloudServiceName	The Azure cloud service name under which the VM was created.
ResourceGroupName	The Azure resource group name under which the VM was created.
RecoveryPointId	The timestamp for when the VM is recovered.

- Ensure that the Automation account has the following modules:

- AzureRM.profile
- AzureRM.Resources
- AzureRM.Automation
- AzureRM.Network
- AzureRM.Compute

All modules should be of compatible versions. An easy way to ensure that all modules are compatible is to use the latest versions of all the modules.

Access all VMs of the VMMMap in a loop

Use the following code to loop across all VMs of the Microsoft VMMMap:

```

$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
    }
}

```

NOTE

The resource group name and role name values are empty when the script is a pre-action to a boot group. The values are populated only if the VM of that group succeeds in failover. The script is a post-action of the boot group.

Use the same Automation runbook in multiple recovery plans

You can use a single script in multiple recovery plans by using external variables. You can use [Azure Automation variables](#) to store parameters that you can pass for a recovery plan execution. 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 of a recovery plan.

For the script to detect which recovery plan is running, use the recovery plan context:

```

workflow AddPublicIPAndNSG {
    param (
        [parameter(Mandatory=$false)]
        [Object]$RecoveryPlanContext
    )

    $RPName = $RecoveryPlanContext.RecoveryPlanName

```

To apply an existing NSG, you must know the NSG name and the NSG resource group name. Use these variables as inputs for recovery plan scripts. To do this, create two variables in the Automation account assets. Add the name of the recovery plan that you are creating the parameters for as a prefix to the variable name.

1. Create a variable to store the NSG name. Add a prefix to the variable name by using the name of the recovery plan.

 RPscripttest-NSG ★ □ ×

Variable

■ Save ✖ Discard trash 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

2. Create a variable to store the NSG's resource group name. Add a prefix to the variable name by using the name of the recovery plan.

 RPscripttest-NSGRG ★ □ ×

Variable

 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



3. In the script, use the following 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
```

4. 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, see [Add a public IP and NSG to VMs during test failover of a Site Recovery recovery plan](#).

Use a complex variable to store more information

Consider a scenario in which you want a single script to turn on a public IP on specific VMs. In another scenario,

you might want to apply different NSGs on different VMs (not on all VMs). You can make a script that is 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. You cannot create separate variables for each recovery plan.

In the following example, we use a new technique and create a [complex variable](#) in the Azure Automation account assets. You do this by specifying multiple values. You must use Azure PowerShell to complete the following steps:

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 by using the name of the recovery plan:

```
$VMDetails =  
@{"VMGUID"=@{ "ResourceGroupName"="RGNameOfNSG" ; "NSGName"="NameOfNSG" } ; "VMGUID2"=@{ "ResourceGroupName"="R  
GNameOfNSG" ; "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:

The screenshot shows the Azure portal interface. On the left, there's a sidebar with 'RESOURCE MANAGEMENT' and 'GENERAL' sections. Under 'GENERAL', 'Properties' is selected. On the right, the 'Properties' blade is open for a VM. It shows the following details:

Active location	FTPV2A
Replication policy	
ID	/Subscriptions/7c943c1b-5122-4097-90c8- 200d7b22-cced-11e6-8166-0050568f7993
Source VM Id	200d7b22-cced-11e6-8166-0050568f7993
Operating system	-
Source location	
Daily data change rate	0 MB

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
```

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) {
    Write-output $VMDetailsObj.value.$VMID

    if ($VMDetailsObj.value.$VMID -ne $Null) { #If the VM exists in the context, this will not be Null
        $VM = $vmMap.$VMID
        # Access the properties of the variable
        $NSGname = $VMDetailsObj.value.$VMID.'NSGName'
        $NSGRGname = $VMDetailsObj.value.$VMID.'NSGRGName'

        # 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.



For another example, see the following video. It demonstrates how to recover a two-tier WordPress application to Azure:

Additional resources

- [Azure Automation service Run As account](#)
- [Azure Automation overview](#)
- [Azure Automation sample scripts](#)

Next steps

[Learn more](#) about running failovers.

Set up a process server in Azure for failback

7/9/2018 • 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

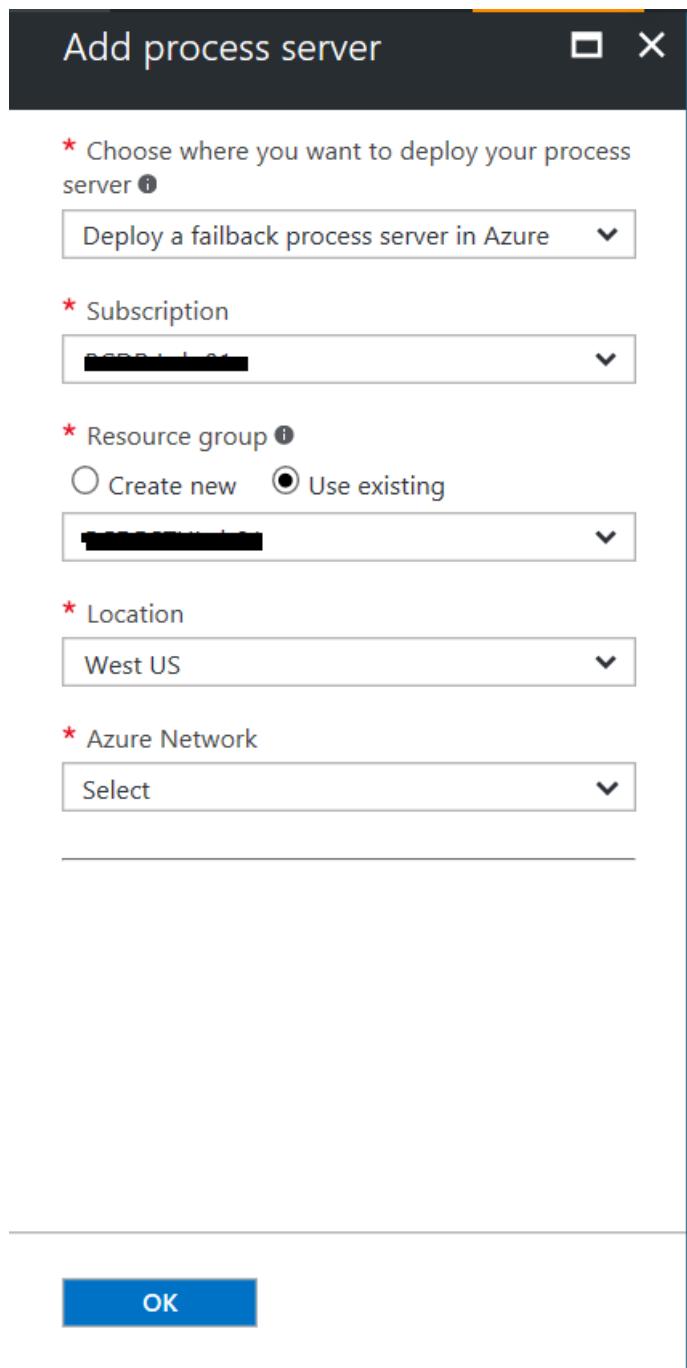
1. A **Site to Site VPN** or an **Express Route** connection between your on-premises network and the Azure Virtual Network has already been established.
2. Your user account has permissions to create a new virtual machine in the Azure Subscription that the virtual machines have been failed over into.
3. Your subscription has a minimum of 4 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.

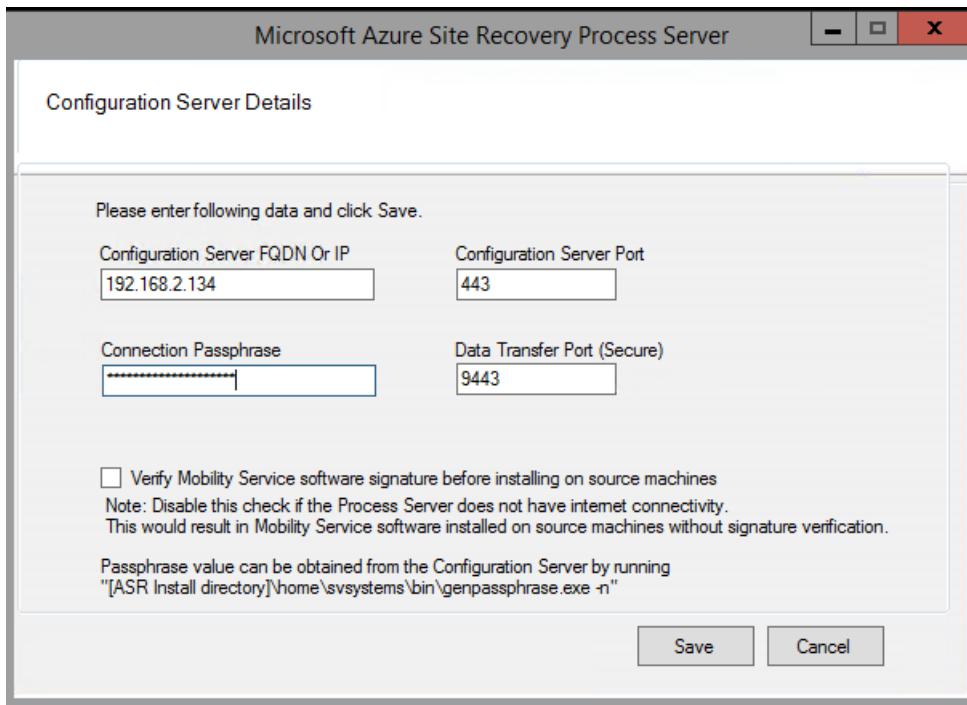
>

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:

- Connect to the Process Server virtual machine using Remote Desktop Connection.
- You can launch the `cspconfigtool.exe` by clicking on the shortcut available on the desktop. (The tool will be automatically launched if this is the first time you are logging into the process server).

- Configuration Server's fully qualified name (FQDN) or IP Address
- Port on which the Configuration server is listening on. The value should be 443
- Connection Passphrase to connect to the configuration server.
- Data Transfer port to be configured for this Process Server. Leave the default value as is unless you have changed it to a different port number in your environment.



- Click the save button to save the configuration and register the Process Server.

Install a Linux master target server

7/9/2018 • 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.

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 supported Ubuntu kernels are supported.

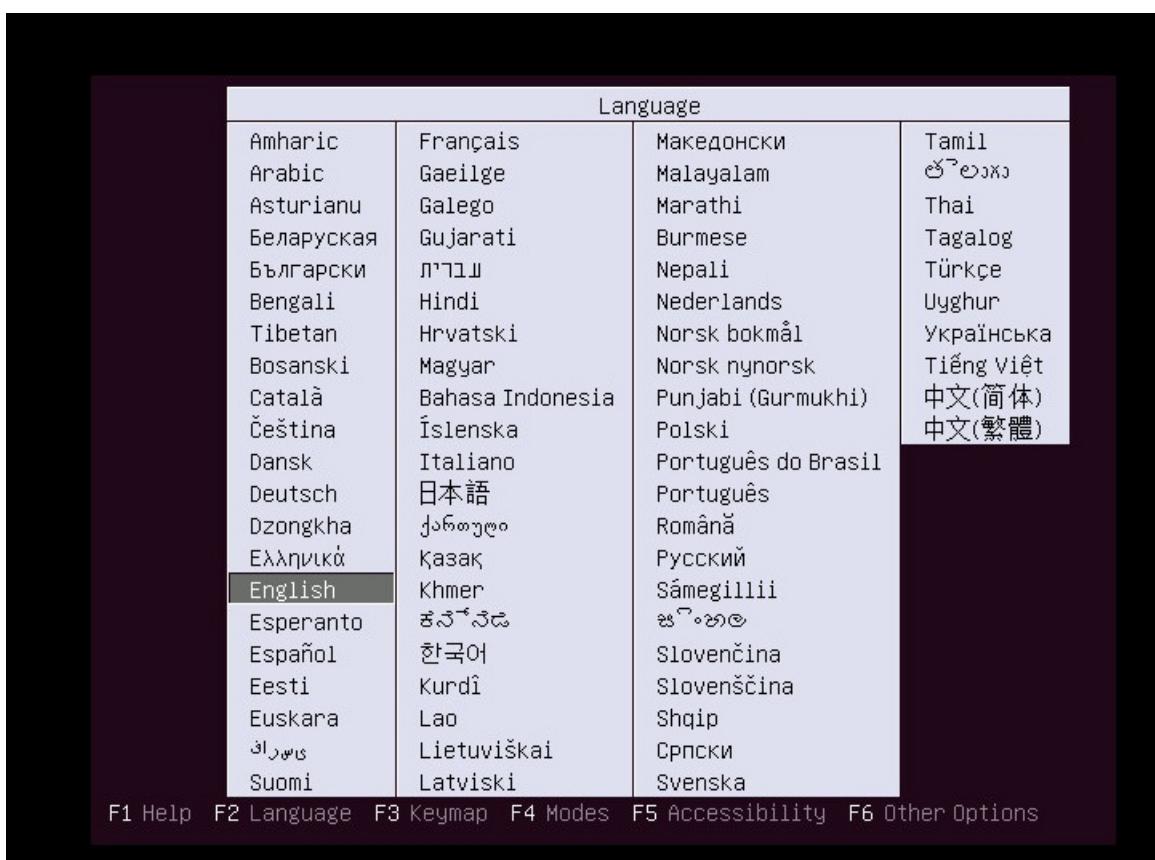
KERNEL SERIES	SUPPORT UP TO
4.4	4.4.0-81-generic
4.8	4.8.0-56-generic
4.10	4.10.0-24-generic

Deploy the master target server

Install Ubuntu 16.04.2 Minimal

Take the following steps to install the Ubuntu 16.04.2 64-bit operating system.

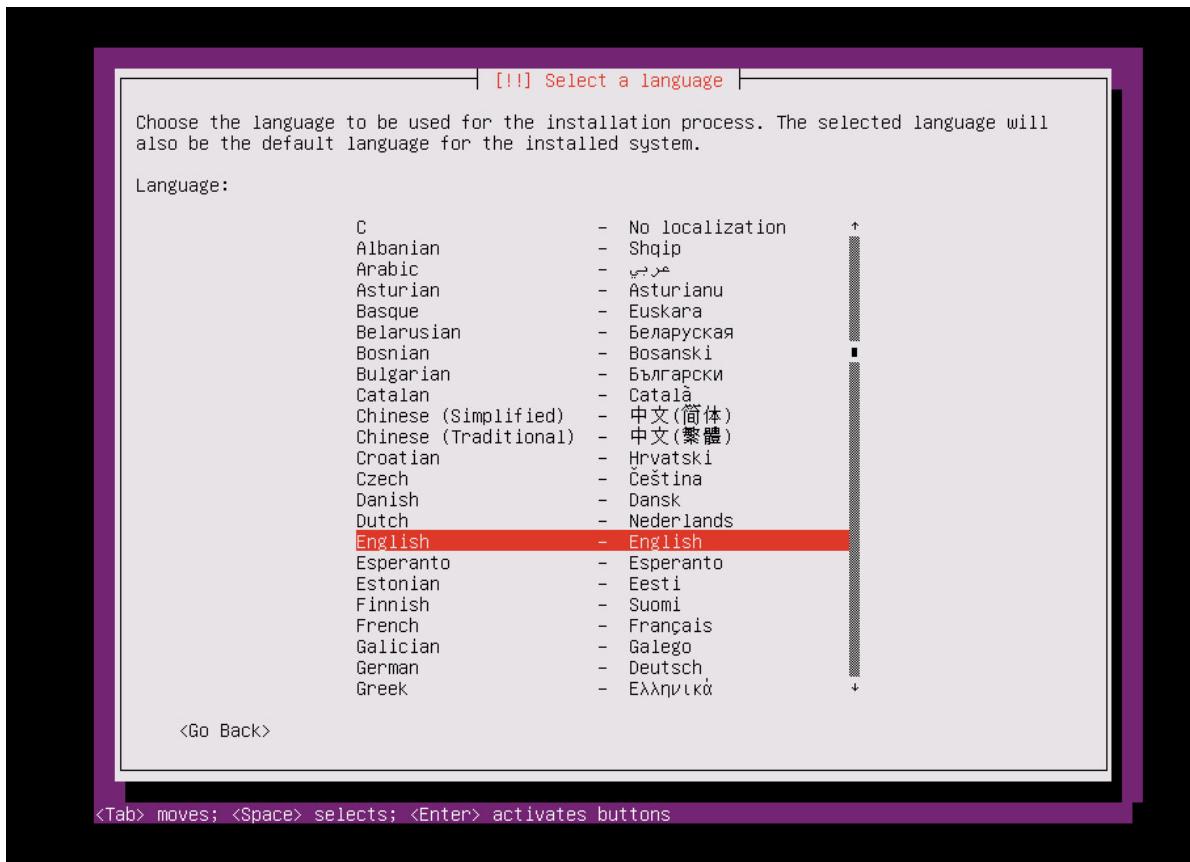
1. Go to the [download link](#), choose the closest mirror and download an Ubuntu 16.04.2 minimal 64-bit ISO.
Keep an Ubuntu 16.04.2 minimal 64-bit ISO in the DVD drive and start the system.
2. Select **English** as your preferred language, and then select **Enter**.



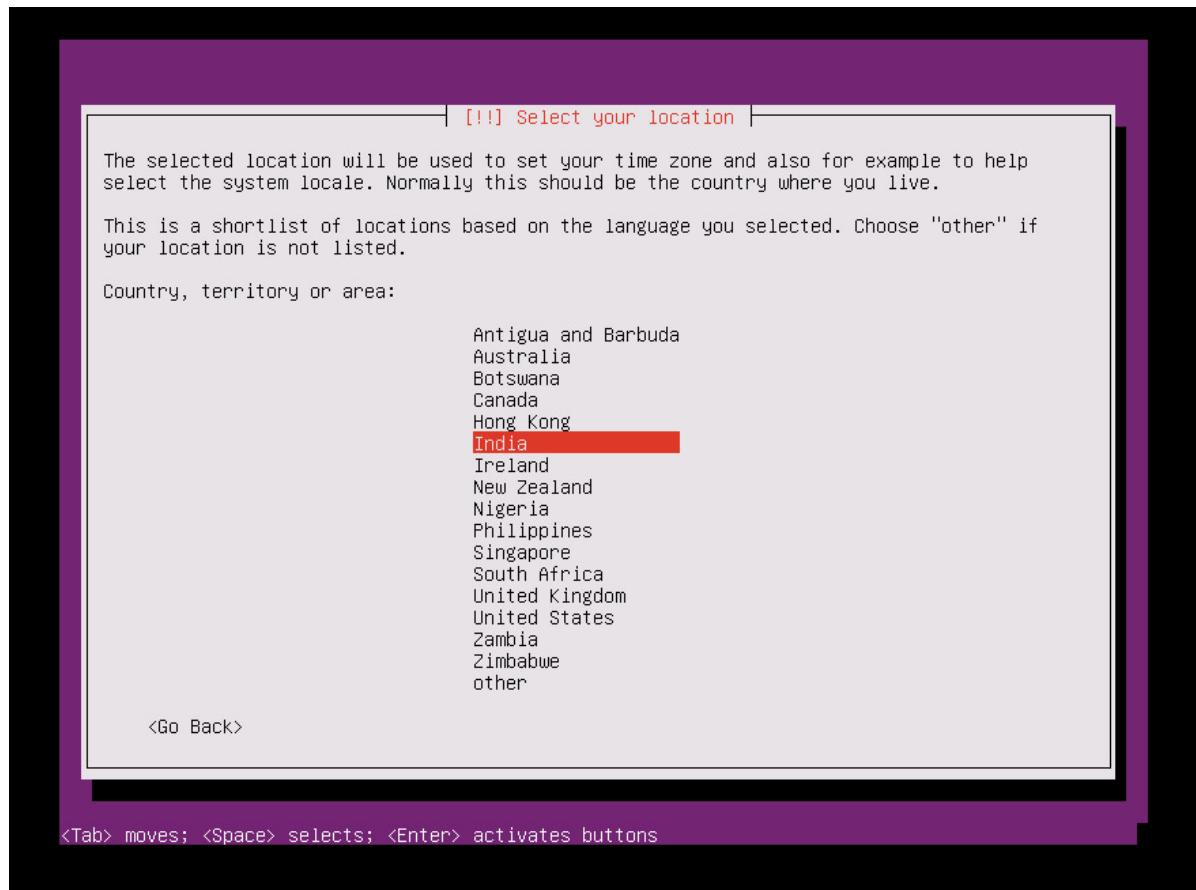
3. Select **Install Ubuntu Server**, and then select **Enter**.



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**.

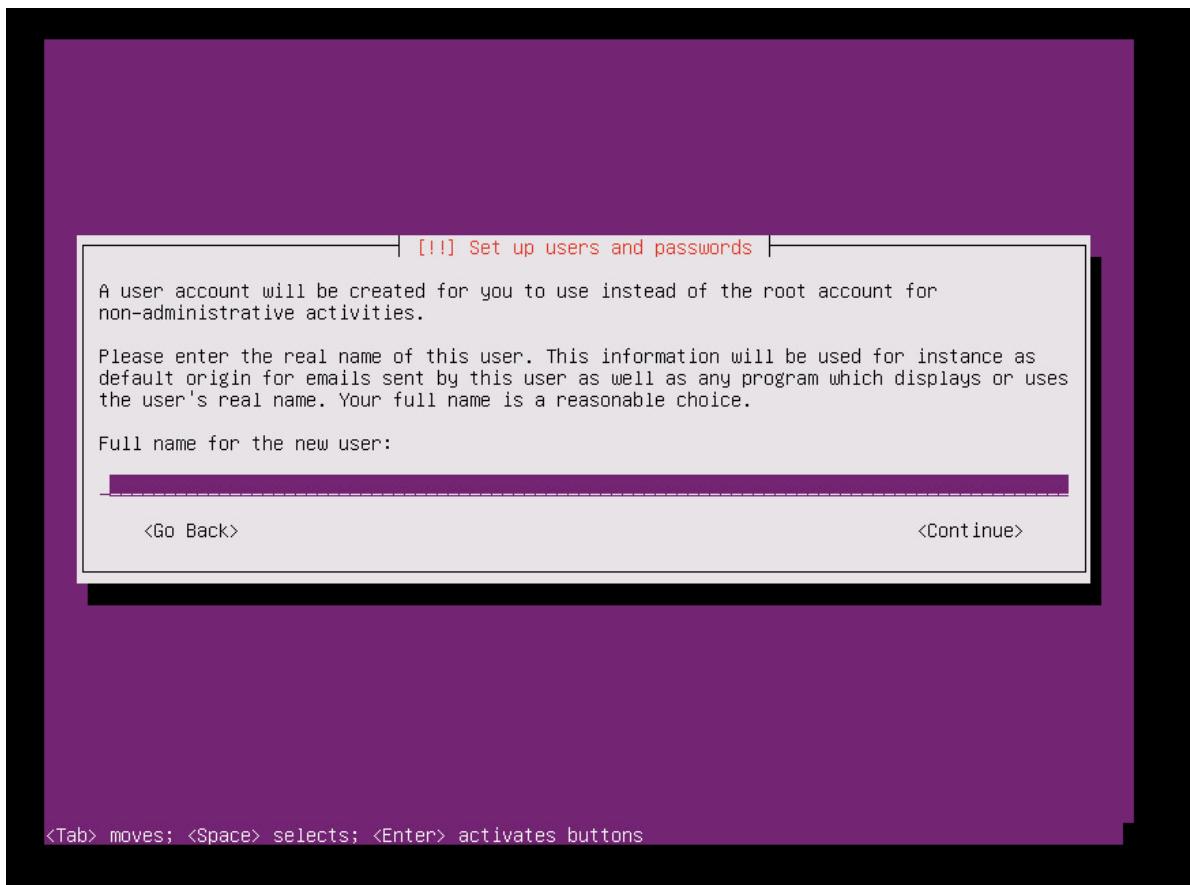


6. Select **No** (the default option), and then select **Enter**.



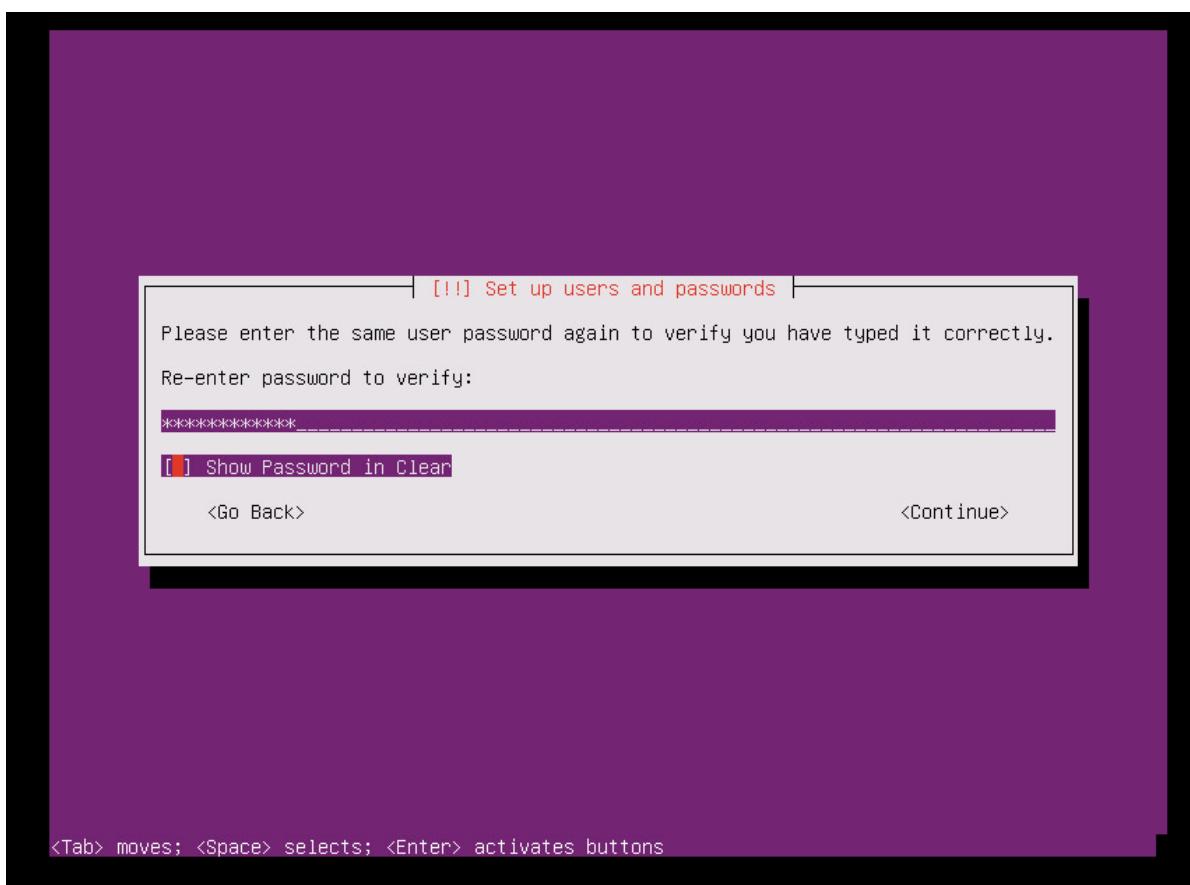
7. Select **English (US)** as the country of origin for the keyboard, and then select **Enter**.
8. Select **English (US)** as the keyboard layout, and then select **Enter**.
9. Enter the hostname for your server in the **Hostname** box, and then select **Continue**.

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**.

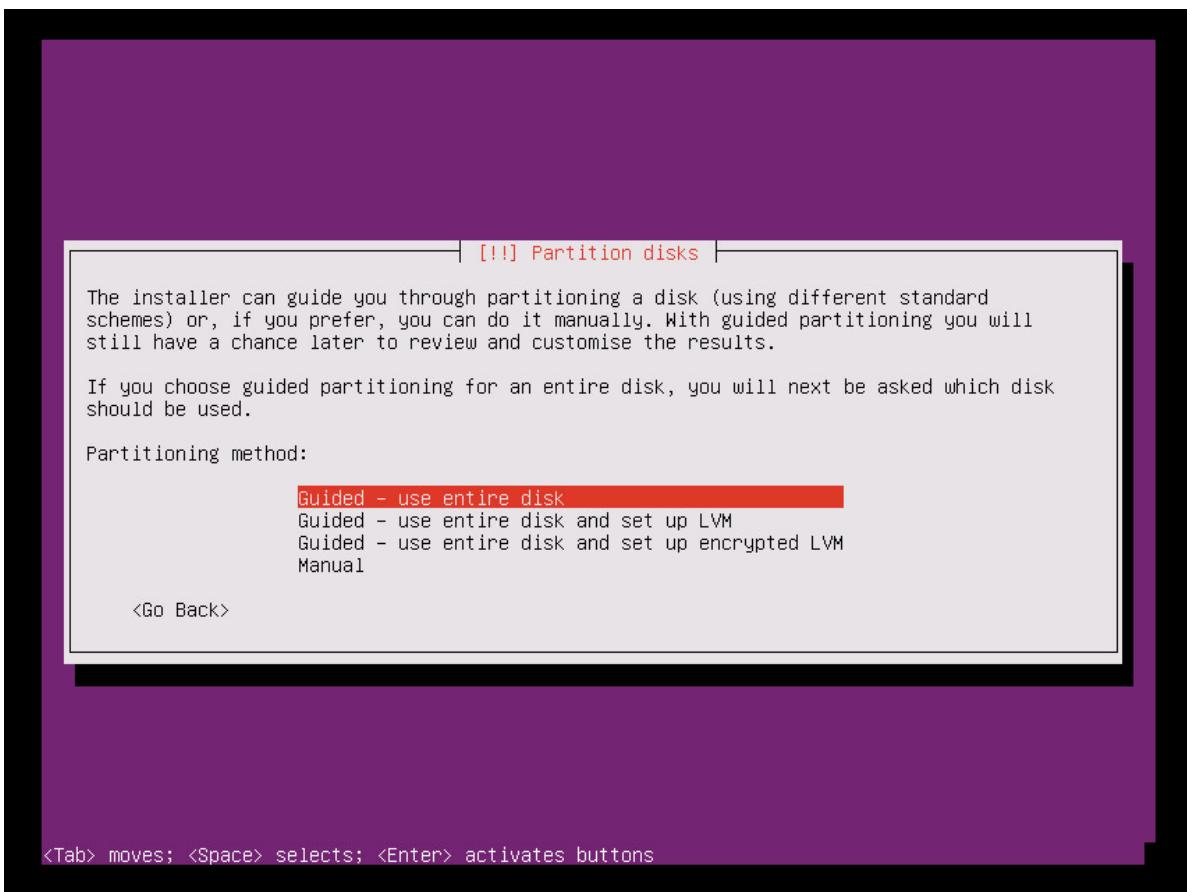
12. Confirm the password for the new user, and then select **Continue**.



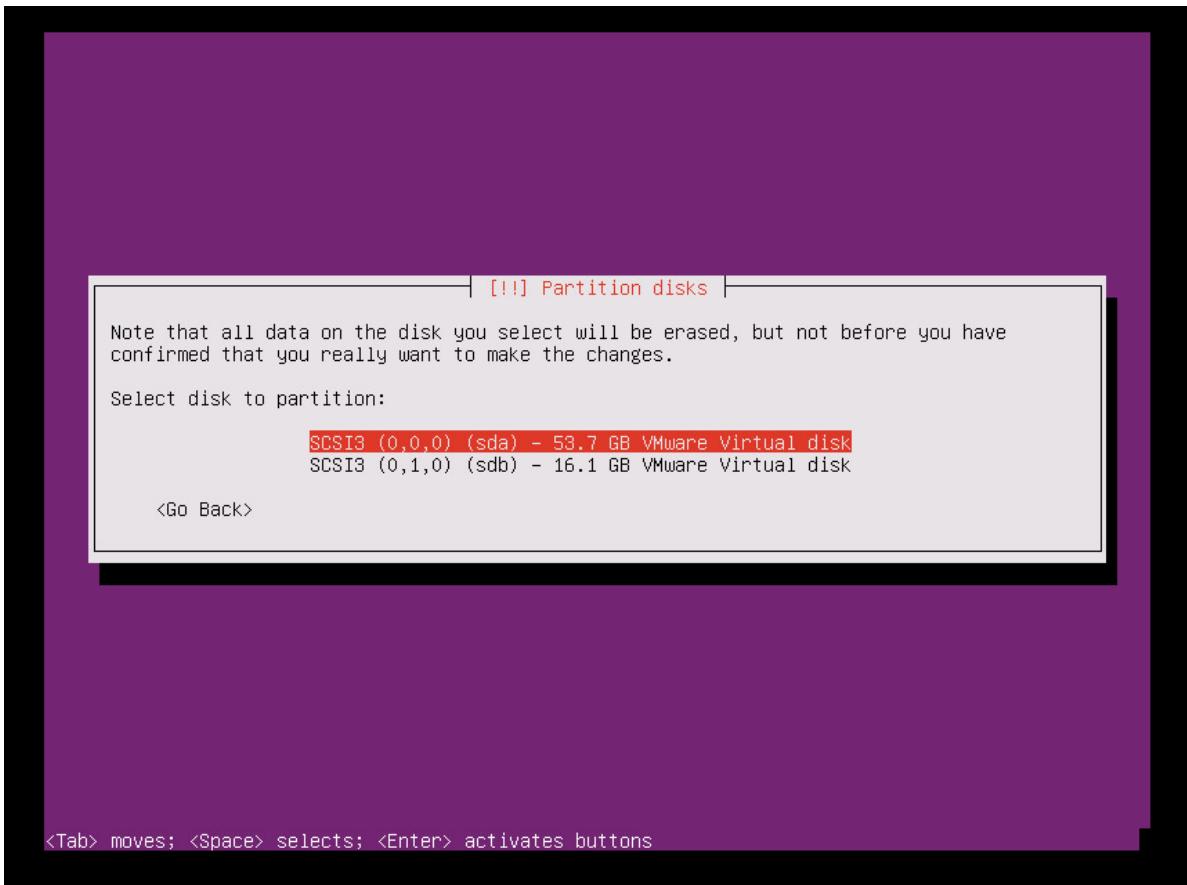
13. In the next selection for encrypting your home directory, select **No** (the default option), and then select **Enter**.

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**.

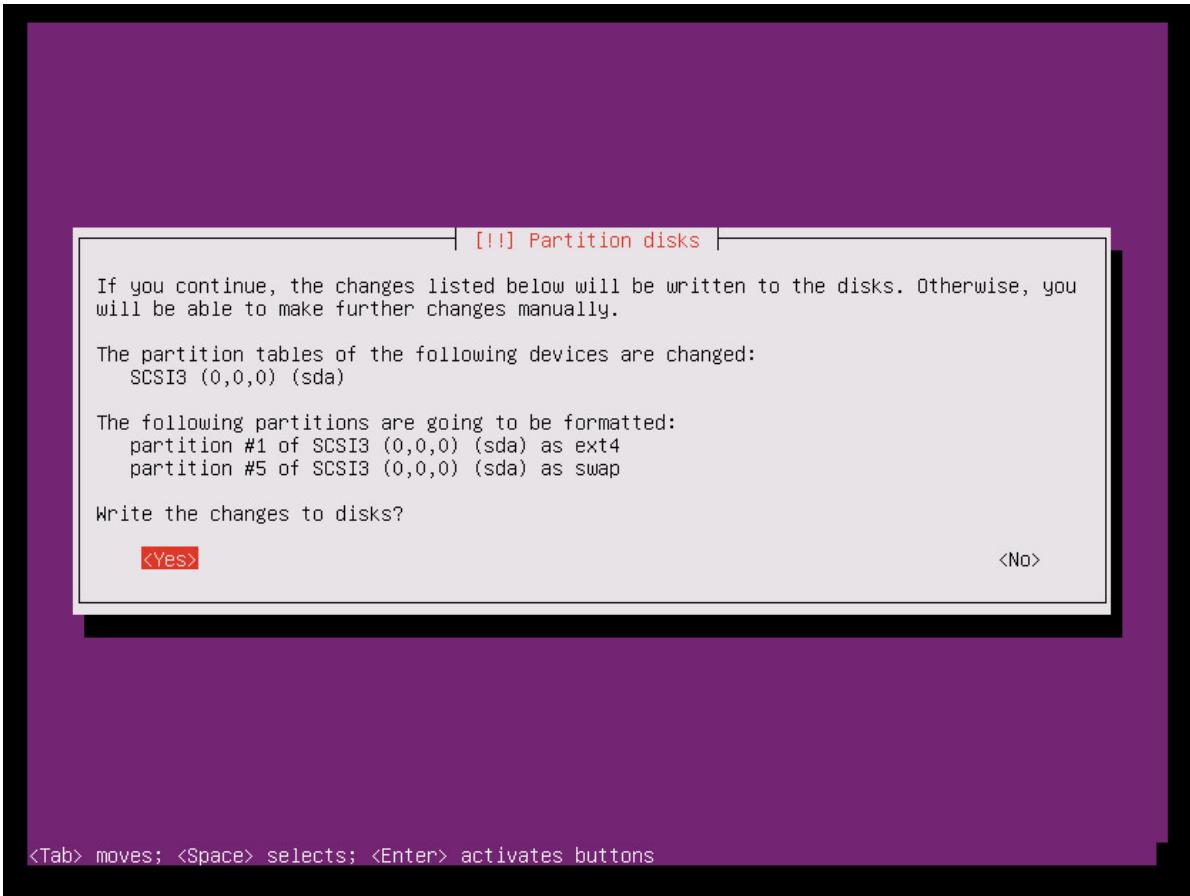
15. From the partitioning method options, select **Guided - use entire disk**, and then select **Enter**.



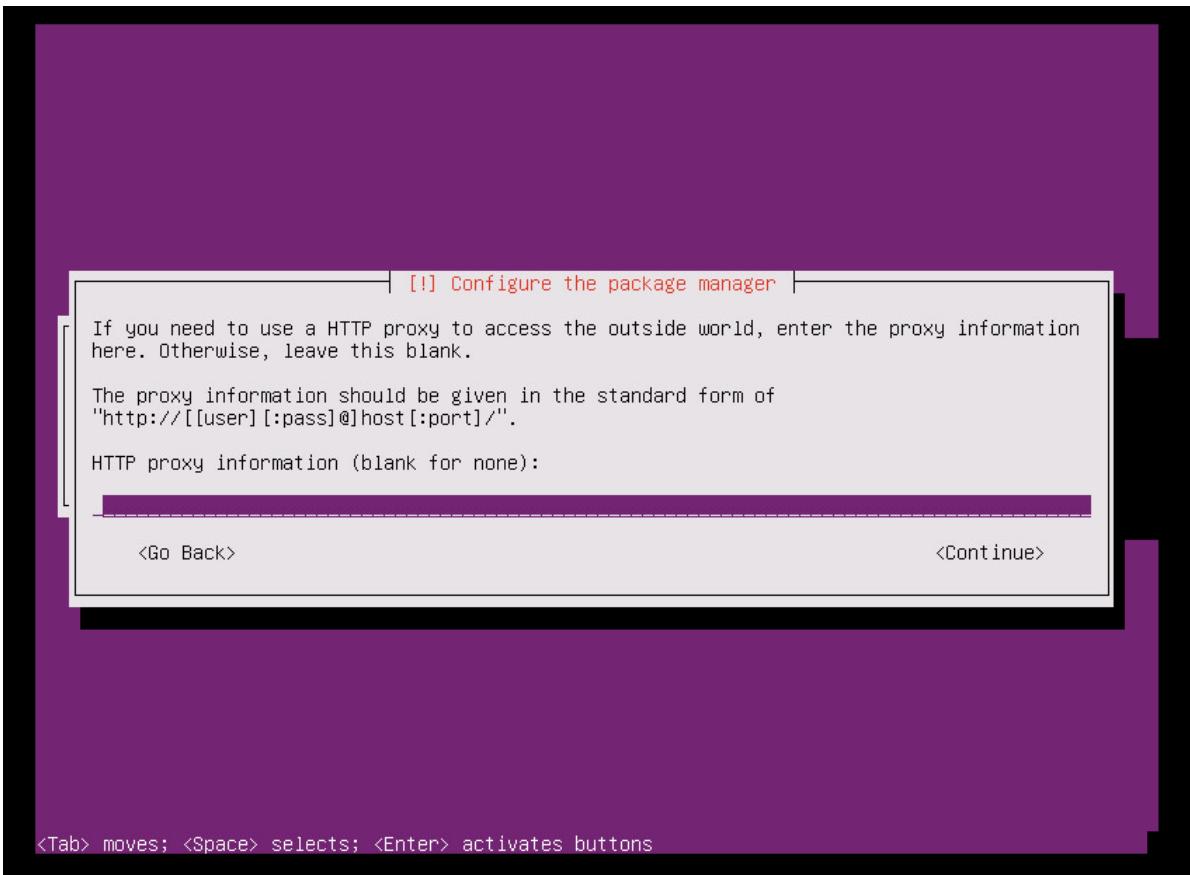
16. Select the appropriate disk from the **Select disk to partition** options, and then select **Enter**.



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**.

```
[!] Configuring tasksel

Applying updates on a frequent basis is an important part of keeping your system secure.

By default, updates need to be applied manually using package management tools.
Alternatively, you can choose to have this system automatically download and install
security updates, or you can choose to manage this system over the web as part of a group
of systems using Canonical's Landscape service.

How do you want to manage upgrades on this system?

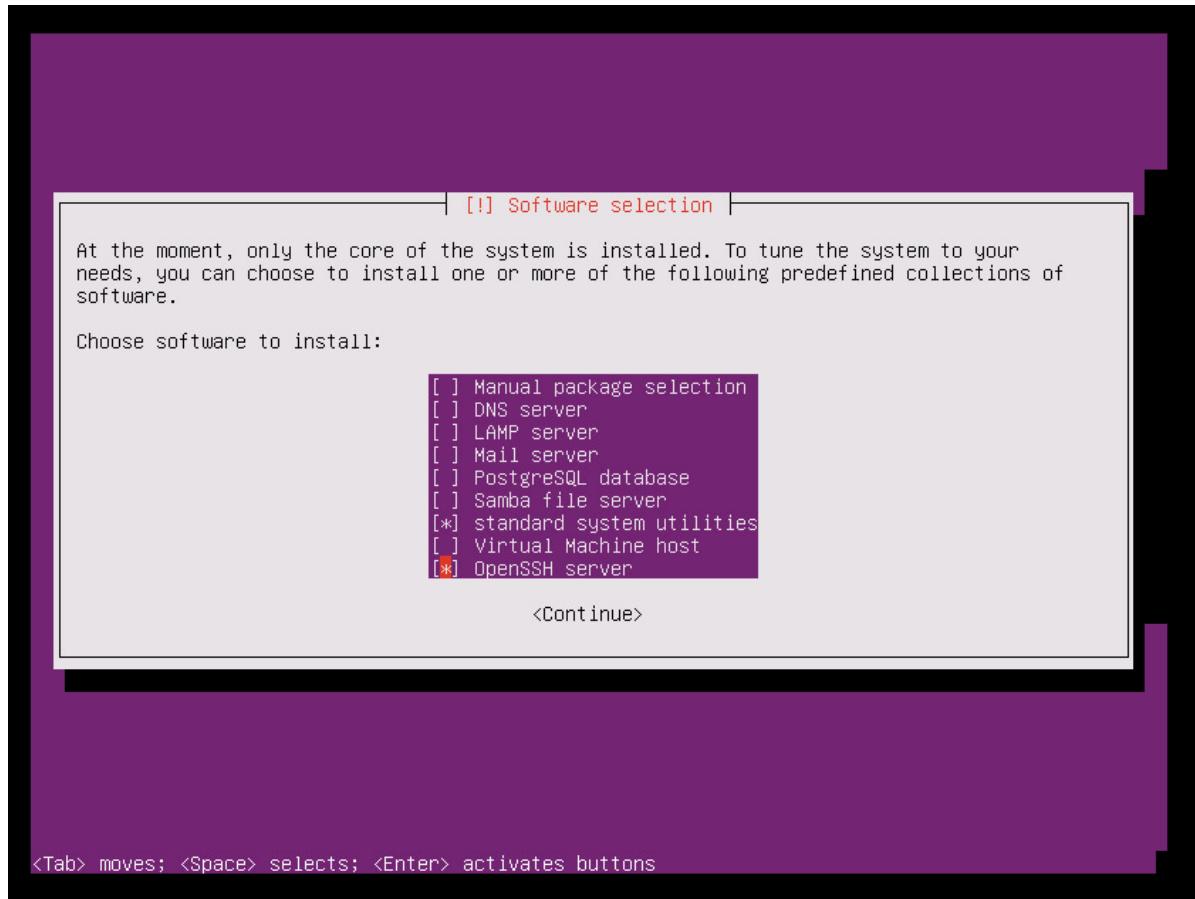
No automatic updates
Install security updates automatically
Manage system with Landscape

<Tab> moves; <Space> selects; <Enter> activates buttons
```

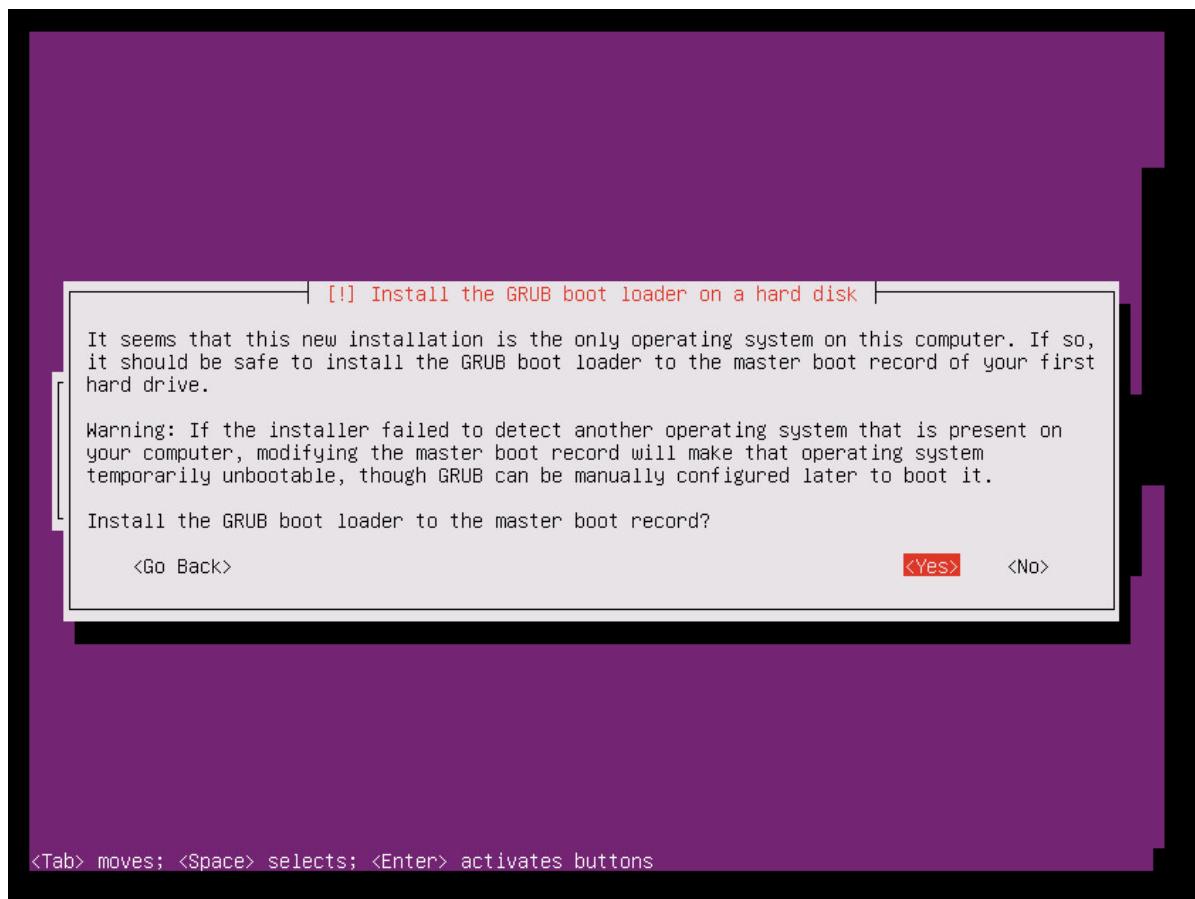
WARNING

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.

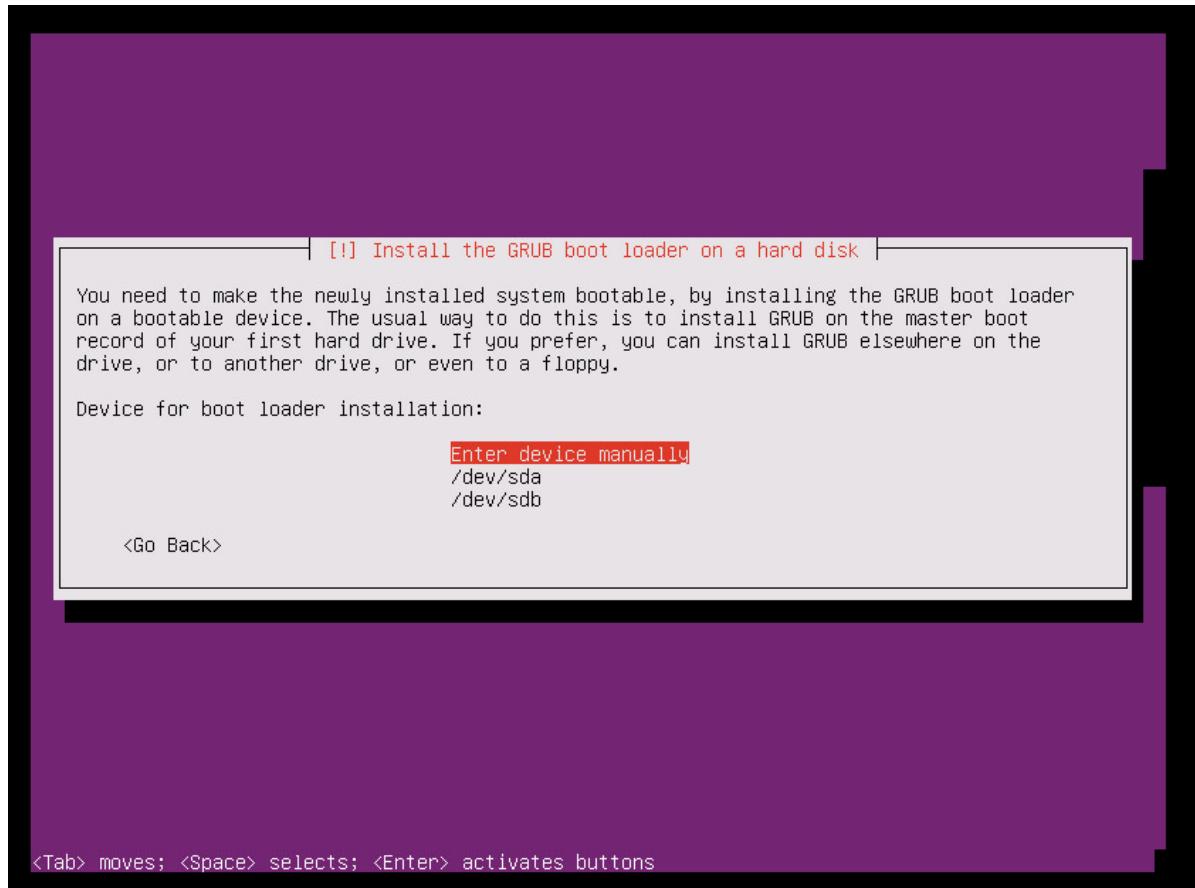
20. Select default options. If you want openSSH for SSH connect, select the **OpenSSH server** option, and then select **Continue**.



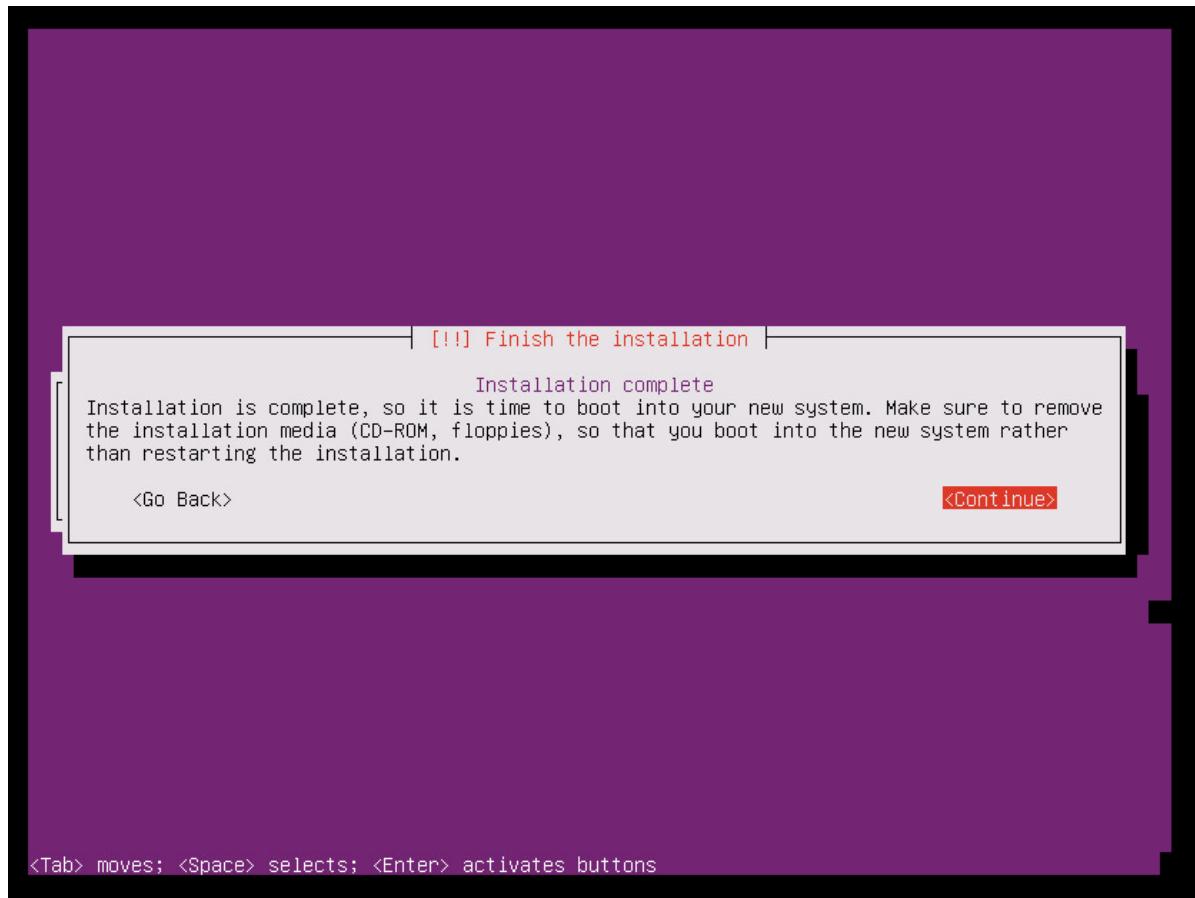
21. In the selection for installing the GRUB boot loader, Select **Yes**, and then select **Enter**.



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.

```

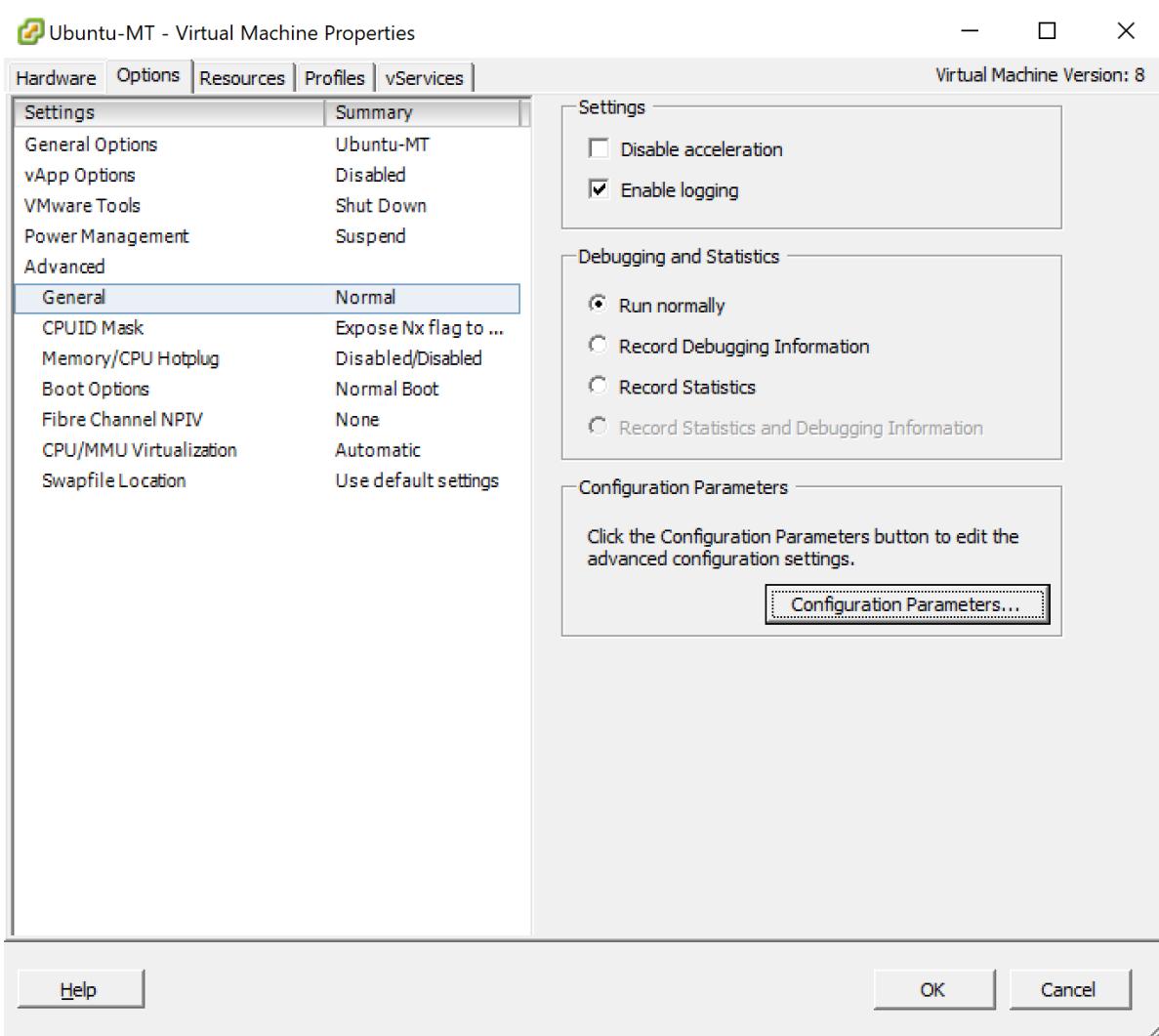
mtuser@UbuntuMT:~#
mtuser@UbuntuMT:~# sudo passwd root
[sudo] password for mtuser:
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
mtuser@UbuntuMT:~#
mtuser@UbuntuMT:~#
mtuser@UbuntuMT:~# su
Password:
root@UbuntuMT:~#

```

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.

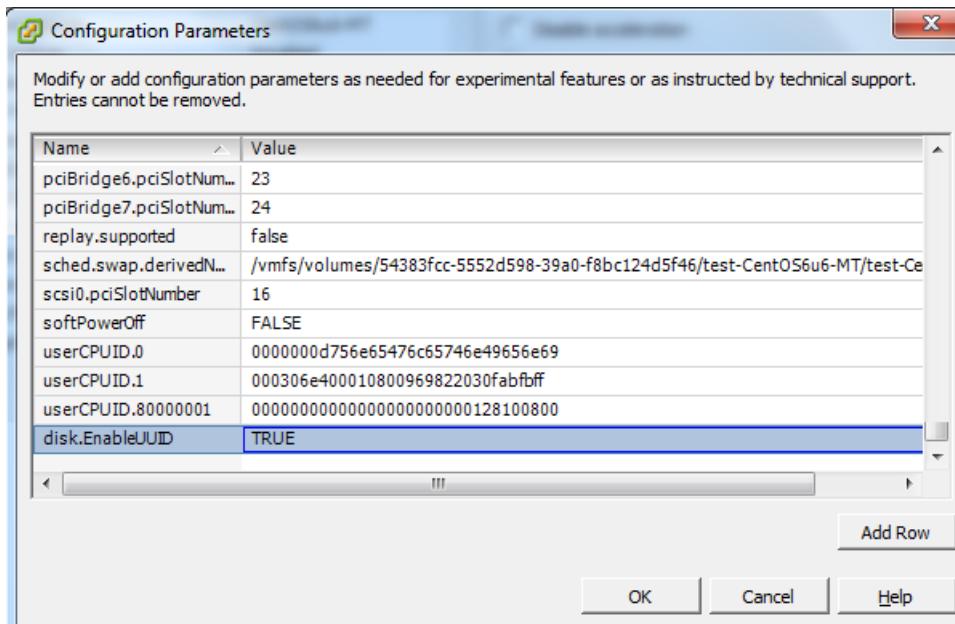


The **Configuration Parameters** option is not available when the machine is running. To make this tab

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 RPM 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:

1. Run the following command to untar the binary.

```
tar -zxvf latestlinuxmobsvc.tar.gz
```

```
[csadmin@ContosoLinMT1 ~]$ [csadmin@ContosoLinMT1 ~]$ tar -xvzf Microsoft-ASR_UA_8.2.0.0_RHEL6-64_017_01_May2015_reduced.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]#
```

- After you create the file system, mount the retention disk.

```
mkdir /mnt/retention
mount /dev/mapper/<Retention disk's multipath id> /mnt/retention
```

- 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/ /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.

- 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.

```
./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 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.

Failover in Site Recovery

7/9/2018 • 7 minutes to read • [Edit Online](#)

This article describes how to failover virtual machines and physical servers protected by Site Recovery.

Prerequisites

1. Before you do a failover, do a [test failover](#) to ensure that everything is working as expected.
2. [Prepare the network](#) at target location before you do a failover.

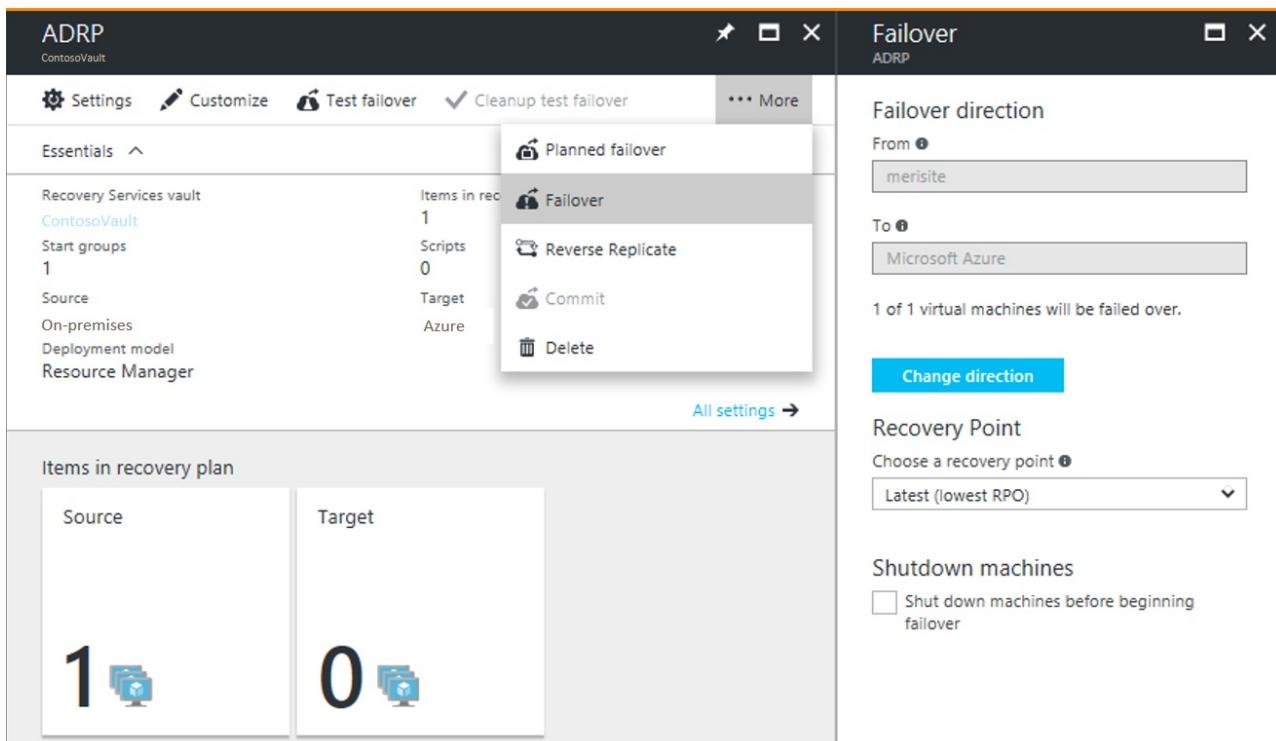
Use the following table to know about the failover options provided by Azure Site Recovery. These options are also listed for different failover scenarios.

SCENARIO	APPLICATION RECOVERY REQUIREMENT	WORKFLOW FOR HYPER-V	WORKFLOW FOR VMWARE
Planned failover due to an upcoming datacenter downtime	Zero data loss for the application when a planned activity is performed	<p>For Hyper-V, ASR replicates data at a copy frequency that is specified by the user. Planned Failover is used to override the frequency and replicate the final changes before a failover is initiated.</p> <p>1. Plan a maintenance window as per your business's change management process.</p> <p>2. Notify users of upcoming downtime.</p> <p>3. Take the user-facing application offline.</p> <p>4. Initiate Planned Failover using the ASR portal. The on-premises virtual machine is automatically shut-down.</p> <p>Effective application data loss = 0</p> <p>A journal of recovery points is also provided in a retention window for a user who wants to use an older recovery point. (24 hours retention for Hyper-V).</p>	<p>For VMware, ASR replicates data continually using CDP. Failover gives the user the option to failover to the Latest data (including post application shut-down)</p> <p>1. Plan a maintenance window as per the change management process</p> <p>2. Notify users of upcoming downtime</p> <p>3. Take the user-facing application offline.</p> <p>4. Initiate a Planned Failover using ASR portal to the Latest point after the application is offline. Use the "Unplanned Failover" option on the portal and select the Latest point to failover. The on-premises virtual machine is automatically shut-down.</p> <p>Effective application data loss = 0</p> <p>A journal of recovery points in a retention window is provided for a customer who wants to use an older recovery point. (72 hours of retention for VMware).</p>

SCENARIO	APPLICATION RECOVERY REQUIREMENT	WORKFLOW FOR HYPER-V	WORKFLOW FOR VMWARE
Failover due to an unplanned datacenter downtime (natural or IT disaster)	Minimal data loss for the application	1. Initiate the organization's BCP plan 2. Initiate Unplanned Failover using ASR portal to the Latest or a point from the retention window (journal).	1. Initiate the organization's BCP plan. 2. Initiate unplanned Failover using ASR portal to the Latest or a point from the retention window (journal).

Run a failover

This procedure describes how to run a failover for a [recovery plan](#). Alternatively you can run the failover for a single virtual machine or physical server from the **Replicated items** page



1. Select **Recovery Plans** > *recoveryplan_name*. Click **Failover**
2. On the **Failover** screen, select a **Recovery Point** to failover to. You can use one of the following options:
 - a. **Latest** (default): This option starts the job by first processing all the data that has been sent to Site Recovery service. Processing the data creates a recovery point for each virtual machine. This recovery point is used by the virtual machine during failover. This option provides the lowest RPO (Recovery Point Objective) as the virtual machine created after failover has all the data that has been replicated to Site Recovery service when the failover was triggered.
 - b. **Latest processed**: This option fails over all virtual machines of the recovery plan to the latest recovery point that has already been processed by Site Recovery service. When you are doing test failover of a virtual machine, time stamp of the latest processed recovery point is also shown. If you are doing failover of a recovery plan, you can go to individual virtual machine and look at **Latest Recovery Points** tile to get this information. As no time is spent to process the unprocessed data, this option provides a low RTO (Recovery Time Objective) failover option.
 - c. **Latest app-consistent**: This option fails over all virtual machines of the recovery plan to the latest application consistent recovery point that has already been processed by Site Recovery service. When you are doing test failover of a virtual machine, time stamp of the latest app-consistent recovery point is also shown. If you are doing failover of a recovery plan, you can go to individual virtual machine and look

at **Latest Recovery Points** tile to get this information.

- d. **Latest multi-VM processed:** This option is only available for recovery plans that have at least one virtual machine with multi-VM consistency ON. Virtual machines that are part of a replication group failover to the latest common multi-VM consistent recovery point. Other virtual machines failover to their latest processed recovery point.
- e. **Latest multi-VM app-consistent:** This option is only available for recovery plans that have at least one virtual machine with multi-VM consistency ON. Virtual machines that are part of a replication group failover to the latest common multi-VM application-consistent recovery point. Other virtual machines failover to their latest application-consistent recovery point.
- f. **Custom:** If you are doing test failover of a virtual machine, then you can use this option to failover to a particular recovery point.

NOTE

The option to choose a recovery point is only available when you are failing over to Azure.

3. If some of the virtual machines in the recovery plan were failed over in a previous run and now the virtual machines are active on both source and target location, you can use **Change direction** option to decide the direction in which the failover should happen.
4. If you're failing over to Azure and data encryption is enabled for the cloud (applies only when you have protected Hyper-v virtual machines from a VMM Server), in **Encryption Key** select the certificate that was issued when you enabled data encryption during setup on the VMM server.
5. Select **Shut-down machine before beginning failover** if you want Site Recovery to attempt to do a shutdown of source virtual machines before triggering the failover. Failover continues even if shut-down fails.

NOTE

If Hyper-v virtual machines are protected, the option to shut-down also tries to synchronize the on-premises data that has not yet been sent to the service before triggering the failover.

6. You can follow the failover progress on the **Jobs** page. Even if errors occur during an unplanned failover, the recovery plan runs until it is complete.
7. After the failover, validate the virtual machine by logging-in to it. If you want to switch to another recovery point of the virtual machine, then you can use **Change recovery point** option.
8. Once you are satisfied with the failed over virtual machine, you can **Commit** the failover. **Commit deletes all the recovery points available with the service** and **Change recovery point** option is no longer available.

Planned failover

Virtual machines/physical servers protected using Site Recovery also support **Planned failover**. 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.

NOTE

During failover of Hyper-v virtual machines from one on-premises site to another on-premises site, to come back to the primary on-premises site you have to first **reverse-replicate** the virtual machine back to primary site and then trigger a failover. If the primary virtual machine is not available, then before starting to **reverse-replicate** you have to restore the virtual machine from a backup.

Failover job

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	...

When a failover is triggered, it involves following steps:

1. Prerequisites check: This step ensures that all conditions required for failover are met
2. Failover: This step processes the data and makes it ready so that an Azure virtual machine can be created out of it. If you have chosen **Latest** recovery point, this step creates a recovery point from the data that has been sent to the service.
3. Start: This step creates an Azure virtual machine using the data processed in the previous step.

WARNING

Don't Cancel an in progress failover: Before failover is started, replication for the virtual machine is stopped. If you **Cancel** an in progress job, failover stops but the virtual machine will not start to replicate. Replication cannot be started again.

Time taken for failover to Azure

In certain cases, failover of virtual machines requires an extra intermediate step that usually takes around 8 to 10 minutes to complete. In the following cases, the time taken to failover will be higher than usual:

- VMware virtual machines using mobility service of version older than 9.8
- Physical servers
- VMware Linux virtual machines
- Hyper-V virtual machines protected as physical servers
- VMware virtual machines where following drivers are not present as boot drivers
 - storvsc
 - vmbus

- storflt
- intelide
- atapi
- VMware virtual machines that don't have DHCP service enabled irrespective of whether they are using DHCP or static IP addresses

In all the other cases, this intermediate step is not required and the time taken for the failover is lower.

Using scripts in Failover

You might want to automate certain actions while doing a failover. You can use scripts or [Azure automation runbooks](#) in [recovery plans](#) to do that.

Post failover considerations

Post failover you might want to consider the following recommendations:

Retaining drive letter after failover

To retain the drive letter on virtual machines after failover, you can set the **SAN Policy** for the virtual machine to **OnlineAll**. [Read more.](#)

Next steps

WARNING

Once you have failed over virtual machines and the on-premises data center is available, you should **Reprotect** VMware virtual machines back to the on-premises data center.

Use **Planned failover** option to **Fallback** Hyper-v virtual machines back to on-premises from Azure.

If you have failed over a Hyper-v virtual machine to another on-premises data center managed by a VMM server and the primary data center is available, then use **Reverse replicate** option to start the replication back to the primary data center.

Fail over and fail back physical servers replicated to Azure

7/9/2018 • 6 minutes to read • [Edit Online](#)

This tutorial describes how to fail over a physical server to Azure. After you've failed over, you fail the server back to your on-premises site when it's available.

Preparing for failover and fallback

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.

Failover and fallback has four stages:

1. **Fail over to Azure:** Fail machines over from the on-premises site to Azure.
2. **Reprotect Azure VMs:** Reprotect the Azure VMs, so that they start replicating back to on-premises VMware VMs.
3. **Fail over to on-premises:** Run a failover, to fail back from Azure.
4. **Reprotect on-premises VMs:** After data has failed back, reprotect the on-premises VMware VMs that you failed back to, so that they start replicating to Azure.

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.

Run a failover 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** (default): 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.

Create a process server in Azure

The process server receives data from the Azure VM, and sends it to the on-premises site. A low-latency network is required between the process server and the protected machine.

- For test purposes, if you have an Azure ExpressRoute connection, you can use the on-premises process server that's automatically installed on the configuration server.
- If you have a VPN connection, or you're running failback in a production environment, you must set up an Azure VM as a Azure-based process server for failback.
- Follow the instructions in [this article](#) to set up a process server in Azure.

Configure the master target server

By default, the master target server receives failback data. It runs on the on-premises configuration server.

- If the VMware VM to which you fail back is on an ESXi host that's managed by VMware vCenter Server, the master target server must have access to the VM's datastore (VMDK), to write replicated data to the VM disks. Make sure that the VM datastore is mounted on the master target's host, with read/write access.
- If the ESXi host that isn't managed by a vCenter server, Site Recovery service creates a new VM during reprottection. The VM is created on the ESX host on which you create the master target VM. 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.
- For physical machines that you fail back, you should complete discovery of the host on which the master target server is running, before you can reprotect the machine.
- 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 ESX host. When you fail back to an alternate location, the data is recovered to the same datastore and the same ESX host as that used by the on-premises master target server.
- You can't use Storage vMotion on the master target server. If you do, failback won't work, because the disks aren't available to it. Exclude the master target servers from your vMotion list.

Reprotect Azure VMs

This procedure presumes that the on-premises VM isn't available and you're reprotecting to an alternate location.

1. In **Settings > Replicated items**, right-click the VM 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 when the on-premises VM has been deleted, and you need to create new disks. This settings is

ignored if the disks already exist, 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 virtual machine from Azure 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.

Run a failover from Azure to on-premises

To replicate back to on-premises, a fallback policy is used. This policy is automatically created when you created a replication policy for replication to Azure:

- The policy is automatically associated with the configuration server.
- The policy can't be modified.
- The policy values are:
 - RPO threshold = 15 minutes
 - Recovery point retention = 24 hours
 - App-consistent snapshot frequency = 60 minutes

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. An app-consistent recovery point occurs before the most recent point in time, and it will cause some data loss. 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.
4. Right-click the machine, and click **Commit**. This triggers a job that removes the Azure VMs.
5. 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**.

After the reprottection finishes, the VM replicates back to Azure, and you can run a failover as required.

Fail back from Azure to an on-premises site

7/9/2018 • 5 minutes to read • [Edit Online](#)

This article describes how to fail back virtual machines from Azure Virtual Machines to an on-premises VMware environment. Follow the instructions in this article to fail back your VMware virtual machines or Windows/Linux physical servers after they've failed over from the on-premises site to Azure by using the [Failover in Azure Site Recovery](#) tutorial.

Prerequisites

- Make sure that you have read the details about the [different types of failback](#) and corresponding caveats.

WARNING

You can't fail back after you have either completed migration, moved a virtual machine to another resource group, or deleted the Azure virtual machine. If you disable protection of the virtual machine, you can't fail back.

WARNING

A Windows Server 2008 R2 SP1 physical server, if protected and failed over to Azure, can't be failed back.

NOTE

If you have failed over VMware virtual machines, you can't fail back to a Hyper-V host.

- Before you continue, complete the reprotect steps so that the virtual machines are in a replicated state and you can start a failover back to an on-premises site. For more information, see [How to reprotect from Azure to on-premises](#).
- Make sure that the vCenter is in a connected state before you do a failback. Otherwise, disconnecting disks and attaching them back to the virtual machine fails.
- During failover to Azure, the on-premises site might not be accessible, and the configuration server might be either unavailable or shut down. During reprotect and failback, the on-premises configuration server should be running and in a connected OK state.
- During failback, the virtual machine must exist in the configuration server database or failback won't succeed. Make sure that you take regularly scheduled backups of your server. If a disaster occurs, you need to restore the server with the original IP address for failback to work.
- The master target server should not have any snapshots before triggering reprotect/failback.

Overview of failback

After you have failed over to Azure, you can fail back to your on-premises site by executing the following steps:

- Reprotect the virtual machines on Azure so that they start to replicate to VMware virtual machines in your on-premises site. As part of this process, you also need to:
 - Set up an on-premises master target. Use a Windows master target for Windows virtual machines and a

[Linux master target](#) for Linux virtual machines.

- Set up a [process server](#).
 - Start [reprotect](#) to turn off the on-premises virtual machine and synchronize the Azure virtual machine's data with the on-premises disks.
2. After your virtual machines on Azure replicate to your on-premises site, you start a failover from Azure to the on-premises site.
 3. After your data fails back, you reprotect the on-premises virtual machines again so that they start replicating to Azure.

For a quick overview, watch the following video about how to fail back to an on-premises site:

Steps to fail back

IMPORTANT

Before you start failback, make sure that you finished reprottection of the virtual machines. The virtual machines should be in a protected state, and their health should be **OK**. To reprotect the virtual machines, read [How to reprotect](#).

1. On the replicated items page, select the virtual machine. Right-click it to select **Unplanned Failover**.
2. In **Confirm Failover**, verify the failover direction (from Azure). Then select the recovery point (latest, or the latest app consistent) that you want to use for the failover. The app consistent point is behind the latest point in time and causes some data loss.
3. During failover, Site Recovery shuts down the virtual machines on Azure. After you check that failback completed as expected, you can check that the virtual machines on Azure shut down.
4. **Commit** is required to remove the failed-over virtual machine from Azure. Right-click the protected item, and then select **Commit**. A job removes the failed-over virtual machines in Azure.

To what recovery point can I fail back the virtual machines?

During failback, you have two options to fail back the virtual machine/recovery plan.

- If you select the latest processed point in time, all virtual machines fail over to their latest available point in time. If there is a replication group within the recovery plan, each virtual machine of the replication group fails over to its independent latest point in time.

You can't fail back a virtual machine until it has at least one recovery point. You can't fail back a recovery plan until all its virtual machines have at least one recovery point.

NOTE

A latest recovery point is a crash-consistent recovery point.

- If you select the application-consistent recovery point, a single virtual machine failback recovers to its latest available application-consistent recovery point. In the case of a recovery plan with a replication group, each replication group recovers to its common available recovery point. Application-consistent recovery points can be behind in time, and there might be loss in data.

What happens to VMware tools post failback?

In the case of a Windows virtual machine, Site Recovery disables the VMware tools during failover. During failback of the Windows virtual machine, the VMware tools are reenabled.

Reprotect from on-premises to Azure

After failback finishes and you have started commit, the recovered virtual machines in Azure are deleted. Now, the virtual machine is back on the on-premises site, but it won't be protected. To start to replicate to Azure again, do the following:

1. Select **Vault > Setting > Replicated items**, select the virtual machines that failed back, and then select **Re-Protect**.
2. Enter the value of the process server that needs to be used to send data back to Azure.
3. Select **OK** to begin the reprotect job.

NOTE

After an on-premises virtual machine boots up, it takes some time for the agent to register back to the configuration server (up to 15 minutes). During this time, reprotect fails and returns an error message stating that the agent isn't installed. Wait for a few minutes, and then try reprotect again.

Next steps

After the reprotect job finishes, the virtual machine replicates back to Azure, and you can do a [failover](#) to move your virtual machines to Azure again.

Reprotect machines from Azure to an on-premises site

7/30/2018 • 12 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.

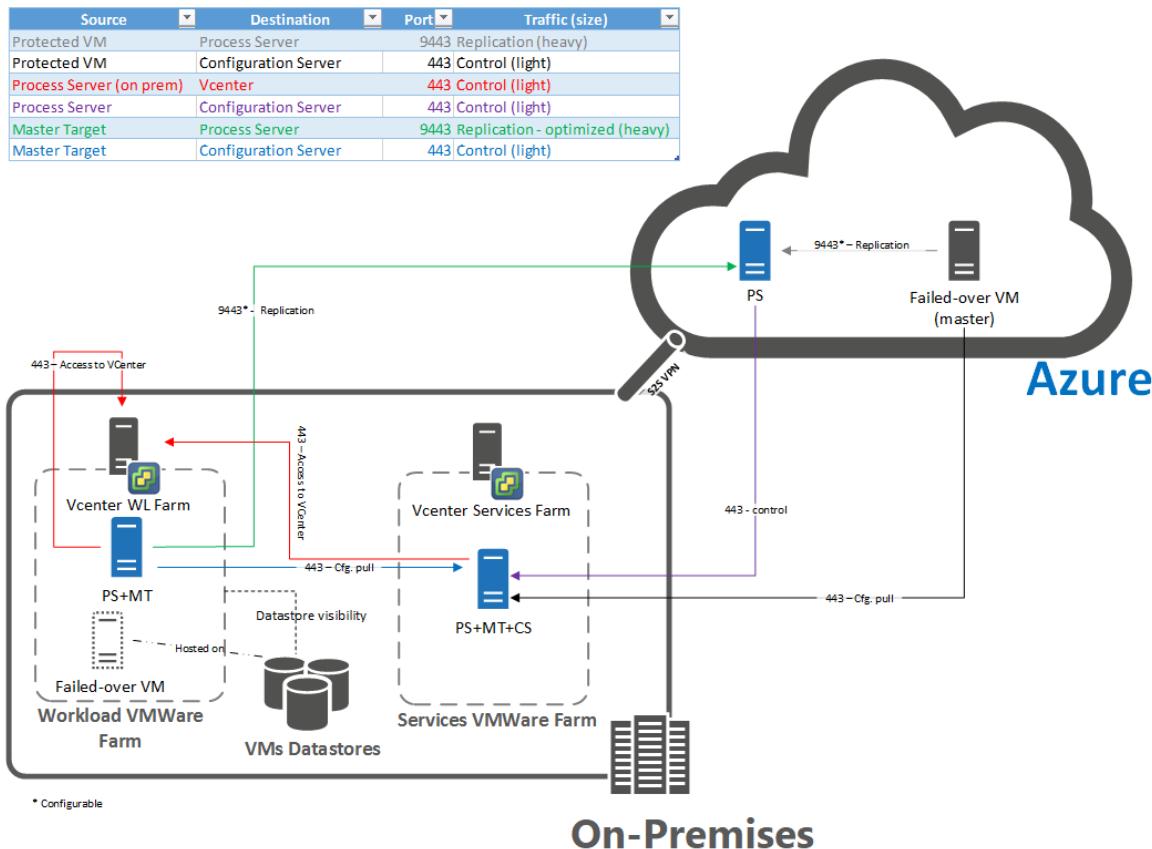
For a quick overview, watch the following video about how to fail over from Azure to an on-premises site.

Before you begin

If you used a template to create your virtual machines, ensure that each virtual machine has its own UUID for the disks. If the on-premises virtual machine's UUID clashes with the UUID of the master target because both were created from the same template, reprottection fails. Deploy another master target that wasn't created from the same template. Note the following information:

- If you are trying to fail back to an alternate vCenter, make sure that your new vCenter and the master target server are discovered. A typical symptom is that the datastores aren't accessible or aren't visible in the **Reprotect** dialog box.
- To replicate back to on-premises, you need a failback policy. This policy is automatically created when you create a forward direction policy. Note the following information:
 - This policy is auto associated with the configuration server during creation.
 - This policy isn't editable.
 - The set values of the policy are (RPO Threshold = 15 Mins, Recovery Point Retention = 24 Hours, App Consistency Snapshot Frequency = 60 Mins).
- During reprottection and failback, the on-premises configuration server must be running and connected.
- If a vCenter server manages the virtual machines to which you'll fail back, make sure that you have the [required permissions](#) for discovery of VMs on vCenter servers.
- Delete snapshots on the master target server before you reprotect. If snapshots are present on the on-premises master target or on the virtual machine, reprottection fails. The snapshots on the virtual machine are automatically merged during a reprotect job.
- All virtual machines of a replication group must be of the same operating system type (either all Windows or all Linux). A replication group with mixed operating systems currently isn't supported for reprotect and failback to on-premises. This is because the master target must be of the same operating system as the virtual machine. All the virtual machines of a replication group must have the same master target.
- A configuration server is required on-premises when you fail back. During failback, the virtual machine must exist in the configuration server database. Otherwise, failback is unsuccessful. Make sure that you make regularly scheduled backups of your configuration server. If there's a disaster, restore the server with the same IP address so that failback works.
- Reprotection and failback require a site-to-site (S2S) VPN to replicate data. Provide the network so that the failed-over virtual machines in Azure can reach (ping) the on-premises configuration server. You also might want to deploy a process server in the Azure network of the failed-over virtual machine. This process server must also be able to communicate with the on-premises configuration server.

- Make sure that you open the following ports for failover and fallback:



- Read all the [prerequisites for ports and URL whitelisting](#).

Deploy a process server in Azure

You might need a process server in Azure before you fail back to your on-premises site:

- The process server receives data from the protected virtual machine in Azure, and then sends data to the on-premises site.
- A low-latency network is required between the process server and the protected virtual machine. In general, you need to consider latency when deciding whether you need a process server in Azure:
 - If you have an Azure ExpressRoute connection set up, you can use an on-premises process server to send data because the latency between the virtual machine and the process server is low.
 - However, if you have only a S2S VPN, we recommend deploying the process server in Azure.
 - We recommend using an Azure-based process server during failback. The replication performance is higher if the process server is closer to the replicating virtual machine (the failed-over machine in Azure). For a proof of concept, you can use the on-premises process server and ExpressRoute with private peering.

To deploy a process server in Azure:

1. If you need to deploy a process server in Azure, see [Set up a process server in Azure for failback](#).
2. The Azure VMs send replication data to the process server. Configure networks so that the Azure VMs can reach the process server.
3. Remember that replication from Azure to on-premises can happen only over the S2S VPN or over the private peering of your ExpressRoute network. Ensure that enough bandwidth is available over that network channel.

Deploy a separate master target server

The master target server receives failback data. By default, the master target server runs on the on-premises

configuration server. However, depending on the volume of failed-back traffic, you might need to create a separate master target server for failback. Here's how to create one:

- [Create a Linux master target server](#) for failback of Linux VMs. This is required.
- Optionally, create a separate master target server for Windows VM failback. To do this, run Unified Setup again, and select to create a master target server. [Learn more](#).

After you create a master target server, do the following tasks:

- If the virtual machine is present on-premises on the vCenter server, the master target server needs access to the on-premises virtual machine's Virtual Machine Disk (VMDK) file. Access is required to write the replicated data to the virtual machine's disks. Ensure that the on-premises virtual machine's datastore is mounted on the master target's host with read/write access.
- If the virtual machine isn't present on-premises on the vCenter server, the Site Recovery service needs to create a new virtual machine during reprottection. This virtual machine is created on the ESX host on which you create the master target. Choose the ESX host carefully, so that the failback virtual machine is created on the host that you want.
- You can't use Storage vMotion for the master target server. Using Storage vMotion for the master target server might cause the failback to fail. The virtual machine can't start because the disks aren't available to it. To prevent this from occurring, exclude the master target servers from your vMotion list.
- If a master target undergoes a Storage vMotion task after reprottection, the protected virtual machine disks that are attached to the master target migrate to the target of the vMotion task. If you try to fail back after this, detachment of the disk fails because the disks are not found. It then becomes hard to find the disks in your storage accounts. You need to find them manually and attach them to the virtual machine. After that, the on-premises virtual machine can be booted.
- Add a retention drive to your 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 virtual machine replicates back to the on-premises site. Following are some criteria of a retention drive. If these criteria 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 target of replication.
 - The volume isn't in lock mode.
 - The volume isn't a cache volume. The master target installation can't exist on that 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.
- You must add a new drive if you're using an existing process server/configuration server machine or a scale or process server/master target server machine. The new drive must meet the preceding requirements. 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 also refresh the configuration server if the drive doesn't appear after 15 minutes.
- 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.
- Set the `disk.EnableUUID=true` setting in the configuration parameters of the master target virtual machine 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.
- The ESX host on which the master target is created must have at least one virtual machine file system (VMFS) datastore attached to it. If no VMFS datastores are attached, the **Datastore** input on the reprotect page is

empty and you can't proceed.

- The master target server can't have snapshots on the disks. If there are snapshots, reprotector and failback fail.
- The master target can't have a Paravirtual SCSI controller. The controller can only be an LSI Logic controller. Without an LSI Logic controller, reprotector fails.
- For any instance, the master target can have at most 60 disks attached to it. If the number of virtual machines being reprotected to the on-premises master target has more than a total number of 60 disks, reprotects to the master target begin to fail. Ensure that you have enough master target disk slots, or deploy additional master target servers.

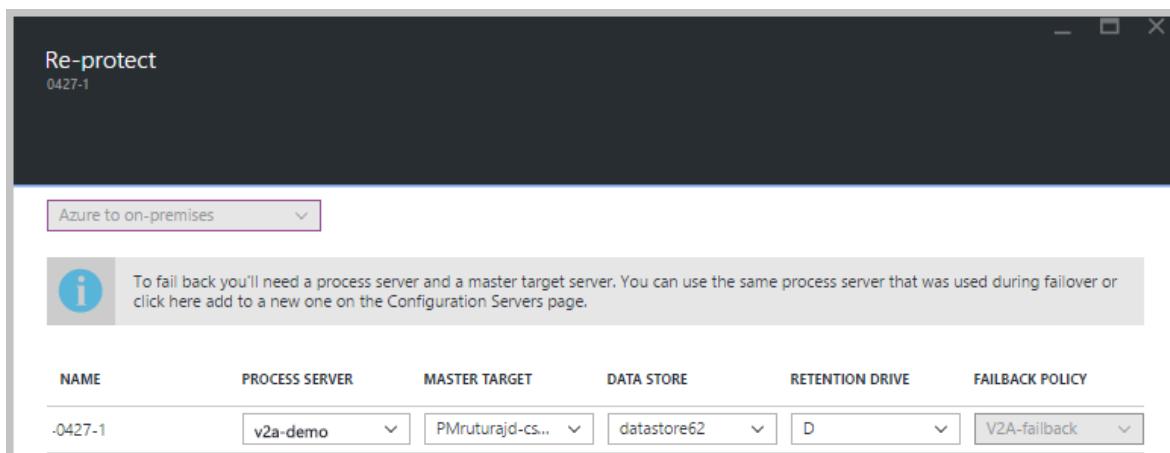
Enable reprotector

After a virtual machine boots in Azure, 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 try reprotector again:

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 failback policy is automatically selected.
7. Select **OK** to begin reprotector. A job begins to replicate the virtual machine from Azure to the on-premises site. You can track the progress on the **Jobs** tab. When the reprotector succeeds, the virtual machine enters a protected state.

Note the following information:

- If you want to recover to an alternate location (when the on-premises virtual machine is deleted), 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 failback protection plan use the same datastore as the master target server. A new virtual machine is then created in vCenter.
- If you want to recover the virtual machine on Azure to an existing on-premises virtual machine, mount the on-premises virtual machine's datastores with read/write access on the master target server's ESXi host.



- You can also reprotect at the level of a recovery plan. A replication group can be reprotected only through

a recovery plan. When you reprotect by using a recovery plan, you must provide the values for every protected machine.

- Use the same master target server to reprotect a replication group. If you use a different master target server to reprotect a replication group, the server can't provide a common point in time.
- The on-premises virtual machine is turned off during reprottection. This helps ensure data consistency during replication. Don't turn on the virtual machine after reprottection finishes.

Common issues

- Currently, Site Recovery supports failing back only to a VMFS or vSAN datastore. An NFS datastore isn't supported. Due to this limitation, the datastore selection input on the reprotect screen is empty for NFS datastores, or it shows the vSAN datastore but fails during the job. If you intend to fail back, you can create a VMFS datastore on-premises and fail back to it. This failback causes a full download of the VMDK.
- 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.

Next steps

After the virtual machine has entered a protected state, you can [initiate a failback](#). The failback shuts down the virtual machine in Azure and boots the on-premises virtual machine. Expect some downtime for the application. Choose a time for failback when the application can tolerate downtime.

Manage the configuration server for VMware VMs

7/30/2018 • 5 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.

Modify VMware settings

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, select **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.

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. Enter the new credentials, and then select **OK**.

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	Edit	Delete
Windows	MyWinCreds	fareast\anoopkv	Edit	Delete
Linux	LinuxRoot	root	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.

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 reregister 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
```

Upgrade the configuration server

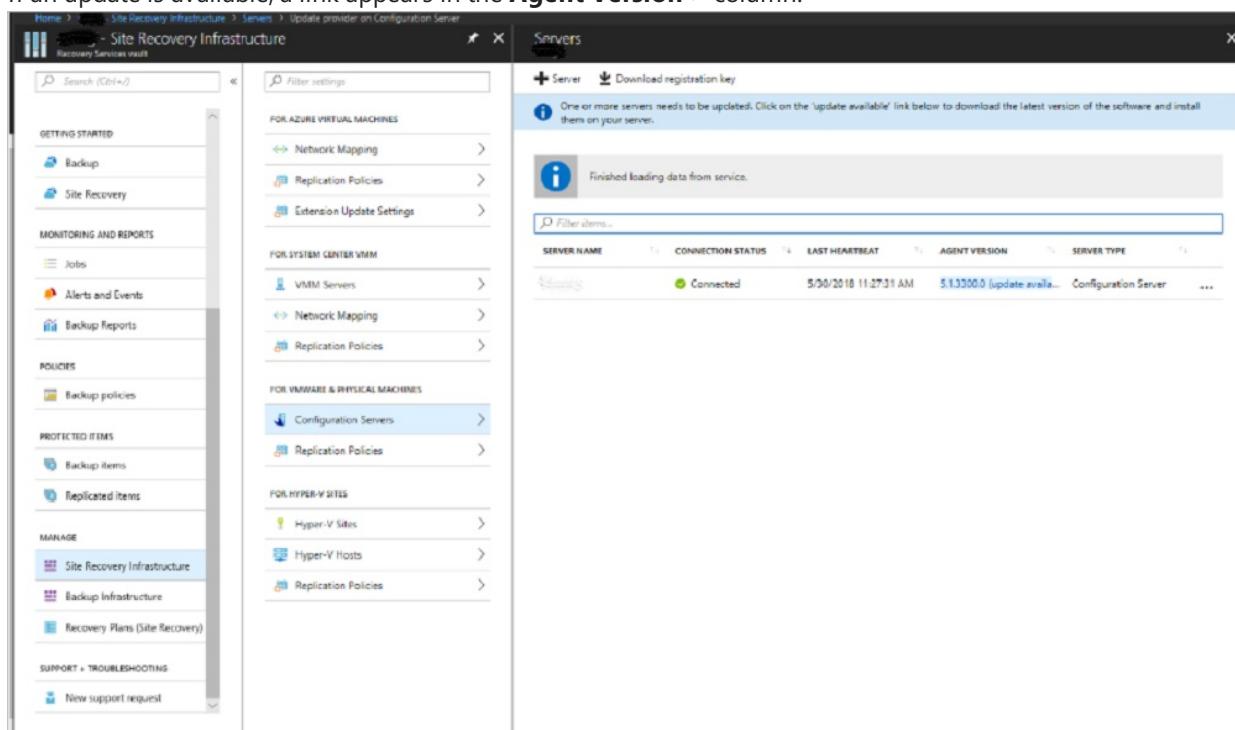
You run update rollups to update the configuration server. Updates can be applied for up to N-4 versions. For example:

- 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.

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. 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.



3. Download the update installer file to the configuration server.

The screenshot shows two windows side-by-side. The left window is titled 'Servers' and displays a table of servers. One server row has a green 'Connected' status and an 'update available' link in the 'AGENT VERSION' column. The right window is titled 'Update provider on Configuration Server' and contains steps for updating the configuration server, with a red box highlighting the 'Click here to download...' link.

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.

The screenshot shows the 'Installation Progress' window of the Azure Site Recovery setup. On the left, a vertical list of steps is shown, with 'Installation Progress' highlighted. On the right, a table lists the installation steps and their status. All steps are marked as 'Done' with green checkmarks. A 'Finish' button is at the bottom right.

Steps	Status
Install third-party components	Done
Install configuration server and process server	Done
Install Microsoft azure site recovery provider	Done
Install master target server	Done
Install Microsoft azure recovery services agent	Done
Install Azure Site Recovery Configuration Manager	Done
Validating server configuration	Done

7. Click **Finish** to close the installer.

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 'CONFIGSRV01' Configuration Server interface. At the top right, there is a 'More' button with a red box around it. A context menu is open over a vault entry, with the 'Delete' option highlighted by a red box. The vault details shown are:

Recovery Services vault	Connection
ConsotoVault	Connected
IP address	Last heartbeat
10.10.20.66	2/14/2017
Configuration Server version	Provider version
9.3.0.0	5.1.1700.0
Connected agents	Server ID
4	aeb54dc5-6e9d-4e16-89e7-49985f282072
Protected items	
4	

Below this, there is a section for 'Associated servers' with three entries:

NAME	STATUS	SERVER ROLE	VERSION	LAST HEART BEAT	...
▶ Process Ser...					...
▶ vCenter Ser...					...
▶ Master Targ...					...

At the bottom, there is a 'Configuration Server health' section with the following status items:

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
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-AzureRmAccount
```

3. Select the vault subscription.

```
Get-AzureRmSubscription -SubscriptionName <your subscription name> | Select-AzureRmSubscription
```

4. Set the vault context.

```
$vault = Get-AzureRmRecoveryServicesVault -Name <name of your vault>
Set-AzureRmSiteRecoveryVaultSettings -ARSVault $vault
```

5. Retrieve the configuration server.

```
$fabric = Get-AzureRmSiteRecoveryFabric -FriendlyName <name of your configuration server>
```

6. Delete the configuration server.

```
Remove-AzureRmSiteRecoveryFabric -Fabric $fabric [-Force]
```

NOTE

You can use the **-Force** option in Remove-AzureRmSiteRecoveryFabric 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**.

Next steps

Review the tutorials for setting up disaster recovery of [VMware VMs](#) to Azure.

Manage the configuration server for physical server disaster recovery

7/10/2018 • 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.

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 Windows Server 2016
Operating system locale	English (US)
VMware vSphere PowerCLI version	PowerCLI 6.0
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 - Enable Anonymous Authentication - Enable FastCGI setting - No pre-existing website/application listening on port 443

COMPONENT	REQUIREMENT
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"> - *.accesscontrol.windows.net - *.backup.windowsazure.com - *.store.core.windows.net - *.blob.core.windows.net - *.hypervrecoverymanager.windowsazure.com - https://management.azure.com - *.services.visualstudio.com - <p>https://dev.mysql.com/get/Downloads/MySQLInstaller/mysql-installer-community-5.7.20.0.msi (not required for Scale-out Process Servers)</p> <ul style="list-style-type: none"> - time.nist.gov - time.windows.com
Ports	443 (Control channel orchestration) 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.

The screenshot shows the 'Server' section of the Azure Site Recovery portal. On the left, there's a message 'Finished loading data from service.' and a 'Filter items...' search bar. A table header includes columns for SERVER NAME, CONNECTION STATUS, LAST HEARTBEAT, AGENT VERSION, and SERVER TYPE. Below the table, a note says 'No servers are registered yet. Click on + Servers to read more on how to get started'. On the right, a sidebar titled 'Server type' shows 'Configuration Server' selected. It contains a message about adding a configuration server taking 15 minutes to 30 minutes, a link to register the Configuration Server (On-premises), and a numbered list of 8 steps for setting up the Configuration Server. Step 4 includes a 'Download' button.

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 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**.

The screenshot shows the 'Before You Begin' step of the Azure Site Recovery Unified Setup wizard. The left sidebar lists steps: Before You Begin, Third Party Software License, Registration, Configuration Server Details, Internet Settings, Prerequisites Check, MySQL Configuration, Environment Details, Install Location, Network Selection, Summary, and Installation Progress. The main pane describes the wizard's purpose: setting up protection for workloads running on physical servers and VMware virtual machines by replicating them to Azure. It offers two options:

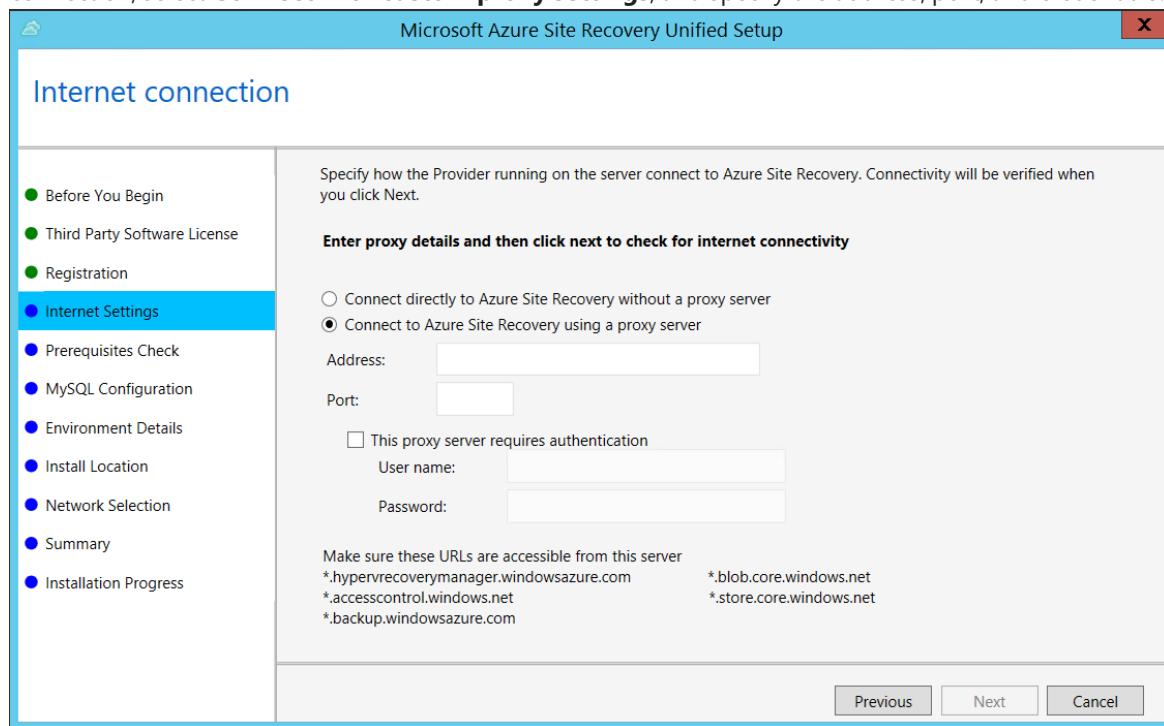
- Install the configuration server and process server**: Select this option if you are setting up Site Recovery for the first time.
- Add additional process servers to scale out deployment**: Select this option to add more process servers to handle the replication load.

At the bottom are 'Previous', 'Next', and 'Cancel' buttons.

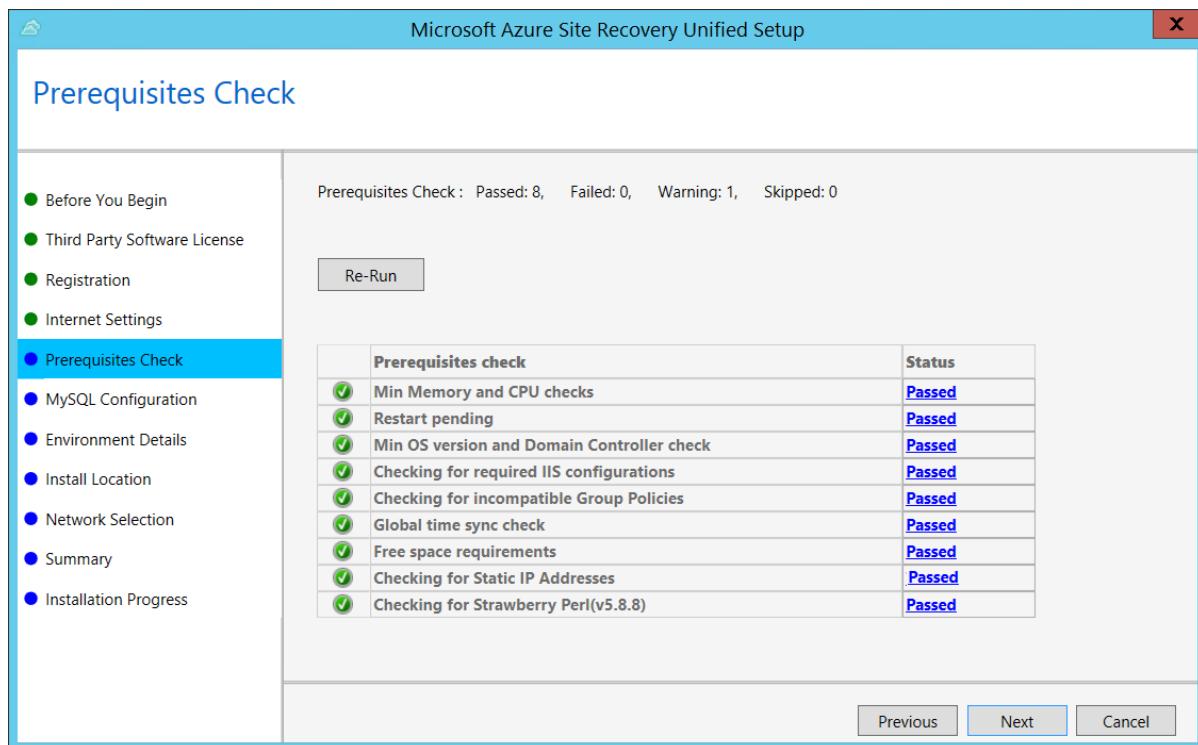
3. In **Third Party Software License**, click **I Accept** to download and install MySQL.
4. In **Internet Settings**, specify how the Provider running on the configuration server connects to Azure Site Recovery over the Internet. Make sure you've allowed the required URLs.
 - If you want to connect 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.

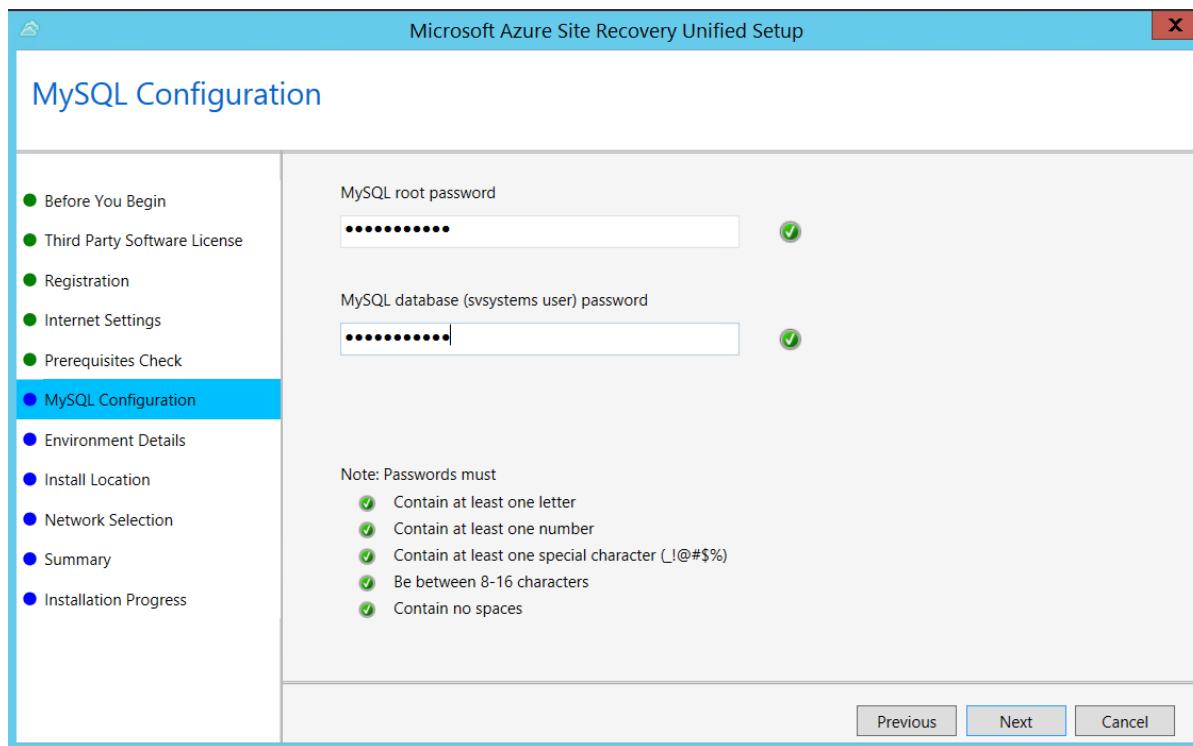
- If the existing proxy requires authentication, or if you want to use a custom proxy for the Provider connection, select **Connect with custom proxy settings**, and specify the address, port, and credentials.



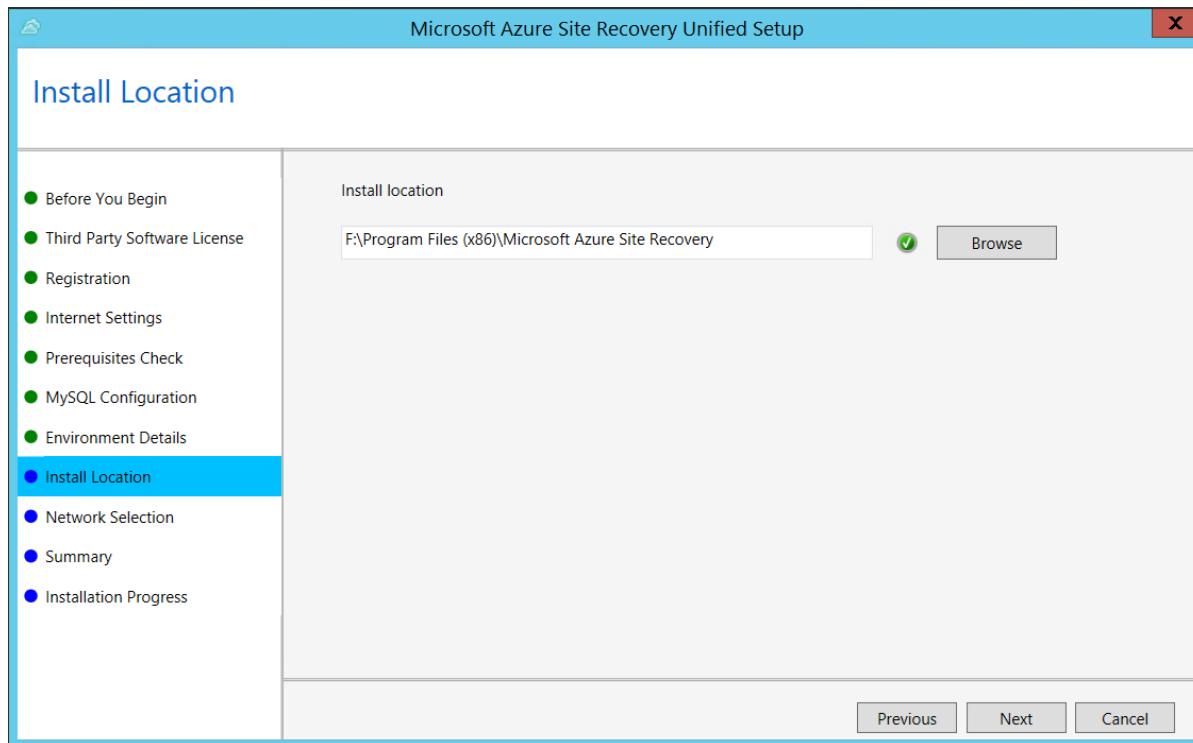
- In **Prerequisites Check**, Setup runs a check to make sure that installation can run. If a warning appears about the **Global time sync check**, verify that the time on the system clock (**Date and Time** settings) is the same as the time zone.



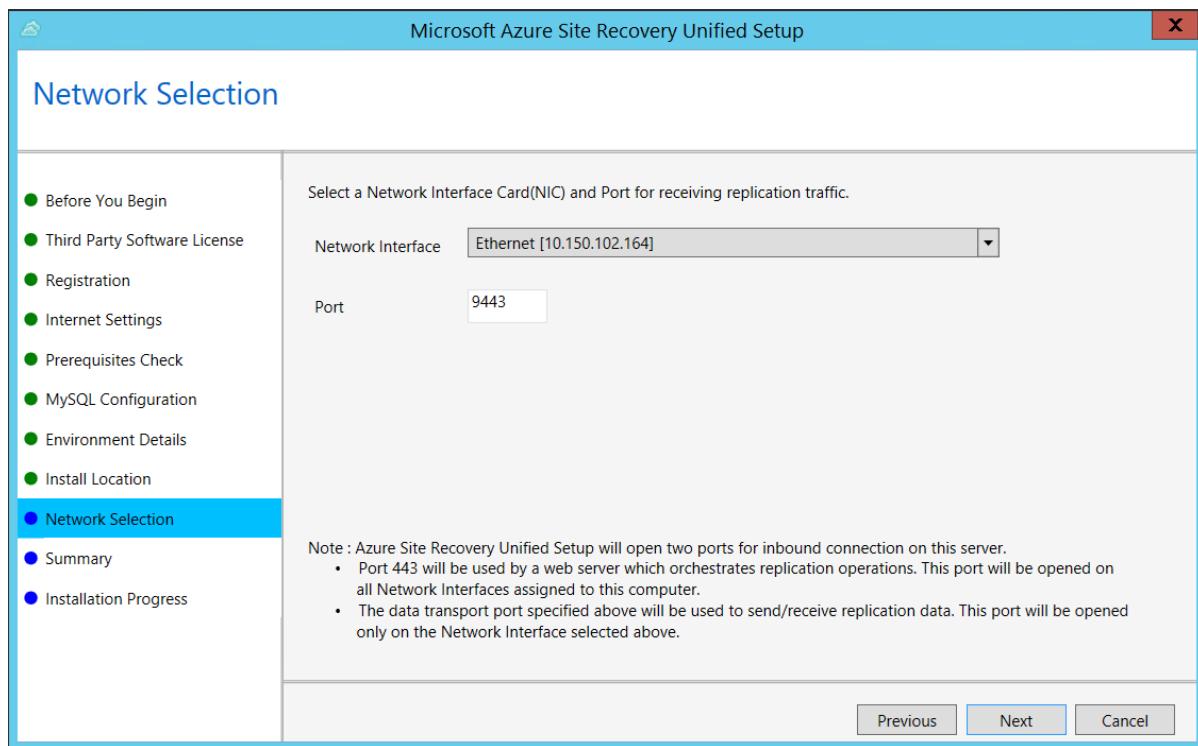
- In **MySQL Configuration**, create credentials for logging on to the MySQL server instance that is installed.



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**, 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.



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 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 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

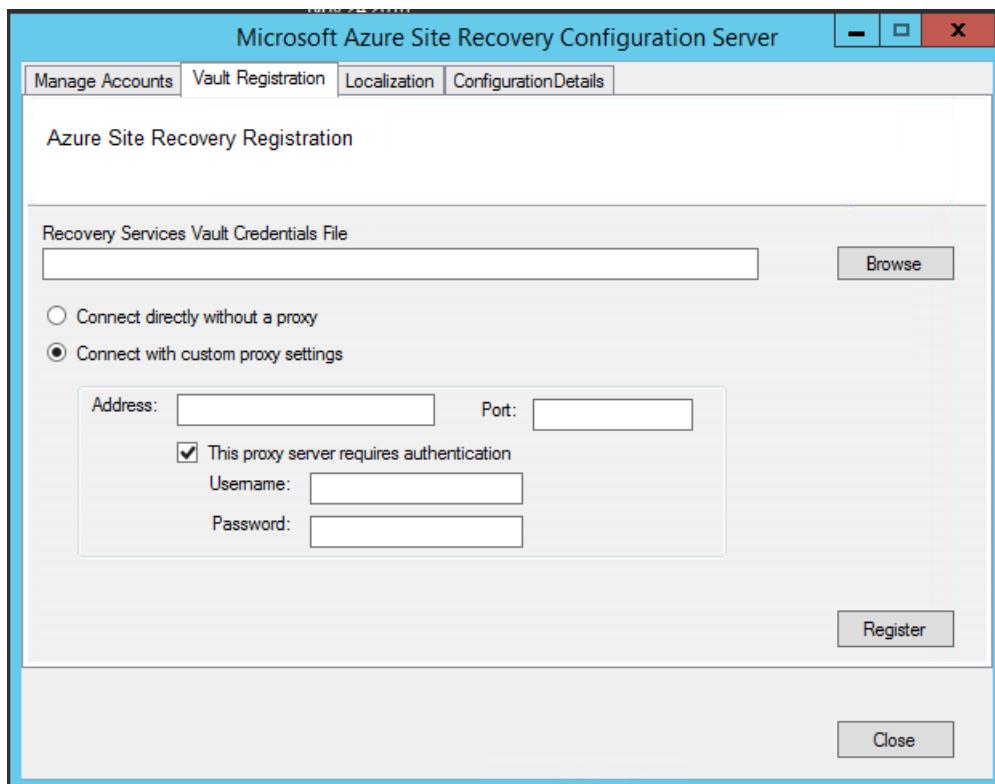
ProxySettingsFilePath parameter.

```
[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.
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:

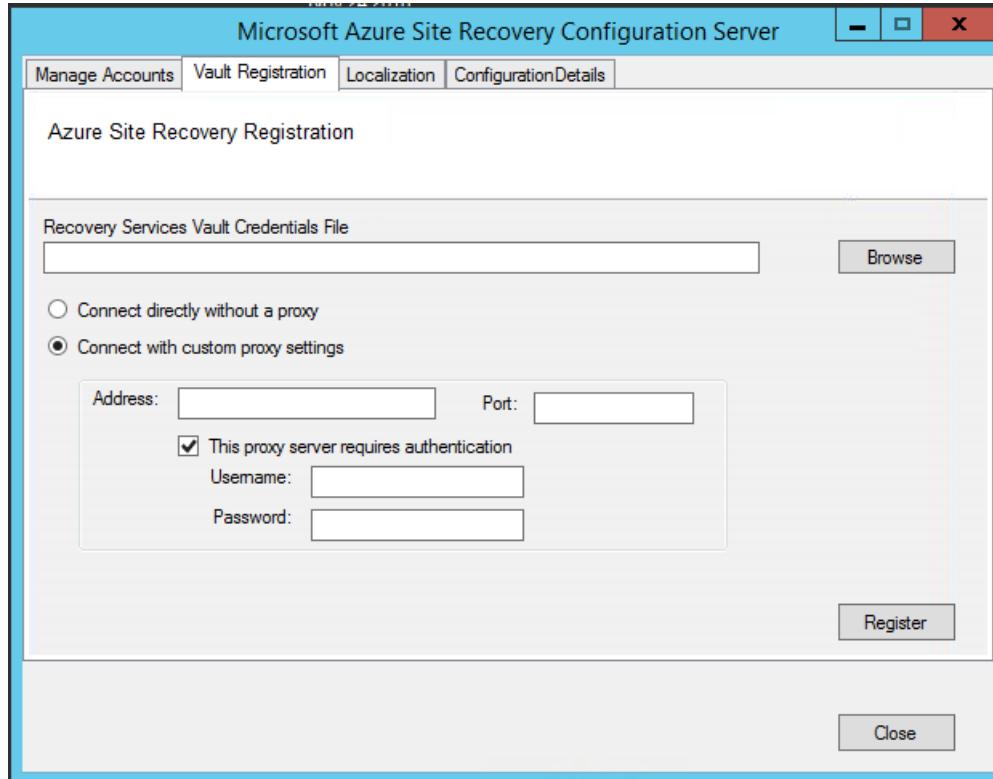
```
$pwd = ConvertTo-SecureString -String MyProxyUserPassword
Set-OBMachineSetting -ProxyServer http://myproxyserver.domain.com -ProxyPort PortNumber - ProxyUserName
domain\username -ProxyPassword $pwd
net stop obengine
net start obengine
```

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 an 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 your Azure account using the command

```
Connect-AzureRmAccount
```

3. Select the subscription under which the vault is present

```
Get-AzureRmSubscription -SubscriptionName <your subscription name> | Select-AzureRmSubscription
```

4. Now set up your vault context

```
$vault = Get-AzureRmRecoveryServicesVault -Name <name of your vault>
Set-AzureRmSiteRecoveryVaultSettings -ARSVault $vault
```

5. Get select your configuration server

```
$fabric = Get-AzureRmSiteRecoveryFabric -FriendlyName <name of your configuration server>
```

6. Delete the Configuration Server

```
Remove-AzureRmSiteRecoveryFabric -Fabric $fabric [-Force]
```

NOTE

The **-Force** option in the Remove-AzureRmSiteRecoveryFabric cmdlet 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 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

- In the vault, open **Site Recovery Infrastructure > Configuration Server**, and click the required configuration server.
- The expiry date appears under **Configuration Server health**
- Click **Renew Certificates**.

Common issues

Installation failures

SAMPLE ERROR MESSAGE	RECOMMENDED ACTION
ERROR Failed to load Accounts. Error: System.IO.IOException: Unable to read data from the transport connection when 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
09:20:06: InnerException.Type: SrsRestApiClientLib.AcsException,InnerException. Message: ACS50008: SAML token is invalid. Trace ID: 1921ea5b-4723-4be7-8087-a75d3f9e1072 Correlation ID: 62fea7e6-2197-4be4-a2c0-71ceb7aa2d97> Timestamp: 2016-12-12 14:50:08Z	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.
09:35:27 : 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. Trace ID: e5ad1af1-2d39-4970-8eef-096e325c9950 Correlation ID: abe9deb8-3e64-464d-8375-36db9816427a Timestamp: 2016-05-19 01:35:39Z	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.
06:28:45:Failed to create certificate 06:28:45:Setup cannot proceed. A certificate required to authenticate to Site Recovery cannot be created. Rerun Setup	Ensure you are running setup as a local administrator.

Next steps

Review the tutorials for setting up disaster recovery of [physical servers](#) to Azure.

Manage process servers

7/23/2018 • 3 minutes to read • [Edit Online](#)

By default the process server used when you're replicating VMware VMs or physical servers to Azure is installed on the on-premises configuration server machine. There are a couple of instances in which you need to set up a separate process server:

- For large deployments, you might need additional on-premises process servers to scale capacity.
- For failback, you need a temporary process server set up in Azure. You can delete this VM when failback is done.

This article summarizes typical management tasks for these additional process servers.

Upgrade a process server

Upgrade an process server running on premises, or in Azure (for failback purposes), as follows:

1. Sign in to the process server as an Administrator.
2. Download the latest version of the [Unified Setup](#).
3. Double-click the installer to launch the update process.
4. The installer will detect the various components that are installed and upgrade them to the latest version.

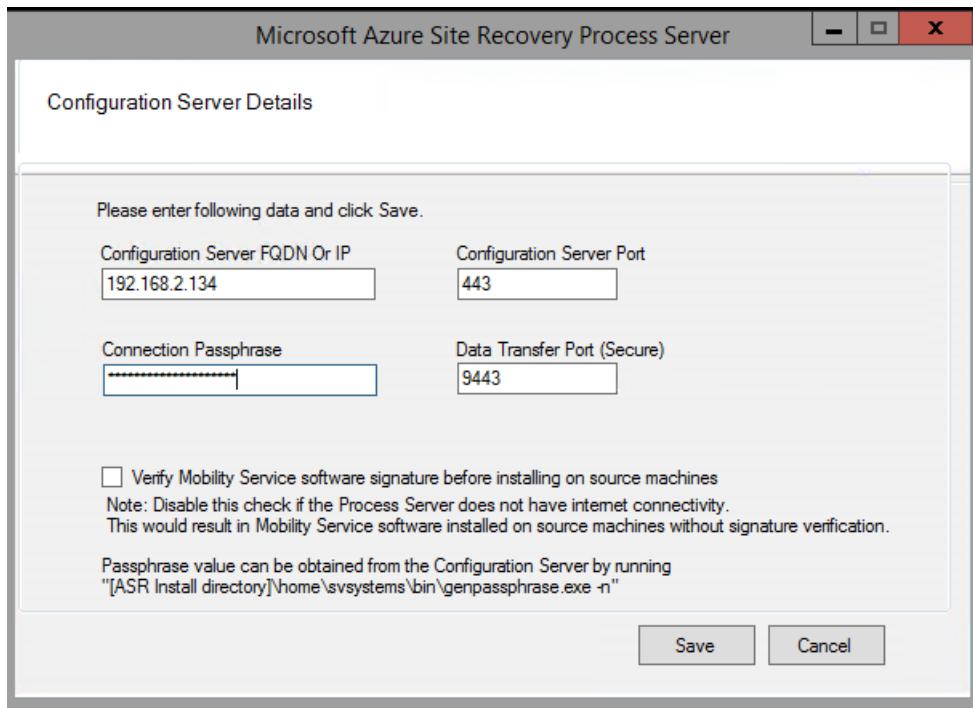
NOTE

Typically, when you use the Azure Gallery Image to create a process server in Azure for the purposes of failback, it's running the latest version available. The Site Recovery teams release fixes and enhancements on a regular basis, and we recommend you keep process servers up-to-date.

Reregister a process server

If you need to reregister a process server running on-premises, or in Azure, with the configuration server, do the following:

- Connect to the Process Server virtual machine using Remote Desktop Connection.
- You can launch the cspconfigtool.exe by clicking on the shortcut available on the desktop. (The tool will be automatically launched if this the first time you are logging into the process sever).
 - Configuration Server's fully qualified name (FQDN) or IP Address
 - Port on which the Configuration server is listening on. The value should be 443
 - Connection Passphrase to connect to the configuration server.
 - Data Transfer port to be configured for this Process Server. Leave the default value as is unless you have changed it to a different port number in your environment.



- Click the save button to save the configuration and register the Process Server.

After you've saved the settings, do the following:

- On the process server, open an administrator command prompt.
- 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 the process server uses a proxy to connect to Site Recovery in Azure, use this procedure if you need to modify existing proxy settings.

- Log onto the process server machine.
- 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
```
- Browse to folder **%PROGRAMDATA%\ASR\Agent**, and run the following command:

```
cmd  
cdpcli.exe --registermt  
  
net stop obengine  
  
net start obengine  
  
exit
```

Remove a process server

The steps to unregister a process server differs depending on its connection status with the Configuration Server.

Unregister a process server that is in a connected state

1. Remote into the process server as an Administrator.
2. Launch the **Control Panel** and open **Programs > Uninstall a program**
3. Uninstall a program by the name **Microsoft Azure Site Recovery Configuration/Process Server**
4. Once step 3 is completed, you can uninstall **Microsoft Azure Site Recovery Configuration/Process Server Dependencies**

Unregister a process server that is in a disconnected state

WARNING

Use the below steps should be used if there is no way to revive the virtual machine on which the Process Server was installed.

1. Sign in to your configuration server as an Administrator.
2. Open an Administrative command prompt and browse to the directory `%ProgramData%\ASR\home\svsystems\bin`.
3. Now run the command.

```
perl Unregister-ASRComponent.pl -IPAddress <IP_of_Process_Server> -Component PS
```

4. The above command will provide the list of process server(s) (can be more than one, in case of duplicate entries) with serial number(S.No), IP address (IP), name of the VM on which process server is deployed (Name), Heart beat of the VM (Heartbeat) as shown below.

```
=====
S.No   IP       Name      Heartbeat
=====
```

```
1    [REDACTED] testVM 2018-08-02 11:54:38
=====
```

Please choose one of the above servers to un-register

5. Now, enter the serial number of the process server you wish to un-register.
6. This will purge the details of the process server from the system and will display the message: **Successfully unregistered server-name> (server-IP-address)**

Manage VMware vCenter servers

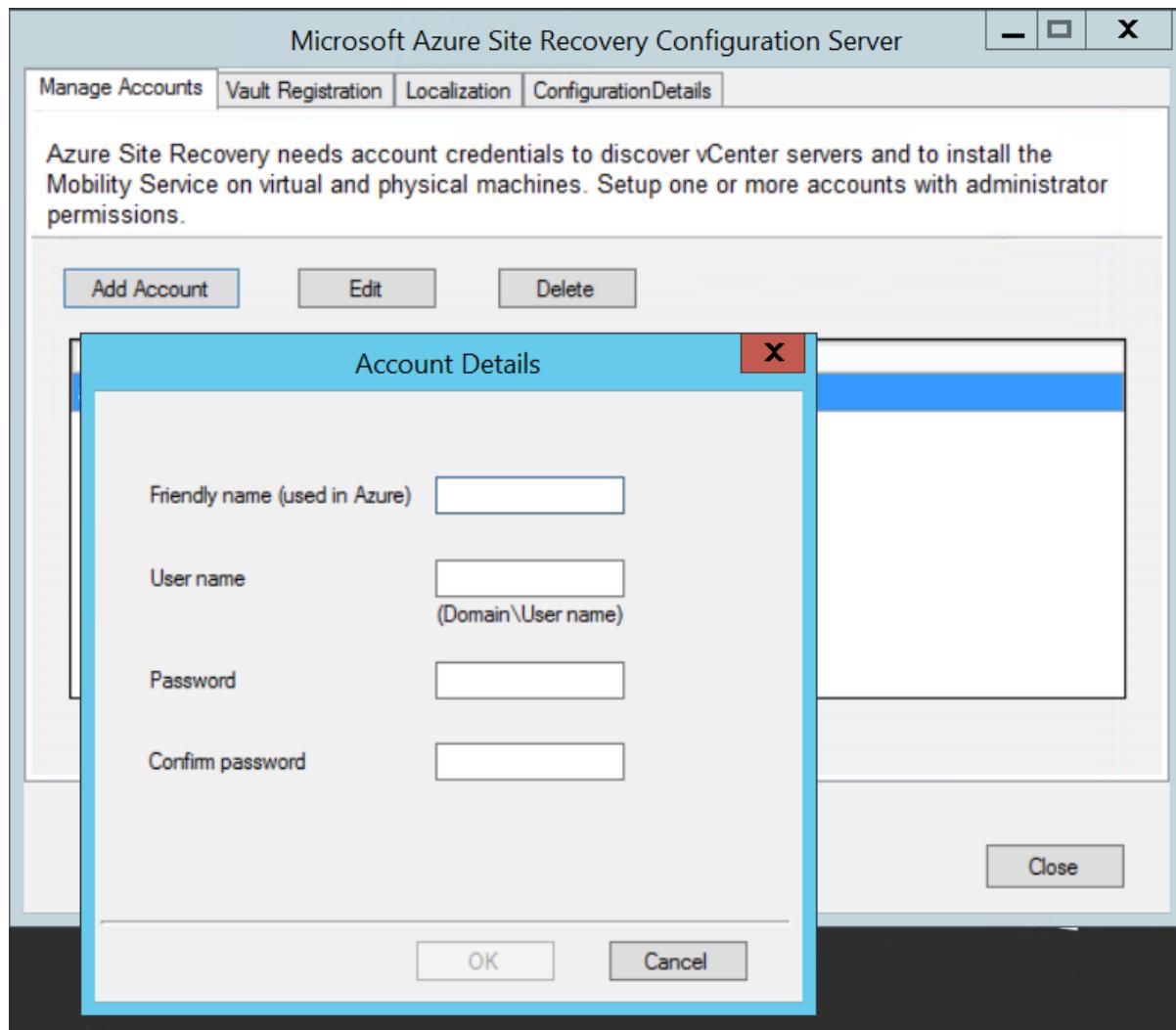
7/10/2018 • 3 minutes to read • [Edit Online](#)

This article discusses the various Site Recovery operations that can be performed on a VMware vCenter. Verify the [prerequisites](#) before you start.

Set up an account for automatic discovery

Site Recovery needs access to VMware for the process server to automatically discover virtual machines, and for failover and failback of virtual machines. Create an account for access as follows:

1. Log onto the configuration server machine.
2. Open the launch the cspconfigtool.exe using the Desktop shortcut.
3. Click **Add Account** on the **Manage Account** tab.



4. Provide the account details, and click **OK** to add it. The account should have the privileges summarized in the following table.

It takes about 15 minutes for the account information to be synced up with the Site Recovery service.

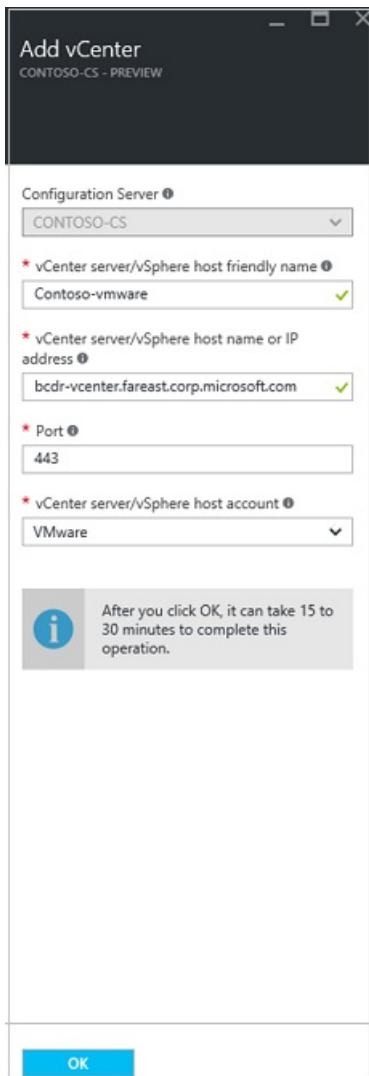
Account permissions

Task	Account	Permissions	Details
Automatic discovery/Migrate (without failback)	You need at least a read-only user	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. To restrict access, assign the No access role with the Propagate to child object, to the child objects (vSphere hosts, datastores, virtual machines, and networks).
Replication/Failover	You need at least a read-only user	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. To restrict access, assign the No access role with the Propagate to child object to the child objects (vSphere hosts, datastores, virtual machines, and networks). Useful for migration purposes, but not full replication, failover, failback.

Task	Account	Permissions	Details
Replication/failover/failback	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 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 Virtual machine -> Configuration Virtual machine -> Interact -> answer question, device connection, configure CD media, configure floppy media, power off, power on, VMware tools install Virtual machine -> Inventory -> Create, register, unregister Virtual machine -> Provisioning -> Allow virtual machine download, allow virtual machine files upload Virtual machine -> Snapshots -> Remove snapshots	User assigned at datacenter level, and has access to all the objects in the datacenter. To restrict access, assign the No access role with the Propagate to child object, to the child objects (vSphere hosts, datastores, virtual machines, and networks).

Add VMware server to the vault

- On the Azure portal, open your vault > **Site Recovery Infrastructure > Configuration Servers**, and open the configuration server.
- On the **Details** page, click **+vCenter**.
 - In **Add vCenter**, specify a friendly name for the vSphere host or vCenter server, and then specify the IP address or FQDN of the server. Leave the port as 443 unless your VMware servers are configured to listen for requests on a different port. Select the account that is to connect to the VMware vCenter or vSphere ESXi server. Click **OK**.



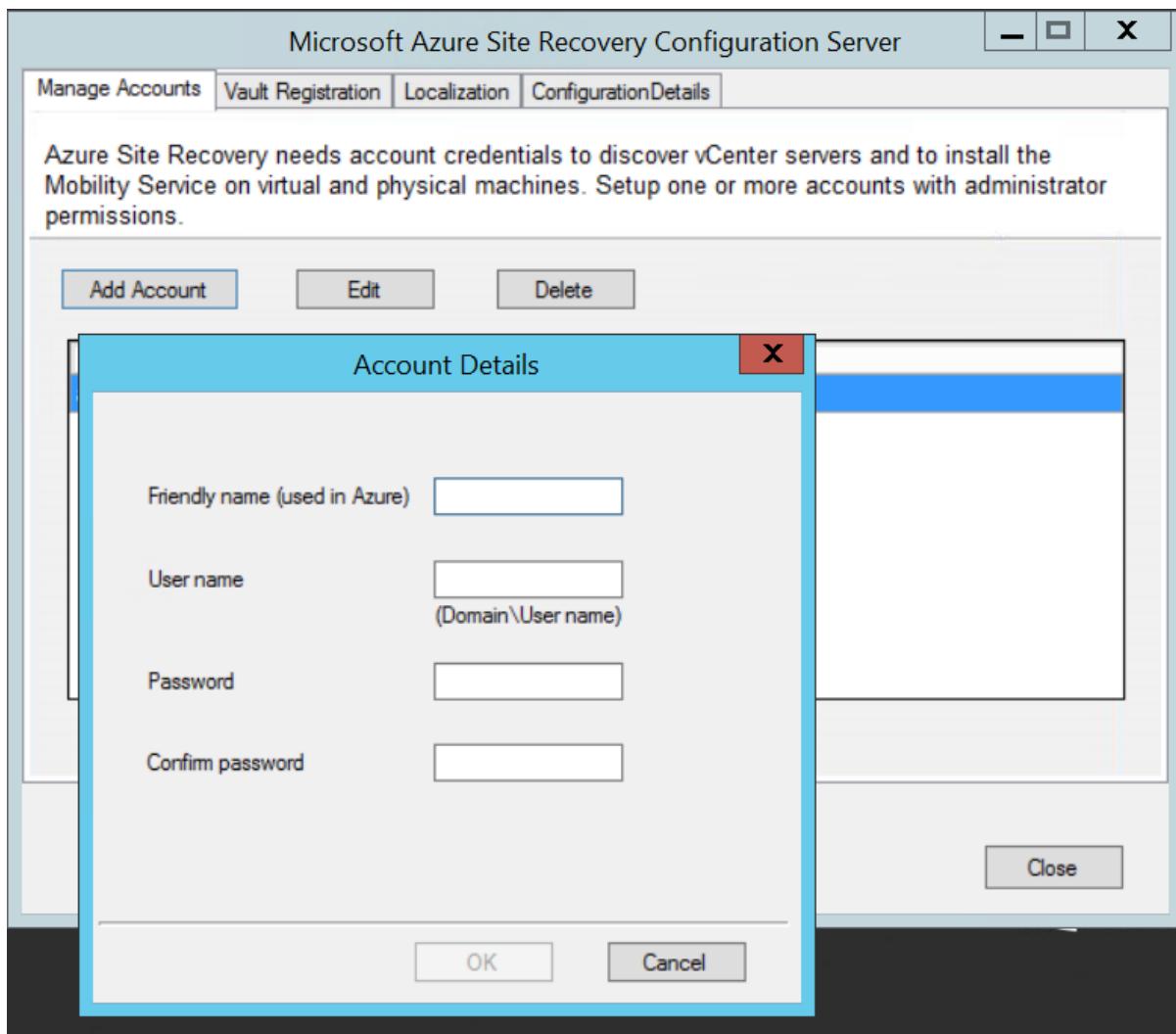
NOTE

If you're adding the VMware vCenter server or VMware vSphere host with an account that doesn't have administrator privileges on the vCenter or host server, make sure that the account has these privileges enabled: Datacenter, Datastore, Folder, Host, Network, Resource, Virtual machine, and vSphere Distributed Switch. In addition, the VMware vCenter server needs the Storage views privilege enabled.

Modify credentials

Modify the credentials used to connect to the vCenter server or ESXi host as follows:

1. Log onto the configuration server, and launch the cspconfigtool.exe from the desktop.
2. Click **Add Account** on the **Manage Account** tab.



3. Provide the new account details, and click **OK** to add it. The account should have the privileges listed [above](#).
4. On the Azure portal, open the vault > **Site Recovery Infrastructure** > **Configuration Servers**, and open the configuration server.
5. In the **Details** page, click **Refresh Server**.
6. After the Refresh Server job completes, select the vCenter Server, to open the vCenter **Summary** page.
7. Select the newly added account in the **vCenter server/vSphere host account** field, and click **Save**.

The screenshot shows two adjacent browser tabs. The left tab is titled 'Configuration Server' and displays the 'Essentials' section with details like Recovery Services vault, IP address, Configuration Server version, Connected agents, and Protected items. It also lists 'Associated servers' with columns for Name, Status, Server Role, Version, and Last Heart Beat. The right tab is titled 'vCenter Summary' and shows configuration fields for a vCenter server, including vCenter server/vSphere host friendly name, vCenter server/vSphere host name or IP address, Port, and vCenter server/vSphere host account.

NAME	STATUS	SERVER ROLE	VERSION	LAST HEART BEAT
Process Ser...	Connected	vCenter Server	5.1.2100.0	2/17/2017 8:16...
vcenter	Connected	vCenter Server	5.1.2100.0	2/17/2017 8:16...
Master Targ...	Connected	vCenter Server	5.1.2100.0	2/17/2017 8:16...

Delete a vCenter server

1. In the Azure portal, open your vault > **Site Recovery Infrastructure** > **Configuration Servers**, and 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 links for 'vCenter', 'Process Server', 'Master Target Server', 'Refresh Server', and 'More'. The main area displays 'Essentials' information and a table of 'Associated servers'. A context menu is open over the 'vcenter' entry in the server list, showing options like 'Save', 'Discard', 'Delete', and 'Error Details'. The 'Delete' option is highlighted.

Configuration Server

vCenter Summary

Essentials

Recovery Services vault	Connection status
[REDACTED]	Connected
IP address	Last heartbeat at 2/17/2017 8:40:40 PM
Configuration Server version 9.7.0.0	Provider version 5.1.2100.0
Connected agents 26	Server ID f6229d83-76e4-4581-8da0-476d0c76524a
Protected items 16	

Associated servers

NAME	STATUS	SERVER ROLE	VERSION	LAST HEART BEAT	...
▶ Process Ser...	Connected				...
▼ vCenter Ser...					...
vcenter	Connected	vCenter Server		2/17/2017 8:16...	...
▶ Master Targ...					...

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

NOTE

If you need to modify the vCenter IP address, FQDN, or port, then you need to delete the vCenter server, and add it back to the portal.

Remove servers and disable protection

7/9/2018 • 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'

    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
        }
        "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 occured" -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 remove 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.
 - **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.

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 remove 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.

3. 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 removes 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 removes 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 vault

7/11/2018 • 2 minutes to read • [Edit Online](#)

Dependencies can prevent you from deleting an Azure Site Recovery vault. The actions you need to take vary based on the Site Recovery scenario. To delete a vault used in Azure Backup, see [Delete a Backup vault in Azure](#).

Delete a Site Recovery vault

To delete the vault, follow the recommended steps for your scenario.

VMware VMs to Azure

1. Delete all protected VMs by following the steps in [Disable protection for a VMware](#).
2. Delete all replication policies by following the steps in [Delete a replication policy](#).
3. Delete references to vCenter by following the steps in [Delete a vCenter server](#).
4. Delete the configuration server by following the steps in [Decommission a configuration server](#).
5. Delete the vault.

Hyper-V VMs (with VMM) to Azure

1. Delete all protected VMs by following the steps in [Disable protection for a Hyper-V VM \(with VMM\)](#).
2. Disassociate & delete all replication policies by browsing to your Vault -> **Site Recovery Infrastructure** -> **For System Center VMM** -> **Replication Policies**
3. Delete references to VMM servers by following the steps in [Unregister a connected VMM server](#).
4. Delete the vault.

Hyper-V VMs (without Virtual Machine Manager) to Azure

1. Delete all protected VMs by following the steps in [Disable protection for a Hyper-V virtual machine \(Hyper-V to Azure\)](#).
2. Disassociate & delete all replication policies by browsing to your Vault -> **Site Recovery Infrastructure** -> **For Hyper-V Sites** -> **Replication Policies**
3. Delete references to Hyper-V servers by following the steps in [Unregister a Hyper-V host](#).
4. Delete the Hyper-V site.
5. 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-AzureRmAccount

Select-AzureRmSubscription -SubscriptionName "XXXXX"

$vault = Get-AzureRmRecoveryServicesVault -Name "vaultname"

Remove-AzureRmRecoveryServicesVault -Vault $vault
```

Learn more about [Get-AzureRMRecoveryServicesVault](#), and [Remove-AzureRMRecoveryServicesVault](#).

Monitor and troubleshoot Site Recovery

8/6/2018 • 9 minutes to read • [Edit Online](#)

In this article, you learn how to use Azure Site Recovery's in built monitoring features for monitoring and troubleshooting.

Use the dashboard

1. In the vault, click **Overview** to open the Site Recovery dashboard. There are dashboard pages for both Site Recovery and Backup, and you can switch between them.

The screenshot shows the Site Recovery Overview dashboard for the 'RayneTestVault' recovery services vault. The left sidebar includes links for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Properties, Locks, Automation script, Backup, Site Recovery, Monitoring and Reports, and Policies. The main area has tabs for Backup and Site Recovery, with Site Recovery selected. Key metrics include 'Replicated items' (9 healthy, 0 critical, 0 warning, 0 not applicable), 'Failover test success' (0 recommended, 0 performed successfully, 0 not applicable), 'Configuration issues' (0 errors), and 'Recovery Plans' (0). The 'ERROR SUMMARY' section shows 'No errors'. The 'INFRASTRUCTURE VIEW' section shows 'machines replicating to Azure' (Azure virtual machine(s), VMWare, Hyper-V) and 'Jobs - Last 24 hours' (0 failed, 0 in progress, 0 waiting for input).

2. The dashboard consolidates all monitoring information for the vault in a single location. From the dashboard, you can drill down into different areas.

The screenshot shows the Site Recovery Overview dashboard for the 'Contoso-vault' recovery services vault. The left sidebar is identical to the previous dashboard. The main area is annotated with yellow circles numbered 1 through 8:

- 1: 'Site Recovery' tab (highlighted by a red box)
- 2: 'Recovery Plans' section (highlighted by a red box)
- 3: 'Replicated items' summary (highlighted by a red box)
- 4: 'Configuration issues' summary (highlighted by a red box)
- 5: 'ERROR SUMMARY' section (highlighted by a red box)
- 6: 'INFRASTRUCTURE VIEW' section showing On-premises (vCenter server 1, Virtual machine(s) 9) connected to Infrastructure server(s) 1, which are connected to Azure Site Recovery and Storage account(s) 5 (highlighted by a red box)
- 7: 'Jobs - Last 24 hours' section (highlighted by a red box)
- 8: 'Jobs - Last 24 hours' section (highlighted by a red box)

The dashboard also displays 'Backup' and 'Site Recovery' tabs at the top.

3. On **Replicated items**, click **View All** to see all the servers in the vault.
4. Drill down by clicking the status details in each section. In **Infrastructure view**, you can sort monitoring information by the type of machines you're replicating.

Monitor replicated items

The replicated items section shows the health of all machines that have replication enabled in the vault.

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

You can view the test 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 one 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

The **Configuration issues** section shows a list of issues that may impact your ability to successfully fail over.

- 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 the **needs attention** in the **Target configurations** column. The 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	<p>The available subscription resource quota balance is compared against the balance needed to fail over all of the machines in the vault.</p> <p>If there aren't enough resources, an insufficient quota balance is reported.</p> <p>Quotas are monitoring for VM core count, VM family core count, network interface card (NIC) count.</p>
Software updates	The availability of new software updates, and information about expiring software versions.

Monitoring errors

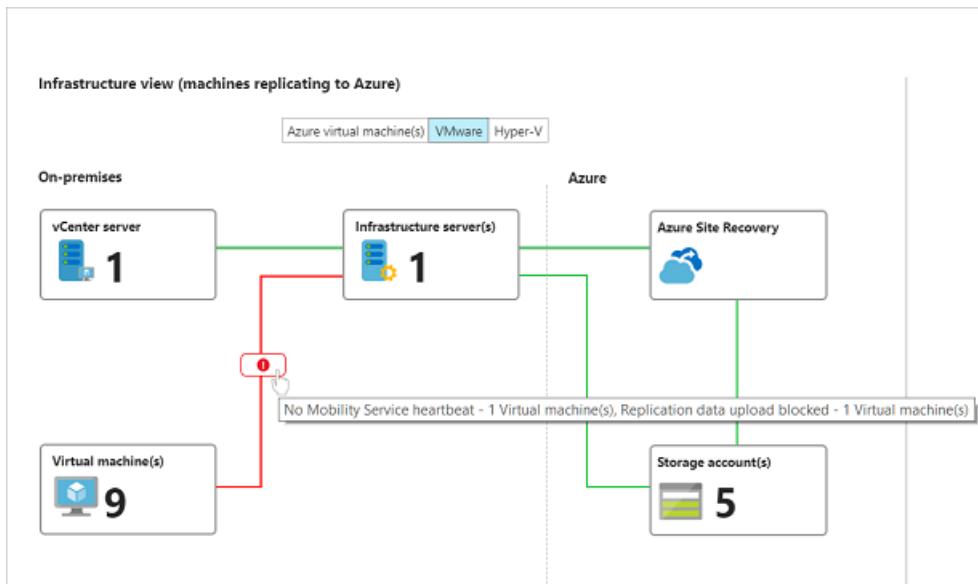
The **Error summary** section shows currently active error symptoms that may impact replication of servers in the vault, and the number of impacted machines.

- At the beginning of the section, errors impacting on-premises infrastructure components are shown. For example, non-receipt of a heartbeat from the Azure Site Recovery Provider running on the on-premises configuration server, VMM 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 may be impacting multiple machines. For example, a network glitch could potentially impact all machines replicating 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.

The **Infrastructure view** shows 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
Azure VM replication between Azure regions	Replication enabled/initial replication in progress	Yes
Azure VM replication between Azure regions	Failed over/fail back	No
VMware replication to Azure	Replication enabled/initial replication in progress	Yes
VMware replication to Azure	Failed over/failed back	No
Hyper-V replication to Azure	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.

Common questions

Why is the count of virtual machines in the vault infrastructure view different from the total count shown in the replicated items?

The vault infrastructure view is scoped by replication scenarios. Only machines in 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 shown in the Essentials drawer 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 the Essentials drawer. On the replicated items the total includes all the machines in the vault, including those for which initial replication is currently in progress.

Monitor recovery plans

In the **Recovery plans section** you can review the number of plans, create new plans, and modify existing ones.

Monitor jobs

The **Jobs** section reflects 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:

1. 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.
2. 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**.

3. In the **Site Recovery Jobs** list, a list of jobs is displayed. On the top menu you can get error details for a specific job, filter the jobs list based on specific criteria, and export selected job details to Excel.
4. You can drill into a job by clicking it.

Monitor virtual machines

In addition dashboard, you can monitor machines in the virtual machines page.

1. In the vault, click **Replicated items** to get a list of replicated machines. Alternately, you can get to a filtered list of the protected items by clicking any of the scoped shortcuts on the dashboard page.

The screenshot shows the 'Replicated items' page in the Azure Recovery Services vault. The left sidebar includes sections for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, SETTINGS (Properties, 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), and a pinned Replicated items item. The main area displays a table with the following data:

NAME	REPLICATION HEALTH	STATUS	RPO	TARGET CONFIGURATIONS
ContosoVM9	Healthy	Protected	5 minutes	OK
ContosoVM7	Healthy	Protected	1 minute	Needs attention
ContosoVM1	Healthy	Protected	3 minutes	OK
ContosoVM2	Critical	Protected	32 minutes	OK
ContosoVM3	Healthy	Protected	4 minutes	OK
ContosoVM4	Healthy	Protected	3 minutes	OK
ContosoVM5	Healthy	Protected	2 minutes	OK
ContosoVM6	Healthy	Protected	6 minutes	OK
ContosoVM8	Healthy	Protected	4 minutes	OK

A context menu is open for ContosoVM7, listing options: Pin to dashboard, Failover, Test Failover, Cleanup test failover, Change recovery point, Commit, Complete Migration, Re-protect, Resynchronize, Error Details, and Disable Replication.

- On the **Replicated items** page, 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.
- Click **Columns** to show additional columns, For example to show RPO, target configuration issues, and replication errors.
- Click **Filter** to view information based on specific parameters such as replication health, or a particular replication policy.
- Right-click a machine to initiate operations such as test failover for it, or to view specific error details associated with it.
- 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.

Common questions

How is RPO 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 to identify a recoverable point, are written to the storage account in the target region.
- Site Recovery can now generate a recoverable point for the virtual machine.
- At this point, the RPO has been met for the changes uploaded to the storage account thus far. In other words, the machine RPO at this point is equal to amount of time 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.

NOTE

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.

Subscribe to email notifications

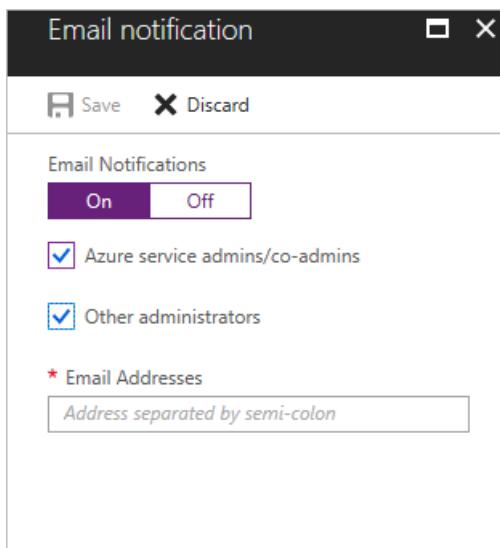
You can subscribe to receive email notifications for these critical events:

- 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 and Reports** 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.



Troubleshoot replication issues for VMware VMs and physical servers

7/18/2018 • 4 minutes to read • [Edit Online](#)

You may receive a specific error message when protecting your VMware virtual machines or physical servers using Azure Site Recovery. This article describes some common issues you might encounter when replicating on-premises VMware VMs and physical servers to Azure using [Azure Site Recovery](#).

Initial replication issues.

In many cases, initial replication failures that we encounter at support are due to connectivity issues between source server-to-process server or process server-to-Azure. For most cases, you can troubleshoot these issues by following the steps listed below.

Verify the source machine

- From Source Server machine command line, use Telnet to ping the Process Server with https port (default 9443) as shown below to see if there are any network connectivity issues or firewall port blocking issues.

```
telnet <PS IP address> <port>
```

NOTE

Use Telnet, don't use PING to test connectivity. If Telnet is not installed, follow the steps list [here](#)

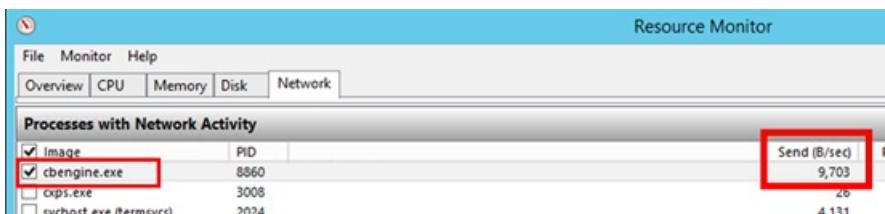
If unable to connect, allow inbound port 9443 on the Process Server and check if the problem still exists. There has been some cases where process server was behind DMZ, which was causing this problem.

- Check the status of service [InMage Scout VX Agent – Sentinel/OutpostStart](#) if it is not running and check if the problem still exists.

Verify the process server

- Check if process server is actively pushing data to Azure**

From Process Server machine, open the Task Manager (press Ctrl-Shift-Esc). Go to the Performance tab and click 'Open Resource Monitor' link. From Resource Manager, go to Network tab. Check if cbengine.exe in 'Processes with Network Activity' is actively sending large volume (in Mbs) of data.



If not, follow the steps listed below:

- Check if Process server is able to connect Azure Blob:** Select and check cbengine.exe to view the 'TCP Connections' to see if there is connectivity from Process server to Azure Storage blob URL.

The screenshot shows the Windows Resource Monitor. In the CPU tab, 'cbengine.exe' is listed with PID 8860, status Running, and threads 19. In the Network tab, 'Filtered by cbengine.exe' shows a single entry for 'cbengine.exe' with PID 8860, sending 3,907 bytes/sec, receiving 72 bytes/sec, and a total of 3,979 bytes/sec. A red arrow points from the 'cbengine.exe' row in the CPU table to the 'Address' column in the Network table.

If not then go to Control Panel > Services, check if the following services are up and running:

```
* cxprocessserver
* InMage Scout VX Agent - Sentinel/Outpost
* Microsoft Azure Recovery Services Agent
* Microsoft Azure Site Recovery Service
* tmansvc
*
```

(Re)Start any service, which is not running and check if the problem still exists.

- **Check if Process server is able to connect to Azure Public IP address using port 443**

Open the latest CBEngineCurr.errlog from `%programfiles%\Microsoft Azure Recovery Services Agent\Temp` and search for: 443 and connection attempt failed.

The screenshot shows a Windows File Explorer window with the path 'This PC > Local Disk (C:) > Program Files > Microsoft Azure Recovery Services Agent > Temp'. A red box highlights the 'Temp' folder. Inside, there are multiple 'CBEngineX.errlog' files and one 'CBEngineCurr.errlog' file. A red box highlights 'CBEngineCurr.errlog'. Below it, a yellow callout box contains the error message: '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'.

If there are issues, then from Process Server command line, use telnet to ping your Azure Public IP address (masked in above image) found in the CBEngineCurr.currLog using port 443.

```
telnet <your Azure Public IP address as seen in CBEngineCurr.errlog> 443
```

If you are unable to connect, then check if the access issue is due to firewall or Proxy as described in next step.

- **Check if IP address-based firewall on Process server is not blocking access:** If you are using an IP address-based firewall rules on the server, then download the complete list of Microsoft Azure Datacenter IP Ranges from [here](#) and add them to your firewall configuration to ensure they allow communication to Azure (and the HTTPS (443) port). Allow IP address ranges for the Azure region of your subscription, and for West US (used for Access Control and Identity Management).

- **Check if URL-based firewall on Process server is not blocking access:** If you are using a URL-based firewall rules on the server, ensure the following URLs are added to firewall configuration.

NAME	COMMERCIAL URL	GOVERNMENT URL	DESCRIPTION
Azure AD	login.microsoftonline.com	login.microsoftonline.us	Used for access control and identity management using AAD
Backup	*.backup.windowsazure.com	*.backup.windowsazure.us	Used for replication data transfer and coordination
Replication	*.hypervrecoverymanager.windows.net	*.hypervrecoverymanager.windows.us	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.nist.gov` and `time.windows.com` are used to check time synchronization between system and global time in all deployments.

- **Check if Proxy Settings on Process server are not blocking access.** If you are using a Proxy Server, ensure the proxy server name is resolving by the DNS server. To check what you have provided at the time of Configuration Server setup. Go to registry key

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Azure Site Recovery\ProxySettings`

Now ensure that the same settings are being used by Azure Site Recovery agent to send data. Search Microsoft Azure Backup

Open it and click on Action > Change Properties. Under Proxy Configuration tab, you should see the proxy address, which should be same as shown by the registry settings. If not, please change it to the same address.

- **Check if Throttle bandwidth is not constrained on Process server:** Increase the bandwidth and check if the problem still exists.

Next steps

If you need more help, then post your query to [Azure Site Recovery forum](#). We have an active community and one of our engineers will be able to assist you.

Troubleshoot Mobility Service push installation issues

7/10/2018 • 4 minutes to read • [Edit Online](#)

This article describes how to troubleshoot common errors you might face when you try to install Azure Site Recovery Mobility Service on the source server to enable protection.

Error 78007 - The requested operation could not be completed

This error can be thrown by the service for several reasons. Choose the corresponding provider error to troubleshoot further.

- [Error 95103](#)
- [Error 95105](#)
- [Error 95107](#)
- [Error 95108](#)
- [Error 95117](#)
- [Error 95213](#)
- [Error 95224](#)
- [Error 95265](#)

Error 95105 - Protection could not be enabled (EP0856)

ERROR CODE	POSSIBLE CAUSES	ERROR-SPECIFIC RECOMMENDATIONS
95105 Message: Push installation of Mobility Service to the source machine failed with error code EP0856 . Either File and Printer Sharing isn't allowed on the source machine or there are network connectivity problems between the process server and the source machine.	File and Printer Sharing isn't enabled.	Allow File and Printer Sharing on the source machine in Windows Firewall. On the source machine, under Windows Firewall > Allow an app or feature through Firewall , select File and Printer Sharing for all profiles . In addition, check the following prerequisites to successfully finish the push installation. Read more about troubleshooting WMI issues .

Error 95107 - Protection could not be enabled (EP0858)

ERROR CODE	POSSIBLE CAUSES	ERROR-SPECIFIC RECOMMENDATIONS
95107 Message: Push installation of Mobility Service to the source machine failed with error code EP0858 . Either the credentials provided to install Mobility Service are incorrect or the user account has insufficient privileges.	User credentials provided to install Mobility Service on the source machine are incorrect.	Ensure that the user credentials provided for the source machine on the configuration server are correct. To add or edit user credentials, go to the configuration server, and select Cpsconfigtool > Manage account . In addition, check the following prerequisites to successfully finish the push installation.

Error 95117 - Protection could not be enabled (EP0865)

ERROR CODE	POSSIBLE CAUSES	ERROR-SPECIFIC RECOMMENDATIONS
95117 Message: Push installation of Mobility Service to the source machine failed with error code EP0865 . Either the source machine isn't running or there are network connectivity problems between the process server and the source machine.	Network connectivity problems between the process server and the source server.	Check connectivity between the process server and the source server. In addition, check the following prerequisites to successfully finish the push installation.

Error 95103 - Protection could not be enabled (EP0854)

ERROR CODE	POSSIBLE CAUSES	ERROR-SPECIFIC RECOMMENDATIONS
95103 Message: Push installation of Mobility Service to the source machine failed with error code EP0854 . Either Windows Management Instrumentation (WMI) isn't allowed on the source machine or there are network connectivity problems between the process server and the source machine.	WMI is blocked in Windows Firewall.	Allow WMI in Windows Firewall. Under Windows Firewall > Allow an app or feature through Firewall , select WMI for all profiles . In addition, check the following prerequisites to successfully finish the push installation.

Error 95213 - Protection could not be enabled (EP0874)

ERROR CODE	POSSIBLE CAUSES	ERROR-SPECIFIC RECOMMENDATIONS
95213 Message: Installation of Mobility Service to the source machine %SourceIP%; failed with error code EP0874 .	The operating system version on the source machine isn't supported.	Ensure that the source machine OS version is supported. Read the support matrix . In addition, check the following prerequisites to successfully finish the push installation.

Error 95108 - Protection could not be enabled (EP0859)

ERROR CODE	POSSIBLE CAUSES	ERROR-SPECIFIC RECOMMENDATIONS
95108 Message: Push installation of Mobility Service to the source machine failed with error code EP0859 .	Either the credentials provided to install Mobility Service are incorrect or the user account has insufficient privileges.	Ensure that the credentials provided are the root account's credentials. To add or edit user credentials, go to the configuration server and select the Cpsconfigtool shortcut icon on the desktop. Select Manage account to add or edit credentials.

Error 95265 - Protection could not be enabled (EP0902)

ERROR CODE	POSSIBLE CAUSES	ERROR-SPECIFIC RECOMMENDATIONS
95265 Message: Push installation of Mobility Service to the source machine succeeded but the source machine requires a restart for some system changes to take effect.	An older version of Mobility Service was already installed on the server.	Replication of the virtual machine continues seamlessly. Reboot the server during your next maintenance window to get benefits of the new enhancements in Mobility Service.

Error 95224 - Protection could not be enabled (EP0883)

ERROR CODE	POSSIBLE CAUSES	ERROR-SPECIFIC RECOMMENDATIONS
95224 Message: Push installation of Mobility Service to the source machine %SourceIP; failed with error code EP0883 . A system restart from a previous installation or update is pending.	The system wasn't restarted when uninstalling an older or incompatible version of Mobility Service.	Ensure that no version of Mobility Service exists on the server. Reboot the server, and rerun the enable protection job.

Resource to troubleshoot push installation problems

Troubleshoot file and print sharing issues

- [Enable or disable file sharing with Group Policy](#)
- [Enable file and print sharing through Windows Firewall](#)

Troubleshoot WMI issues

- [Basic WMI testing](#)
- [WMI troubleshooting](#)
- [Troubleshooting problems with WMI scripts and WMI services](#)

Next steps

[Learn how](#) to set up disaster recovery for VMware VMs.

Troubleshoot errors when failover a virtual machine to Azure

8/2/2018 • 3 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.

Unable to connect/RDP/SSH to the failed over virtual machine due to grayed out Connect button on the virtual machine

If Connect button is grayed out and you are not connected to Azure via an Express Route or Site-to-Site VPN connection, then,

1. Go to **Virtual machine** > **Networking**, click on the name of required network interface.

Virtual network/subnet: AzureTestNetwork/Subnet-1 Public IP: **None** Private IP: **10.1.0.4** Accelerated networking: **Disabled**

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
110	Cleanupool-3389-Corpnet...	3389	TCP	167.220.148.0...	Any	<input checked="" type="checkbox"/> Allow

2. Navigate to **Ip Configurations**, then click on the name field of required IP configuration.

IP forwarding settings

IP forwarding: **Enabled**

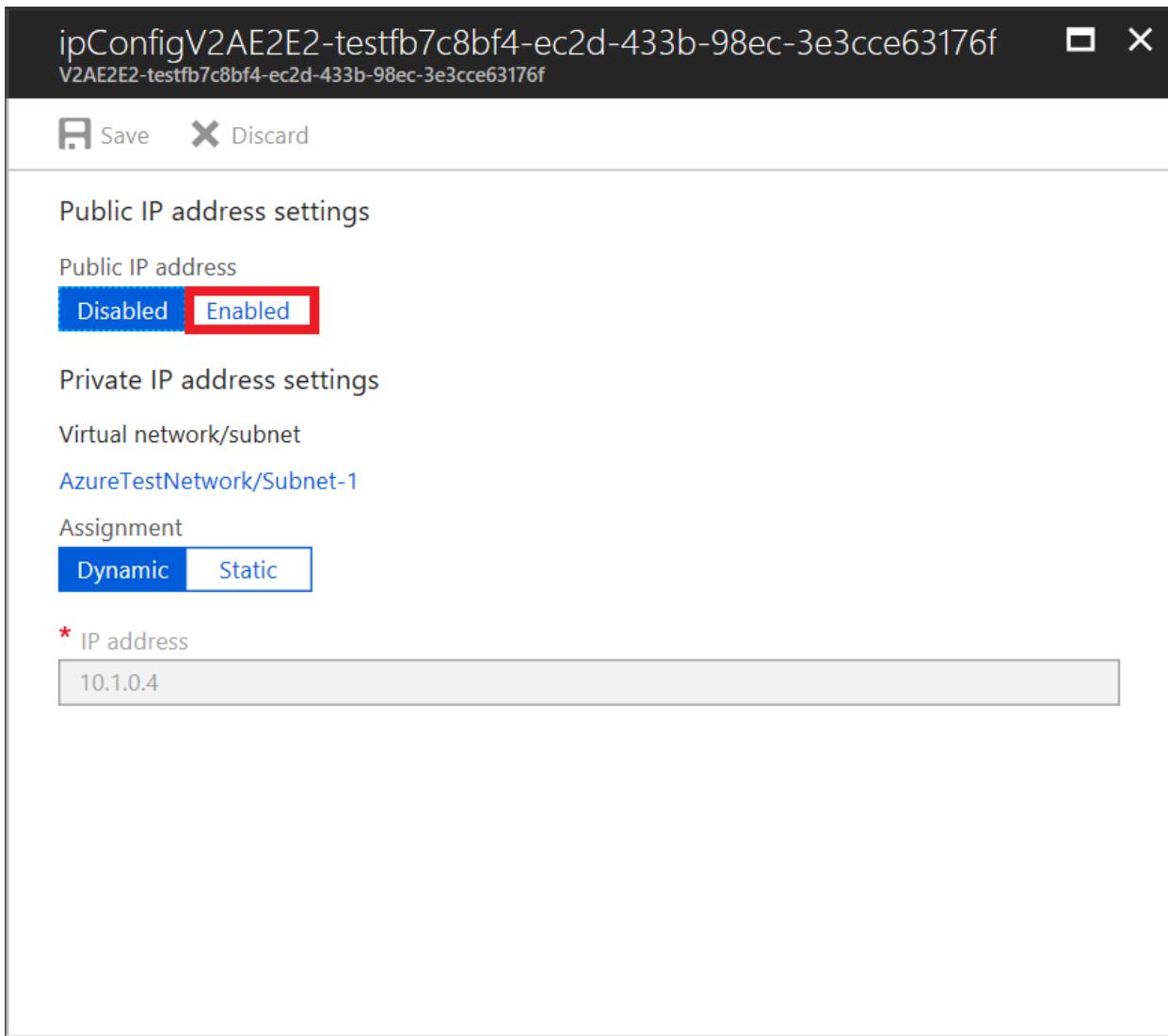
Virtual network: AzureTestNetwork

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**.



4. Click on **Configure required settings** > **Create new**.

This screenshot shows the 'Choose public IP address' blade. At the top, it says 'ipConfigV2AE2E2-testfb7c8bf4-ec2d-433b-98ec-3e3cce63176f' and has save/discard buttons. The main area is titled 'Choose public IP address' with a sub-instruction 'Dynamic public IP addresses that are not in use won't have an IP address assigned to them.' A blue information icon is present. Below this, a list of existing public IP addresses is shown, each represented by a small blue square icon with three dots. To the right of the list, a red box highlights the 'Create new' button, which is preceded by a blue plus sign icon. The rest of the blade shows the same configuration options as the previous screenshot, such as 'Public IP address settings', 'Assignment', and 'IP address'.

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 to the failed over virtual machine even though Connect button is available (not grayed out) on the virtual machine

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
 - 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

Next steps

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 from Azure to VMware

7/9/2018 • 2 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.

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 (hung state 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.

Set up disaster recovery of on-premises VMware virtual machines or physical servers to a secondary site

8/7/2018 • 15 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
Required components	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
Configuration and orchestration	Recovery Services vault in the Azure portal	Using vContinuum
Replicated	Disk (Windows and Linux)	Volume-Windows Disk-Linux
Shared disk cluster	Not supported	Supported
Data churn limits (average)	10 MB/s data per disk 25MB/s data per VM Learn more	> 10 MB/s data per disk > 25 MB/s data per VM
Monitoring	From Azure portal	From CX (Configuration Server)
Support Matrix	Click here for details	Download ASR Scout compatible matrix

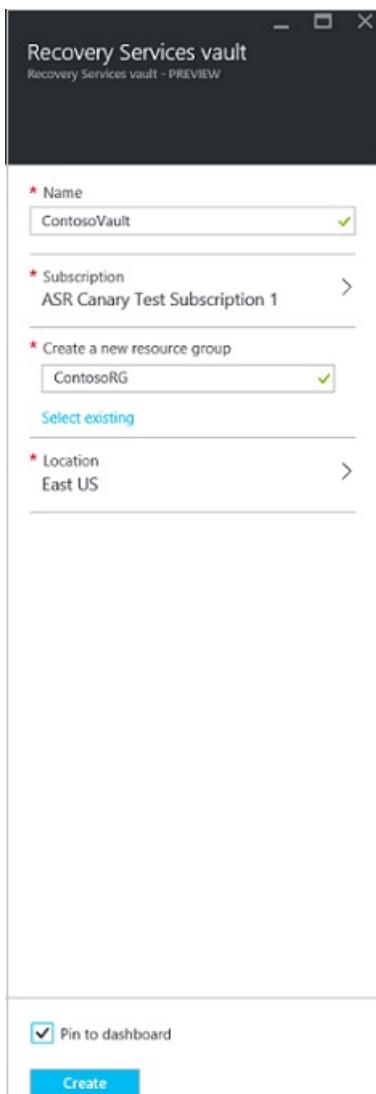
Prerequisites

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](#).

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.

Choose a protection goal

Select what to replicate, and where to replicate it to.

1. Click **Site Recovery > Prepare Infrastructure > Protection goal**.
2. Select **To recovery site > Yes, with VMware vSphere Hypervisor**. Then click **OK**.
3. In **Scout Setup**, download the InMage Scout 8.0.1 GA software, and the registration key. The setup files for all components are included in the downloaded .zip file.

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. 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_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**.

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](#)

Updates

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

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.
- Download the GA package from the portal, as described in [create a vault](#).

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 failback 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 failback 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 fallback, 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.
- Linux VM protection fails when there are more than 26 disks on the master target server.

Manage virtual machine network interfaces for on-premises to Azure replication

7/9/2018 • 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.

The screenshot shows the 'Compute and Network' pane for a replicated item named 'HPVTestVM15'. The 'Compute properties' section includes fields for 'Name' (HPVTestVM15), 'Resource group' (multinicrg), 'Size' (1 cores, 1.00 GB memory, 5 NICs), 'Availability set' (No applicable availability sets in the res...), and 'Use managed disks' (No). The 'Network properties' section shows the 'Virtual network' as 'multinicvnet15'. The 'Network interfaces' section lists five entries:

ON-PREMISES NETWORK NAME	TARGET SUBNET	TARGET IP	TARGET NETWORK INTERFACE TYPE
Microsoft Hyper-V Network ...	default	10.15.0.5 (Static)	Primary
Microsoft Hyper-V Network ...	default	DHCP assigned	Secondary
Microsoft Hyper-V Network ...			Do not use
Microsoft Hyper-V Network ...			Do not use
Microsoft Hyper-V Network ...			Do not use

A note at the bottom states: 'Apply Hybrid Use Benefit and save up to 40% on compute costs with a Windows Server license you already own.' with 'No' and 'Yes' buttons.

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.

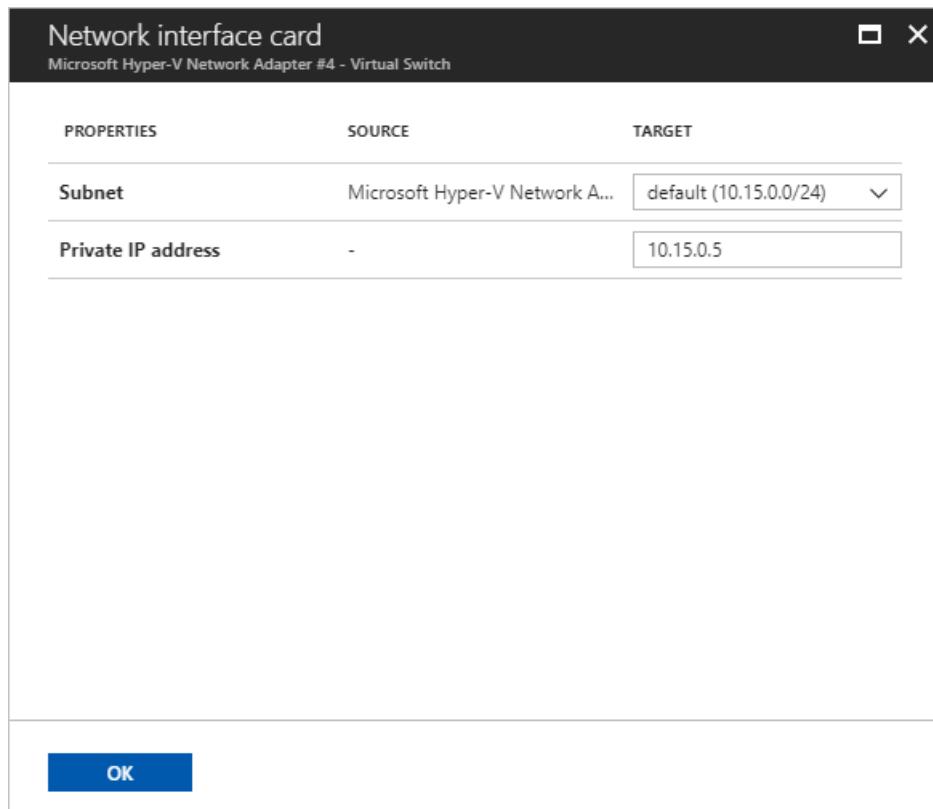
- A **Primary** network interface is required for failover.
- All other selected network interfaces, if any, are **Secondary** network interfaces.
- Select **Do not use** to exclude a network interface from creation at failover.

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.

Set up IP addressing to connect after failover to Azure

7/9/2018 • 3 minutes to read • [Edit Online](#)

This article explains the networking requirements for connecting to Azure VMs, after using the [Azure Site Recovery](#) service for replication and failover to Azure.

In this article you'll learn about:

- The connection methods you can use
- How to use a different IP address for replicated Azure VMs
- How to retain IP addresses for Azure VMs after failover

Connecting to replica VMs

When planning your replication and failover strategy, one of the key questions is how to connect to the Azure VM after failover. There are a couple of choices when designing your network strategy for replica Azure VMs:

- **Use different IP address:** You can select to use a different IP address range for the replicated Azure VM network. In this scenario the VM gets a new IP address after failover, and a DNS update is required.
- **Retain same IP address:** You might want to use the same IP address range as that in your primary on-premises site, for the Azure network after failover. Keeping the same IP addresses simplifies the recovery by reducing network related issues after failover. However, when you're replicating to Azure, you will need to update routes with the new location of the IP addresses after failover.

Retaining IP addresses

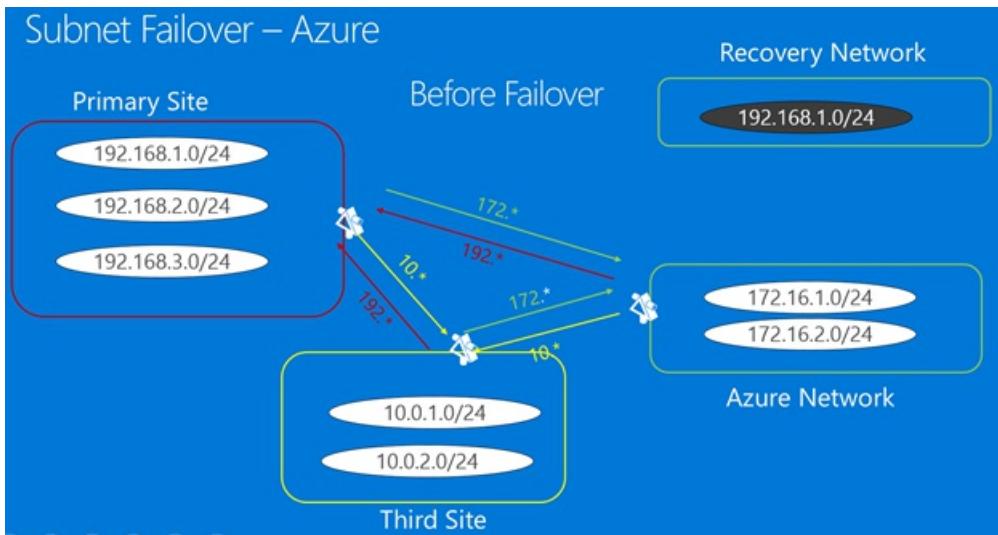
Site Recovery provides the capability to retain fixed IP addresses when failing over to Azure, with a subnet failover.

- With subnet failover, a specific subnet is present at Site 1 or Site 2, but never at both sites simultaneously.
- In order to maintain the IP address space in the event of a failover, you programmatically arrange for the router infrastructure to move the subnets from one site to another.
- During failover, the subnets move with the associated protected VMs. The main drawback is that in the event of a failure, you have to move the whole subnet.

Failover example

Let's look at an example for failover to Azure using a fictitious company, Woodgrove Bank.

- Woodgrove Bank hosts their business apps in an on-premises site. They host their mobile apps on Azure.
- There's VPN site-to-site connectivity between their on-premises edge network and the Azure virtual network. Because of the VPN connection, the virtual network in Azure appears as an extension of the on-premises network.
- Woodgrove wants to replicate on-premises workloads to Azure with Site Recovery.
 - Woodgrove has apps which depend on hard-coded IP addresses, so they need to retain IP addresses for the apps, after failover to Azure.
 - Resources running in Azure use the IP address range 172.16.1.0/24, 172.16.2.0/24.

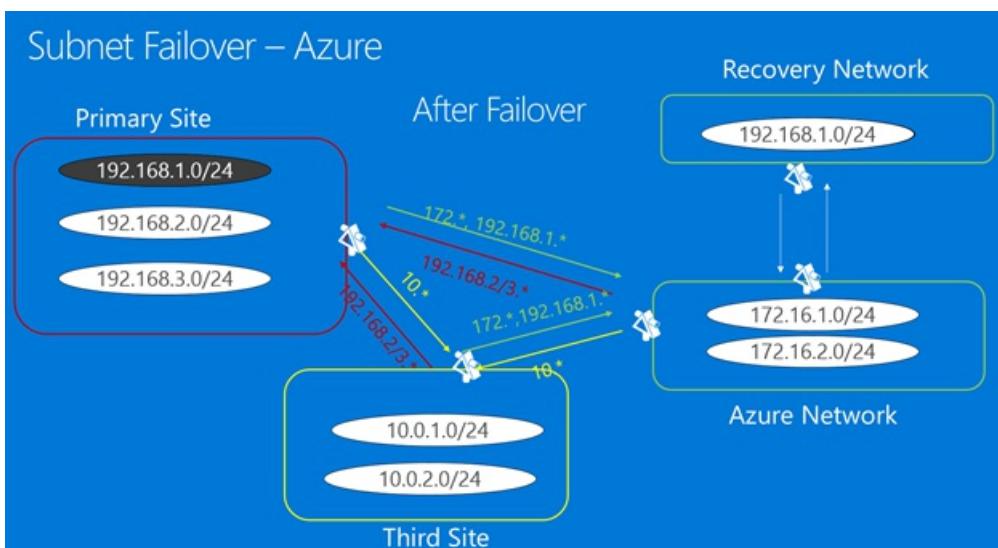


Infrastructure before failover

For Woodgrove to be able to replicate its VMs to Azure while retaining the IP addresses, here's what the company needs to do:

1. Create Azure virtual network in which the Azure VMs will be created after failover of on-premises machines. It should be an extension of the on-premises network, so that applications can fail over seamlessly.
2. Before failover, in Site Recovery, they assign the same IP address in the machine properties. After failover, Site Recovery assigns this address to the Azure VM.
3. After failover runs and the Azure VMs are created with the same IP address, they connect to the network using a [Vnet to Vnet connection](#). This action can be scripted.
4. They need to modify routes, to reflect that 192.168.1.0/24 has now moved to Azure.

Infrastructure after failover



Site-to-site connection

In addition to the vnet-to-vnet connection, after failover, Woodgrove can set up site-to-site VPN connectivity:

- When you set up a site-to-site connection, in the Azure network you can only route traffic to the on-premises location (local-network) if the IP address range is different from the on-premises IP address range. This is because Azure doesn't support stretched subnets. So, if you have subnet 192.168.1.0/24 on-premises, you can't add a local-network 192.168.1.0/24 in the Azure network. This is expected because Azure doesn't know that there are no active VMs in the subnet, and that the subnet is being created for disaster recovery only.
- To be able to correctly route network traffic out of an Azure network, the subnets in the network and the local-network mustn't conflict.

Assigning new IP addresses

This [blog post](#) explains how to set up the Azure networking infrastructure when you don't need to retain IP addresses after failover. It starts with an application description, looks at how to set up networking on-premises and in Azure, and concludes with information about running failovers.

Next steps

[Run a failover](#)

Site Recovery Deployment Planner for Hyper-V to Azure

8/2/2018 • 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 6.5, 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"> Operating system: Microsoft Windows Server 2016 or Microsoft Windows Server 2012 R2 Machine configuration: 8 vCPUs, 16 GB RAM, 300 GB HDD Microsoft .NET Framework 4.5 Microsoft 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 1000 VMs with an average of three disks each, profiled for 30 days) 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. All Hyper-V servers' VMs to be profiled must be added to TrustedHosts list of the client VM from where the tool is being run. Learn more to add servers into TrustedHosts list. The tool should be run from Administrative privileges from PowerShell or command-line console on the client
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_v2.2.zip

E:\ASR Deployment Planner_v2.2\ASRDeploymentPlanner.exe

Updating to the latest version of deployment planner

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 recommended 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 ASR Deployment Planner tool version is 2.2. Refer to [ASR Deployment Planner Version History](#) page for the fixes that are added in each update.

Next steps

- [Run the deployment planner](#).

Run Azure Site Recovery deployment planner for Hyper-V to Azure

7/9/2018 • 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"> • Hyper-V host name or IP address • Hyper-V cluster name or IP address <p>Example: ServerList.txt contains the following servers:</p> <ul style="list-style-type: none"> • Host_1 • 10.8.59.27 • Cluster_1 • Host_2
-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. Example: VMList.txt contains the following VMs: <ul style="list-style-type: none">• Host_1\VM_A• 10.8.59.27\VM_B• Host_2\VM_C
-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 > Storage accounts > <i>storage-account name</i> > Settings > Access Keys > Key1 (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.

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="MaxVmsSupported" 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>Example: VMList.txt contains the following VMs:</p> <ul style="list-style-type: none">• Host_1\VM_A• 10.8.59.27\VM_B• Host_2\VM_C
-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 supported target regions .
-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 supported currencies .

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.

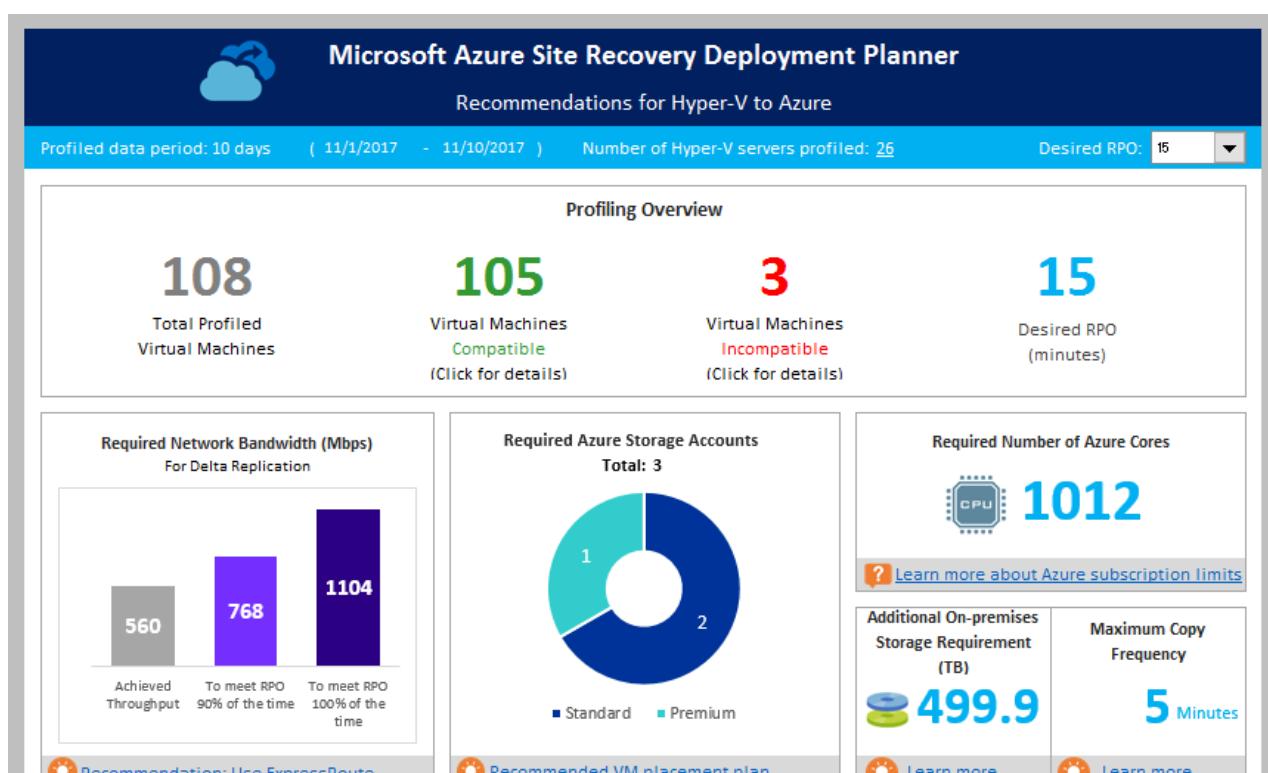
For example, let's say that today your VM fits in a standard storage replication account. Over the next three months, these changes are likely to occur:

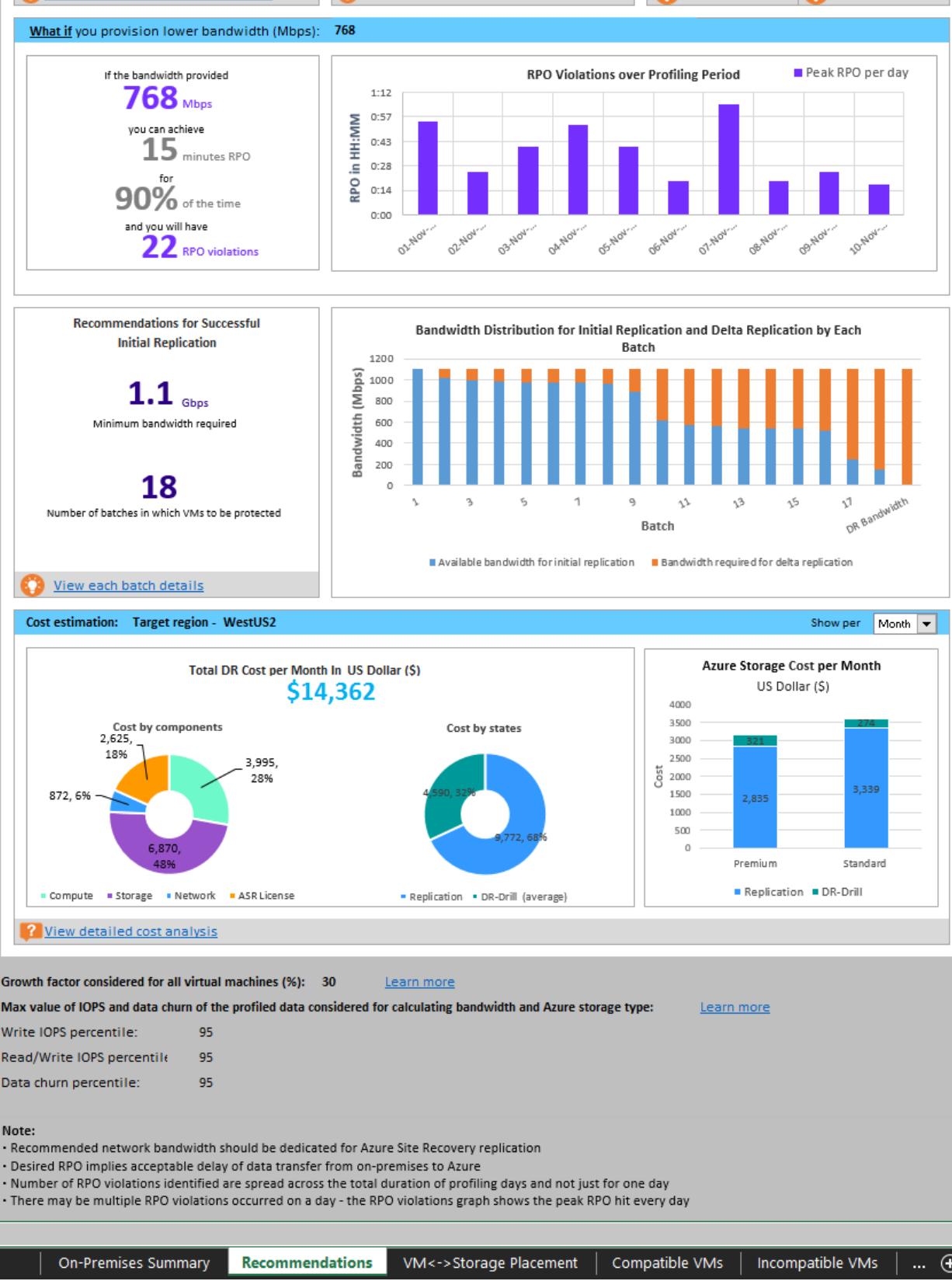
1. The number of users of the application that runs on the VM will increase.
2. The increased churn on the VM will require the VM to go to premium storage so that Azure Site Recovery replication can keep pace.
3. You will have to disable and re-enable protection to a premium storage account.

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**

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 > Storage accounts > <i>storage-account name</i> > Settings > Access Keys > Key1 .
-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. Example: VMList.txt contains the following VMs: <ul style="list-style-type: none"> • Host_1\VM_A • 10.8.59.27\VM_B • Host_2\VM_C
-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.

Example

```
ASRDeploymentPlanner.exe -Operation GetThroughput -Virtualization Hyper-V -Directory "E:\Hyper-V_ProfiledData"
-VMListFile "E:\Hyper-V_ProfiledData\ProfileVMList1.txt" -StorageAccountName asrspfarm1 -StorageAccountKey
by8vdM02xNOcqFlqUwJPLlEt1CDXJ10UzFT50uSRZ6IFsuFq2UVERCz4I6tq/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

7/9/2018 • 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	
Profiled Report for	Hyper-V 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	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.

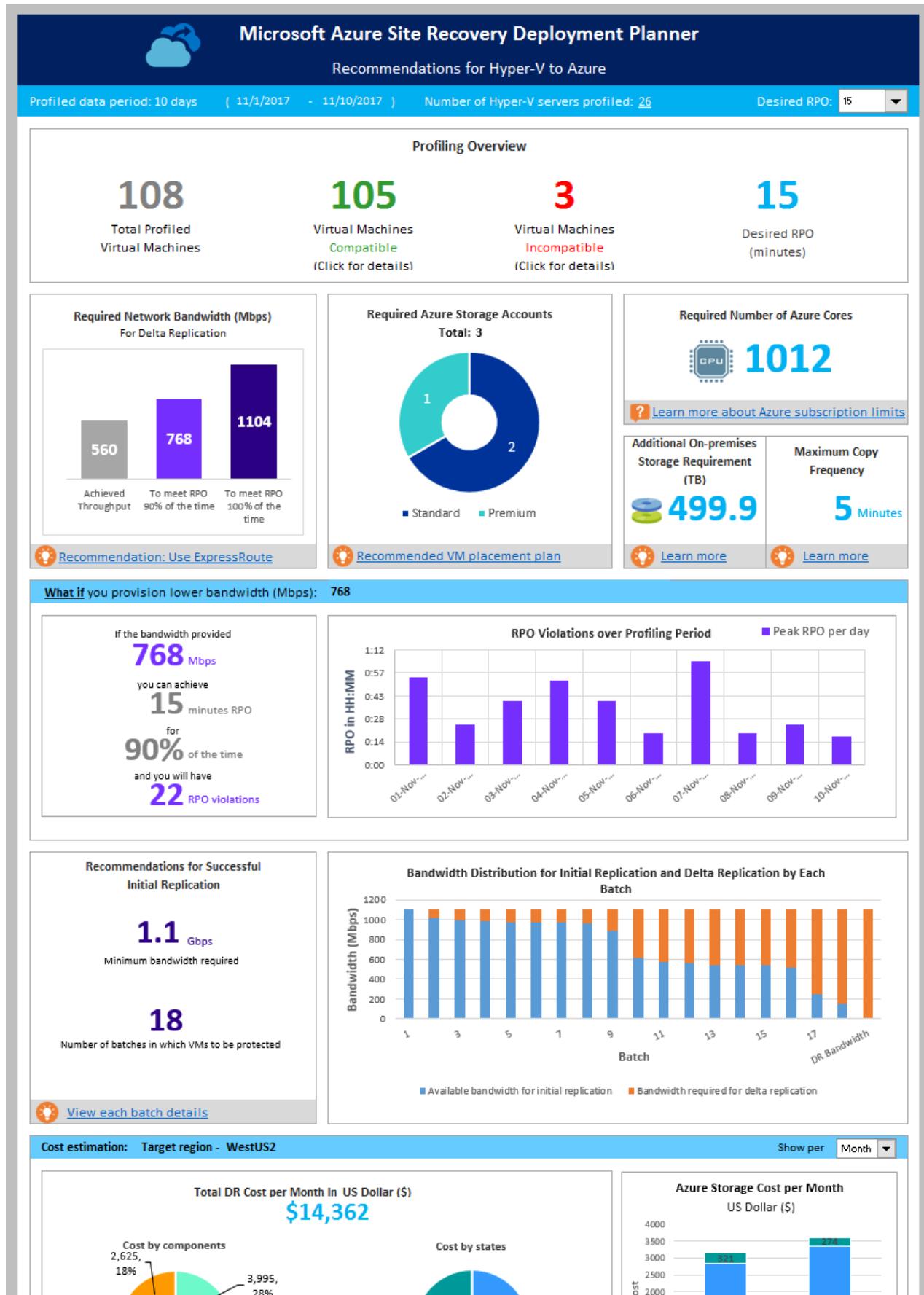
Desired bandwidth (Mbps): The value that you passed for the "Bandwidth" parameter at the time of report

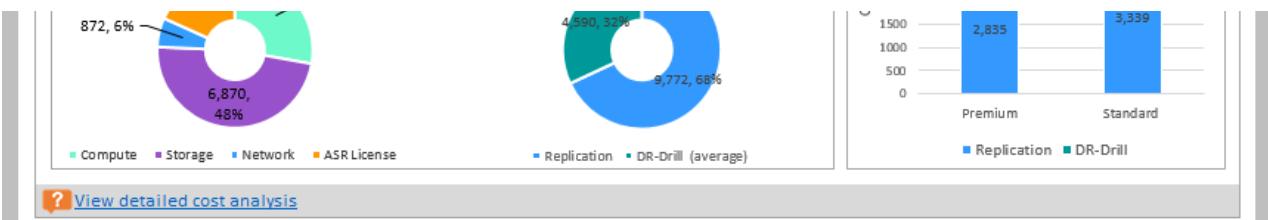
generation to estimate achievable recovery point objective (RPO).

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](#)

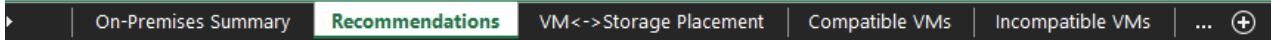
Write IOPS percentile: 95

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

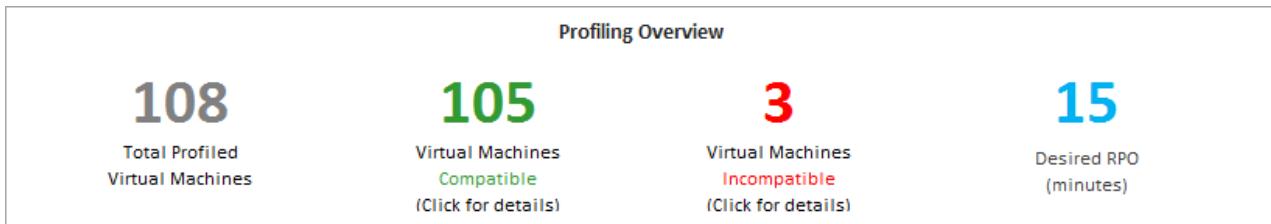
Microsoft Azure Site Recovery Deployment Planner
Recommendations for Hyper-V to Azure
Profiled data period: 10 days (11/1/2017 - 11/10/2017) Number of Hyper-V servers profiled: 26 Desired RPO: 15

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.

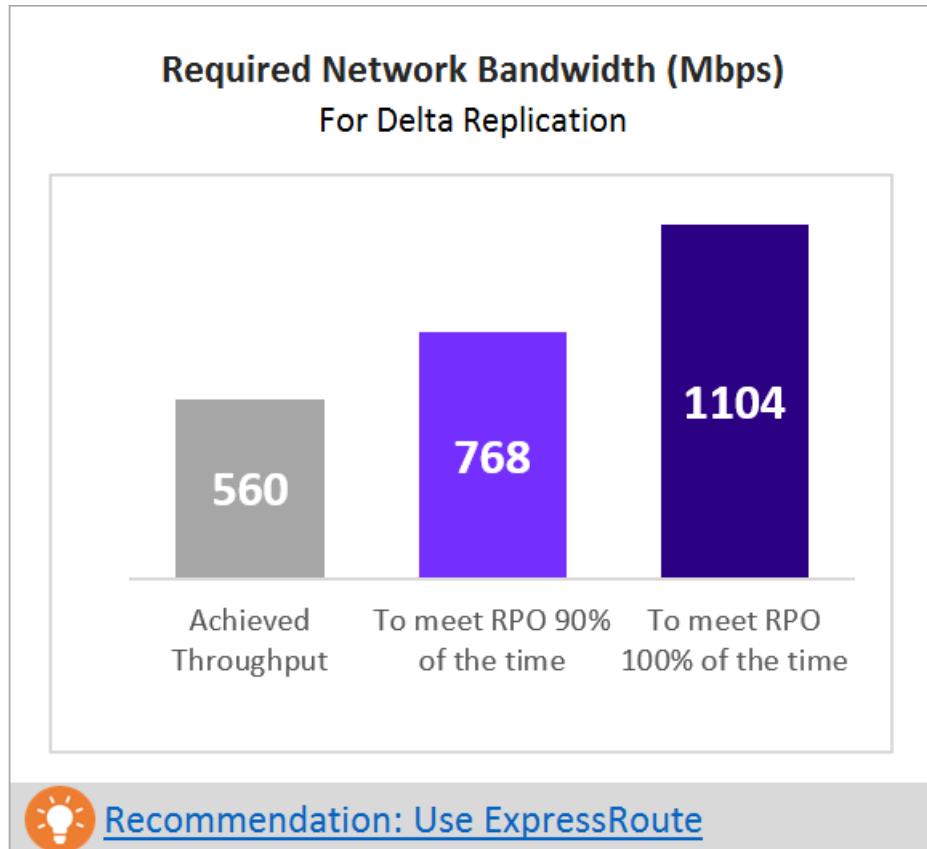
Compatible Virtual Machines: The number of VMs that can be protected to Azure by using Azure Site Recovery. It's the total number of compatible VMs for which the required network bandwidth, number of storage accounts, and number of Azure cores are calculated. The details of every compatible VM are available 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.

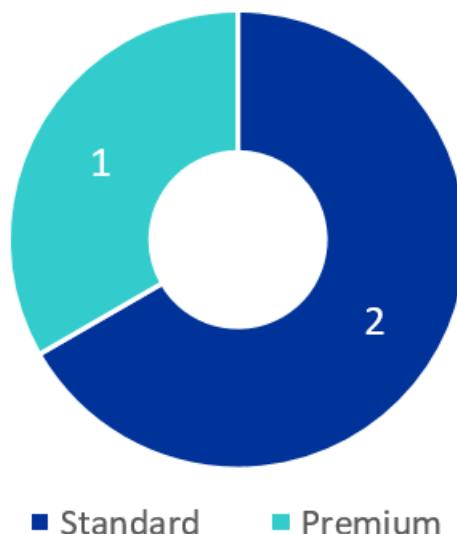
For all enterprise Site Recovery deployments, we recommend that you use [ExpressRoute](#).

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

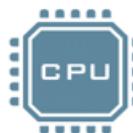


[Recommended VM placement plan](#)

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](#)

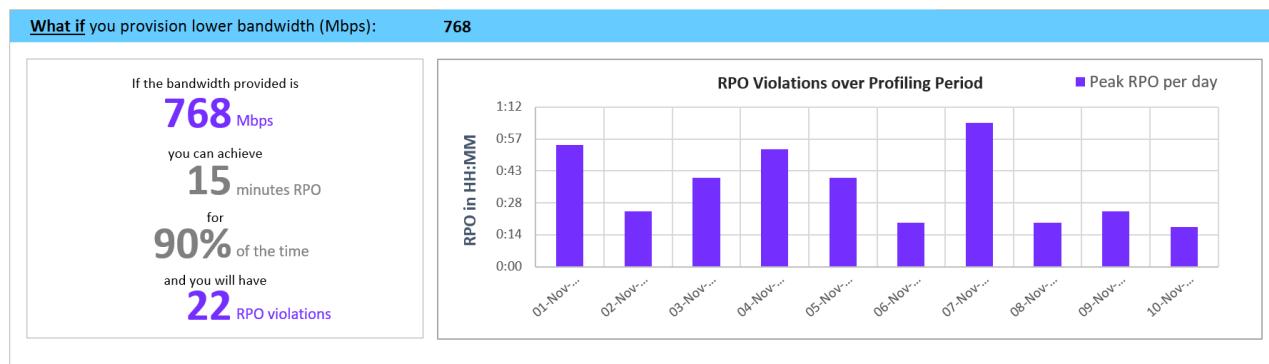


[Learn more](#)

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

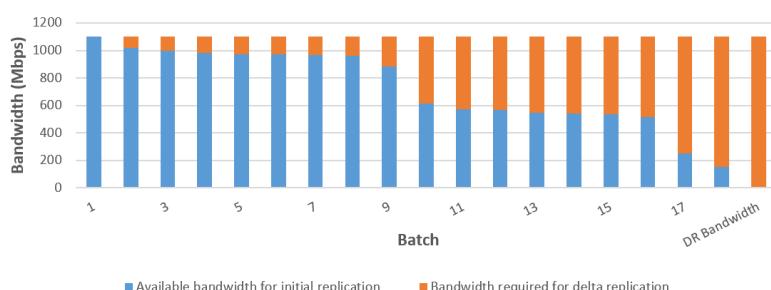
Minimum bandwidth required

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.

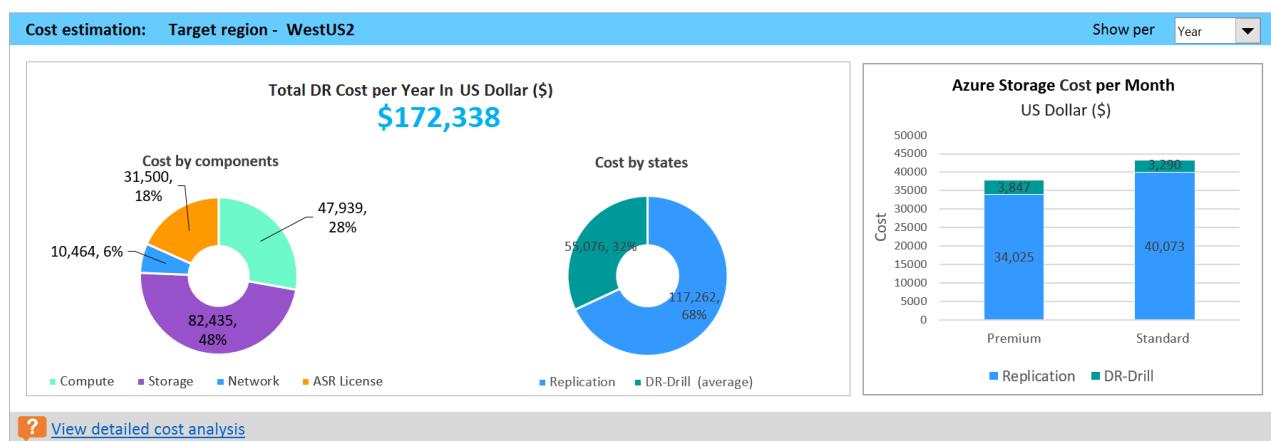
The graph here shows the bandwidth distribution for initial replication and delta replication across batches in the given batch order. When you protect the first batch of VMs, full bandwidth is available for initial replication. After initial replication is finished for the first batch, part of the bandwidth 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](#)

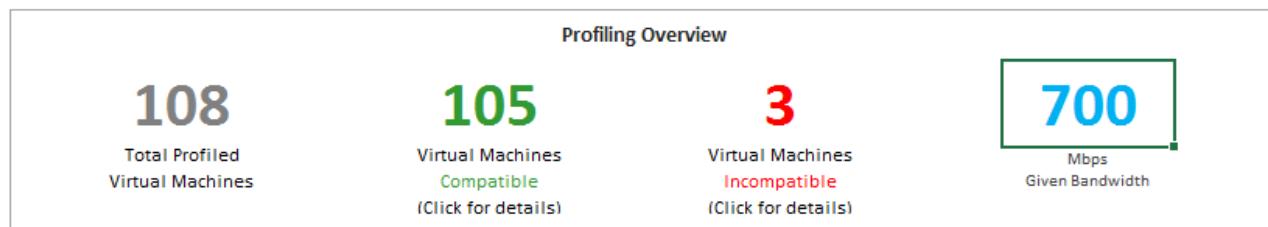
Max value of IOPS and data churn of the profiled data considered for calculating bandwidth and Azure storage type: [Learn more](#)

Write IOPS percentile:	95
Read/Write IOPS percentile:	95
Data churn percentile:	95

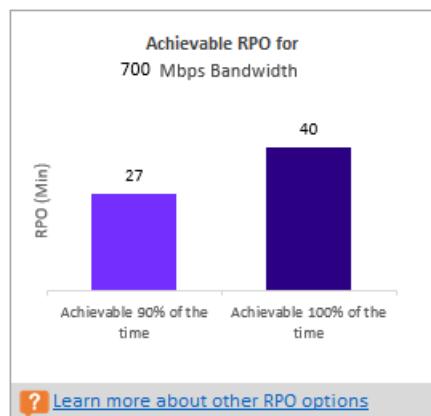
Note:

- 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	hlcpremium1>	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><co1magicsql1_h.vhdx		P40			273	24.17					1832		
C-ClusterStorage-Volume4<co1magicsql1_i><co1magicsql1_j.vhdx		P10			0	0.00					51		
C-ClusterStorage-Volume4<co1magicsql1_k><co1magicsql1_l.vhdx		P20			1789	1.93					500		
C-ClusterStorage-Volume4<co1magicsql1_m><co1magicsql1_n.vhdx		P10			0	0.00					50		
c-clusterstorage-volume<co1magicsql1><co1magicsql1_vm2012t2sp0.vhdx		P10			86	1.58					100		
co1ecitweb05 (CO1-CU-SV-E0003)	Yes*	Premium	hr	hlrpremium1>	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_C01ECITWEB05_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_c><co1ecitweb07_d.vhdx		S6			12	0.09					51		
C-ClusterStorage-Volume2<co1ecitweb07_C01ECITWEB07_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_c><co1plappsm02_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 [Azure premium storage](#). Here, the profiled high churn or IOPS disk fits in higher premium storage disk type 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-E8002)	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_e.vhdx	Not Supported (Disk size > 4095 GB)	0	0.00		5120				
C:\ClusterStorage\Volume4\co1vellumsql10\co1vellumsql10_f.vhdx	Not Supported (Disk size > 4095 GB)	0	0.00		4096				
C:\ClusterStorage\Volume4\co1vellumsql10\co1vellumsql10_g.vhdx	Not Supported (Disk size > 4095 GB)	0	0.00		4096				
C:\ClusterStorage\Volume4\co1vellumsql10\co1vellumsql10_h.vhdx	Not Supported (Disk size > 4095 GB)	3	0.01		5120				
C:\ClusterStorage\Volume4\co1vellumsql10\co1vellumsql10_i.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	Not Supported (Disk size > 4095 GB)	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 10 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	10 MB/s per VM	842 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
Total additional storage to be provisioned (GB)				511,925

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													
Learn more about initial replication batching for Hyper-V to Azure													
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)													
Hyper-V host			Storage requirements										
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	mssx012	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					
CO1-CU-SV-EB005	test-offsite02		C:\ClusterStorage\Volume3	35,316	300	150	0	0.00					
CO1-CU-SV-EB006	co1vmbg1tco0e2		C:\ClusterStorage\Volume6	922	121	61	0	0.30					
CO1-CU-SV-EB007	mssx011	Add additional storage to protect this VM	C:	32	4,299	2,150	4,267	0.23					
CO1-CU-SV-EB008	co1nps-sgrp-01		C:\ClusterStorage\Volume1	39,001	250	125	0	0.03					
	co1gptrvsn01		C:\ClusterStorage\Volume2	32,669	1,001	501	0	0.06					
			C:\ClusterStorage\Volume3	33,307	52,742	26,371	19,435						
				29	52,742	26,371	52,713						
CO1-CU-SV-EC001	co1scnrvqxp01a	Add additional storage to protect this VM	C:\ClusterStorage\SharedStandardPlus_CSV2_1237_00046	30,224	52,742	26,371	22,518						
			C:\ClusterStorage\SharedStandardPlus_CSV1_1237_00090	13,233	52,742	26,371	39,509						
			C:\ClusterStorage\SharedStandardPlus_CSV3_1237_010	19,499	52,742	26,371	33,243	0.47					
CO1-CU-SV-EC005	co1converge001		C:\ClusterStorage\Volume5	43,198	7,408	3,704	0	0.26					
CO1-CU-SV-ED001	co1-sfsq0-07	Add additional storage to protect this VM	C:	41,217	10,557	5,279	0	0.16					
CO1-CU-SV-ED004	co1-sfsq0-03	Add additional storage to protect this VM	C:\ClusterStorage\Volume2	38,062	10,865	5,433	0	0.11					
			C:	30	10,865	5,433	10,835						
CO1-CU-SV-ED004	co1-sfsq0-03	Add additional storage to protect this VM	C:\ClusterStorage\Volume2	38,052	10,865	5,433	0	0.11					
			C:	30	10,865	5,433	10,835						
CO1-CU-SV-ED006	co1-sfsq0-02		C:\ClusterStorage\Volume1	43,214	10,857	5,429	0	0.11					
CO1-CU-SV-EE002	co1-corp-a-01		C:\ClusterStorage\HighPerf_CSV1_0360_0003	15,127	10,857	5,429	0	0.08					
CO1-CU-SV-EE003	co1pdmuets01		C:\ClusterStorage\Volume2	31,216	5,037	2,519	0	0.93					
CO1-CU-SV-EE004	co1etprodwe02		C:\ClusterStorage\Volume3	35,059	2,619	1,310	0	0.01					
CO1-CU-SV-EE005	co1-dsake-03		C:\ClusterStorage\Volume1	46,276	250	125	0	0.03					
CO1-CU-SV-GA001	co1vmfseddt01		C:\ClusterStorage\SharedStandardPlus_CSV1_1640_0105	34,585	13,102	6,551	0	0.27					
Network Utilization Details for Batch 1													
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)													
Hyper-V host			Storage requirements										
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	co1d0sf0101		C:\ClusterStorage\Volume4	58,876	615	308	0	0.25					
CO1-CU-SV-EB002	co1d0ssq00b	Add additional storage to protect this VM	C:\ClusterStorage\Volume5	862	2,102	1,051	1,240	0.22					
CO1-CU-SV-EB004	co1ectheweb1		C:\ClusterStorage\Volume3	53,356	650	325	0	0.01					
	co1pprappm02		C:\ClusterStorage\Volume2	31,558	200	100	0	0.05					
			C:\ClusterStorage\Volume3	4,516	26,273	13,137	19,337						
			C:	28	26,273	13,137	26,245						
CO1-CU-SV-EC007	co1icesq010a	Add additional storage to protect this VM	C:\ClusterStorage\SharedStandardPlus_CSV3_1237_0100	4,672	26,273	13,137	33,145	0.23					
Each batch provides the following information													
Hyper-V host: The Hyper-V host of the VM to be protected.													
Virtual Machine: The VM to be protected.													
Comments: 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."													
Volume (VHD path): The volume name where the VM's VHDs reside.													
Free space available on the volume (GB): 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.													
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													

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](#).

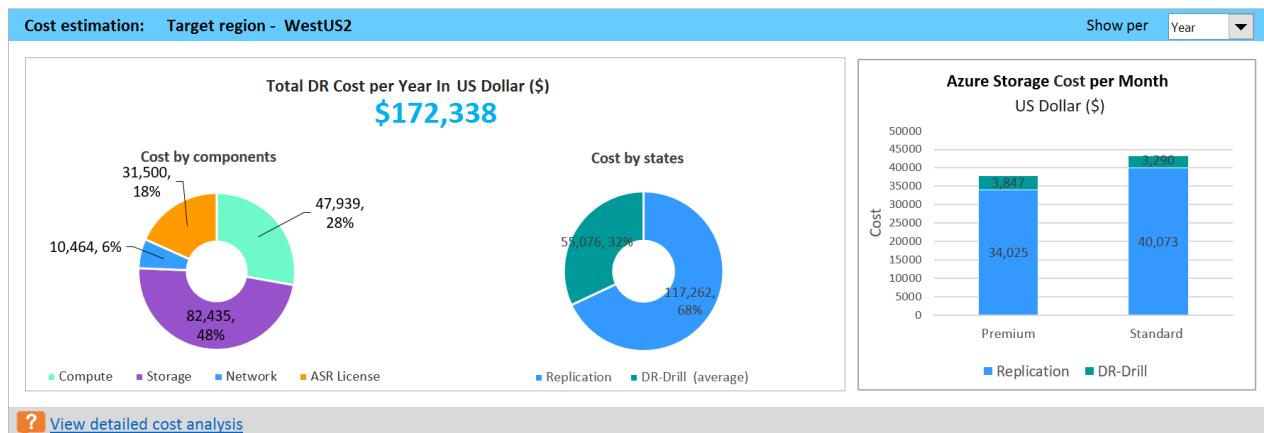
Cost estimation report by Azure Site Recovery Deployment Planner

8/2/2018 • 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
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)		Storage cost - Month (with discount)	
Replication	DR-Drill	Replication	DR-Drill	Replication	DR-Drill
Premium	\$34,025	\$3,847	\$34,025	\$3,847	\$2,835
Standard	\$40,073	\$3,290	\$40,073	\$3,290	\$3,339
Total	\$74,098	\$7,137	\$74,098	\$7,137	\$6,175
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 (\$)	
Apply overall discount if applicable	Discount in (%)		Cost duration	Year	
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	VM total storage size (GB) (Replication)	Number of DR-Drills in a year	Each DR-Drill duration (Days)
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
copiapippsm02 (CO1-CU-SV-EB004)	1	Standard_A2	Standard_A2	Standard	200.00	4	7
co1su1407 (CO1-CU-SV-EB004)	1	Standard_A4	Standard_A4	Standard	300.00	4	7
co1xitexsqla (CO1-CU-SV-EB004)	1	Standard_D5_v2	Standard_D5_v2	Standard	1194.00	4	7
co1bimsspol01 (CO1-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.

ASR 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 'Insert row' button below to insert a new row between Start and End 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 'Re-calculate cost' to update the cost.													
Learn more about cost estimation													
Insert row		Re-calculate cost		IaaS characteristics									
				Cost breakdown									
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 + Licenses)	Steady state replication cost per Year (Storage)	Total DR-Drill cost per Year (Compute + Storage)
START/INSERT A ROW BELOW TO ADD A NEW ENTRY											\$0	\$0	\$0
colmagisql1 (CO1-CU-SV-E0003)	1	Standard_D5S_v2	Standard_D5S_v2	Premium	2849.00	4	7	Windows LRS	Apply to all	Yes	\$5,862	\$4,954	\$608
collectiveb05 (CO1-CU-SV-E0003)	1	Standard_D5S_v2	Standard_D5S_v2	Premium	652.00	4	7	Windows LRS	Yes	Yes	\$1,577	\$1,095	\$181
colisus1407 (CO1-CU-SV-E0003)	1	Standard_A2	Standard_A2	Standard	652.00	4	7	Windows LRS	Yes	Yes	\$831	\$520	\$31
colisus1407 (CO1-CU-SV-E0003)	1	Standard_A2	Standard_A2	Standard	200.00	4	7	Windows LRS	Yes	Yes	\$544	\$320	\$24
colisus1407 (CO1-CU-SV-E0004)	1	Standard_A4	Standard_A4	Standard	300.00	4	7	Windows LRS	Yes	Yes	\$767	\$5180	\$287
colibrimsspol01 (CO1-CU-SV-E001)	1	Standard_D5_v2	Standard_D5_v2	Standard	1194.00	4	7	Windows LRS	Yes	Yes	\$1,205	\$716	\$189
colibrimsspol01 (CO1-CU-SV-E001)	1	Standard_A4	Standard_A4	Standard	550.00	4	7	Windows LRS	Yes	Yes	\$928	\$530	\$298
colisus1407 (CO1-CU-SV-E0004)	1	Standard_A2	Standard_A2	Standard	50.00	4	7	Windows LRS	Yes	Yes	\$400	\$320	\$30
collectiveb11 (CO1-CU-SV-E0004)	1	Standard_A2	Standard_A2	Standard	50.00	4	7	Windows LRS	Yes	Yes	\$884	\$500	\$164
colisusw10 (CO1-CU-SV-E0004)	1	Standard_G5	Standard_G5	Standard	1221.00	4	7	Windows LRS	Yes	Yes	\$6,391	\$733	\$5,358
col1vnsynweb10 (CO1-CU-SV-E8)	1	Standard_G5	Standard_G5	Standard	200.00	4	7	Windows LRS	Yes	Yes	\$5,701	\$120	\$5,281

The table lists the cost breakdown for each compatible VM. You also can use this table to get the estimated Azure DR cost of nonprofiled VMs by manually adding VMs. This information is useful in cases where you need to estimate Azure costs for a new DR deployment without detailed profiling.

To manually add VMs:

- Select **Insert row** to insert a new row between the **Start** and **End** rows.
- Fill in the following columns based on approximate VM size and the number of VMs 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**
 - Azure Hybrid Use Benefit**
- You can apply the same value to all VMs in the table by selecting **Apply to all** for **Number of DR-Drills in a year**, **Each DR-Drill duration (Days)**, **Data redundancy**, and **Azure Hybrid Use Benefit**.
- Select **Re-calculate cost** to update the 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 existing VMs if a similar configuration of VMs isn't profiled but protected.

IaaS size (Recommendation): The VM role size of the compatible VM that the tool recommends.

IaaS size (Your selection): By default, the size is the same as the 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 storage that is used by the VM. It's either standard or premium storage.

VM total storage size (GB): The total storage of the VM.

Number of DR-Drills in a year: The number of times you perform DR drills in a year. By default, it's four times in a year. You can modify the period for specific VMs or apply the new value to all VMs. Enter the new value in the top row, and select **Apply to all**. Based on the 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'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.

ASR 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](#).

Set up disaster recovery to Azure for Hyper-V VMs using PowerShell and Azure Resource Manager

8/10/2018 • 6 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.

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. Read [Getting started with Windows PowerShell](#), 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 1.0. For information about this release and how to install it, see [Azure PowerShell 1.0](#).
- The [AzureRM.SiteRecovery](#) and [AzureRM.RecoveryServices](#) modules. You can get the latest versions of these modules from the [PowerShell gallery](#)

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-AzureRmAccount**.
 - Alternately, you can include your account credentials as a parameter in the **Connect-AzureRmAccount** cmdlet, using the **-Credential** parameter.

- If you are 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-AzureRmAccount -Tenant "fabrikam.com"**
- Associate the subscription you want to use with the account, since an account can have several subscriptions:

```
Select-AzureRmSubscription -SubscriptionName $SubscriptionName
```

- Verify that your subscription is registered to use the Azure providers for Recovery Services and Site Recovery, using these commands:

```
Get-AzureRmResourceProvider -ProviderNamespace Microsoft.RecoveryServices
Get-AzureRmResourceProvider -ProviderNamespace Microsoft.SiteRecovery
```

- 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-AzureRmResourceProvider -ProviderNamespace Microsoft.SiteRecovery
Register-AzureRmResourceProvider -ProviderNamespace Microsoft.RecoveryServices
```

- Verify that the Providers registered successfully, using the following commands:

```
Get-AzureRmResourceProvider -ProviderNamespace Microsoft.RecoveryServices
Get-AzureRmResourceProvider -ProviderNamespace Microsoft.SiteRecovery .
```

Step 2: Set up the vault

- 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-AzureRmResourceGroup -Name $ResourceGroupName -Location $Geo
```

- To obtain a list of resource groups in your subscription run the **Get-AzureRmResourceGroup** cmdlet.
- Create a new Azure Recovery Services vault as follows:

```
$vault = New-AzureRmRecoveryServicesVault -Name <string> -ResourceGroupName <string> -Location <string>
```

You can retrieve a list of existing vaults with the **Get-AzureRmRecoveryServicesVault** cmdlet.

Step 3: Set the Recovery Services vault context

Set the vault context as follows:

```
Set-AzureRmSiteRecoveryVaultSettings -ARSVault $vault
```

Step 4: Create a Hyper-V site

- Create a new Hyper-V site as follows:

```
$sitename = "MySite" #Specify site friendly name
New-AzureRmSiteRecoverySite -Name $sitename
```

- 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-AzureRmSiteRecoveryJob 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-AzureRmSiteRecoverySite -Name $sitename | Select -ExpandProperty SiteIdentifier
Get-AzureRmRecoveryServicesVaultSettingsFile -Vault $vault -SiteIdentifier $SiteIdentifier -
SiteFriendlyName $sitename -Path $Path
```

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 theHyper-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-AzureRmSiteRecoveryServer -FriendlyName $server-friendlyname
```

Step 6: Create a replication policy

Before you start, note that 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-AzureRmStorageAccount -Name "mystorea" -ResourceGroupName "MyRG" | Select -
ExpandProperty Id

$PolicyResult = New-AzureRmSiteRecoveryPolicy -Name $PolicyName -ReplicationProvider
"HyperVReplicaAzure" -ReplicationFrequencyInSeconds $ReplicationFrequencyInSeconds -RecoveryPoints
$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-AzureRmSiteRecoveryProtectionContainer
```

4. Associate the protection container with the replication policy, as follows:

```
$Policy = Get-AzureRmSiteRecoveryPolicy -FriendlyName $PolicyName $associationJob = Start-
AzureRmSiteRecoveryPolicyAssociationJob -Policy $Policy -PrimaryProtectionContainer
$protectionContainer
```

5. Wait for the association job to complete successfully.

Step 7: Enable VM protection

1. Retrieve the protection entity that corresponds to the VM you want to protect, as follows:

```
$VMFriendlyName = "Fabrikam-app"           #Name of the VM
$protectionEntity = Get-AzureRmSiteRecoveryProtectionEntity -ProtectionContainer $protectionContainer
-FriendlyName $VMFriendlyName
```

2. Protect the VM. If the VM you are 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 = Set-AzureRmSiteRecoveryProtectionEntity -ProtectionEntity $protectionEntity -Policy $Policy -
Protection Enable -RecoveryAzureStorageAccountId $storageaccountID -OS $Ostype -OSDiskName
$protectionEntity.Disks[0].Name
```

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-AzureRmSiteRecoveryJob -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-AzureRmVirtualNetwork -Name "FailoverNw" -ResourceGroupName "MyRG"

PS C:\> $VMFriendlyName = "Fabrikam-App"

PS C:\> $VM = Get-AzureRmSiteRecoveryVM -ProtectionContainer $protectionContainer -FriendlyName
$VMFriendlyName

PS C:\> $UpdateJob = Set-AzureRmSiteRecoveryVM -VirtualMachine $VM -PrimaryNic
$VM.NicDetailsList[0].NicId -RecoveryNetworkId $nw1.Id -RecoveryNicSubnetName $nw1.Subnets[0].Name

PS C:\> $UpdateJob = Get-AzureRmSiteRecoveryJob -Job $UpdateJob

PS C:\> $UpdateJob

Name          : b8a647e0-2cb9-40d1-84c4-d0169919e2c5
ID           : /Subscriptions/a731825f-4bf2-4f81-a611-
c331b272206e/resourceGroups/MyRG/providers/Microsoft.RecoveryServices/vault
              s/MyVault/replicationJobs/b8a647e0-2cb9-40d1-84c4-d0169919e2c5
Type         : Microsoft.RecoveryServices/vaults/replicationJobs
JobType       : UpdateVmProperties
DisplayName   : Update the virtual machine
ClientRequestId : 805a22a3-be86-441c-9da8-f32685673112-2015-12-10 17:55:51Z-P
State         : Succeeded
StateDescription : Completed
StartTime     : 10-12-2015 17:55:53 +00:00
EndTime       : 10-12-2015 17:55:54 +00:00
TargetObjectId : 289682c6-c5e6-42dc-a1d2-5f9621f78ae6
TargetObjectType : ProtectionEntity
TargetObjectName : Fabrikam-App
AllowedActions  : {Restart}
Tasks          : {UpdateVmPropertiesTask}
Errors         : {}

```

Step 8: Run a test failover

- Run a test failover as follows:

```

$nw = Get-AzureRmVirtualNetwork -Name "TestFailoverNw" -ResourceGroupName "MyRG" #Specify Azure vnet
name and resource group

$protectionEntity = Get-AzureRmSiteRecoveryProtectionEntity -FriendlyName $VMFriendlyName -
ProtectionContainer $protectionContainer

$TFjob = Start-AzureRmSiteRecoveryTestFailoverJob -ProtectionEntity $protectionEntity -Direction
PrimaryToRecovery -AzureVMNetworkId $nw.Id

```

- Verify that the test VM is created in Azure. The test failover job is suspended after creating the test VM in Azure.
- To clean up and complete the test failover, run:

```
$TFjob = Resume-AzureRmSiteRecoveryJob -Job $TFjob
```

Next steps

[Learn more](#) about Azure Site Recovery with Azure Resource Manager PowerShell cmdlets.

Replicate Hyper-V VMs to a secondary site by using PowerShell (Resource Manager)

7/9/2018 • 6 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](#).

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-AzureRmAccount #-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-AzureRmSubscription
```

3. Set the subscription for the vault.

```
Set-AzureRmContext -SubscriptionID <subscriptionId>
```

Create a Recovery Services vault

1. Create an Azure Resource Manager resource group if you don't have one.

```
New-AzureRmResourceGroup -Name #ResourceGroupName -Location #location
```

2. Create a new Recovery Services vault. Save the vault object in a variable to be used later.

```
$vault = New-AzureRmRecoveryServicesVault -Name #vaultname -ResouceGroupName #ResourceGroupName -  
Location #location
```

You can retrieve the vault object after you create it by using the Get-AzureRMRecoveryServicesVault cmdlet.

Set the vault context

1. Retrieve an existing vault.

```
$vault = Get-AzureRmRecoveryServicesVault -Name #vaultname
```

2. Set the vault context.

```
Set-AzureRmSiteRecoveryVaultSettings -ARSVault $vault
```

Install the Site Recovery provider

1. On the Virtual Machine Manager machine, create a directory by running the following command:

```
New-Item c:\ASR -type 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 pints  
$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-AzureRmSiteRecoveryPolicy -Name $policyname -ReplicationProvider $RepProvider -  
ReplicationFrequencyInSeconds $Replicationfrequencyinseconds -RecoveryPoints $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-AzureRmSiteRecoveryProtectionContainer -friendlyName $PrimaryCloud;  
  
$RecoveryCloud = "testrecoverycloud"  
$recoveryprotectionContainer = Get-AzureRmSiteRecoveryProtectionContainer -friendlyName $RecoveryCloud;
```

3. Retrieve the replication policy you created by using the friendly name.

```
$policy = Get-AzureRmSiteRecoveryPolicy -FriendlyName $policynam
```

4. Start the association of the protection container (Virtual Machine Manager cloud) with the replication policy.

```
$associationJob = Start-AzureRmSiteRecoveryPolicyAssociationJob -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-AzureRmSiteRecoveryJob -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-AzureRmSiteRecoveryServer
```

2. Run this command to retrieve the networks for the source Virtual Machine Manager server and the target Virtual Machine Manager server.

```
$PrimaryNetworks = Get-AzureRmSiteRecoveryNetwork -Server $Servers[0]  
  
$RecoveryNetworks = Get-AzureRmSiteRecoveryNetwork -Server $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-AzureRmSiteRecoveryNetworkMapping -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-AzureRmSiteRecoveryProtectionContainer -friendlyName  
$PrimaryCloudName
```

2. Get the protection entity (VM), as follows:

```
$protectionEntity = Get-AzureRmSiteRecoveryProtectionEntity -friendlyName $VMName -  
ProtectionContainer $PrimaryProtectionContainer
```

3. Enable replication for the VM.

```
$jobResult = Set-AzureRmSiteRecoveryProtectionEntity -ProtectionEntity $protectionentity -Protection  
Enable -Policy $policy
```

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-AzureRmSiteRecoveryServer  
$RecoveryNetworks = Get-AzureRmSiteRecoveryNetwork -Server $Servers[1]
```

2. Perform a test failover.

For a single VM:

```
$protectionEntity = Get-AzureRmSiteRecoveryProtectionEntity -FriendlyName $VMName -ProtectionContainer  
$PrimaryProtectionContainer  
  
$jobIDResult = Start-AzureRmSiteRecoveryTestFailoverJob -Direction PrimaryToRecovery -ProtectionEntity  
$protectionEntity -VMNetwork $RecoveryNetworks[1]
```

For a recovery plan:

```
$recoveryplanname = "test-recovery-plan"  
  
$recoveryplan = Get-AzureRmSiteRecoveryRecoveryPlan -FriendlyName $recoveryplanname  
  
$jobIDResult = Start-AzureRmSiteRecoveryTestFailoverJob -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-AzureRmSiteRecoveryProtectionEntity -Name $VMName -ProtectionContainer  
$PrimaryprotectionContainer  
  
$jobIDResult = Start-AzureRmSiteRecoveryPlannedFailoverJob -Direction PrimaryToRecovery -  
ProtectionEntity $protectionEntity
```

For a recovery plan:

```
$recoveryplanname = "test-recovery-plan"  
  
$recoveryplan = Get-AzureRmSiteRecoveryRecoveryPlan -FriendlyName $recoveryplanname  
  
$jobIDResult = Start-AzureRmSiteRecoveryPlannedFailoverJob -Direction PrimaryToRecovery -Recoveryplan  
$recoveryplan
```

2. Perform an unplanned failover.

For a single VM:

```
$protectionEntity = Get-AzureRmSiteRecoveryProtectionEntity -Name $VMName -ProtectionContainer  
$PrimaryprotectionContainer  
  
$jobIDResult = Start-AzureRmSiteRecoveryUnPlannedFailoverJob -Direction PrimaryToRecovery -  
ProtectionEntity $protectionEntity
```

For a recovery plan:

```
$recoveryplanname = "test-recovery-plan"  
  
$recoveryplan = Get-AzureRmSiteRecoveryRecoveryPlan -FriendlyName $recoveryplanname  
  
$jobIDResult = Start-AzureRmSiteRecoveryUnPlannedFailoverJob -Direction PrimaryToRecovery -  
ProtectionEntity $protectionEntity
```

Monitor activity

Use the following commands to monitor failover activity. Wait for the processing to finish in between jobs.

```
Do
{
    $job = Get-AzureSiteRecoveryJob -Id $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.

Prepare network mapping for Hyper-V VM replication to Azure

7/9/2018 • 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

7/9/2018 • 8 minutes to read • [Edit Online](#)

This article describes how to exclude disks from replication. This exclusion can optimize the consumed replication bandwidth or optimize the target-side resources that such disks utilize.

Supported scenarios

FEATURE	VMWARE TO AZURE	HYPER-V TO AZURE	AZURE TO AZURE	HYPER-V TO HYPER-V
Exclude disk	Yes	Yes	No	No

Why exclude disks from replication?

Excluding disks from replication is often necessary because:

- The data that's churned on the excluded disk is not important or doesn't need to be replicated.
- You want to save storage and network resources by not replicating this churn.

What are the typical scenarios?

You can identify specific examples of data churn that are great candidates for exclusion. Examples might 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 file can register a significant amount of churn. However, replicating this data from the primary site to Azure would be resource intensive. Thus, you can use the following steps to optimize replication of a virtual machine with a single virtual disk that has both the operating system and the paging file:

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.

Similarly, you can use the following steps to optimize a disk that has both the Microsoft SQL Server tempdb file and the system database file:

1. Keep the system database and tempdb on two different disks.
2. Exclude the tempdb disk from replication.

How to Exclude disks

Follow the [Enable replication](#) workflow to protect a virtual machine from the Azure Site Recovery portal. In the fourth step of the workflow, use the **DISK TO REPLICATE** column to exclude disks from replication. By default, all disks are selected for replication. Clear the check box of disks that you want to exclude from replication, and then complete the steps to enable replication.

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	...

<input checked="" type="checkbox"/> Sales_FE1-Disk2 [40 GB]
<input checked="" type="checkbox"/> Sales_FE1-Disk3 [100 GB]
<input type="checkbox"/> Sales_FE1-Disk4 [100 GB]
<input checked="" type="checkbox"/> Sales_Frontend1-Disk1-OS [60 GB]

NOTE

- You can exclude only basic disks from replication. You can't exclude operating system disks. We recommend that you do not exclude dynamic disks. Azure Site Recovery cannot identify which virtual hard disk (VHD) is basic or dynamic in the guest virtual machine. If all dependent dynamic volume disks are not excluded, the protected dynamic disk becomes a failed disk on a failover virtual machine, and the data on that disk is not accessible.
- After you enable replication, you can't add or remove disks for replication. If you want to add or exclude a disk, you need to disable protection for the virtual machine and then enable it again.
- If you exclude a disk that's needed for an application to operate, after failover to Azure you need to create the disk manually in Azure so that the replicated application can run. Alternatively, you can integrate Azure automation into a recovery plan to create the disk during failover of the machine.
- Disks that you create manually in Azure will not be failed back. For example, if you fail over three disks and create two disks directly in Azure Virtual Machines, only three disks that were failed over will be failed back from Azure to Hyper-V. You can't include disks that were created manually in failback or in reverse replication from Hyper-V to Azure.

End-to-end scenarios of exclude disks

Let's consider two scenarios to understand the exclude disk feature:

- SQL Server tempdb disk
- Paging file (pagefile.sys) disk

Example 1: Exclude the SQL Server tempdb disk

Let's consider a SQL Server virtual machine that has a tempdb that can be excluded.

The name of the virtual disk is SalesDB.

Disks on the source virtual machine are as follows:

DISK NAME	GUEST OPERATING SYSTEM DISK#	DRIVE LETTER	DATA TYPE ON THE DISK
DB-Disk0-OS	DISK0	C:\	Operating system disk

DISK NAME	GUEST OPERATING SYSTEM DISK#	DRIVE LETTER	DATA TYPE ON THE 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)) Write down the folder path before failover.
DB-Disk4	Disk4	G:\	User Database2

Because data churn on two disks of the virtual machine is temporary, while you protect the SalesDB virtual machine, exclude Disk2 and Disk3 from replication. Azure Site Recovery will not replicate those disks. On failover, those disks will not be present on the failover virtual machine on Azure.

Disks on the Azure virtual machine after failover are as follows:

GUEST OPERATING SYSTEM DISK#	DRIVE LETTER	DATA TYPE ON THE DISK
DISK0	C:\	Operating system disk
Disk1	E:\	Temporary storage Azure adds this disk and assigns the first available drive letter.
Disk2	D:\	SQL system database and User Database1
Disk3	G:\	User Database2

Because Disk2 and Disk3 were excluded from the SalesDB virtual machine, E: is the first drive letter from the available list. Azure assigns E: to the temporary storage volume. For all the replicated disks, the drive letters remain the same.

Disk3, which was the SQL tempdb disk (tempdb folder path F:\MSSQL\Data), was excluded from replication. The disk is not available on the failover virtual machine. As a result, the SQL service is in a stopped state, and it needs the F:\MSSQL\Data path.

There are two ways to create this path:

- Add a new disk and assign tempdb folder path.
- Use an existing temporary storage disk for the tempdb folder path.

Add a new disk:

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 virtual machine with the same or more size as that of the source SQL tempdb disk (Disk3).
3. Sign in to the Azure virtual machine. From the disk management (diskmgmt.msc) console, initialize, and format the newly added disk.

4. Assign the same drive letter that was used by the SQL tempdb disk (F:).
5. Create a tempdb folder on the F: volume (F:\MSSQL\Data).
6. Start the SQL service from the service console.

Use an existing temporary storage disk for the SQL tempdb folder path:

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
```

Refer to the following Azure guideline for temporary storage disk:

- [Using SSDs in Azure VMs to store SQL Server TempDB and Buffer Pool Extensions](#)
- [Performance best practices for SQL Server in Azure Virtual Machines](#)

Fallback (from Azure to an on-premises host)

Now let's understand the disks that are replicated when you fail over from Azure to your on-premises Hyper-V host. Disks that you create manually in Azure will not be replicated. For example, if you fail over three disks and create two directly in Azure Virtual Machines, only three disks that were failed over will be failed back. You can't include disks that were created manually in fallback or in reprotect from on-premises to Azure. It also does not replicate the temporary storage disk to on-premises hosts.

Fallback to original location recovery

In the previous example, the Azure virtual machine disk configuration is as follows:

GUEST OPERATING SYSTEM DISK#	DRIVE LETTER	DATA TYPE ON THE DISK
DISK0	C:\	Operating system disk

GUEST OPERATING SYSTEM DISK#	DRIVE LETTER	DATA TYPE ON THE DISK
Disk1	E:\	Temporary storage Azure adds this disk and assigns the first available drive letter.
Disk2	D:\	SQL system database and User Database1
Disk3	G:\	User Database2

When failback is to the original location, the failback virtual machine disk configuration remains the same as that of original virtual machine disk configuration for Hyper-V. Disks that were excluded from Hyper-V site to Azure are available on the failback virtual machine.

After planned failover from Azure to on-premises Hyper-V, disks on the Hyper-V virtual machine (original location) are as follows:

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:\	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 (pagefile.sys) disk

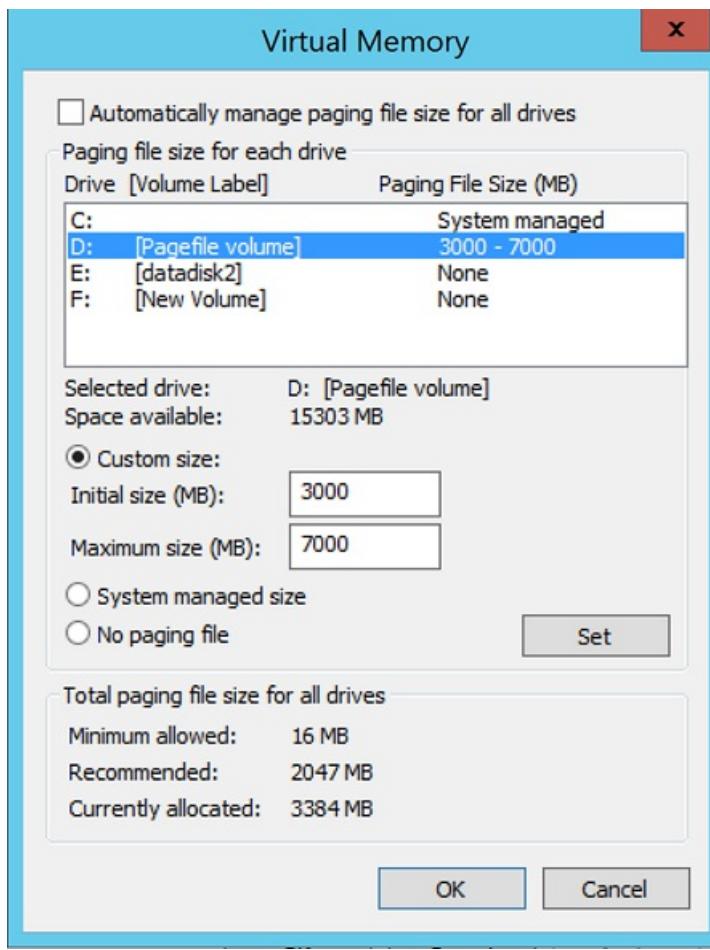
Let's consider a virtual machine that has a paging file disk that can be excluded. There are two cases.

Case 1: The paging file is configured on the D: drive

Here's the disk configuration:

DISK NAME	GUEST OPERATING SYSTEM DISK#	DRIVE LETTER	DATA TYPE ON THE DISK
DB-Disk0-OS	DISK0	C:\	Operating system disk
DB-Disk1 (Excluded the disk from the protection)	Disk1	D:\	pagefile.sys
DB-Disk2	Disk2	E:\	User data 1
DB-Disk3	Disk3	F:\	User data 2

Here are the paging file settings on the source virtual machine:

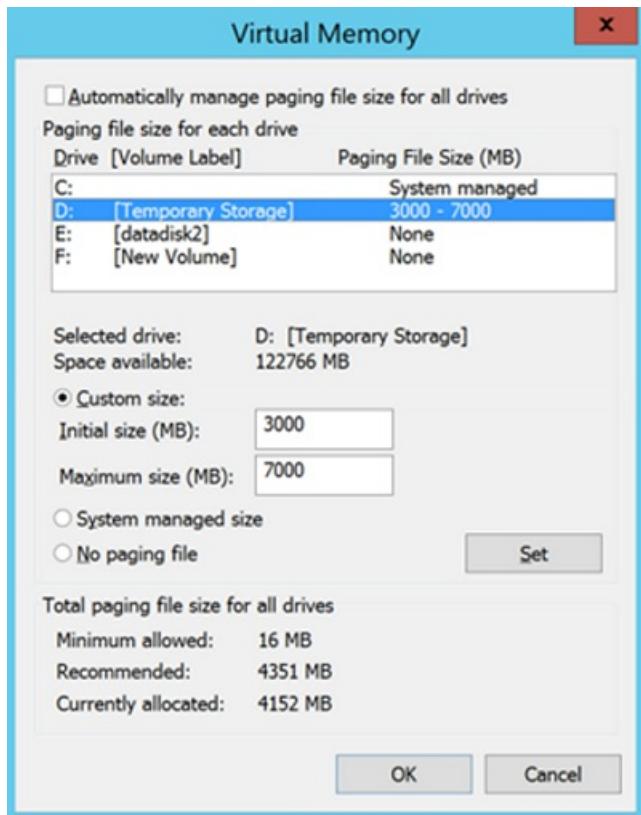


After failover of the virtual machine from Hyper-V to Azure, disks on the Azure virtual machine are as follows:

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:\	Temporary storage pagefile.sys
DB-Disk2	Disk2	E:\	User data 1
DB-Disk3	Disk3	F:\	User data 2

Because Disk1 (D:) was excluded, D: is the first drive letter from the available list. Azure assigns D: to the temporary storage volume. Because D: is available on the Azure virtual machine, the paging file setting of the virtual machine remains the same.

Here are the paging file settings on the Azure virtual machine:

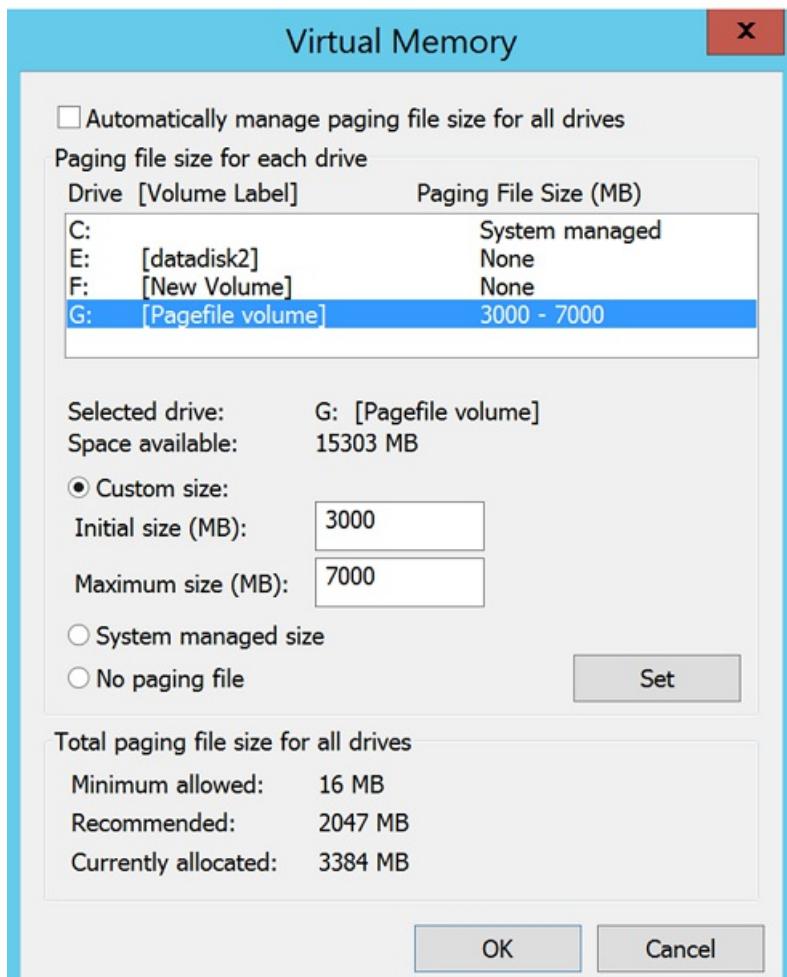


Case 2: The paging file is configured on another drive (other than D: drive)

Here's the source virtual machine disk configuration:

DISK NAME	GUEST OPERATING SYSTEM DISK#	DRIVE LETTER	DATA TYPE ON THE DISK
DB-Disk0-OS	DISK0	C:\	Operating system disk
DB-Disk1 (Excluded the disk from protection)	Disk1	G:\	pagefile.sys
DB-Disk2	Disk2	E:\	User data 1
DB-Disk3	Disk3	F:\	User data 2

Here are the paging file settings on the on-premises virtual machine:

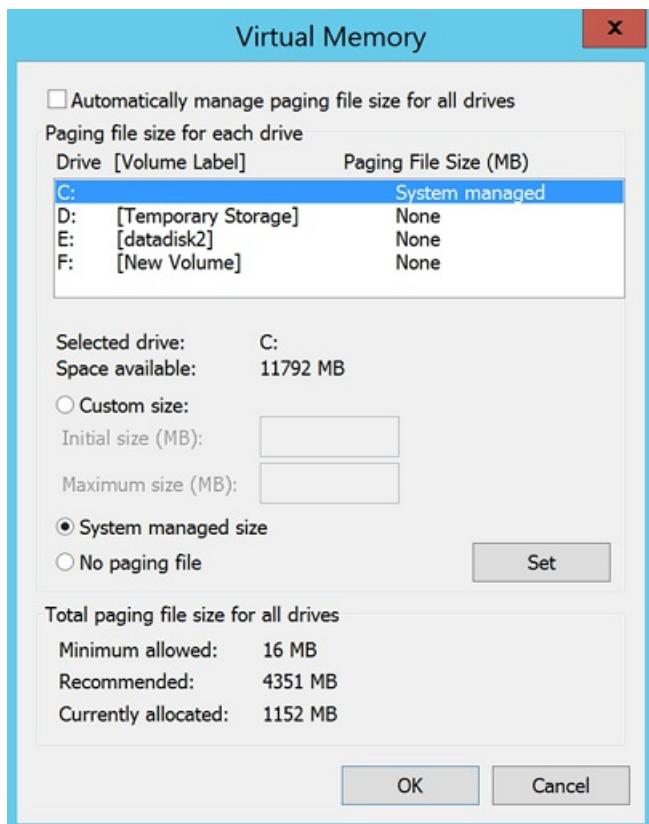


After failover of the virtual machine from Hyper-V to Azure, disks on the Azure virtual machine are as follows:

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:\	Temporary storage pagefile.sys
DB-Disk2	Disk2	E:\	User data 1
DB-Disk3	Disk3	F:\	User data 2

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 is not available, the system will use the C: drive for the paging file.

Here are the paging file settings on the Azure virtual machine:



Next steps

After your deployment is set up and running, [learn more](#) about different types of failover.

Test failover to Azure in Site Recovery

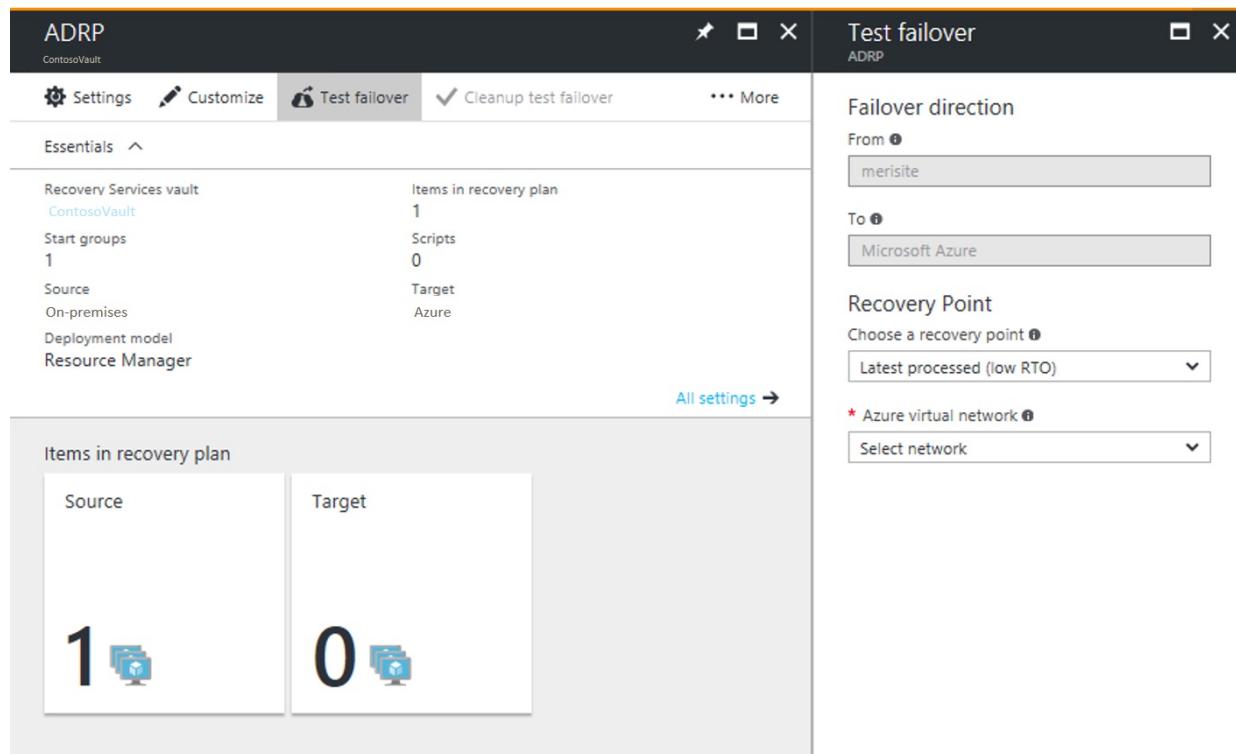
7/13/2018 • 6 minutes to read • [Edit Online](#)

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.



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 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 after failover, follow the requirements summarized in the table.

FAILOVER	LOCATION	ACTIONS
----------	----------	---------

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>

Next steps

After you've completed a disaster recovery drill, learn more about other types of [failover](#).

Create and customize recovery plans

7/24/2018 • 4 minutes to read • [Edit Online](#)

This article describes how to create and customize a recovery plan 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	Azure region	Azure region
VMware to Azure	Configuration server	Azure
Physical machines to Azure	Configuration server	Azure
Hyper-V managed by VMM to Azure	VMM display name	Azure
Hyper-V without VMM to Azure	Hyper-V site name	Azure
VMM to VMM	VMM friendly name	VMM display name

NOTE

A recovery plan can contain machines with the same source and target. VMware and Hyper-V VMs managed by VMM can't be in the same plan. VMware VMs and physical servers can be in the same plan, where the source is a configuration server.

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 failback 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 \\MSSCVMLibrary\\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

8/2/2018 • 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](#).

Add Azure Automation runbooks to recovery plans

8/6/2018 • 7 minutes to read • [Edit Online](#)

In this article, we describe how Azure Site Recovery integrates with Azure Automation to help you extend your recovery plans. Recovery plans can orchestrate recovery of VMs that are protected with Site Recovery. Recovery plans work both for replication to a secondary cloud, and for replication to Azure. Recovery plans also help make the recovery **consistently accurate, repeatable**, and **automated**. If you fail over your VMs to Azure, integration with Azure Automation extends your recovery plans. You can use it to execute runbooks, which offer powerful automation tasks.

If you are new to Azure Automation, you can [sign up](#) and [download sample scripts](#). For more information, and to learn how to orchestrate recovery to Azure by using [recovery plans](#), see [Azure Site Recovery](#).

In this article, we describe how you can integrate Azure Automation runbooks into your recovery plans. We use examples to automate basic tasks that previously required manual intervention. We also describe how to convert a multi-step recovery to a single-click recovery action.

Customize the recovery plan

1. Go to the **Site Recovery** recovery plan resource blade. For this example, the recovery plan has two VMs added to it, for recovery. To begin adding a runbook, click the **Customize** tab.

The screenshot shows the Azure portal interface for managing a Site Recovery plan. The title bar says "SharepointRecovery" and "IbizaAsrTest". The top navigation bar includes "Settings", "Customize" (which is highlighted in blue), "Test failover", "Planned failover", and "... More".

The main content area is divided into sections:

- Essentials**:
 - Recovery Services vault: IbizaAsrTest
 - Start groups: 2
 - Source: CP-L2B18-X64-15.dratest.nttest.microsoft.c...
 - Target: CP-L2B18-X64-15.dratest.nttest.microsoft.c...
 - Deployment model: -
- Items in recovery plan**:

Source	Target
2	0

2. Right-click **Group 1: Start**, and then select **Add post action**.

This recovery plan contains 2 machine(s).

STAGE NAME	DETAILS
All groups shutdown	2 machines in 2 groups.
▶ All groups failover	
▶ Group 1: Start	1 Machine
▶ Group 2: Start	1 Machine

3. Click **Choose a script**.
4. On the **Update action** blade, name the script **Hello World**.

Name: Hello World

Failover to azure script

Automation account name: RPTTestAutomationAccount1

Runbook name: helloworld1

Failover to on-premise script

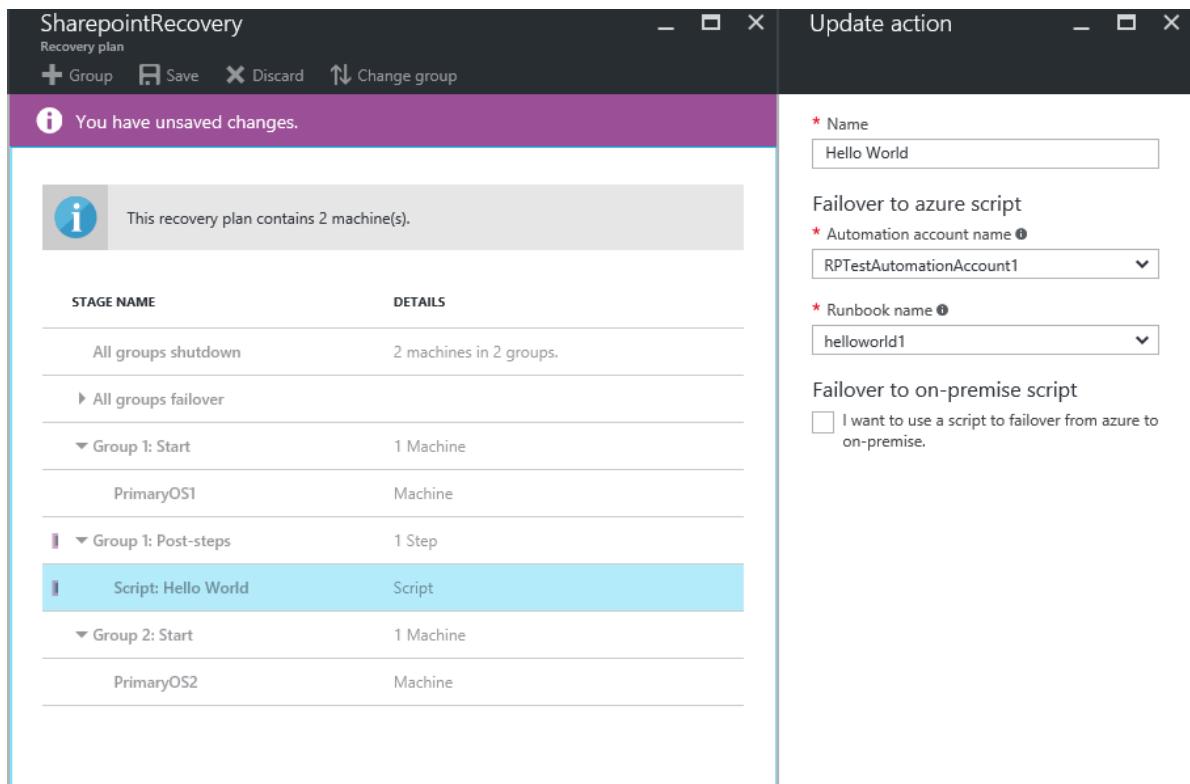
I want to use a script to failover from azure to on-premise.

5. Enter an Automation account name.

NOTE

The Automation account can be in any Azure region. The Automation account must be in the same subscription as the Azure Site Recovery vault.

6. In your Automation account, select a runbook. This runbook is the script that runs during the execution of the recovery plan, after the recovery of the first group.
7. To save the script, click **OK**. The script is added to **Group 1: Post-steps**.



Considerations for adding a script

- For options to **delete a step** or **update the script**, right-click the script.
- A script can run on Azure during failover from an on-premises machine to Azure. It also can run on Azure as a primary-site script before shutdown, during failback from Azure to an on-premises machine.
- When a script runs, it injects a recovery plan context. 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"
 }}
```

The following table lists the name and description of each variable in the context.

VARIABLE NAME	DESCRIPTION
---------------	-------------

VARIABLE NAME	DESCRIPTION
RecoveryPlanName	The name of the plan being run. This variable helps you take different actions based on the recovery plan name. You also can reuse the script.
FailoverType	Specifies whether the failover is a test, planned, or unplanned.
FailoverDirection	Specifies whether recovery is to a primary or secondary site.
GroupID	Identifies the group number in the recovery plan when the plan is running.
VmMap	An array of all VMs in the group.
VMMAP key	A unique key (GUID) for each VM. It's the same as the Azure Virtual Machine Manager (VMM) ID of the VM, where applicable.
SubscriptionId	The Azure subscription ID in which the VM was created.
RoleName	The name of the Azure VM that's being recovered.
CloudServiceName	The Azure cloud service name under which the VM was created.
ResourceGroupName	The Azure resource group name under which the VM was created.
RecoveryPointId	The timestamp for when the VM is recovered.

- Ensure that the Automation account has the following modules:

- AzureRM.profile
- AzureRM.Resources
- AzureRM.Automation
- AzureRM.Network
- AzureRM.Compute

All modules should be of compatible versions. An easy way to ensure that all modules are compatible is to use the latest versions of all the modules.

Access all VMs of the VMMAP in a loop

Use the following code to loop across all VMs of the Microsoft VMMAP:

```

$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
    }
}

```

NOTE

The resource group name and role name values are empty when the script is a pre-action to a boot group. The values are populated only if the VM of that group succeeds in failover. The script is a post-action of the boot group.

Use the same Automation runbook in multiple recovery plans

You can use a single script in multiple recovery plans by using external variables. You can use [Azure Automation variables](#) to store parameters that you can pass for a recovery plan execution. 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 of a recovery plan.

For the script to detect which recovery plan is running, use the recovery plan context:

```

workflow AddPublicIPAndNSG {
    param (
        [parameter(Mandatory=$false)]
        [Object]$RecoveryPlanContext
    )

    $RPName = $RecoveryPlanContext.RecoveryPlanName

```

To apply an existing NSG, you must know the NSG name and the NSG resource group name. Use these variables as inputs for recovery plan scripts. To do this, create two variables in the Automation account assets. Add the name of the recovery plan that you are creating the parameters for as a prefix to the variable name.

1. Create a variable to store the NSG name. Add a prefix to the variable name by using 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

2. Create a variable to store the NSG's resource group name. Add a prefix to the variable name by using the name of the recovery plan.

The screenshot shows the Azure portal interface for managing variables. At the top, there's a blue header bar with the title 'RPscripttest-NSGRG' and a 'Variable' label. Below the header are three buttons: 'Save' (with a save icon), 'Discard' (with a cross icon), and 'Delete' (with a trash bin icon). The main content area has sections for 'Name' (containing 'RPscripttest-NSGRG'), 'Last modified' (containing '1/24/2017, 7:33 PM'), and 'Description' (containing a text box with the placeholder 'Resource group of the NSG you want to apply.' followed by a green checkmark). There are also sections for 'Encrypted' (set to 'No') and 'Type' (set to 'String'). A 'Value' section contains the text 'ContosoRG' with a green checkmark. The entire variable entry is highlighted with a purple border.

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



3. In the script, use the following 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
```

4. 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, see [Add a public IP and NSG to VMs during test failover of a Site Recovery recovery plan](#).

Use a complex variable to store more information

Consider a scenario in which you want a single script to turn on a public IP on specific VMs. In another scenario,

you might want to apply different NSGs on different VMs (not on all VMs). You can make a script that is 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. You cannot create separate variables for each recovery plan.

In the following example, we use a new technique and create a **complex variable** in the Azure Automation account assets. You do this by specifying multiple values. You must use Azure PowerShell to complete the following steps:

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 by 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:

The screenshot shows the Azure portal's 'Properties' page for a VM. The left sidebar has sections for 'RESOURCE MANAGEMENT' (Locks), 'GENERAL' (Properties, Compute and Network, Disks), and 'ADVANCED' (Networking, Security, Monitoring, Metrics). The 'Properties' section is selected. On the right, the VM's properties are listed: Active location (FTPV2A), Replication policy (/Subscriptions/7c943c1b-5122-4097-90c8-), ID (200d7b22-cced-11e6-8166-0050568f7993), Source VM Id (200d7b22-cced-11e6-8166-0050568f7993), Operating system (-), Source location (-), and Daily data change rate (0 MB).

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
```

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) {
    Write-output $VMDetailsObj.value.$VMID

    if ($VMDetailsObj.value.$VMID -ne $Null) { #If the VM exists in the context, this will not be Null
        $VM = $vmMap.$VMID
        # Access the properties of the variable
        $NSGname = $VMDetailsObj.value.$VMID.'NSGName'
        $NSGRGname = $VMDetailsObj.value.$VMID.'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.



For another example, see the following video. It demonstrates how to recover a two-tier WordPress application to Azure:

Additional resources

- [Azure Automation service Run As account](#)
- [Azure Automation overview](#)
- [Azure Automation sample scripts](#)

Next steps

[Learn more](#) about running failovers.

Failover in Site Recovery

7/9/2018 • 7 minutes to read • [Edit Online](#)

This article describes how to failover virtual machines and physical servers protected by Site Recovery.

Prerequisites

1. Before you do a failover, do a [test failover](#) to ensure that everything is working as expected.
2. [Prepare the network](#) at target location before you do a failover.

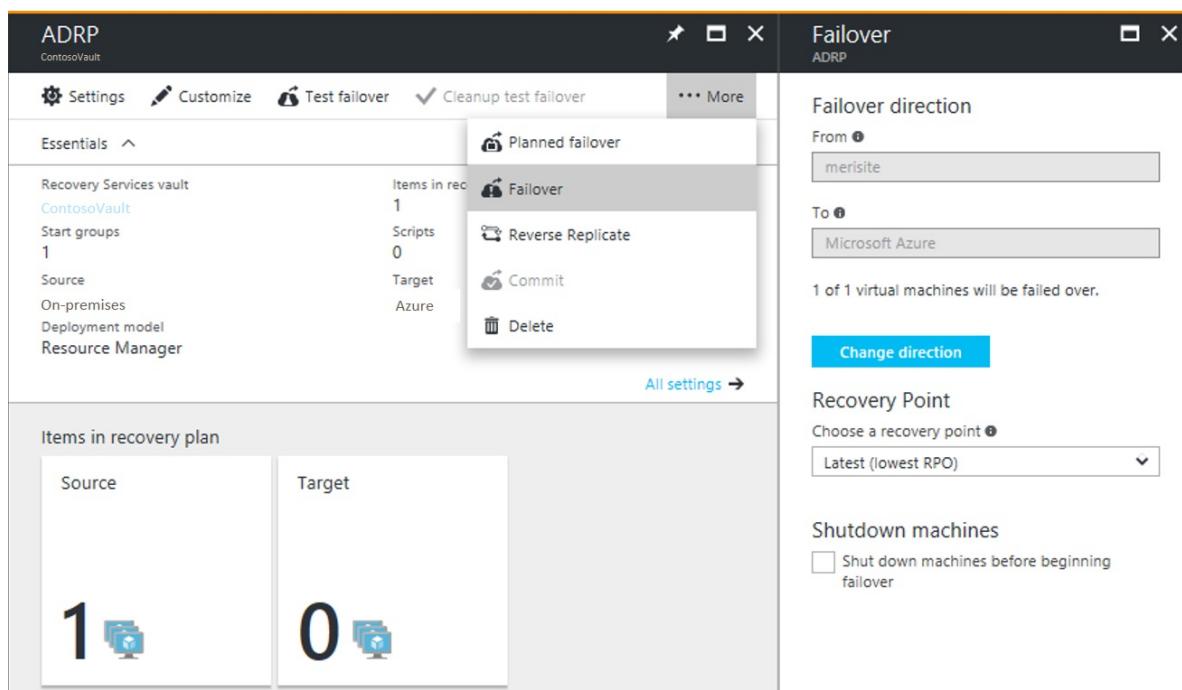
Use the following table to know about the failover options provided by Azure Site Recovery. These options are also listed for different failover scenarios.

SCENARIO	APPLICATION RECOVERY REQUIREMENT	WORKFLOW FOR HYPER-V	WORKFLOW FOR VMWARE
Planned failover due to an upcoming datacenter downtime	Zero data loss for the application when a planned activity is performed	<p>For Hyper-V, ASR replicates data at a copy frequency that is specified by the user. Planned Failover is used to override the frequency and replicate the final changes before a failover is initiated.</p> <p>1. Plan a maintenance window as per your business's change management process.</p> <p>2. Notify users of upcoming downtime.</p> <p>3. Take the user-facing application offline.</p> <p>4. Initiate a Planned Failover using ASR portal to the Latest point after the application is offline. Use the "Unplanned Failover" option on the portal and select the Latest point to failover. The on-premises virtual machine is automatically shut-down.</p> <p>Effective application data loss = 0</p> <p>A journal of recovery points is also provided in a retention window for a user who wants to use an older recovery point. (24 hours retention for Hyper-V).</p>	<p>For VMware, ASR replicates data continually using CDP. Failover gives the user the option to failover to the Latest data (including post application shut-down)</p> <p>1. Plan a maintenance window as per the change management process</p> <p>2. Notify users of upcoming downtime</p> <p>3. Take the user-facing application offline.</p> <p>4. Initiate a Planned Failover using ASR portal to the Latest point after the application is offline. Use the "Unplanned Failover" option on the portal and select the Latest point to failover. The on-premises virtual machine is automatically shut-down.</p> <p>Effective application data loss = 0</p> <p>A journal of recovery points in a retention window is provided for a customer who wants to use an older recovery point. (72 hours of retention for VMware).</p>

SCENARIO	APPLICATION RECOVERY REQUIREMENT	WORKFLOW FOR HYPER-V	WORKFLOW FOR VMWARE
Failover due to an unplanned datacenter downtime (natural or IT disaster)	Minimal data loss for the application	1. Initiate the organization's BCP plan 2. Initiate Unplanned Failover using ASR portal to the Latest or a point from the retention window (journal).	1. Initiate the organization's BCP plan. 2. Initiate unplanned Failover using ASR portal to the Latest or a point from the retention window (journal).

Run a failover

This procedure describes how to run a failover for a [recovery plan](#). Alternatively you can run the failover for a single virtual machine or physical server from the **Replicated items** page



1. Select **Recovery Plans** > *recoveryplan_name*. Click **Failover**
2. On the **Failover** screen, select a **Recovery Point** to failover to. You can use one of the following options:
 - a. **Latest** (default): This option starts the job by first processing all the data that has been sent to Site Recovery service. Processing the data creates a recovery point for each virtual machine. This recovery point is used by the virtual machine during failover. This option provides the lowest RPO (Recovery Point Objective) as the virtual machine created after failover has all the data that has been replicated to Site Recovery service when the failover was triggered.
 - b. **Latest processed**: This option fails over all virtual machines of the recovery plan to the latest recovery point that has already been processed by Site Recovery service. When you are doing test failover of a virtual machine, time stamp of the latest processed recovery point is also shown. If you are doing failover of a recovery plan, you can go to individual virtual machine and look at **Latest Recovery Points** tile to get this information. As no time is spent to process the unprocessed data, this option provides a low RTO (Recovery Time Objective) failover option.
 - c. **Latest app-consistent**: This option fails over all virtual machines of the recovery plan to the latest application consistent recovery point that has already been processed by Site Recovery service. When you are doing test failover of a virtual machine, time stamp of the latest app-consistent recovery point is also shown. If you are doing failover of a recovery plan, you can go

to individual virtual machine and look at **Latest Recovery Points** tile to get this information.

- d. **Latest multi-VM processed:** This option is only available for recovery plans that have at least one virtual machine with multi-VM consistency ON. Virtual machines that are part of a replication group failover to the latest common multi-VM consistent recovery point. Other virtual machines failover to their latest processed recovery point.
- e. **Latest multi-VM app-consistent:** This option is only available for recovery plans that have at least one virtual machine with multi-VM consistency ON. Virtual machines that are part of a replication group failover to the latest common multi-VM application-consistent recovery point. Other virtual machines failover to their latest application-consistent recovery point.
- f. **Custom:** If you are doing test failover of a virtual machine, then you can use this option to failover to a particular recovery point.

NOTE

The option to choose a recovery point is only available when you are failing over to Azure.

3. If some of the virtual machines in the recovery plan were failed over in a previous run and now the virtual machines are active on both source and target location, you can use **Change direction** option to decide the direction in which the failover should happen.
4. If you're failing over to Azure and data encryption is enabled for the cloud (applies only when you have protected Hyper-v virtual machines from a VMM Server), in **Encryption Key** select the certificate that was issued when you enabled data encryption during setup on the VMM server.
5. Select **Shut-down machine before beginning failover** if you want Site Recovery to attempt to do a shutdown of source virtual machines before triggering the failover. Failover continues even if shut-down fails.

NOTE

If Hyper-v virtual machines are protected, the option to shut-down also tries to synchronize the on-premises data that has not yet been sent to the service before triggering the failover.

6. You can follow the failover progress on the **Jobs** page. Even if errors occur during an unplanned failover, the recovery plan runs until it is complete.
7. After the failover, validate the virtual machine by logging-in to it. If you want to switch to another recovery point of the virtual machine, then you can use **Change recovery point** option.
8. Once you are satisfied with the failed over virtual machine, you can **Commit** the failover. **Commit deletes all the recovery points available with the service** and **Change recovery point** option is no longer available.

Planned failover

Virtual machines/physical servers protected using Site Recovery also support **Planned failover**. 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.

NOTE

During failover of Hyper-v virtual machines from one on-premises site to another on-premises site, to come back to the primary on-premises site you have to first **reverse-replicate** the virtual machine back to primary site and then trigger a failover. If the primary virtual machine is not available, then before starting to **reverse-replicate** you have to restore the virtual machine from a backup.

Failover job

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	...

When a failover is triggered, it involves following steps:

1. Prerequisites check: This step ensures that all conditions required for failover are met
2. Failover: This step processes the data and makes it ready so that an Azure virtual machine can be created out of it. If you have chosen **Latest** recovery point, this step creates a recovery point from the data that has been sent to the service.
3. Start: This step creates an Azure virtual machine using the data processed in the previous step.

WARNING

Don't Cancel an in progress failover: Before failover is started, replication for the virtual machine is stopped. If you **Cancel** an in progress job, failover stops but the virtual machine will not start to replicate. Replication cannot be started again.

Time taken for failover to Azure

In certain cases, failover of virtual machines requires an extra intermediate step that usually takes around 8 to 10 minutes to complete. In the following cases, the time taken to failover will be higher than usual:

- VMware virtual machines using mobility service of version older than 9.8
- Physical servers
- VMware Linux virtual machines
- Hyper-V virtual machines protected as physical servers
- VMware virtual machines where following drivers are not present as boot drivers
 - storvsc
 - vmbus

- storflt
- intelide
- atapi
- VMware virtual machines that don't have DHCP service enabled irrespective of whether they are using DHCP or static IP addresses

In all the other cases, this intermediate step is not required and the time taken for the failover is lower.

Using scripts in Failover

You might want to automate certain actions while doing a failover. You can use scripts or [Azure automation runbooks](#) in [recovery plans](#) to do that.

Post failover considerations

Post failover you might want to consider the following recommendations:

Retaining drive letter after failover

To retain the drive letter on virtual machines after failover, you can set the **SAN Policy** for the virtual machine to **OnlineAll**. [Read more](#).

Next steps

WARNING

Once you have failed over virtual machines and the on-premises data center is available, you should **Reprotect** VMware virtual machines back to the on-premises data center.

Use **Planned failover** option to **Fallback** Hyper-v virtual machines back to on-premises from Azure.

If you have failed over a Hyper-v virtual machine to another on-premises data center managed by a VMM server and the primary data center is available, then use **Reverse replicate** option to start the replication back to the primary data center.

Run a failback for Hyper-V VMs

7/9/2018 • 6 minutes to read • [Edit Online](#)

This article describes how to fail back Hyper-V virtual machines protected by Site Recovery.

Prerequisites

1. Ensure that you have read the details about the [different types of failback](#) and corresponding caveats.
2. Ensure that the primary site VMM server or Hyper-V host server is connected to Azure.
3. You should have performed **Commit** on the virtual machine.

Perform failback

After failover from the primary to secondary location, replicated virtual machines aren't protected by Site Recovery, and the secondary location is now acting as the active location. To fail back VMs in a recovery plan, run a planned failover from the secondary site to the primary, as follows.

1. Select **Recovery Plans** > *recoveryplan_name*. Click **Failover** > **Planned Failover**.
2. On the **Confirm Planned Failover** page, choose the source and target locations. Note the failover direction. If the failover from primary worked as expect and all virtual machines are in the secondary location this is for information only.
3. If you're failing back from Azure select settings in **Data Synchronization**:
 - **Synchronize data before failover(Synchronize delta changes only)**—This option minimizes downtime for virtual machines as it synchronizes without shutting them down. It does the following steps:
 - Phase 1: Takes snapshot of the virtual machine in Azure and copies it to the on-premises Hyper-V host. The machine continues running in Azure.
 - Phase 2: Shuts down the virtual machine in Azure so that no new changes occur there. The final set of delta changes are transferred to the on-premises server and the on-premises virtual machine is started up.
 - **Synchronize data during failover only(full download)**—This option is faster.
 - This option is faster because we expect that most of the disk has changed and we don't want to spend time in checksum calculation. It performs a download of the disk. It is also useful when the on-prem virtual machine has been deleted.
 - We recommend you use this option if you've been running Azure for a while (a month or more) or the on-prem virtual machine has been deleted. This option doesn't perform any checksum calculations.
4. 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, once the initial data synchronization is complete and you're ready to shut down the virtual machines in Azure, click **Jobs** planned failover job name **Complete Failover**. This shuts down the Azure machine, transfers the latest changes to the on-premises virtual machine, and starts the VM on-premises.
7. You can now log onto the virtual machine to validate it's available as expected.
8. The virtual machine is in a commit pending state. Click **Commit** to commit the failover.

- Now in order to complete the failback click **Reverse Replicate** to start protecting the virtual machine in the primary site.

Follow these procedures to fail back to the original primary site. This procedure describes how to run a planned failover for a recovery plan. Alternatively you can run the failover for a single virtual machine on the **Virtual Machines** tab.

Fallback to an alternate location in Hyper-V environment

If you've deployed protection between a [Hyper-V site](#) and [Azure](#) you have the ability to failback from Azure to an alternate on-premises location. This is useful if you need to set up new on-premises hardware. Here's how you do it.

- If you're setting up new hardware install Windows Server 2012 R2 and the Hyper-V role on the server.
- Create a virtual network switch with the same name that you had on the original server.
- Select **Protected Items** -> **Protection Group** -> -> you want to fail back, and select **Planned Failover**.
- In **Confirm Planned Failover** select **Create on-premises virtual machine if it does not exist**.
- In Host Name,** select the new Hyper-V host server on which you want to place the virtual machine.
- In Data Synchronization, we recommend you select the option **Synchronize the data before the failover**. This minimizes downtime for virtual machines as it synchronizes without shutting them down. It does the following:
 - Phase 1: Takes snapshot of the virtual machine in Azure and copies it to the on-premises Hyper-V host. The machine continues running in Azure.
 - Phase 2: Shuts down the virtual machine in Azure so that no new changes occur there. The final set of changes are transferred to the on-premises server and the on-premises virtual machine is started up.
- Click the checkmark to begin the failover (failback).
- After the initial synchronization finishes and you're ready to shut down the virtual machine in Azure, click **Jobs** > > **Complete Failover**. This shuts down the Azure machine, transfers the latest changes to the on-premises virtual machine, and starts it.
- You can log on to the on-premises virtual machine to verify everything is working as expected. Then click **Commit** to finish the failover. Commit deletes the Azure virtual machine and its disks and prepares the VM to be protected again.
- Click **Reverse Replicate** to start protecting the on-premises virtual machine.

NOTE

If you cancel the failback job while it is in Data Synchronization step, 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-prem data disks, and until the synchronization completes, the disk data may not be in a consistent state. If the On-prem VM is booted after Data Synchronization is canceled, it may not boot. Retrigger failover to complete the Data Synchronization.

Why is there no button called failback?

On the portal, there is no explicit gesture called failback. Failback is a step where you come back to the primary site. By definition, failback is when you failover the virtual machines from recovery back to primary.

When you initiate a failover, the blade informs you about the direction in which the virtual machines is to be moved, if the direction is from Azure to On-premises, it is a failback.

Why is there only a planned failover gesture to failback?

Azure is a highly available environment and your virtual machines are always available. Failback is a planned activity where you decide to take a small downtime so that the workloads can start running on-premises again. This expects no data loss. Hence only a planned failover gesture is available, that will turn off the VMs in Azure, download the latest changes and ensure there is no data loss.

Do I need a process server in Azure to failback to Hyper-v?

No, a process server is required only when you are protecting VMware virtual machines. No additional components are required to be deployed when protecting/failback of Hyper-v virtual machines.

Time taken to failback

The time taken to complete the data synchronization and boot the virtual machine depends on various factors. To give an insight into the time taken, we explain what happens during data synchronization.

Data synchronization takes a snapshot of the virtual machine's disks and starts checking block by block and calculates its checksum. This calculated checksum is sent to on-premises to compare with the on-premises checksum of the same block. In case the checksums match, the data block is not transferred. If it does not match, the data block is transferred to on-premises. This transfer time depends on the bandwidth available. The speed of the checksum is a few GBs per min.

To speed up the download of data, you can configure your MARS agent to use more threads to parallelize the download. Refer to the [document here](#) on how to change the download threads in the agent.

Next Steps

After **Commit**, you can initiate the *Reverse Replicate*. This starts protecting the virtual machine from on-premises back to Azure. This will only replicate the changes since the VM has been turned off in Azure and hence sends differential changes only.

Remove servers and disable protection

7/9/2018 • 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'

    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
        }
        "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.
 - **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.

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.

3. 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 removes 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 removes 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 vault

7/11/2018 • 2 minutes to read • [Edit Online](#)

Dependencies can prevent you from deleting an Azure Site Recovery vault. The actions you need to take vary based on the Site Recovery scenario. To delete a vault used in Azure Backup, see [Delete a Backup vault in Azure](#).

Delete a Site Recovery vault

To delete the vault, follow the recommended steps for your scenario.

VMware VMs to Azure

1. Delete all protected VMs by following the steps in [Disable protection for a VMware](#).
2. Delete all replication policies by following the steps in [Delete a replication policy](#).
3. Delete references to vCenter by following the steps in [Delete a vCenter server](#).
4. Delete the configuration server by following the steps in [Decommission a configuration server](#).
5. Delete the vault.

Hyper-V VMs (with VMM) to Azure

1. Delete all protected VMs by following the steps in [Disable protection for a Hyper-V VM \(with VMM\)](#).
2. Disassociate & delete all replication policies by browsing to your Vault -> **Site Recovery Infrastructure - > For System Center VMM -> Replication Policies**
3. Delete references to VMM servers by following the steps in [Unregister a connected VMM server](#).
4. Delete the vault.

Hyper-V VMs (without Virtual Machine Manager) to Azure

1. Delete all protected VMs by following the steps in [Disable protection for a Hyper-V virtual machine \(Hyper-V to Azure\)](#).
2. Disassociate & delete all replication policies by browsing to your Vault -> **Site Recovery Infrastructure - > For Hyper-V Sites -> Replication Policies**
3. Delete references to Hyper-V servers by following the steps in [Unregister a Hyper-V host](#).
4. Delete the Hyper-V site.
5. 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-AzureRmAccount

Select-AzureRmSubscription -SubscriptionName "XXXXX"

$vault = Get-AzureRmRecoveryServicesVault -Name "vaultname"

Remove-AzureRmRecoveryServicesVault -Vault $vault
```

Learn more about [Get-AzureRMRecoveryServicesVault](#), and [Remove-AzureRMRecoveryServicesVault](#).

Troubleshoot Hyper-V to Azure replication and failover

7/23/2018 • 7 minutes to read • [Edit Online](#)

This article describes common issues that you might encounter when replicating on-premises Hyper-V VMs to Azure, using [Azure Site Recovery](#).

Enable protection issues

If you encounter issues when you enable protection for Hyper-V VMs, check the following:

1. Check that your Hyper-V hosts and VMs comply with 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 log on 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 do this, open Task Manager on the Hyper V host. On the **Performance** tab, click **Open Resource Monitor**. On the **Network** tab > **Processes 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 do this, 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.

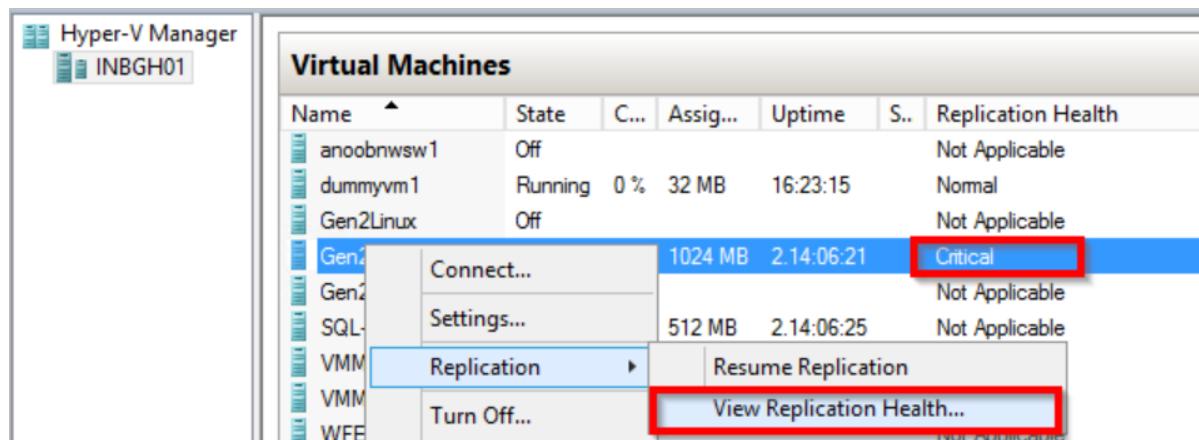
Performance issues

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.

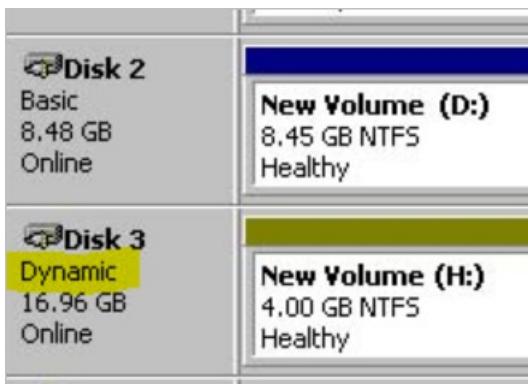
VSS failing inside the VM

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 do this, log onto 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 this 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 do this, 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

1. 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."
2. 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 **et-VMIntegrationService -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.

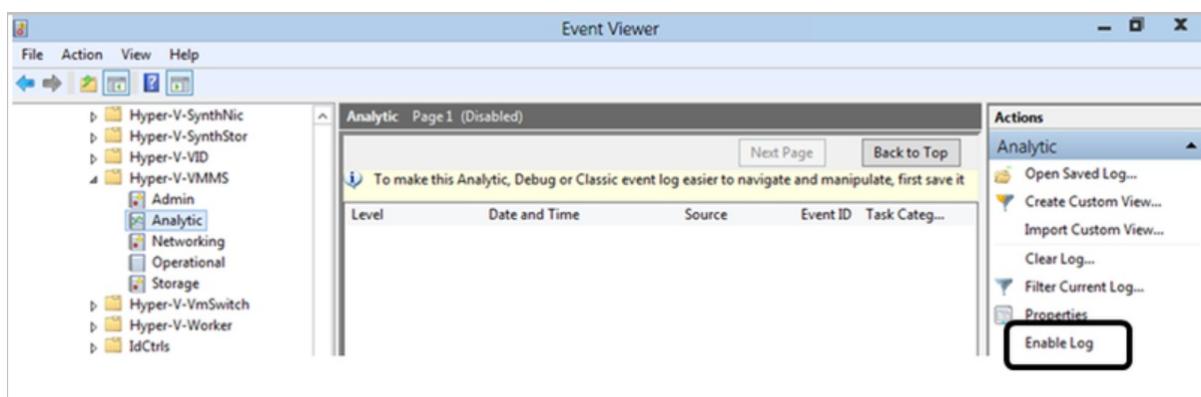
Common errors

ERROR CODE	MESSAGE	DETAILS
0x800700EA	"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.
0x80070032	"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. Upgrade 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 do this, 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
Applications and Service Logs/Microsoft/VirtualMachineManager/Server/Admin (VMM server)	Logs to troubleshoot VMM issues.
Applications and Service Logs/MicrosoftAzureRecoveryServices/Replication (Hyper-V host)	Logs to troubleshoot Microsoft Azure Recovery Services Agent issues.
Applications and Service Logs/Microsoft/Azure Site Recovery/Provider/Operational (Hyper-V host)	Logs to troubleshoot Microsoft Azure Site Recovery Service issues.
Applications and Service Logs/Microsoft/Windows/Hyper-V-VMMS/Admin (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.

Monitor and troubleshoot Site Recovery

8/6/2018 • 9 minutes to read • [Edit Online](#)

In this article, you learn how to use Azure Site Recovery's in built monitoring features for monitoring and troubleshooting.

Use the dashboard

1. In the vault, click **Overview** to open the Site Recovery dashboard. There are dashboard pages for both Site Recovery and Backup, and you can switch between them.

This screenshot shows the Azure Site Recovery Overview dashboard for the RayneTestVault. The left sidebar includes links for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Properties, Locks, Automation script, Jobs, Alerts and Events, Events, Reports, and Policies. The main dashboard has sections for Replicated items (0), Failover test success (0), Configuration issues (0), Recovery Plans (0), Error Summary (No errors), Infrastructure view (machines replicating to Azure), and Jobs - Last 24 hours. A red box highlights the 'Overview' link in the sidebar, and another red box highlights the 'Site Recovery' button in the top right.

2. The dashboard consolidates all monitoring information for the vault in a single location. From the dashboard, you can drill down into different areas.

This screenshot shows the Azure Site Recovery Overview dashboard for the Contoso-vault. The left sidebar is identical to the previous dashboard. The main dashboard includes sections for Replicated items (9), Failover test success (9), Configuration issues (4), Recovery Plans (2), Error Summary (No errors), Infrastructure view (machines replicating to Azure), and Jobs - Last 24 hours. A red box highlights the 'Overview' link in the sidebar. Callouts numbered 1 through 9 point to various parts of the dashboard: 1 points to the 'Site Recovery' button; 2 points to the 'Replicated items' section; 3 points to the 'Failover test success' section; 4 points to the 'Configuration issues' section; 5 points to the 'Error Summary' section; 6 points to the 'Infrastructure view' section; 7 points to the 'Recovery Plans' section; 8 points to the 'Jobs - Last 24 hours' section; and 9 points to the 'Virtual machine(s)' count in the Infrastructure view.

3. On **Replicated items**, click **View All** to see all the servers in the vault.
4. Drill down by clicking the status details in each section. In **Infrastructure view**, you can sort monitoring information by the type of machines you're replicating.

Monitor replicated items

The replicated items section shows the health of all machines that have replication enabled in the vault.

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

You can view the test 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

The **Configuration issues** section shows a list of issues that may impact your ability to successfully fail over.

- 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 the **needs attention** in the **Target configurations** column. The 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	<p>The available subscription resource quota balance is compared against the balance needed to fail over all of the machines in the vault.</p> <p>If there aren't enough resources, an insufficient quota balance is reported.</p> <p>Quotas are monitoring for VM core count, VM family core count, network interface card (NIC) count.</p>
Software updates	The availability of new software updates, and information about expiring software versions.

Monitoring errors

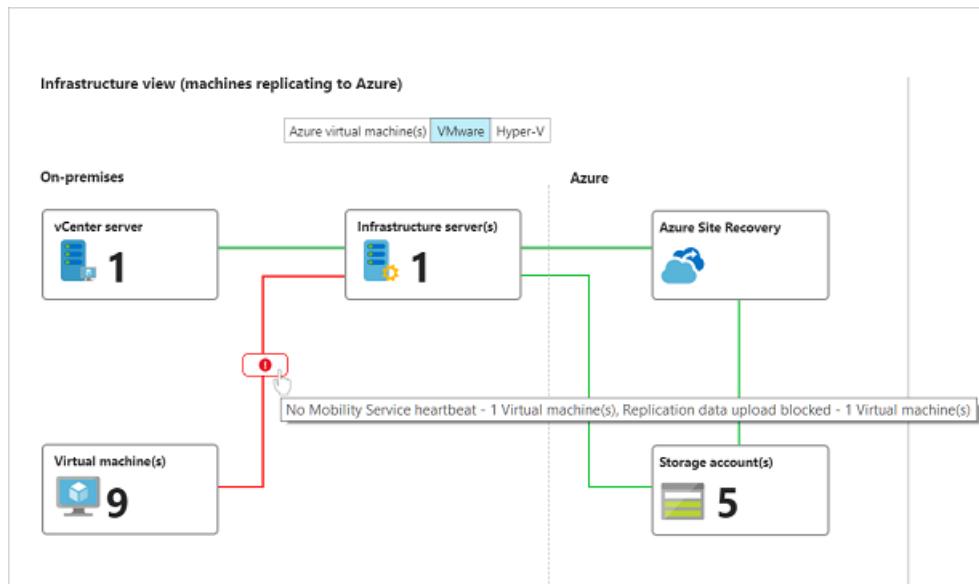
The **Error summary** section shows currently active error symptoms that may impact replication of servers in the vault, and the number of impacted machines.

- At the beginning of the section, errors impacting on-premises infrastructure components are shown. For example, non-receipt of a heartbeat from the Azure Site Recovery Provider running on the on-premises configuration server, VMM 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 may be impacting multiple machines. For example, a network glitch could potentially impact all machines replicating 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.

The **Infrastructure view** shows 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
Azure VM replication between Azure regions	Replication enabled/initial replication in progress	Yes
Azure VM replication between Azure regions	Failed over/fail back	No
VMware replication to Azure	Replication enabled/initial replication in progress	Yes
VMware replication to Azure	Failed over/failed back	No
Hyper-V replication to Azure	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.

Common questions

Why is the count of virtual machines in the vault infrastructure view different from the total count shown in the replicated items?

The vault infrastructure view is scoped by replication scenarios. Only machines in 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 shown in the Essentials drawer 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 the Essentials drawer. On the replicated items the total includes all the machines in the vault, including those for which initial replication is currently in progress.

Monitor recovery plans

In the **Recovery plans section** you can review the number of plans, create new plans, and modify existing ones.

Monitor jobs

The **Jobs** section reflects 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:

1. 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.
2. 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**.

3. 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.
4. You can drill into a job by clicking it.

Monitor virtual machines

In addition dashboard, you can monitor machines in the virtual machines page.

1. In the vault, click **Replicated items** to get a list of replicated machines. Alternately, you can get to a filtered list of the protected items by clicking any of the scoped shortcuts on the dashboard page.

The screenshot shows the 'Replicated items' page in the Azure Recovery Services Vault. The left sidebar includes sections for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, SETTINGS (Properties, Locks, Automation script), GETTING STARTED (Backup, Site Recovery), MONITORING AND REPORTS (Jobs, Alerts and Events, Backup Reports), POLICIES (Backup policies), and PROTECTED ITEMS (Backup Items). The 'Replicated items' section is highlighted with a red box. The main content area displays a table with the following data:

NAME	REPLICATION HEALTH	STATUS	RPO	TARGET CONFIGURATIONS
ContosoVM9	Healthy	Protected	5 minutes	OK
ContosoVM7	Healthy	Protected	1 minute	Needs attention
ContosoVM1	Healthy	Protected	3 minutes	OK
ContosoVM2	Critical	Protected	32 minutes	OK
ContosoVM3	Healthy	Protected	4 minutes	OK
ContosoVM4	Healthy	Protected	3 minutes	OK
ContosoVMS	Healthy	Protected	2 minutes	OK
ContosoVM6	Healthy	Protected	6 minutes	OK
ContosoVM8	Healthy	Protected	4 minutes	OK

A context menu is open for the last row (ContosoVM8), listing options: Pin to dashboard, Failover, Test Failover, Cleanup test failover, Change recovery point, Commit, Complete Migration, Re-protect, Resynchronize, Error Details, and Disable Replication.

- On the **Replicated items** page, 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.
- Click **Columns** to show additional columns. For example to show RPO, target configuration issues, and replication errors.
- Click **Filter** to view information based on specific parameters such as replication health, or a particular replication policy.
- Right-click a machine to initiate operations such as test failover for it, or to view specific error details associated with it.
- 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.

Common questions

How is RPO 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 to identify a recoverable point, are written to the storage account in the target region.
- Site Recovery can now generate a recoverable point for the virtual machine.
- At this point, the RPO has been met for the changes uploaded to the storage account thus far. In other words, the machine RPO at this point is equal to amount of time 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.

NOTE

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.

Subscribe to email notifications

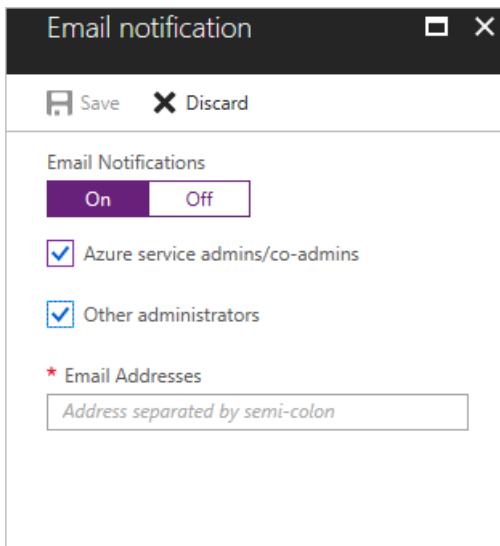
You can subscribe to receive email notifications for these critical events:

- 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 and Reports** 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.



Set up disaster recovery for Hyper-V VMs to a secondary on-premises site

7/9/2018 • 7 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 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:

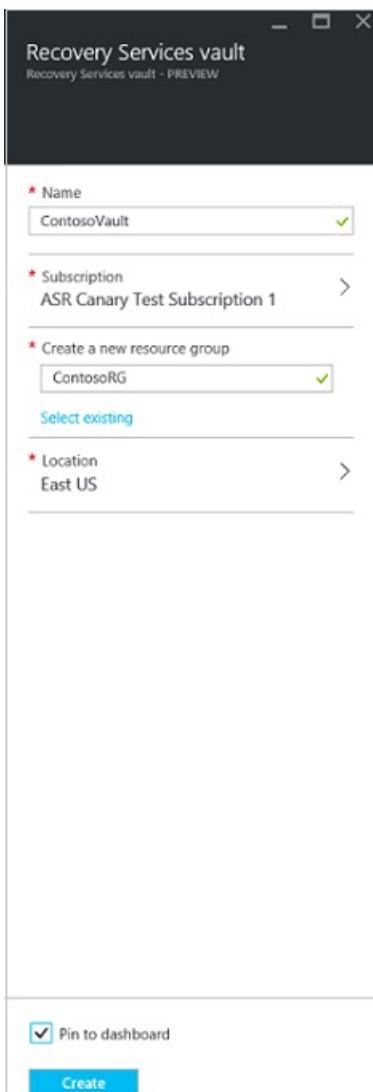
1. Make sure you have [VMM logical networks](#) on the source and target VMM servers.
 - The logical network on the source server should be associated with the source cloud in which Hyper-V hosts are located.
 - The logical network on the target server should be associated with the target cloud.
2. Make 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.

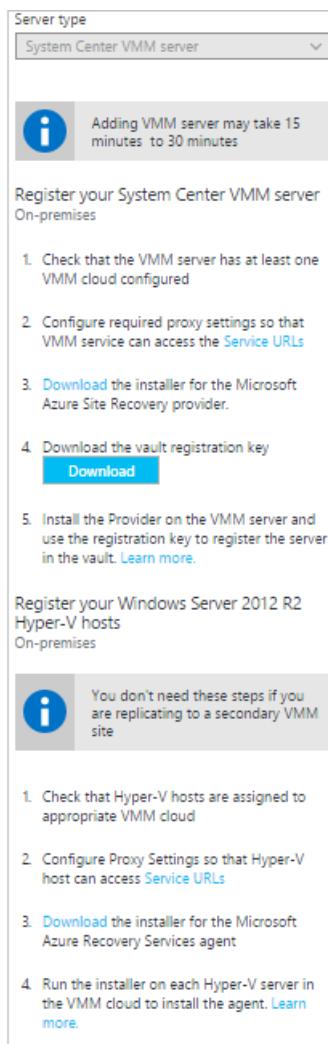
1. Click **Site Recovery > Step 1: Prepare Infrastructure > Protection goal**.
2. Select **To recovery site**, and select **Yes, with Hyper-V**.
3. Select **Yes** to indicate you're using VMM to manage the Hyper-V hosts.
4. Select **Yes** if you have a secondary VMM server. If you're deploying replication 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.

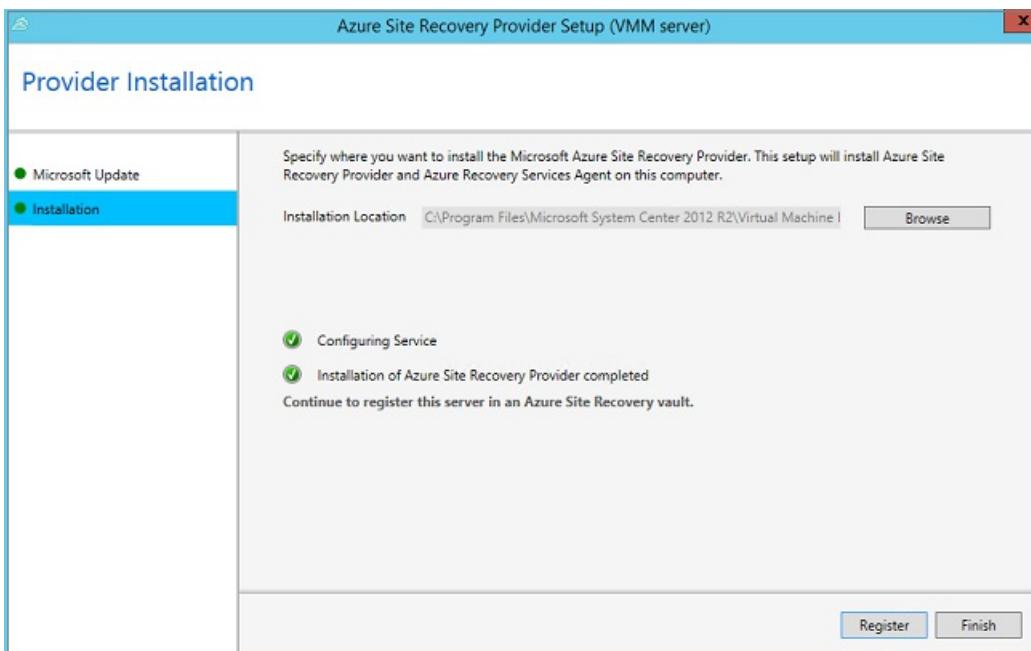
5. Download the registration key. You need this when you install the Provider. The key is valid for five days after you generate it.



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.

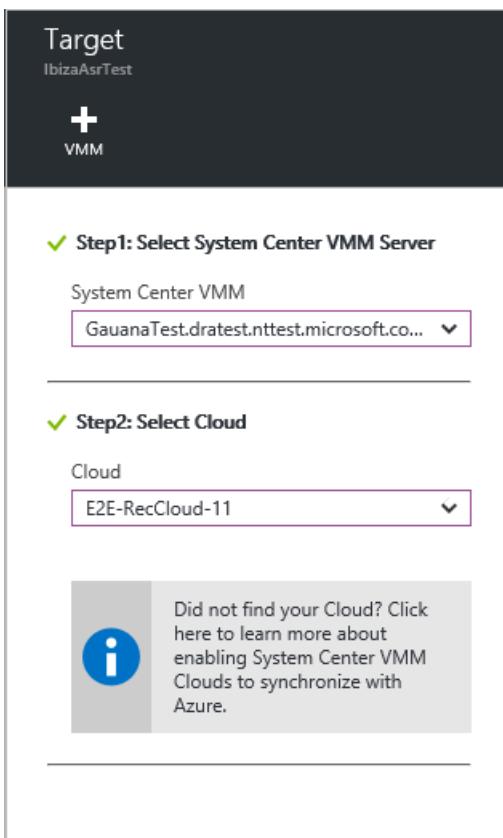


6. In **Vault name**, verify the name of the vault in which the server will be registered. Click **Next**.
7. In **Proxy Connection**, specify how the Provider running on the VMM server connects to Azure.
 - You can specify that the provider should connect directly to the internet, or via a proxy. Specify 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.

- 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.
- 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)

A note at the bottom states: "The new policy is automatically associated with the VMM cloud. In Replication policy, click OK."

- The new policy is automatically associated with the VMM cloud. In **Replication policy**, click **OK**.

Enable replication

- Click **Replicate application > Source**.
- In **Source**, select the VMM server, and the cloud in which the Hyper-V hosts you want to replicate are located. Then click **OK**.
- In **Target**, verify the secondary VMM server and cloud.
- 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](#)

Replicate Hyper-V VMs to a secondary site by using PowerShell (Resource Manager)

7/9/2018 • 6 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](#).

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-AzureRmAccount #-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-AzureRmSubscription
```

3. Set the subscription for the vault.

```
Set-AzureRmContext -SubscriptionID <subscriptionId>
```

Create a Recovery Services vault

1. Create an Azure Resource Manager resource group if you don't have one.

```
New-AzureRmResourceGroup -Name #ResourceGroupName -Location #location
```

2. Create a new Recovery Services vault. Save the vault object in a variable to be used later.

```
$vault = New-AzureRmRecoveryServicesVault -Name #vaultname -ResouceGroupName #ResourceGroupName -  
Location #location
```

You can retrieve the vault object after you create it by using the Get-AzureRMRecoveryServicesVault cmdlet.

Set the vault context

1. Retrieve an existing vault.

```
$vault = Get-AzureRmRecoveryServicesVault -Name #vaultname
```

2. Set the vault context.

```
Set-AzureRmSiteRecoveryVaultSettings -ARSVault $vault
```

Install the Site Recovery provider

1. On the Virtual Machine Manager machine, create a directory by running the following command:

```
New-Item c:\ASR -type 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 /startvmmsservice
```

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 pints  
$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-AzureRmSiteRecoveryPolicy -Name $policyname -ReplicationProvider $RepProvider -  
ReplicationFrequencyInSeconds $Replicationfrequencyinseconds -RecoveryPoints $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-AzureRmSiteRecoveryProtectionContainer -friendlyName $PrimaryCloud;

$RecoveryCloud = "testrecoverycloud"
$recoveryprotectionContainer = Get-AzureRmSiteRecoveryProtectionContainer -friendlyName $RecoveryCloud;
```

3. Retrieve the replication policy you created by using the friendly name.

```
$policy = Get-AzureRmSiteRecoveryPolicy -FriendlyName $policyname
```

4. Start the association of the protection container (Virtual Machine Manager cloud) with the replication policy.

```
$associationJob = Start-AzureRmSiteRecoveryPolicyAssociationJob -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-AzureRmSiteRecoveryJob -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-AzureRmSiteRecoveryServer
```

2. Run this command to retrieve the networks for the source Virtual Machine Manager server and the target Virtual Machine Manager server.

```
$PrimaryNetworks = Get-AzureRmSiteRecoveryNetwork -Server $Servers[0]

$RecoveryNetworks = Get-AzureRmSiteRecoveryNetwork -Server $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-AzureRmSiteRecoveryNetworkMapping -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-AzureRmSiteRecoveryProtectionContainer -friendlyName  
$PrimaryCloudName
```

2. Get the protection entity (VM), as follows:

```
$protectionEntity = Get-AzureRmSiteRecoveryProtectionEntity -friendlyName $VMName -  
ProtectionContainer $PrimaryProtectionContainer
```

3. Enable replication for the VM.

```
$jobResult = Set-AzureRmSiteRecoveryProtectionEntity -ProtectionEntity $protectionentity -Protection  
Enable -Policy $policy
```

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-AzureRmSiteRecoveryServer  
$RecoveryNetworks = Get-AzureRmSiteRecoveryNetwork -Server $Servers[1]
```

2. Perform a test failover.

For a single VM:

```
$protectionEntity = Get-AzureRmSiteRecoveryProtectionEntity -FriendlyName $VMName -ProtectionContainer  
$PrimaryProtectionContainer  
  
$jobIDResult = Start-AzureRmSiteRecoveryTestFailoverJob -Direction PrimaryToRecovery -  
ProtectionEntity $protectionEntity -VMNetwork $RecoveryNetworks[1]
```

For a recovery plan:

```
$recoveryplanname = "test-recovery-plan"

$recoveryplan = Get-AzureRmSiteRecoveryRecoveryPlan -FriendlyName $recoveryplanname

$jobIDResult = Start-AzureRmSiteRecoveryTestFailoverJob -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-AzureRmSiteRecoveryProtectionEntity -Name $VMName -ProtectionContainer
$PrimaryprotectionContainer

$jobIDResult = Start-AzureRmSiteRecoveryPlannedFailoverJob -Direction PrimaryToRecovery -
ProtectionEntity $protectionEntity
```

For a recovery plan:

```
$recoveryplanname = "test-recovery-plan"

$recoveryplan = Get-AzureRmSiteRecoveryRecoveryPlan -FriendlyName $recoveryplanname

$jobIDResult = Start-AzureRmSiteRecoveryPlannedFailoverJob -Direction PrimaryToRecovery -Recoveryplan
$recoveryplan
```

2. Perform an unplanned failover.

For a single VM:

```
$protectionEntity = Get-AzureRmSiteRecoveryProtectionEntity -Name $VMName -ProtectionContainer
$PrimaryprotectionContainer

$jobIDResult = Start-AzureRmSiteRecoveryUnPlannedFailoverJob -Direction PrimaryToRecovery -
ProtectionEntity $protectionEntity
```

For a recovery plan:

```
$recoveryplanname = "test-recovery-plan"

$recoveryplan = Get-AzureRmSiteRecoveryRecoveryPlan -FriendlyName $recoveryplanname

$jobIDResult = Start-AzureRmSiteRecoveryUnPlannedFailoverJob -Direction PrimaryToRecovery -
ProtectionEntity $protectionEntity
```

Monitor activity

Use the following commands to monitor failover activity. Wait for the processing to finish in between jobs.

```
Do
{
    $job = Get-AzureSiteRecoveryJob -Id $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.

Run a DR drill for Hyper-V VMs to a secondary site

7/9/2018 • 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
None	<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>
Use existing	<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>
Create a network	<p>A temporary test network is created automatically based on the setting that you specify in Logical Network and its related network sites.</p> <p>Failover checks that VMs are created.</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:

```

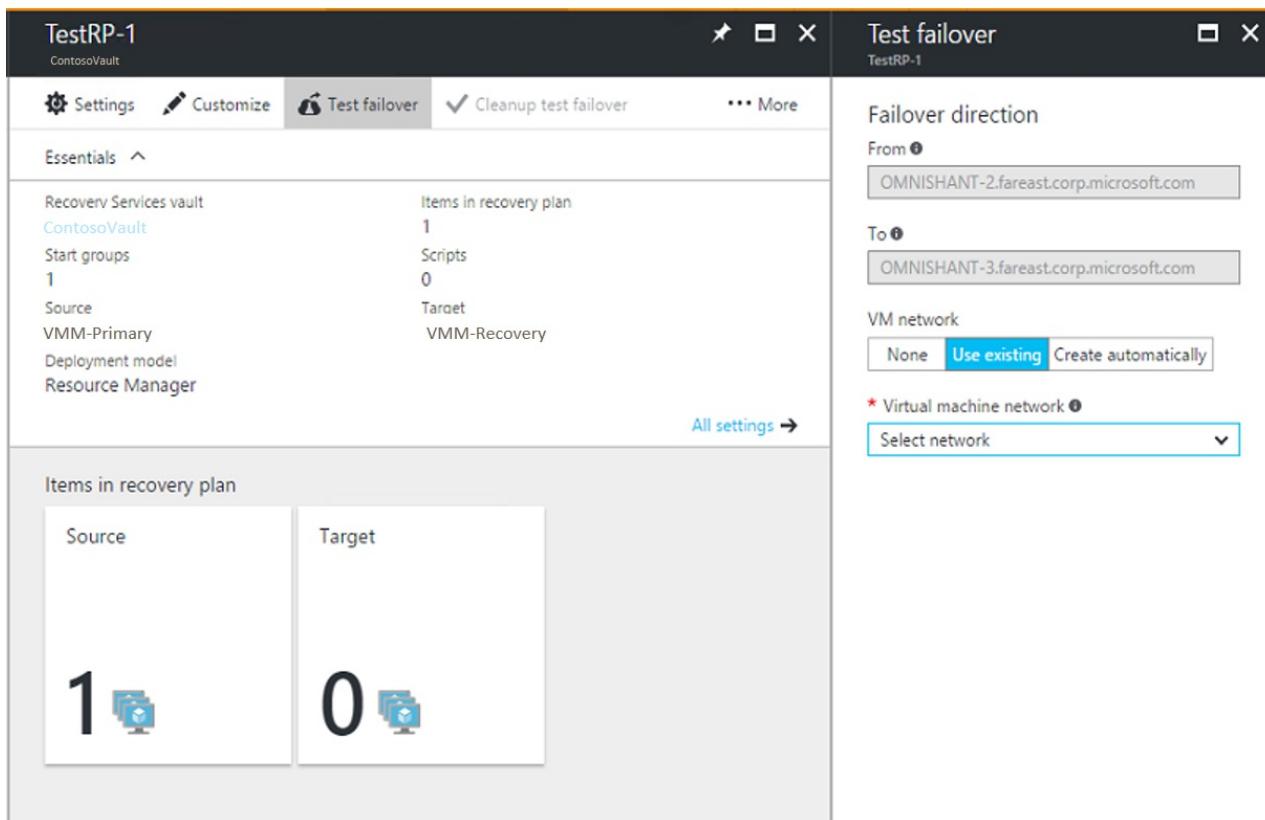
Param(
    [string]$Zone,
    [string]$name,
    [string]$IP
)
$Record = Get-DnsServerResourceRecord -ZoneName $zone -Name $name
$newrecord = $record.clone()
$newrecord.RecordData[0].IPv4Address = $IP
Set-DnsServerResourceRecord -zonename $zone -OldInputObject $record -NewInputObject $Newrecord

```

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

7/9/2018 • 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.

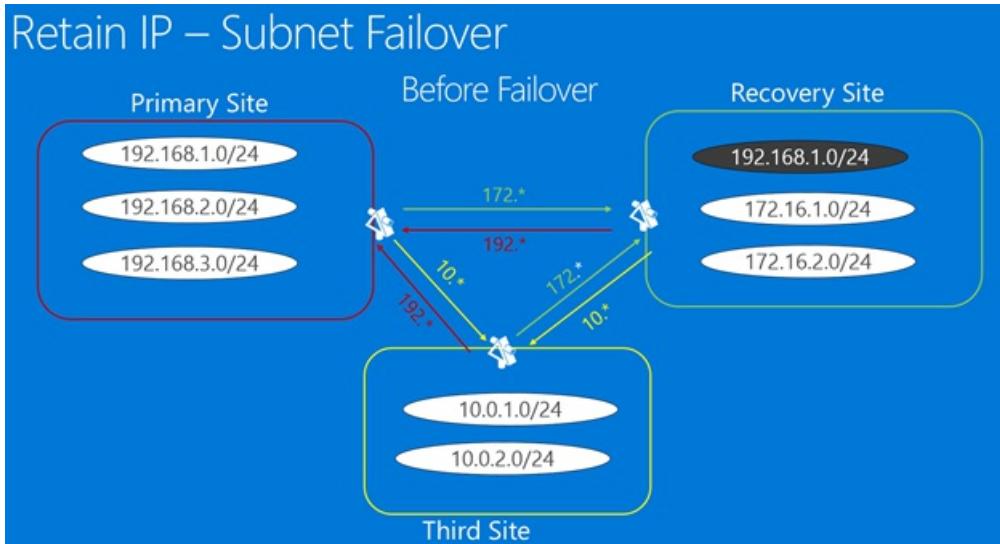
Example

Here's an example of complete subnet failover.

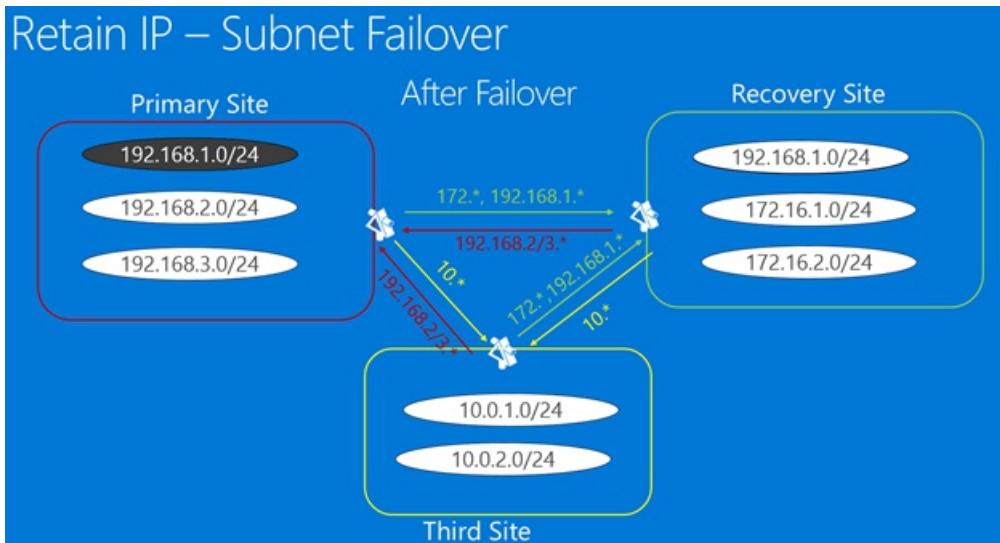
- Before failover, the primary site has applications running in subnet 192.168.1.0/24.
- During failover, all of the VMs in this subnet are failed over to the secondary site, and retain their IP addresses.
- Routes between all sites need to be modified to reflect the fact that all the VMs in subnet 192.168.1.0/24 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.

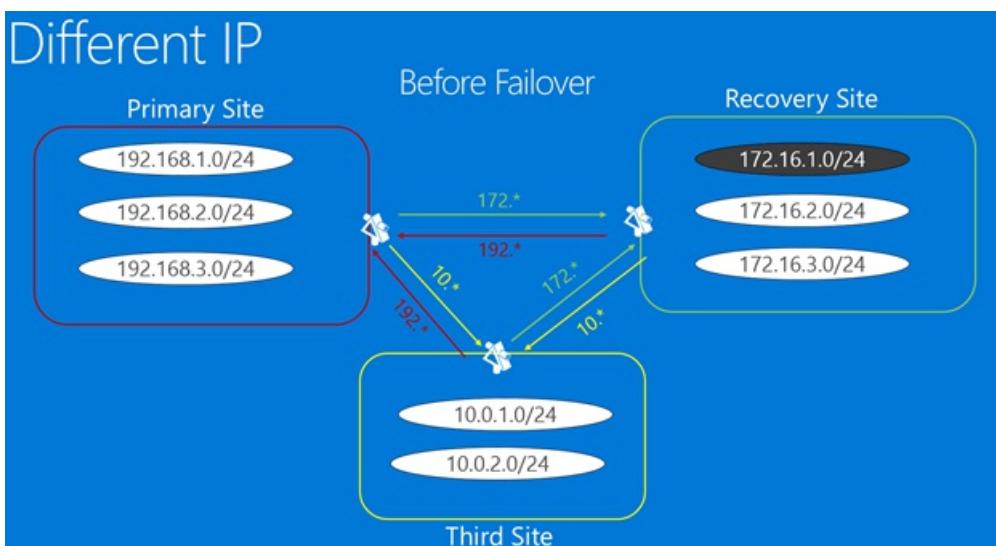
```
param(
    [string]$Zone,
    [string]$name,
    [string]$IP
)
$Record = Get-DnsServerResourceRecord -ZoneName $zone -Name $name
$newrecord = $record.clone()
$newrecord.RecordData[0].IPv4Address = $IP
Set-DnsServerResourceRecord -zonename $zone -OldInputObject $record -NewInputObject $Newrecord
```

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.

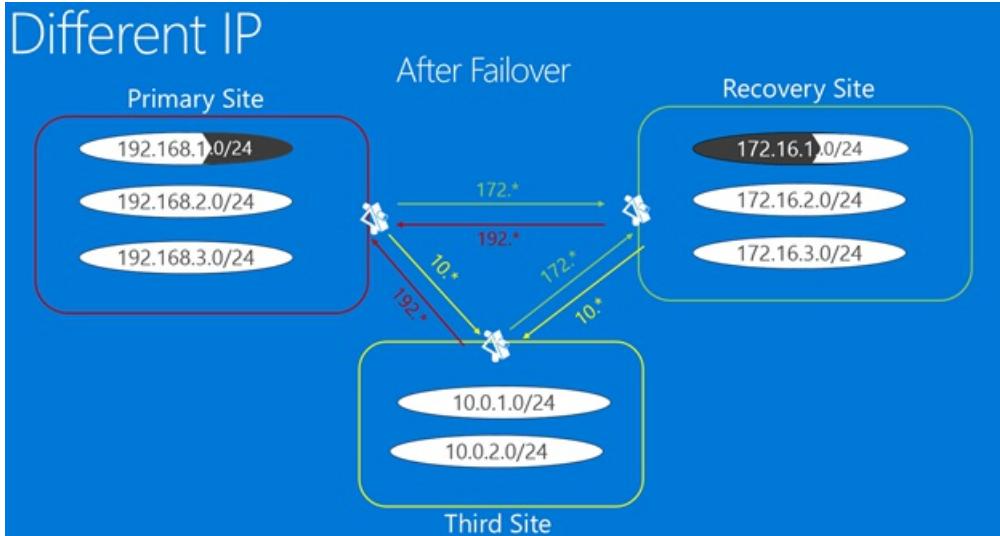
- Before failover, apps are hosted subnet 192.168.1.0/24 on the primary site.
- After failover, apps are configured in subnet 172.16.1.0/24 in the secondary site.
- All three sites can access each other.
- After failover, apps will be restored in the recovery subnet.
- In this scenario there's no need 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

8/2/2018 • 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

7/9/2018 • 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

7/13/2018 • 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

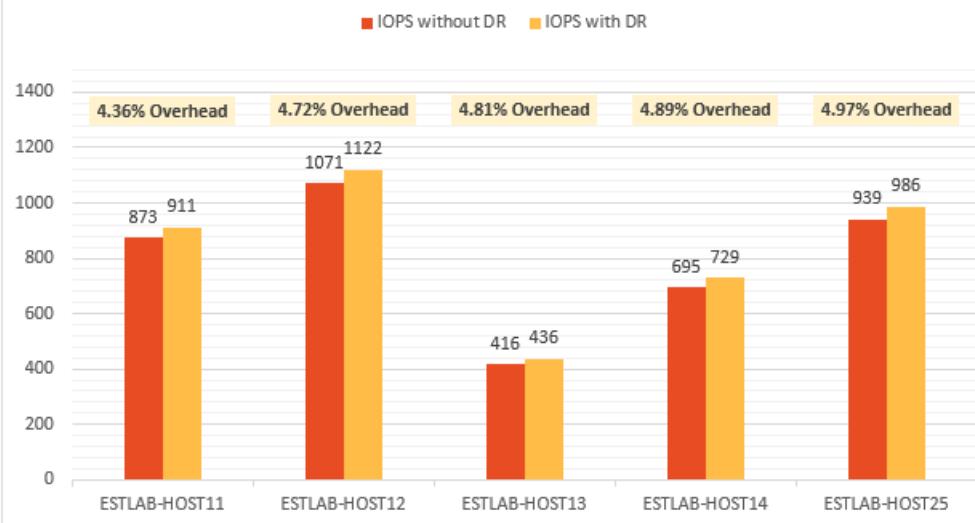
Here's what we did in the test pass:

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

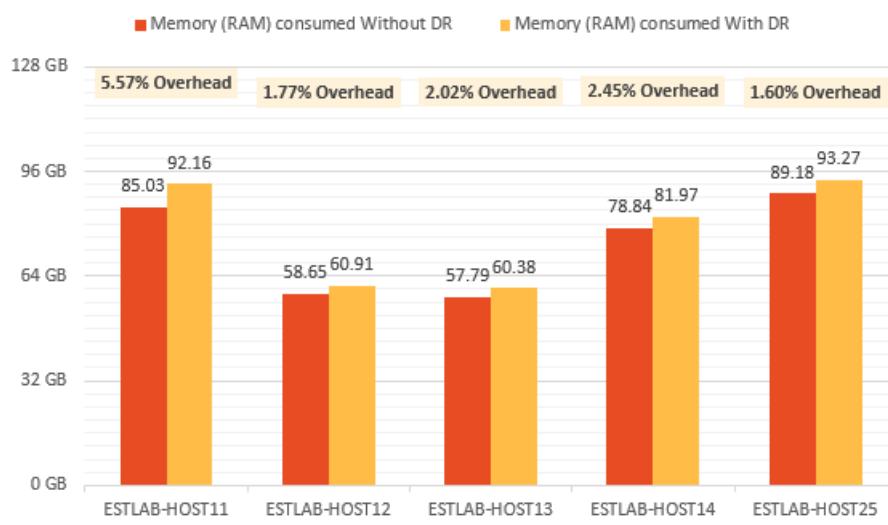
- Hyper-V Replica (used by Site Recovery) asynchronously tracks changes to a log file, with minimum storage overhead on the primary server.
- Hyper-V Replica utilizes self-maintained memory cache to minimize IOPS overhead for tracking. It stores writes to the VHDX in memory, and flushes them into the 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.

Total IOPS on Primary Nodes

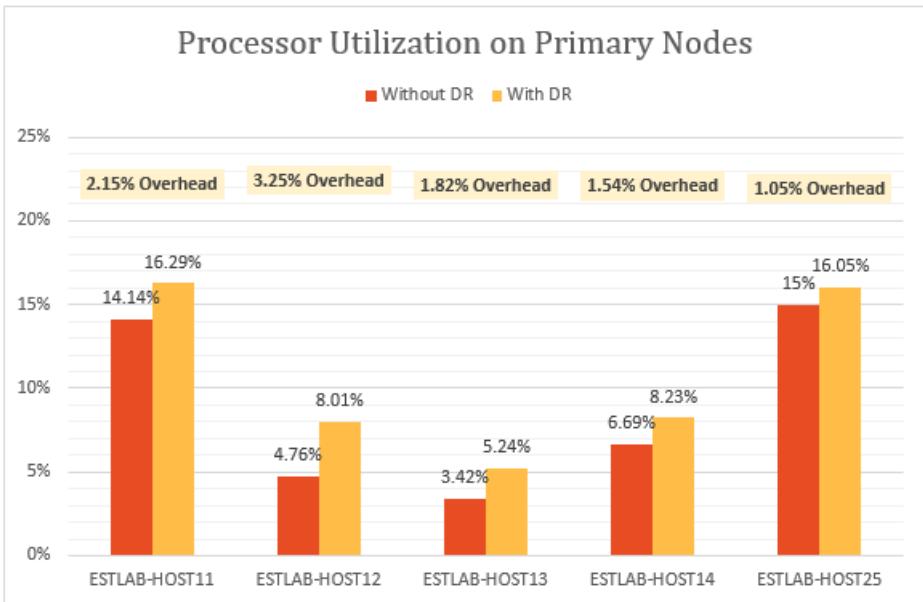


Hyper-V Replica uses memory on the primary server, to optimize disk performance. As shown in the following graph, memory overhead on all servers in the primary cluster is marginal. The memory overhead shown is the percentage of memory used by replication, compared to the total installed memory on the Hyper-V server.

Memory used (GB) on Primary Nodes

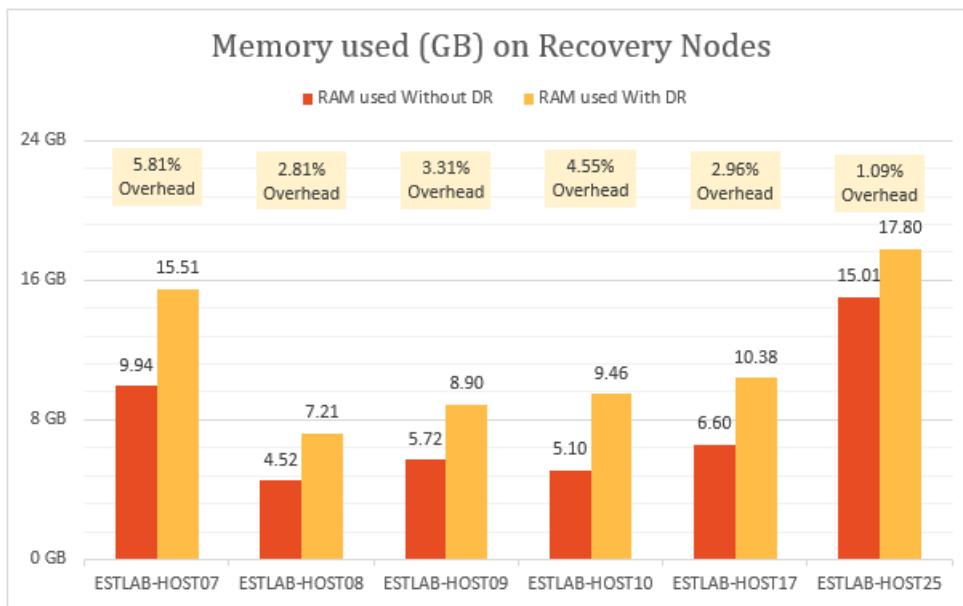


Hyper-V Replica has minimum CPU overhead. As shown in the graph, replication overhead is in the range of 2-3%.



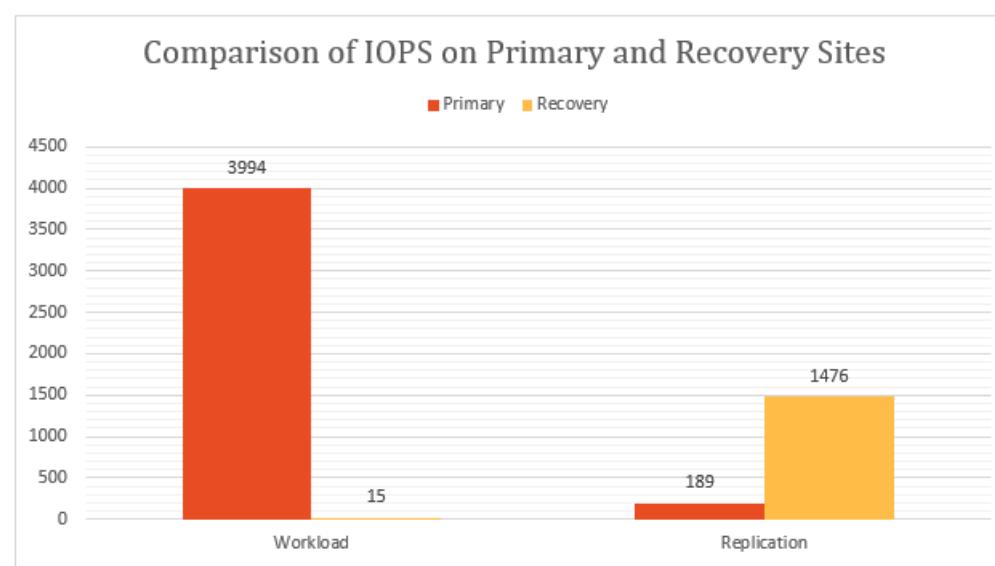
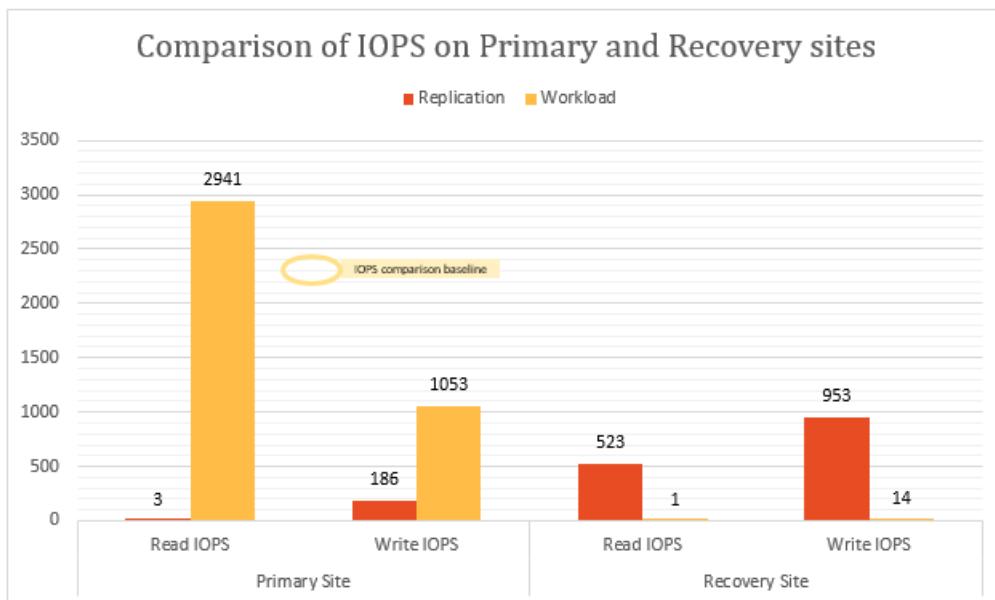
Secondary server performance

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.



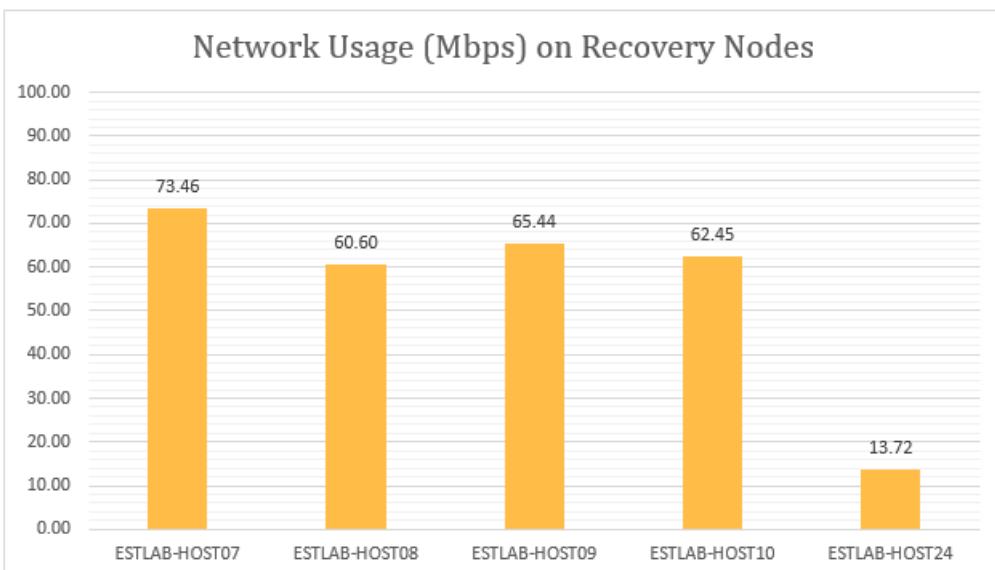
The amount of I/O operations on the recovery site is a function of the number of write operations on the primary site. Let's look at the total I/O operations on the recovery site in comparison with the total I/O operations and write operations on the primary site. The graphs show that the total IOPS 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

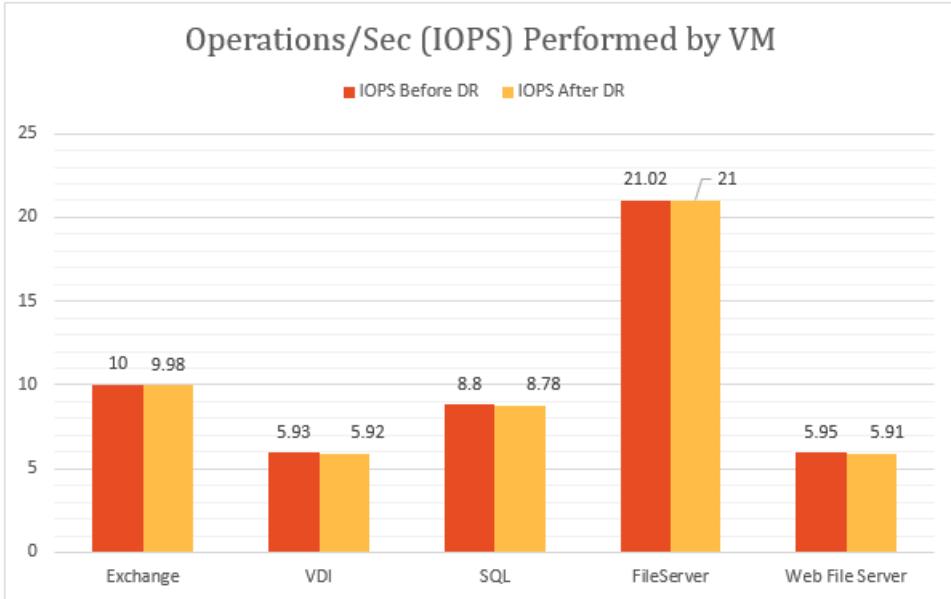
An average of 275 Mb per second of network bandwidth was used between the primary and recovery nodes (with compression enabled), against an existing bandwidth of 5 Gb per second.



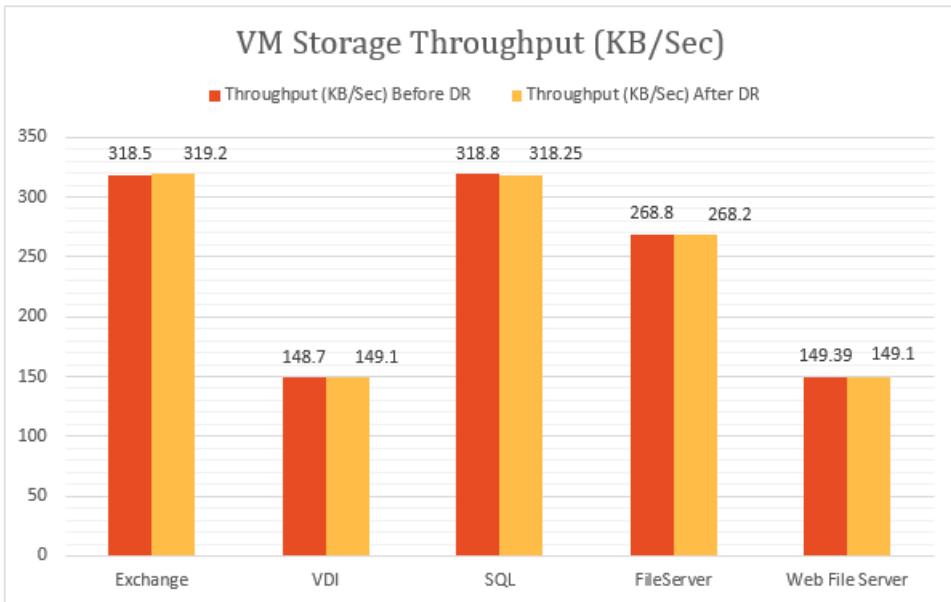
Effect on VM performance

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.



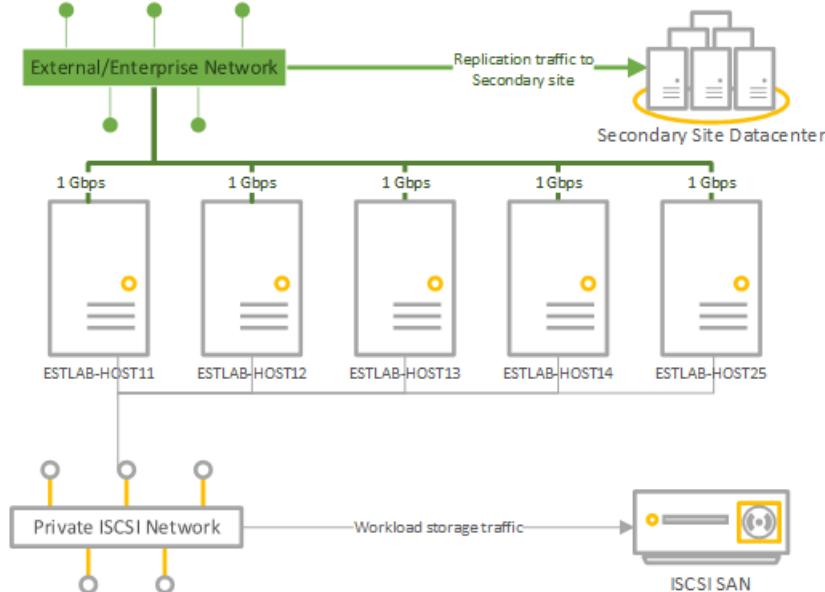
Conclusion

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

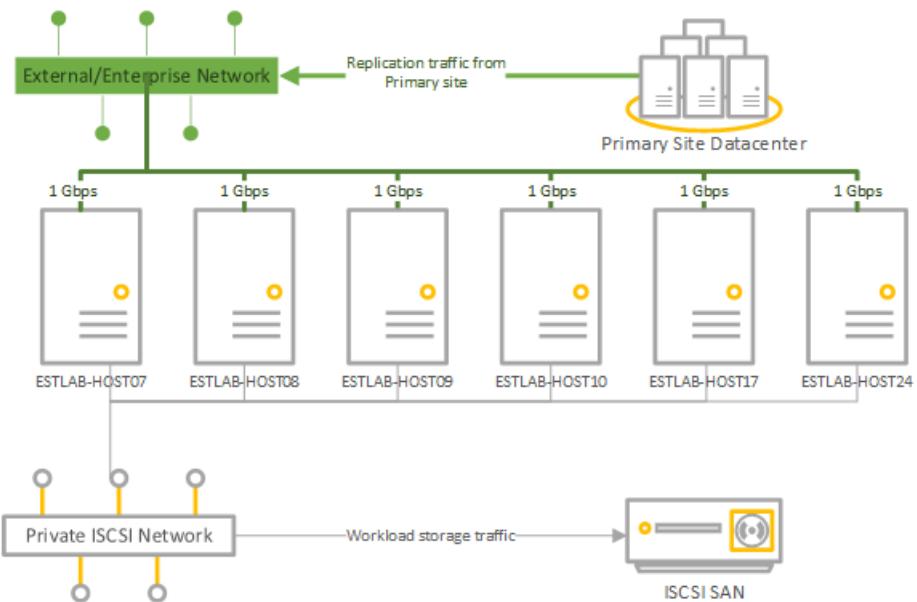
- The primary site has a cluster containing five Hyper-V servers, running 470 virtual machines.
- The VMs run different workloads, and all have Site Recovery protection enabled.
- Storage for the cluster node is provided by an iSCSI SAN. Model – Hitachi HUS130.
- Each cluster server has four network 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 | 128ESTLAB-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 | 48163264 | 60%20%5%5%10% | 80%80%80%80%80% | 88888 | All 100% random |
| SQL Server (volume 1)SQL Server (volume 2) | 864 | 100%100% | 70%0% | 88 | 100% random100% sequential |
| Exchange | 32 | 100% | 67% | 8 | 100% random |
| Workstation/VDI | 464 | 66%34% | 70%95% | 11 | Both 100% random |
| Web File Server | 4864 | 33%34%33% | 95%95%95% | 888 | All 75% random |

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 |
| 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()\Read Operations/Sec |
| VM write (IOPS) operations/sec | \Hyper-V Virtual Storage Device()\Write Operations/S |
| VM read throughput | \Hyper-V Virtual Storage Device()\Read Bytes/sec |
| VM write throughput | \Hyper-V Virtual Storage Device()\Write Bytes/sec |

Next steps

[Set up replication](#)

Use Azure Site Recovery to protect Active Directory and DNS

7/20/2018 • 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

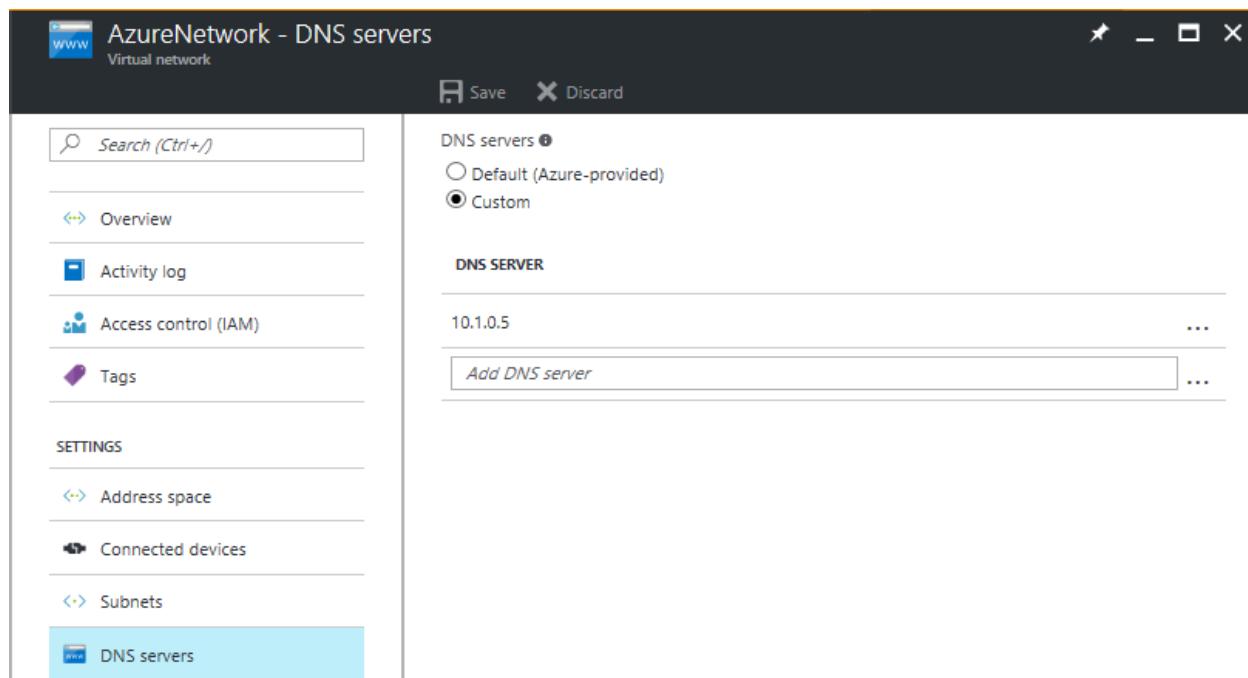
Site-to-site protection

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.

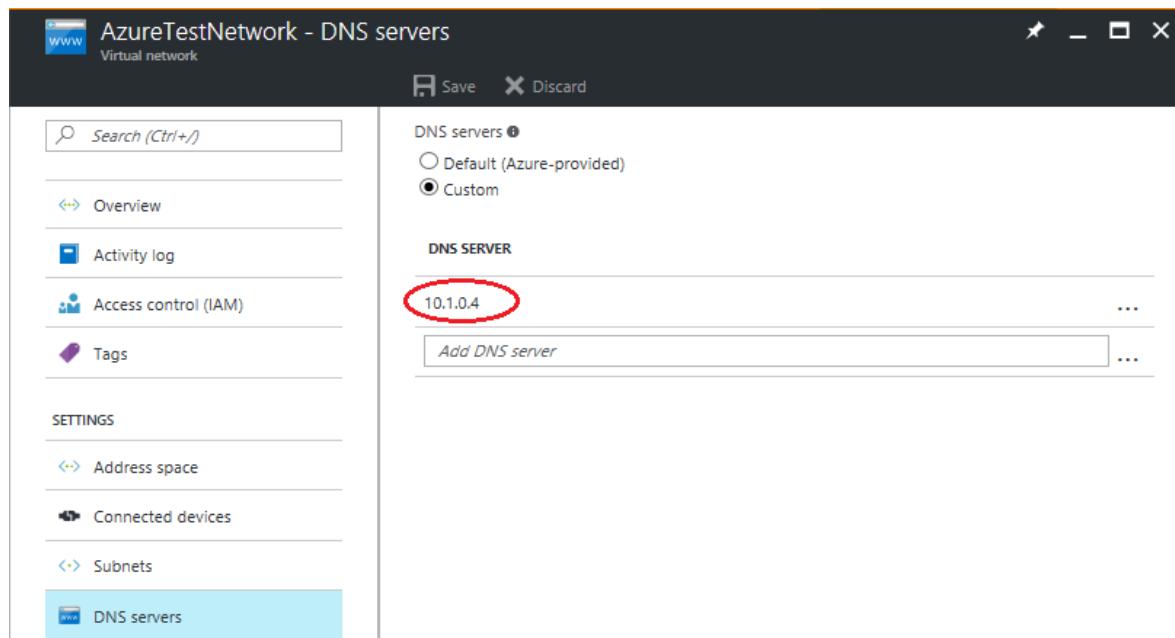
Test failover considerations

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.



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 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 log in to the domain controller virtual machine.

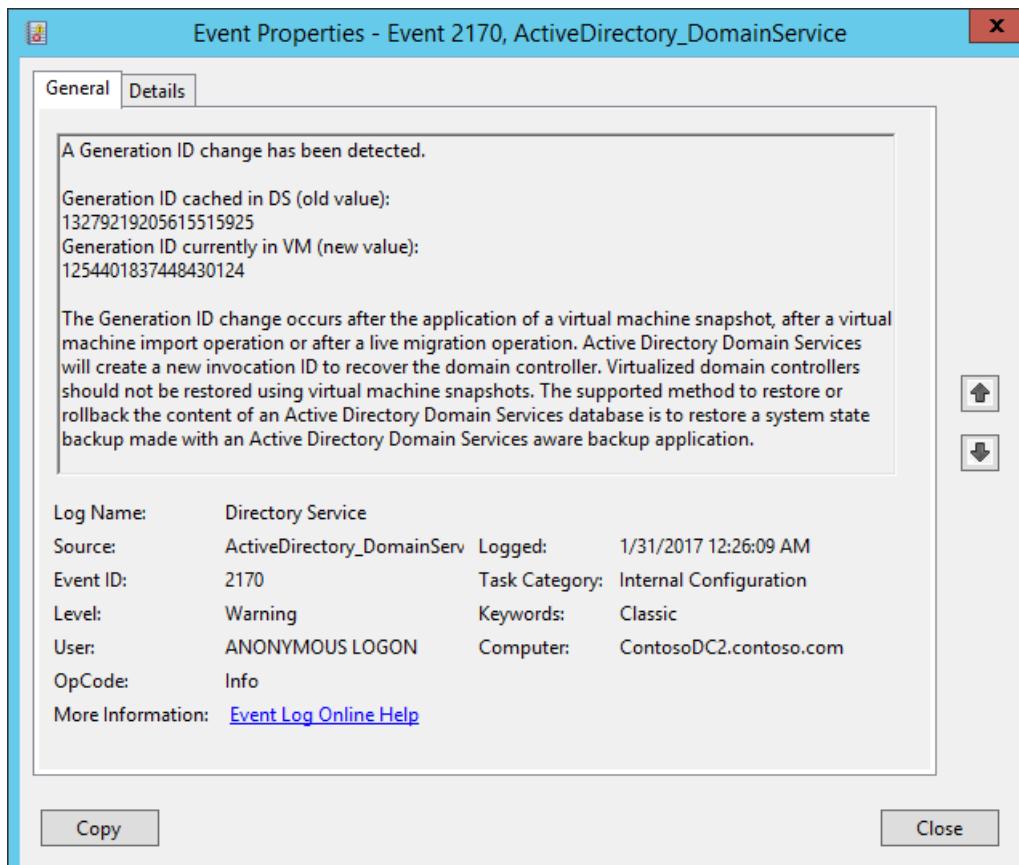
Because this domain controller is used only in a test failover, virtualization safeguards aren't necessary. To ensure that the **VM-GenerationID** value for the domain controller virtual machine doesn't change, you can change the value of following DWORD to **4** in the on-premises domain controller:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\gencounter\Start

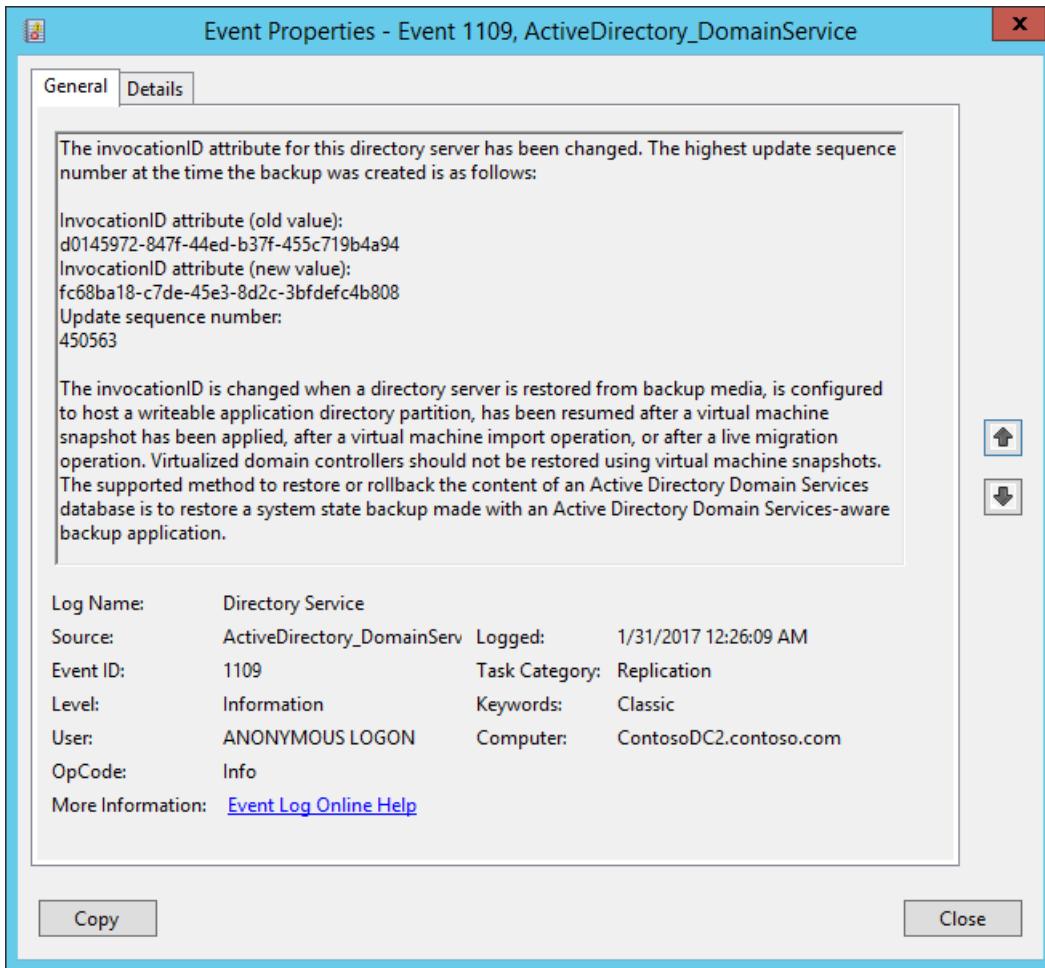
Symptoms of virtualization safeguards

If virtualization safeguards are triggered after a test failover, you might see one or more of following symptoms:

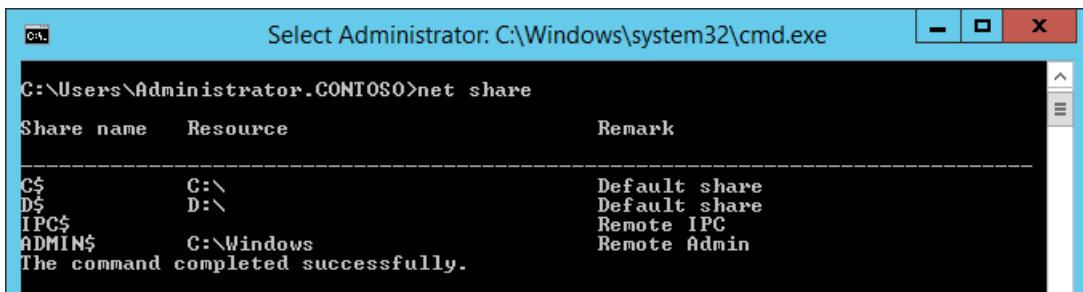
- The **GenerationID** value changes.

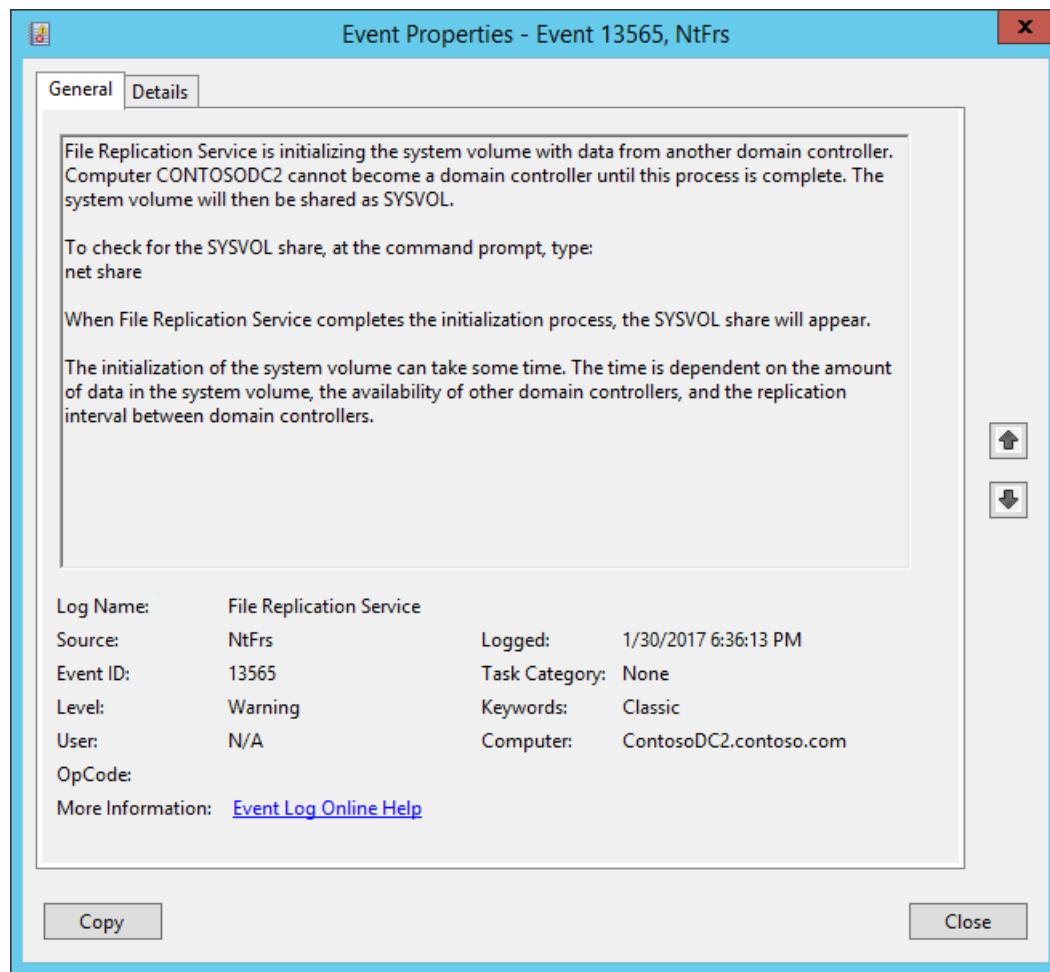


- The **InvocationID** value changes.

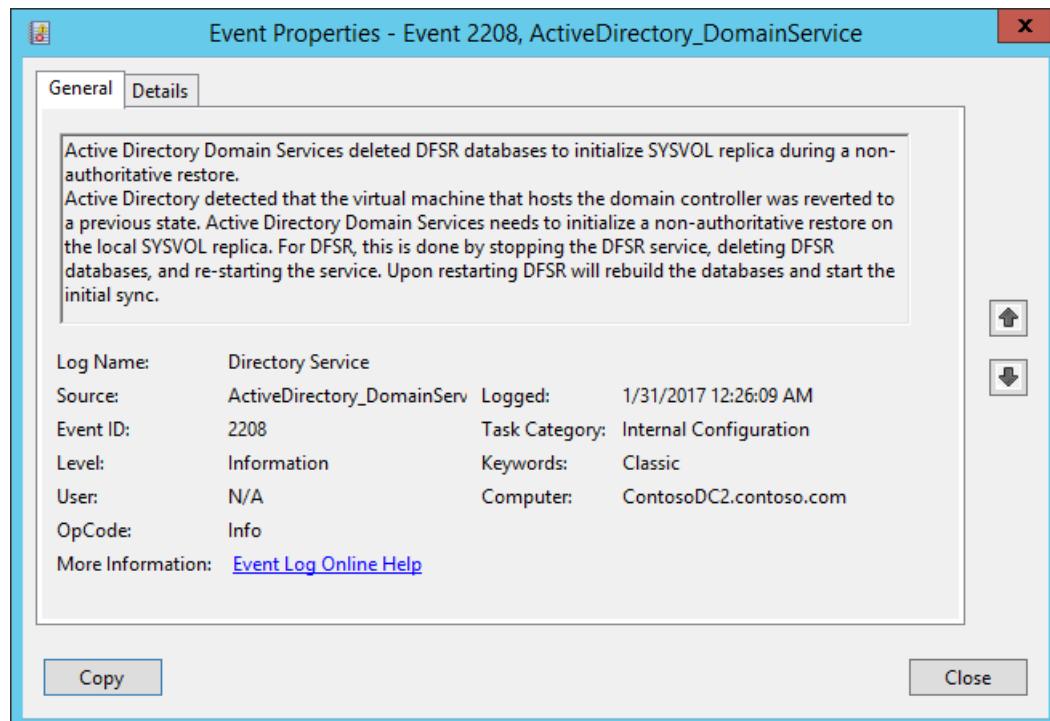


- SYSVOL and NETLOGON shares aren't available.





- DFS 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.

1. At the command prompt, run the following command to check whether SYSVOL and NETLOGON folders are shared:

```
NET SHARE
```

2. At the command prompt, run the following command to ensure that the domain controller is functioning properly:

```
dcdiag /v > dcdiag.txt
```

3. 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:

1. 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 \(like "D4/D2" for FRS\)](#).

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](#).

Protect SQL Server using SQL Server disaster recovery and Azure Site Recovery

8/13/2018 • 9 minutes to read • [Edit Online](#)

This article describes how to protect the SQL Server back end of an application 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, including failover clustering, Always On availability groups, database mirroring, and log shipping.

SQL Server deployments

Many workloads use SQL Server as a foundation, and it can be integrated with apps such as SharePoint, Dynamics, and SAP, to implement data services. SQL Server can be deployed in a number of ways:

- **Standalone SQL Server:** SQL Server and all databases are hosted on a single machine (physical or a virtual). When virtualized, host clustering is used for local high availability. Guest-level high availability isn't implemented.
- **SQL Server Failover Clustering Instances (Always On FCI):** Two or more nodes running SQL Server instanced with shared disks are configured in a Windows Failover cluster. If a node is down, the cluster can fail SQL Server over to another instance. This setup is typically used to implement high availability at a primary site. This deployment doesn't protect against failure or outage in the shared storage layer. A shared disk can be implemented using iSCSI, fiber channel or shared vhdx.
- **SQL Always On Availability Groups:** Two or more nodes are set up in a shared nothing cluster, with SQL Server databases configured in an availability group, with synchronous replication and automatic failover.

This article leverages the following native SQL disaster recovery technologies for recovering databases to a remote site:

- SQL Always On Availability Groups, to provide for disaster recovery for SQL Server 2012 or 2014 Enterprise editions.
- SQL database mirroring in high safety mode, for SQL Server Standard edition (any version), or for SQL Server 2008 R2.

Site Recovery support

Supported scenarios

Site Recovery can protect SQL Server as summarized in the table.

| SCENARIO | TO A SECONDARY SITE | TO AZURE |
|-----------------|---------------------|----------|
| Hyper-V | Yes | Yes |
| VMware | Yes | Yes |
| Physical server | Yes | Yes |

| SCENARIO | TO A SECONDARY SITE | TO AZURE |
|----------|---------------------|----------|
| Azure | NA | Yes |

Supported SQL Server versions

These SQL Server versions are supported, for the supported scenarios:

- SQL Server 2016 Enterprise and Standard
- SQL Server 2014 Enterprise and Standard
- SQL Server 2012 Enterprise and Standard
- SQL Server 2008 R2 Enterprise and Standard

Supported SQL Server integration

Site Recovery can be integrated with native SQL Server BCDR technologies summarized in the table, to provide a disaster recovery solution.

| FEATURE | DETAILS | SQL SERVER |
|--|---|---|
| Always On availability group | <p>Multiple standalone instances of SQL Server each run in a failover cluster that has multiple nodes.</p> <p>Databases can be grouped into failover groups that can be copied (mirrored) on SQL Server instances so that no shared storage is needed.</p> <p>Provides disaster recovery between a primary site and one or more secondary sites. Two nodes can be set up in a shared nothing cluster with SQL Server databases configured in an availability group with synchronous replication and automatic failover.</p> | SQL Server 2016, SQL Server 2014 & SQL Server 2012 Enterprise edition |
| Failover clustering (Always On FCI) | <p>SQL Server leverages Windows failover clustering for high availability of on-premises SQL Server workloads.</p> <p>Nodes running instances of SQL Server with shared disks are configured in a failover cluster. If an instance is down the cluster fails over to different one.</p> <p>The cluster doesn't protect against failure or outages in shared storage. The shared disk can be implemented with iSCSI, fiber channel, or shared VHDXs.</p> | SQL Server Enterprise editions
SQL Server Standard edition (limited to two nodes only) |
| Database mirroring (high safety mode) | Protects a single database to a single secondary copy. Available in both high safety (synchronous) and high performance (asynchronous) replication modes. Doesn't require a failover cluster. | SQL Server 2008 R2
SQL Server Enterprise all editions |

| FEATURE | DETAILS | SQL SERVER |
|------------------------------|--|--------------------------------|
| Standalone SQL Server | The SQL Server and database are hosted on a single server (physical or virtual). Host clustering is used for high availability if the server is virtual. No guest-level high availability. | Enterprise or Standard edition |

Deployment recommendations

This table summarizes our recommendations for integrating SQL Server BCDR technologies with Site Recovery.

| VERSION | EDITION | DEPLOYMENT | ON-PREM TO ON-PREM | ON-PREM TO AZURE |
|-------------------------------|------------------------|---|---|---|
| SQL Server 2016, 2014 or 2012 | Enterprise | Failover cluster instance | Always On availability groups | Always On availability groups |
| | Enterprise | Always On availability groups for high availability | Always On availability groups | Always On availability groups |
| | Standard | Failover cluster instance (FCI) | Site Recovery replication with local mirror | Site Recovery replication with local mirror |
| | Enterprise or Standard | Standalone | Site Recovery replication | Site Recovery replication |
| SQL Server 2008 R2 or 2008 | Enterprise or Standard | Failover cluster instance (FCI) | Site Recovery replication with local mirror | Site Recovery replication with local mirror |
| | Enterprise or Standard | Standalone | Site Recovery replication | Site Recovery replication |
| SQL Server (Any version) | Enterprise or Standard | Failover cluster instance - DTC application | Site Recovery replication | Not Supported |

Deployment prerequisites

- An on-premises SQL Server deployment, running a supported SQL Server version. Typically, you also need Active Directory for your SQL server.
- The requirements for the scenario you want to deploy. Learn more about support requirements for [replication to Azure](#) and [on-premises](#), and [deployment prerequisites](#).
- To set up recovery in Azure, run the [Azure Virtual Machine Readiness Assessment](#) tool on your SQL Server virtual machines, to make sure they're compatible with Azure and Site Recovery.

Set up Active Directory

Set up Active Directory, in the secondary recovery site, for SQL Server to run properly.

- **Small enterprise**—With a small number of applications, and single domain controller for the on-premises site, if you want to fail over the entire site, we recommend you use Site Recovery replication to replicate the domain controller to the secondary datacenter, or to Azure.

- **Medium to large enterprise**—If you have a large number of applications, an Active Directory forest, and you want to fail over by application or workload, we recommend you set up an additional domain controller in the secondary datacenter, or in Azure. If you're using Always On availability groups to recover to a remote site, we recommend you set up another additional domain controller on the secondary site or in Azure, to use for the recovered SQL Server instance.

The instructions in this article presume that a domain controller is available in the secondary location. [Read more](#) about protecting Active Directory with Site Recovery.

Integrate with SQL Server Always On for replication to Azure

Here's what you need to do:

1. Import scripts into your Azure Automation account. This contains the scripts to failover SQL Availability Group in a [Resource Manager virtual machine](#) and a [Classic virtual machine](#).

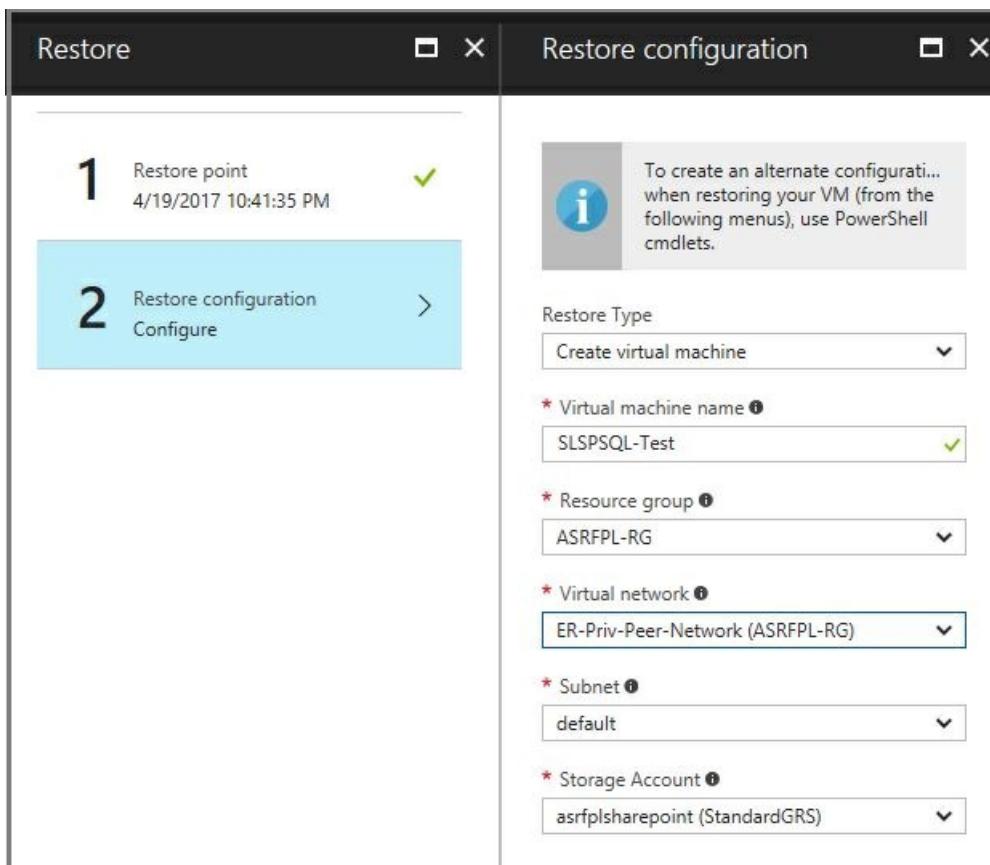


2. Add ASR-SQL-FailoverAG as a pre action of the first group of the recovery plan.
3. Follow the instructions available in the script to create an automation variable to provide the name of the availability groups.

Steps to do a test failover

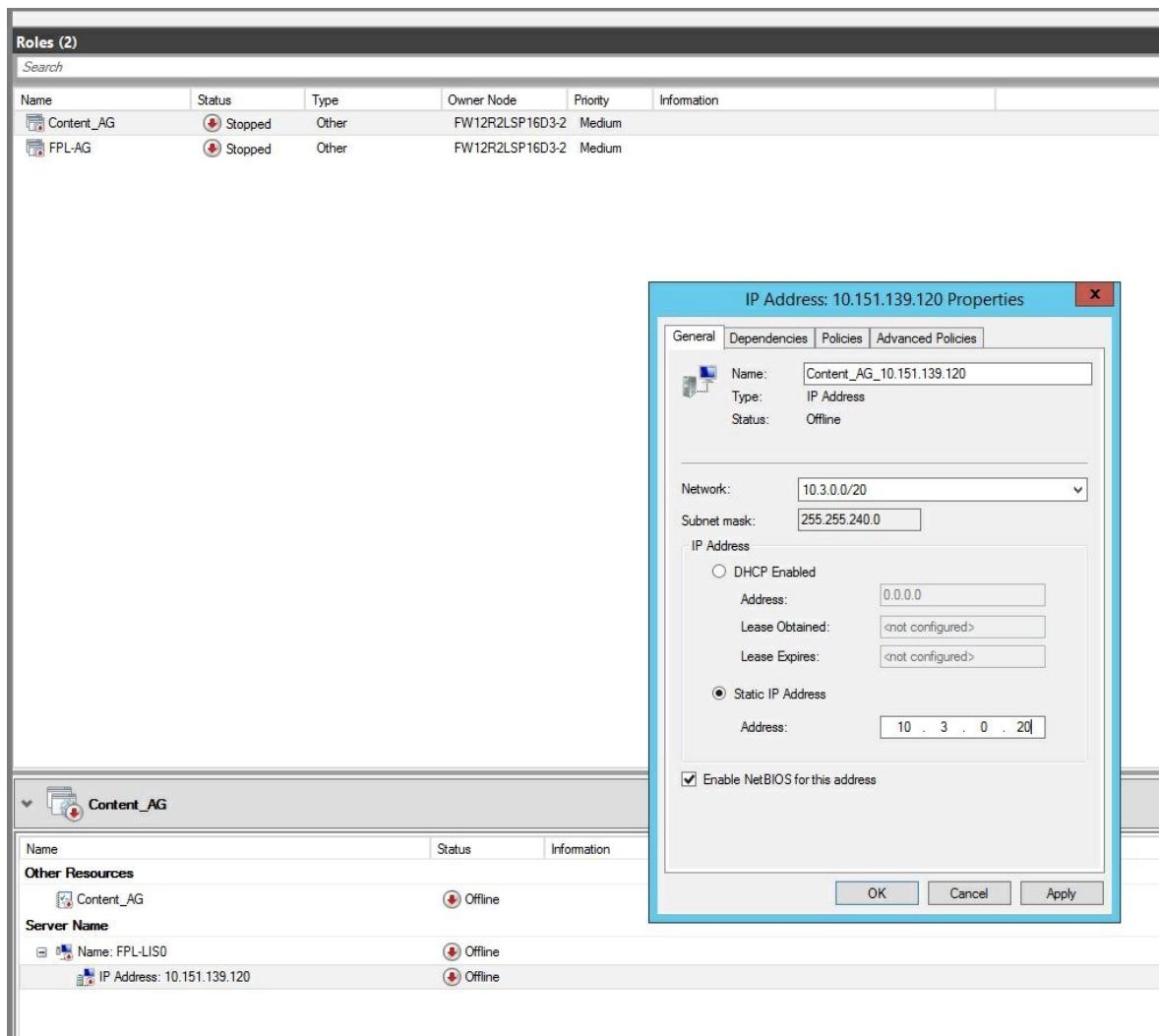
SQL Always On doesn't natively support test failover. Therefore, we recommend the following:

1. Set up [Azure Backup](#) on the virtual machine that hosts the availability group replica in Azure.
2. Before triggering test failover of the recovery plan, recover the virtual machine from the backup taken in the previous step.

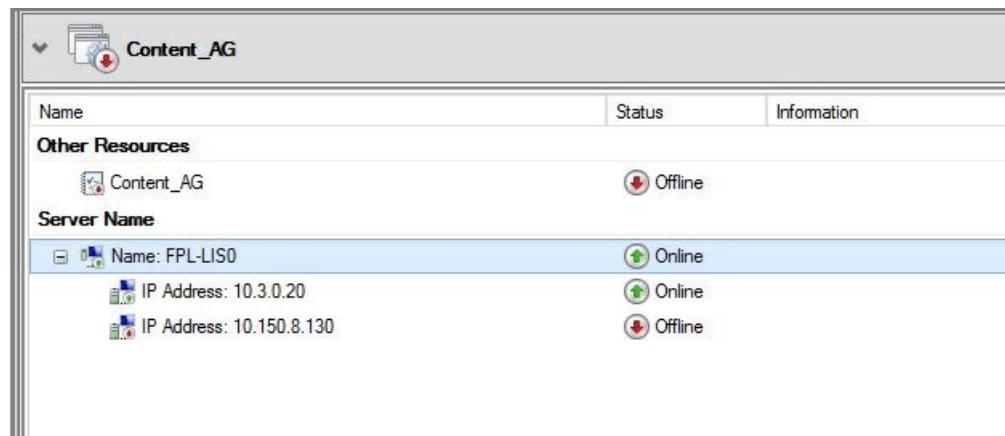


3. Force a quorum in the virtual machine restored from backup.

4. Update IP of the listener to an IP available in the test failover network.



5. Bring listener online.



6. Create a load balancer with one IP created under frontend IP pool corresponding to each availability group listener and with the SQL virtual machine added in the backend 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) | Running | SLSPSQL-Test-nic-efe654ea23934d8585dd82fe... | 10.3.0.6 |

7. Do a test failover of the recovery plan.

Steps to do a failover

Once you have added the script in the recovery plan and validated the recovery plan by doing a test failover, you can do failover of the recovery plan.

Integrate with SQL Server Always On for replication to a secondary on-premises site

If the SQL Server is using availability groups for high availability (or an FCI), we recommend using availability groups on the recovery site as well. Note that this applies to apps that don't use distributed transactions.

1. [Configure databases](#) into availability groups.
2. Create a virtual network on the secondary site.
3. Set up a site-to-site VPN connection between the virtual network, and the primary site.
4. Create a virtual machine on the recovery site, and install SQL Server on it.
5. Extend the existing Always On availability groups to the new SQL Server VM. Configure this SQL Server instance as an asynchronous replica copy.
6. Create an availability group listener, or update the existing listener to include the asynchronous replica virtual machine.
7. Make sure that the application farm is set up using the listener. If it's setup up using the database server name, update it to use the listener, so you don't need to reconfigure it after the failover.

For applications that use distributed transactions, we recommend you deploy Site Recovery with [VMware/physical server site-to-site replication](#).

Recovery plan considerations

1. Add this sample script to the VMM library, on the primary and secondary sites.

```
Param(  
[string]$SQLAvailabilityGroupPath  
)  
import-module sqlps  
Switch-SqlAvailabilityGroup -Path $SQLAvailabilityGroupPath -AllowDataLoss -force
```

2. When you create a recovery plan for the application, add a pre action to Group-1 scripted step, that invokes the script to fail over availability groups.

Protect a standalone SQL Server

In this scenario, we recommend that you use Site Recovery replication to protect the SQL Server machine. The exact steps will depend whether SQL Server is a VM or a physical server, and whether you want to replicate to Azure or a secondary on-premises site. Learn about [Site Recovery scenarios](#).

Protect a SQL Server cluster (standard edition/Windows Server 2008 R2)

For a cluster running SQL Server Standard edition, or SQL Server 2008 R2, we recommend you use Site Recovery replication to protect SQL Server.

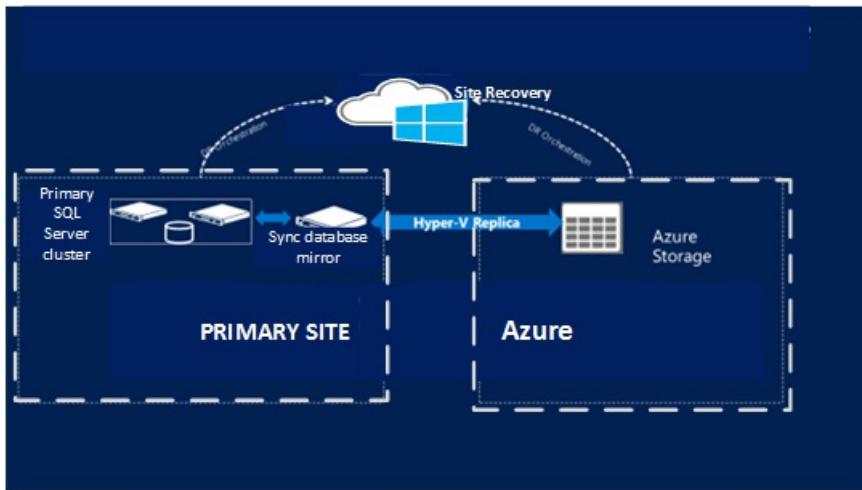
On-premises to on-premises

- If the app uses distributed transactions we recommend you deploy [Site Recovery with SAN replication](#) for a Hyper-V environment, or [VMware/physical server to VMware](#) for a VMware environment.
- For non-DTC applications, use the above approach to recover the cluster as a standalone server, by leveraging a local high safety DB mirror.

On-premises to Azure

Site Recovery doesn't provide guest cluster support when replicating to Azure. SQL Server also doesn't provide a low-cost disaster recovery solution for Standard edition. In this scenario, we recommend you protect the on-premises SQL Server cluster to a standalone SQL Server, and recover it in Azure.

1. Configure an additional standalone SQL Server instance on the on-premises site.
2. Configure the instance to serve as a mirror for the databases you want to protect. Configure mirroring in high safety mode.
3. Configure Site Recovery on the on-premises site, for ([Hyper-V](#) or [VMware VMs/physical servers](#)).
4. Use Site Recovery replication to replicate the new SQL Server instance to Azure. Since it's a high safety mirror copy, it will be synchronized with the primary cluster, but it will be replicated to Azure using Site Recovery replication.



Fallback considerations

For SQL Server Standard clusters, failback after an unplanned failover requires a SQL server backup and restore, from the mirror instance to the original cluster, with reestablishment of the mirror.

Next steps

[Learn more](#) about Site Recovery architecture.

Replicate a multi-tier SharePoint application for disaster recovery using Azure Site Recovery

7/9/2018 • 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

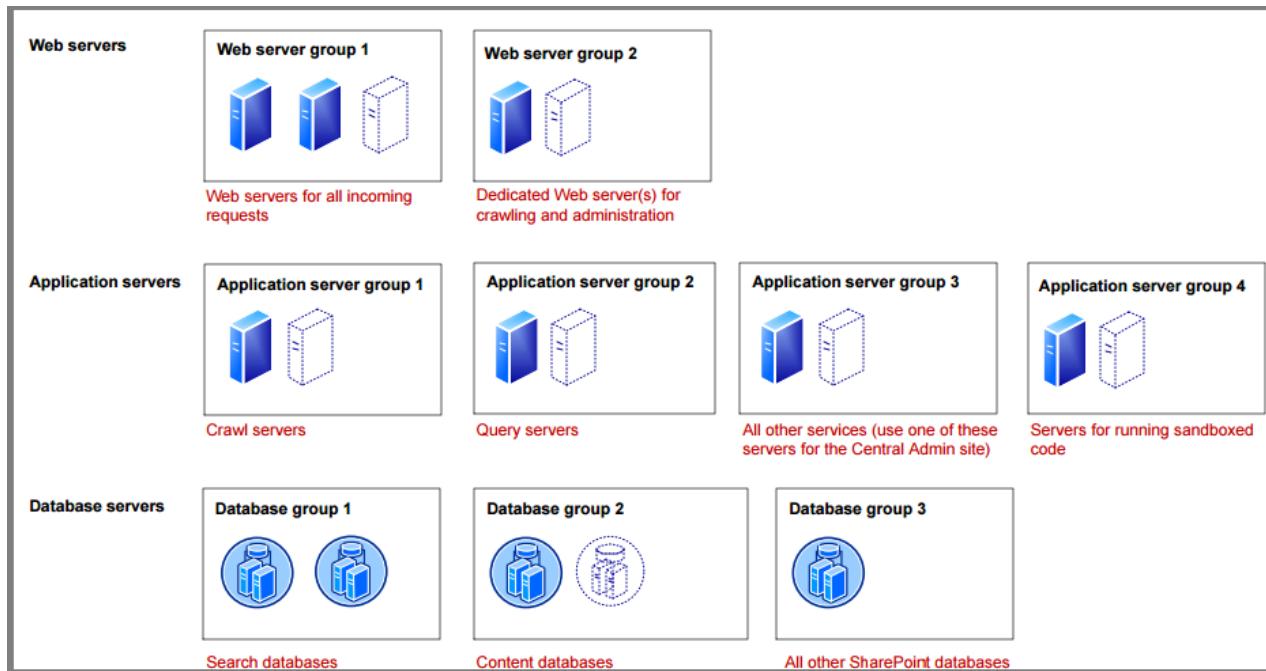
Before you start, make sure you understand the following:

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

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. As Site Recovery replication is application agnostic, the recommendations provided here are expected to hold on for following scenarios as well.

Source and target

| SCENARIO | TO A SECONDARY SITE | TO AZURE |
|------------------------|---------------------|----------|
| Hyper-V | Yes | Yes |
| VMware | Yes | Yes |
| Physical server | Yes | Yes |
| Azure | NA | Yes |

SharePoint Versions

The following SharePoint server versions are supported.

- SharePoint server 2013 Standard
- SharePoint server 2013 Enterprise
- SharePoint server 2016 Standard
- SharePoint server 2016 Enterprise

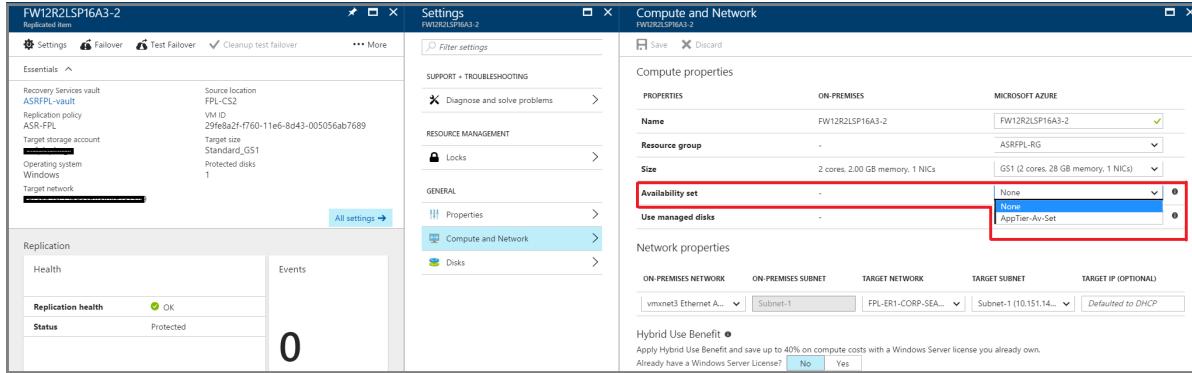
Things to keep in mind

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.

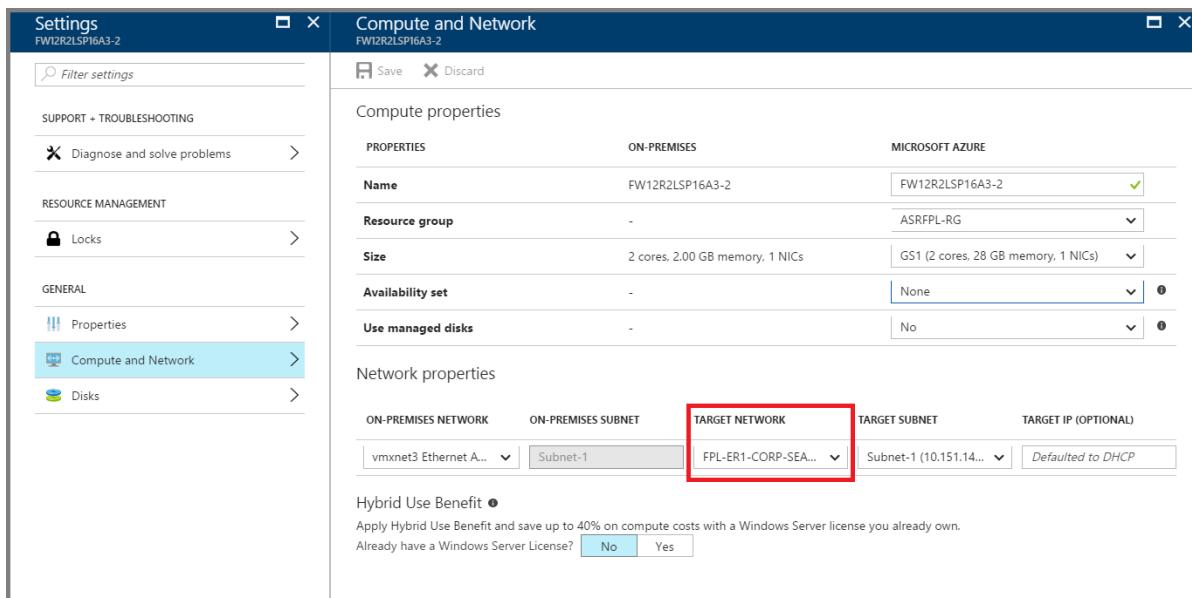


- For guidance on protecting Active Directory and DNS, refer to [Protect Active Directory and DNS](#) document.
- For guidance on protecting database tier running on SQL server, refer to [Protect SQL Server](#) document.

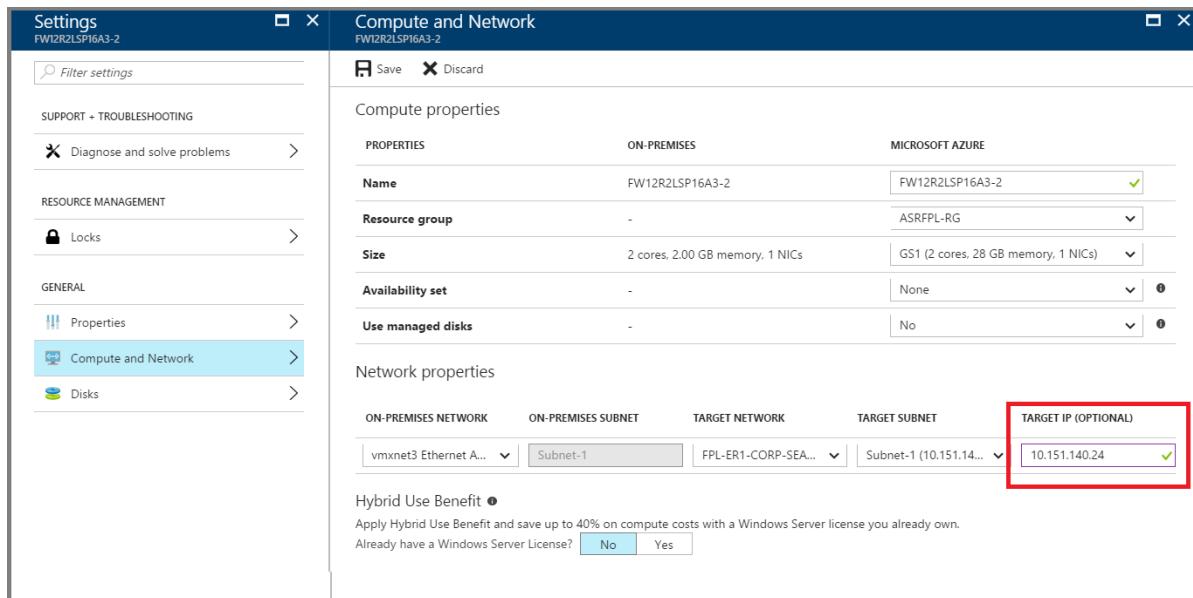
Networking configuration

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.



- 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 | Delete
Add protected items
Add pre action
Add post action |
| 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 | |

The screenshot shows the 'AlwaysOnSP-Test' Recovery plan editor. The 'Insert action' dialog is open, set to 'Script'. It includes fields for 'Name' (Add Frontend Load Balancer), 'Automation account name' (ASRAutomation), and 'Runbook name' (ASR-AddSingleLoadBalancer). The main pane displays a table of recovery steps:

| 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 side-by-side windows. The left window is titled 'AlwaysOnSP-Test ASRFL-vault' and displays the 'Recovery Services vault' settings. It shows '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 the 'Items in recovery plan'. It indicates 6 items in the plan, with 0 items moved to the target environment. The target environment is listed as Microsoft Azure. Below these windows is a detailed view of the 'Items in recovery plan' table, which lists various stages and their details, such as 'All groups shutdown', 'All groups failover', and multiple groups for start and post-steps involving machines like FW12R2LSP16A3-2, FW12R2LSP16A1-2, FW12R2LSP16A2-2, FW12R2LSP16W1-2, FW12R2LSP16W2-2, FW12R2LSP16W3-2, and manual actions for DNS update and search service restoration.

| 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 [Doing Test failover for SQL Server Always On](#) 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.

Replicate a multitier Dynamics AX application by using Azure Site Recovery

7/9/2018 • 6 minutes to read • [Edit Online](#)

Overview

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 Azure portal. At the top, there's a dark blue header with the title 'Replicated items' and a 'rmdv2a' label. Below the header are three buttons: 'Refresh', 'Replicate', and 'Columns'. A prominent orange banner at the top 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 circular icon with an 'i' contains the text 'Finished loading data from service.'. A search bar labeled 'Filter items...' is present. The main table has columns: NAME, HEALTH, STATUS, and ACTIVE LOCATION. Two rows are listed: 'DynamicsAOS' (OK, Protected, Contoso-CSPS) and 'DynamicsClient' (OK, Protected, Contosos-CSPS). Each row has a '...' button on the far right.

| 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 two main sections: 'Compute properties' and 'Network properties'.

Compute properties

| PROPERTIES | ON-PREMISES | MICROSOFT AZURE |
|------------------|---------------------------------|--|
| Name | DynamicsAOSVM1 | DynamicsAOSVM1 ✓ |
| Resource group | - | DynamicsAX |
| Size | 1 cores, 3.50 GB memory, 1 NICs | D1_v2 (1 cores, 3.5 GB memory, 1 NICs) |
| Availability set | - | AOSAVset |

Network properties

| ON-PREMISES NETWORK | ON-PREMISES SUBNET | TARGET NETWORK | TARGET SUBNET | TARGET IP (OPTIONAL) |
|--------------------------|--------------------|----------------|--------------------------|----------------------|
| Intel(R) PRO/1000 M... ▾ | Subnet-1 | AzureNetwork | default (10.38.0.0/24) ▾ | 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 'Create recovery plan' dialog box is open. It contains the following fields:

- Name:** dynamicsaxrecoveryplan
- Source:** Contosos-CSPS
- Target:** Microsoft Azure
- Allow items with deployment model:** Resource Manager
- Select items:** 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.

This recovery plan contains 3 machine(s).

| 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?](#).

What workloads can you protect with Azure Site Recovery?

7/23/2018 • 8 minutes to read • [Edit Online](#)

This article describes workloads and applications you can replicate 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) and Oracle Data Guard.
- 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 app-specific testing.

| 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 |
| 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 |
|---|------------------------------|---|--------------------------------|--|-------------------------------|--|-------------------------------------|
| Pooled Virtual Desktop (unmanaged) | No | Yes | No | Yes | No | Yes | No |
| Pooled Virtual Desktop (managed and without UPD) | No | Yes | No | Yes | No | Yes | No |
| Remote applications and Desktop sessions (without UPD) | 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.

What workloads can you protect with Azure Site Recovery?

7/23/2018 • 8 minutes to read • [Edit Online](#)

This article describes workloads and applications you can replicate 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) and Oracle Data Guard.
- 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 app-specific testing.

| 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 |
| 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 |
|---|------------------------------|---|--------------------------------|--|-------------------------------|--|-------------------------------------|
| Pooled Virtual Desktop (unmanaged) | No | Yes | No | Yes | No | Yes | No |
| Pooled Virtual Desktop (managed and without UPD) | No | Yes | No | Yes | No | Yes | No |
| Remote applications and Desktop sessions (without UPD) | 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.

Protect a multi-tier SAP NetWeaver application deployment by using Site Recovery

7/9/2018 • 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 (TCO) 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.

This article describes how to protect SAP NetWeaver application deployments by using [Azure Site Recovery](#). The article covers best practices for protecting a three-tier SAP NetWeaver deployment on Azure by replicating to another Azure datacenter by using Site Recovery. It describes supported scenarios and configurations, and how to perform 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 SQL Server](#)

Supported scenarios

You can use Site Recovery to implement a disaster recovery solution in the following scenarios:

- SAP systems running in one Azure datacenter that replicate to another Azure datacenter (Azure-to-Azure disaster recovery). For more information, see [Azure-to-Azure replication architecture](#).
- SAP systems running on VMware (or physical) servers on-premises that replicate 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](#).
- SAP systems running on Hyper-V on-premises that replicate 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 to demonstrate 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

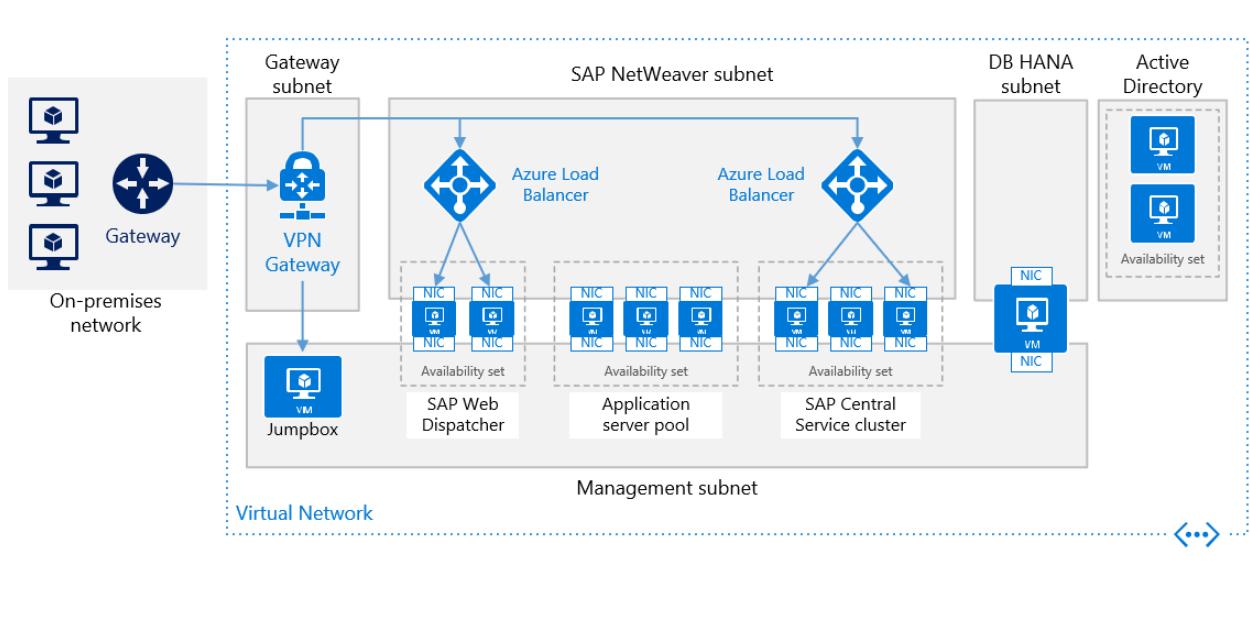
In the scenario we discuss in this article, the following foundation services are deployed:

- Azure ExpressRoute or Azure VPN Gateway
- At least one 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 shows running SAP NetWeaver in a Windows environment on Azure with high availability. This architecture is deployed with specific virtual machine (VM) sizes that can be changed to accommodate your organization's needs.



Disaster Recovery considerations

For disaster recovery (DR), you must be able to fail over to a secondary region. Each tier uses a different strategy to provide disaster recovery (DR) protection.

VMs running SAP Web Dispatcher pool

The Web Dispatcher component is used as a load balancer for SAP traffic among the SAP application servers. To achieve high availability for the Web Dispatcher component, Azure Load Balancer is used to implement the parallel Web Dispatcher setup in a round-robin configuration for HTTP(S) traffic distribution among the available Web Dispatchers in the balancer pool. This will be replicated using Azure Site Recovery(ASR) and automation scripts will be used to configure load balancer on the disaster recovery region.

VMs running application servers pool

To manage logon groups for ABAP application servers, the SMLG transaction is used. It uses the load balancing function within the message server of the Central Services to distribute workload among SAP application servers pool for SAPGUIs and RFC traffic. This will be replicated using Azure Site Recovery

VMs running SAP Central Services cluster

This reference architecture runs Central Services on VMs in the application tier. The Central Services is a potential

single point of failure (SPOF) when deployed to a single VM—typical deployment when high availability is not a requirement.

To implement a high availability solution, either a shared disk cluster or a file share cluster can be used. To configure VMs for a shared disk cluster, use Windows Server Failover Cluster. Cloud Witness is recommended as a quorum witness.

NOTE

Azure Site Recovery does not replicate the cloud witness therefore it is recommended to deploy the cloud witness in the disaster recovery region.

To support the failover cluster environment, [SIOS DataKeeper Cluster Edition](#) performs the cluster shared volume function by replicating independent disks owned by the cluster nodes. Azure does not natively support shared disks and therefore requires solutions provided by SIOS.

Another way to handle clustering is to implement a file share cluster. [SAP](#) recently modified the Central Services deployment pattern to access the /sapmnt global directories via a UNC path. However, it is still recommended to ensure that the /sapmnt UNC share is highly available. This can be done on the Central Services instance by using Windows Server Failover Cluster with Scale Out File Server (SOFS) and the Storage Spaces Direct (S2D) feature in Windows Server 2016.

NOTE

Currently Azure Site Recovery support only crash consistent point replication of virtual machines using storage spaces direct

Disaster recovery considerations

You can use Azure Site Recovery to orchestrate the fail over of full SAP deployment across Azure regions. Below 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

Below is the recommendation for disaster recovery of each tier used in this example.

| SAP TIERS | RECOMMENDATION |
|--|-------------------------------|
| SAP Web Dispatcher pool | Replicate using Site recovery |
| SAP Application server pool | Replicate using Site recovery |
| SAP Central Services cluster | Replicate using Site recovery |
| Active directory virtual machines | Active directory replication |
| SQL database servers | SQL 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, 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

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**.

The screenshot shows three windows side-by-side:

- Left Window (Settings):** Shows the general properties of the VM, including its name (VPNTestVM1), size (DS1_v2), and resource group (vpntestsea).
- Middle Window (Compute and Network):** Shows the compute properties and network properties for the VM. It lists the virtual network (vpntestorg) and the network interface cards (NIC) assigned to the VM.
- Right Window (Network interface card):** A detailed view of the NIC configuration. It shows the NIC name (vpntestvm1752), source subnet (Subnet-1), target subnet (Subnet-1), and private IP address (10.3.0.4). The private IP address field is highlighted with a red box.

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 application server, web dispatcher and SAP Central services VMs.
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, you can update the DNS entry and change bindings and connections by adding corresponding 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.
2. Add a post action script to attach a load balancer on the failed over virtual machines of Web tier (Group 1). 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.

| 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-ascgs-02 | Machine ... |
| sap-ascgs-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, 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

- To 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 Azure Site Recovery](#). The white paper discusses recommendations for various SAP architectures, lists supported applications and VM types for SAP on Azure, and describes testing plan options for your disaster recovery solution.
- Learn more about [replicating other workloads](#) by using Site Recovery.

Protect a file server by using Azure Site Recovery

7/9/2018 • 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.

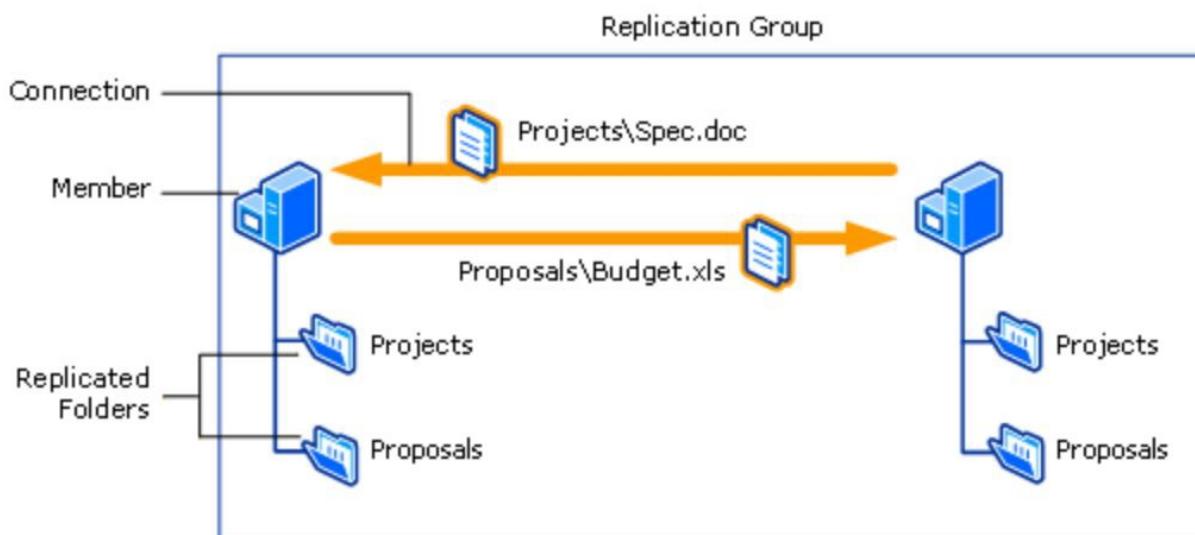
- [Replicate Azure IaaS file server machines](#)
- [Replicate an on-premises file server by using Site Recovery](#)

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.

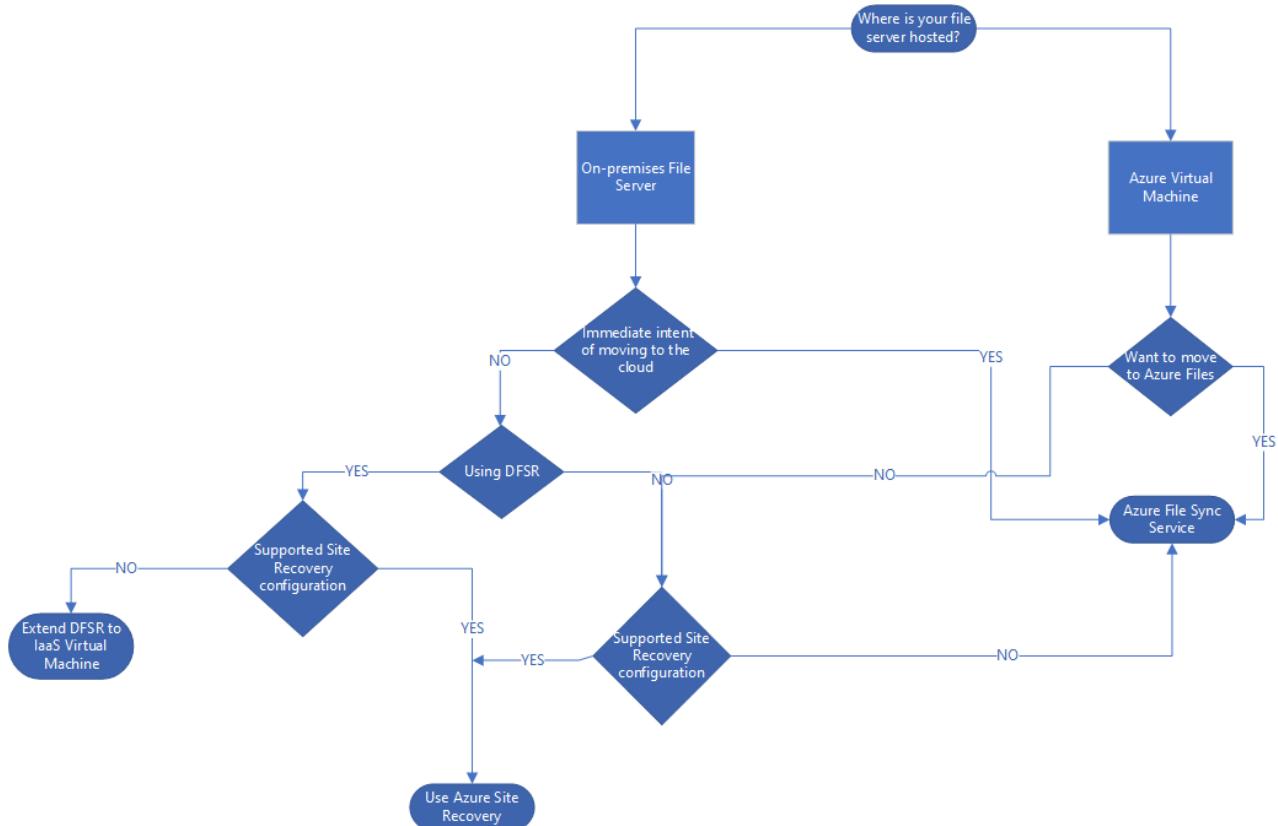


In the previous diagram, multiple file servers called members actively participate in replicating files across a replication group. The contents in the replicated folder are available to all the clients that send requests to either of the members, even if a member goes offline.

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 | Use Site Recovery for replication | 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.
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. |
| File server environment with DFSR | Extend DFSR to an Azure IaaS virtual machine | 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 [Azure file share disaster recovery strategies](#).
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.
2. Establish a site-to-site VPN connection between the on-premises site and the Azure network.
3. Extend on-premises Active Directory.
4. [Prepare on-premises VMware servers](#).
5. [Set up disaster recovery](#) to Azure for on-premises VMs.

Extend DFSR to an Azure IaaS virtual machine

1. Establish a site-to-site VPN connection between the on-premises site and the Azure network.
2. Extend on-premises Active Directory.
3. [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.
4. Install and [configure DFSR](#) on Windows Server.
5. [Implement a DFS namespace](#).
6. 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:

1. [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 [Azure file share disaster recovery strategies](#).
2. [Create a file share](#).
3. [Deploy File Sync](#) in your on-premises 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. The sync group also must contain one server endpoint, which represents a path on the on-premises 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.

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

1. Go to the Azure portal, and select your Recovery Service vault.
2. 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](#).

Replicate a multi-tier IIS-based web application

7/9/2018 • 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](#)

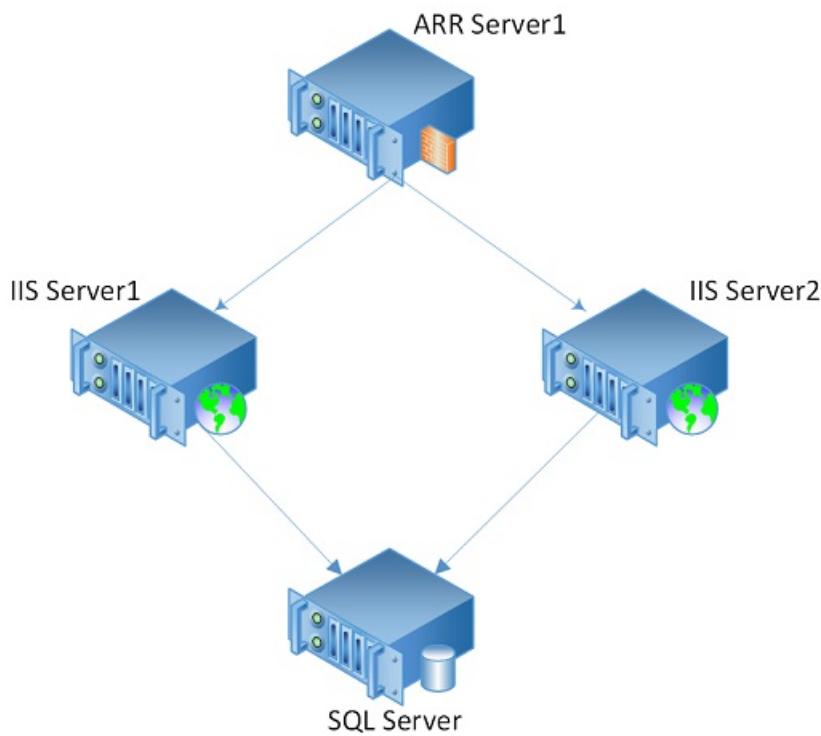
Deployment patterns

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.

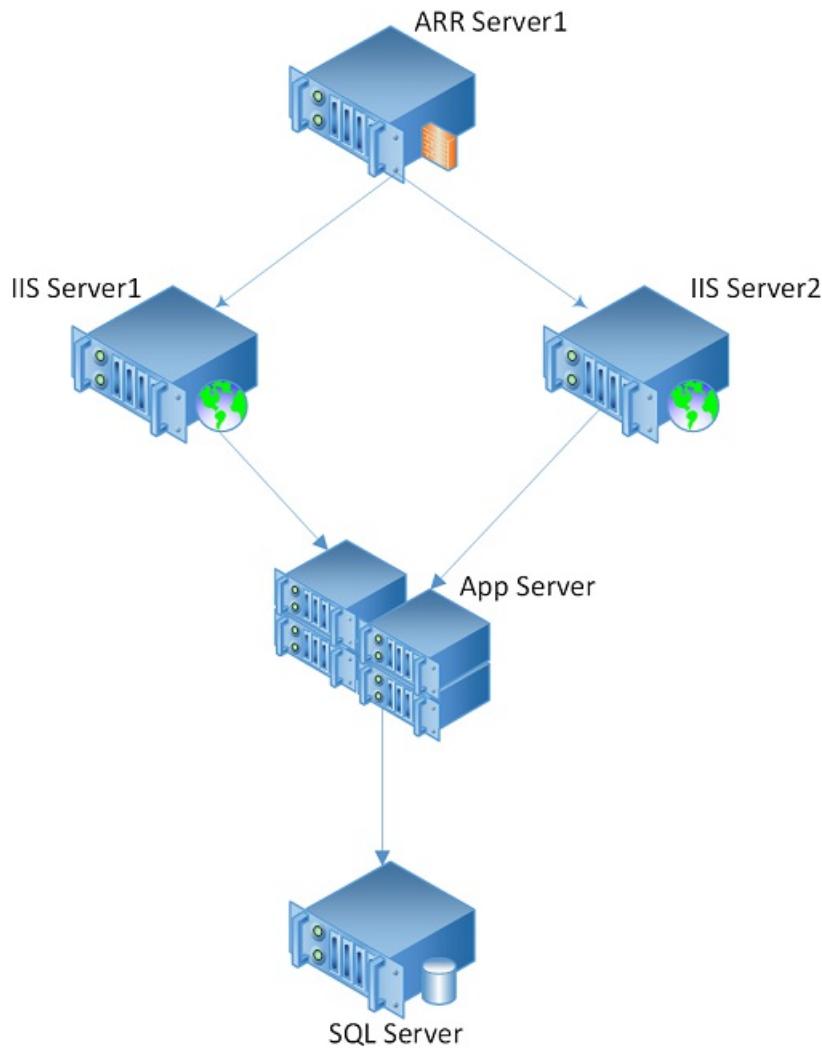
IIS Web Farm – 3 Tier Deployment



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.

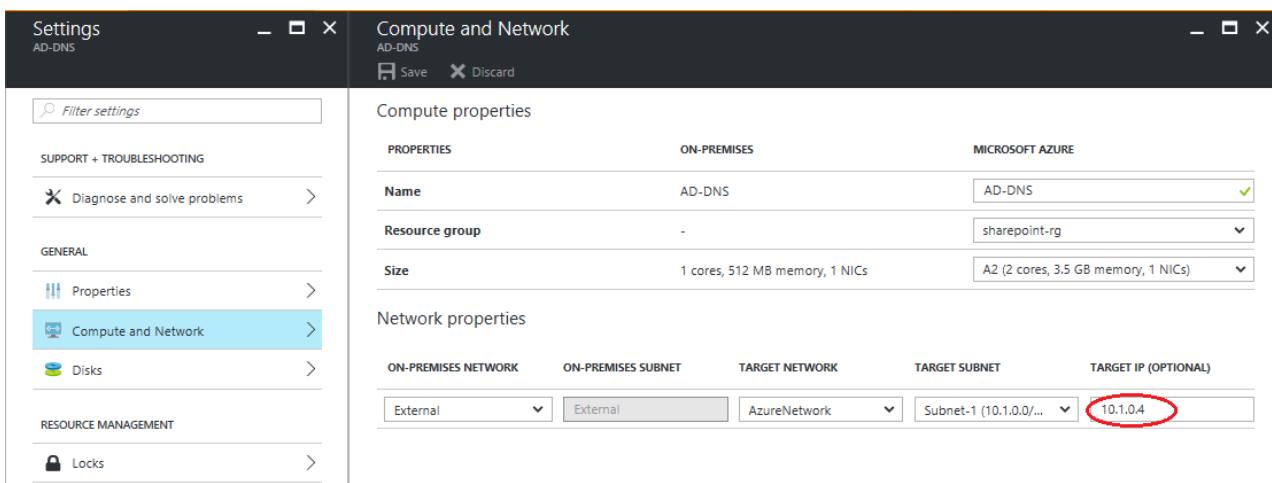
Source and target

| 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>
```

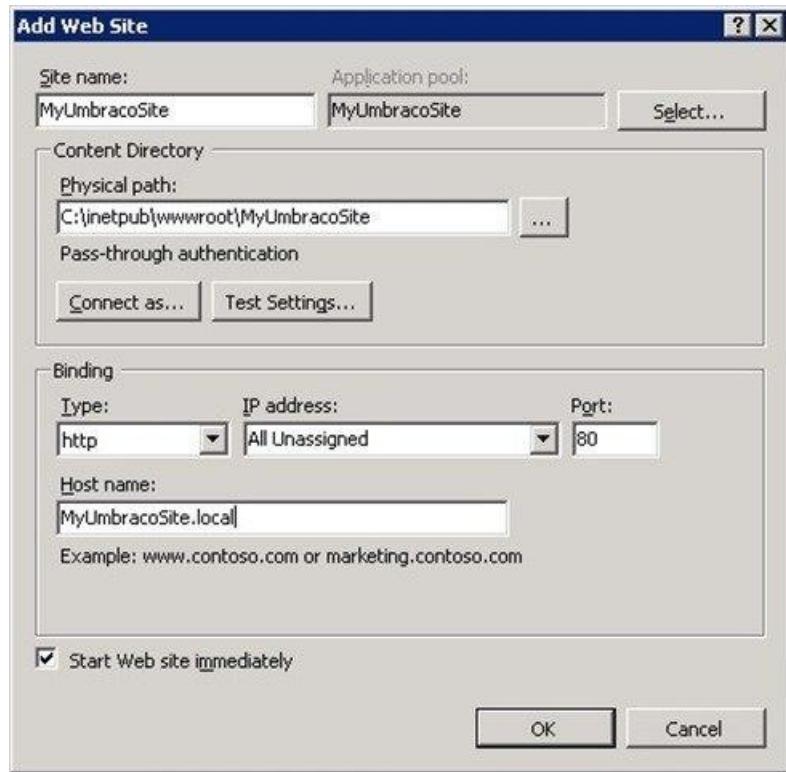
To update the connection string in the web tier, add an [IIS connection update script](#) after Group 3 in the recovery plan.

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.

Replicate a multi-tier Citrix XenApp and XenDesktop deployment using Azure Site Recovery

7/23/2018 • 7 minutes to read • [Edit Online](#)

Overview

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 a 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:

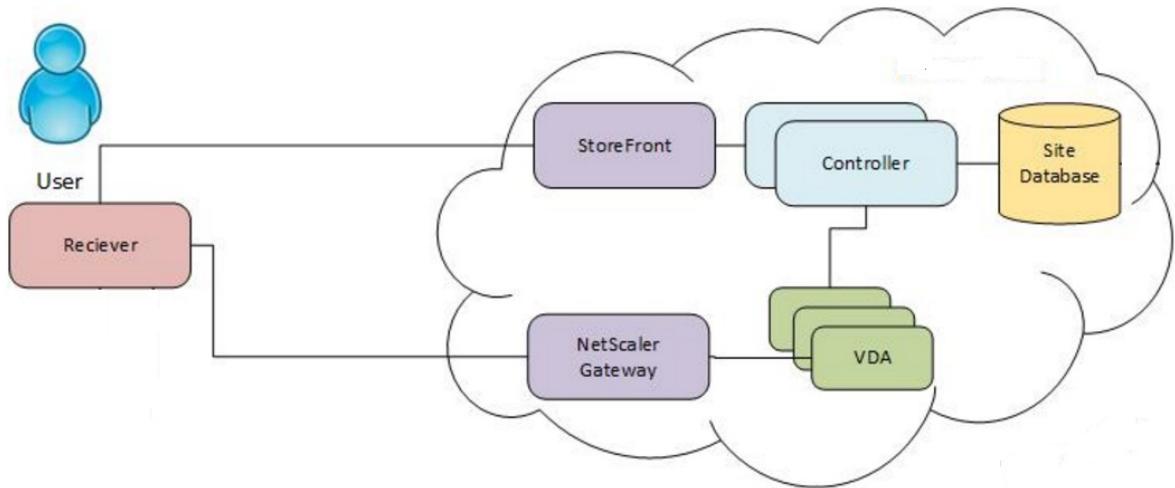
1. [Replicating a virtual machine to Azure](#)
2. How to [design a recovery network](#)
3. [Doing a test failover to Azure](#)
4. [Doing a failover to Azure](#)
5. How to [replicate a domain controller](#)
6. How to [replicate SQL Server](#)

Deployment patterns

A Citrix XenApp and XenDesktop farm typically has 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 |
|------------------------|---------------------|----------|
| Hyper-V | Not in scope | Yes |
| VMware | Not in scope | Yes |
| Physical server | 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 ASR 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

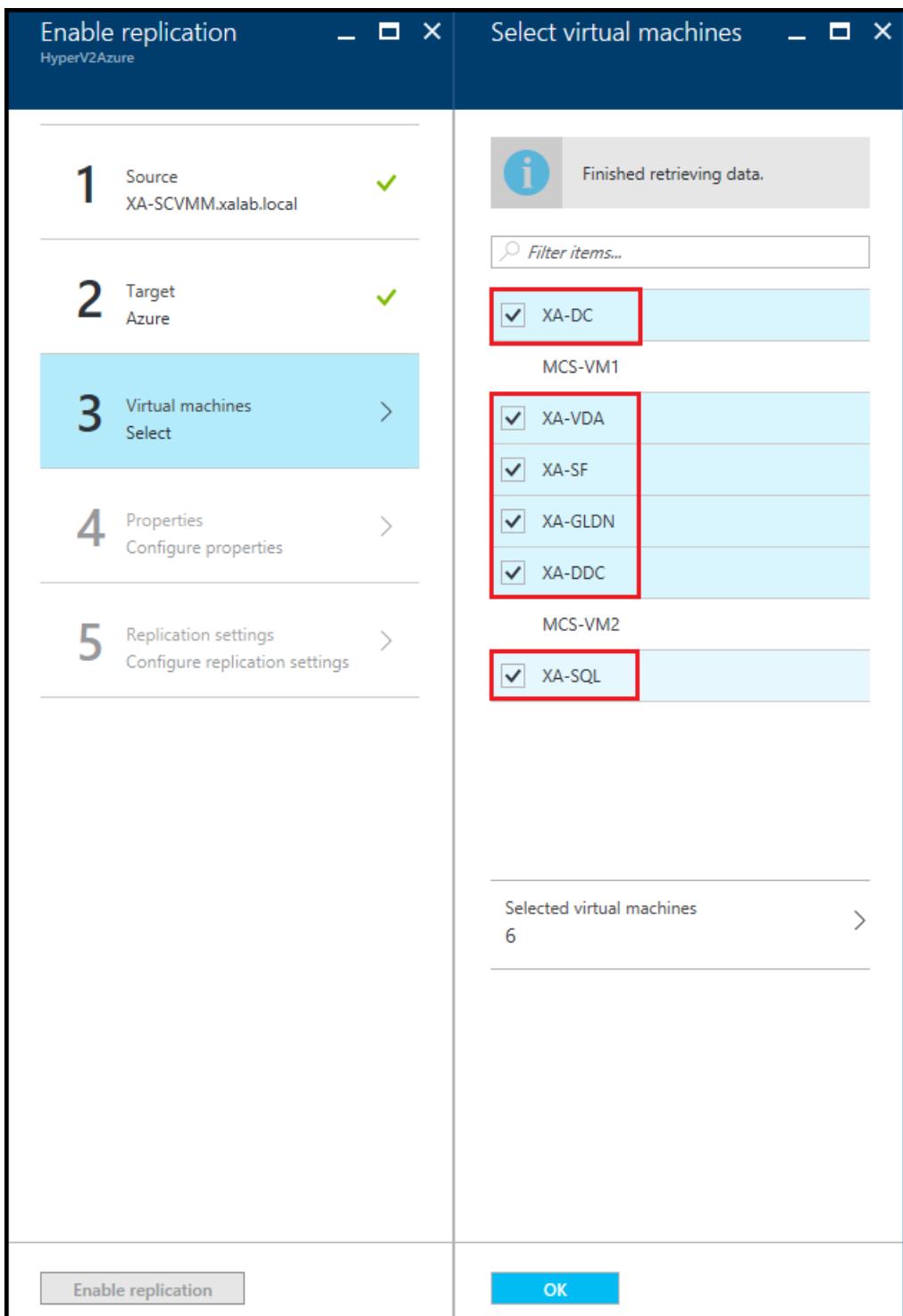
AD DNS server replication

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 be 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: Shutdown 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 ARM 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 ARM 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 ARM 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' and 'Recovery plan' buttons, followed by 'Save', 'Discard', and 'Change group' buttons. A red box highlights the '+ Group' button. Below the toolbar, a message says 'This recovery plan contains 5 machine(s.)'. 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 |

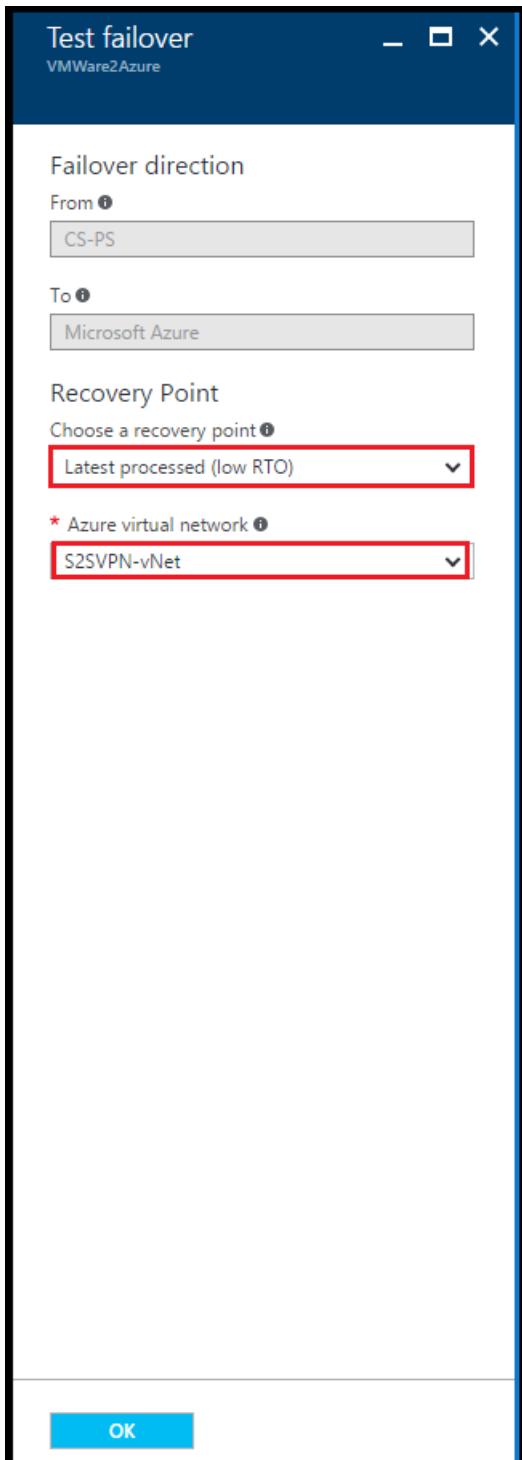
Red boxes highlight three specific actions: 'Manual: Turn off the master VDA fr...', 'Manual: Add Azure ARM Host conn...', and 'Manual: Re-create all MCS Catalogs'.

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.

What workloads can you protect with Azure Site Recovery?

7/23/2018 • 8 minutes to read • [Edit Online](#)

This article describes workloads and applications you can replicate 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) and Oracle Data Guard.
- 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 app-specific testing.

| 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 |
| 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 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 |
|---|------------------------------|---|--------------------------------|--|-------------------------------|--|-------------------------------------|
| Pooled Virtual Desktop (unmanaged) | No | Yes | No | Yes | No | Yes | No |
| Pooled Virtual Desktop (managed and without UPD) | No | Yes | No | Yes | No | Yes | No |
| Remote applications and Desktop sessions (without UPD) | 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.