



AUTOMATED DISASTER RECOVERY SOLUTION USING AZURE SITE RECOVERY  
FOR FILE SHARES HOSTED ON STORSIMPLE

---

## Copyright

---

This document is provided "as-is." Information and views expressed in this document, including URL and other Internet website references, may change without notice. Some examples depicted herein are provided for illustration only and are fictitious. No real association or connection is intended or should be inferred.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy, use and modify this document for your internal, reference purposes.

© 2015 Microsoft Corporation. All rights reserved.

Microsoft, Microsoft Azure, StorSimple, Active Directory, Hyper-V, Internet Explorer, Silverlight, SQL Server, Windows, Windows PowerShell, and Windows Server are trademarks of the Microsoft group of companies. All other trademarks are the property of their respective owners.

## Contents

Overview.....	3
Supported Azure Site Recovery deployment options.....	3
Prerequisites.....	3
Enable Disaster Recovery (DR) using Azure Site Recovery for file shares hosted on StorSimple.....	4
Create a recovery plan .....	8
Perform a test failover.....	13
Perform an unplanned failover.....	14
Perform a planned failover.....	14
Perform a failback.....	14
Best Practices.....	16
Limitations .....	16
Summary .....	17

## Overview

Microsoft Azure StorSimple is a hybrid cloud storage solution that addresses the complexities of unstructured data commonly associated with file shares. StorSimple uses cloud storage as an extension of the on-premises solution and automatically tiers data across on-premises storage and cloud storage. Integrated data protection, with local and cloud snapshots, eliminates the need for a sprawling storage infrastructure.

Azure Site Recovery<sup>1</sup> is an Azure-based service that provides disaster recovery (DR) capabilities by orchestrating replication, failover, and recovery of virtual machines. Azure Site Recovery supports a number of replication technologies to consistently replicate, protect, and seamlessly fail over virtual machines and applications to private/public or hosted clouds.

Using Azure Site Recovery, virtual machine replication, and StorSimple cloud snapshot capabilities, you can protect the complete file server environment. In the event of a disruption, you can use a single click to bring your file shares online in Azure in just a few minutes.

This document explains in detail how you can create a disaster recovery solution for your file shares hosted on StorSimple storage, and perform planned, unplanned, and test failovers using a one-click recovery plan. In addition, it describes supported configurations and prerequisites. This document assumes that you are familiar with the basics of Azure Site Recovery and StorSimple architectures.

## Supported Azure Site Recovery deployment options

Customers can deploy file servers as physical servers or virtual machines (VMs) running on Hyper-V or VMware, and then create file shares from volumes carved out of StorSimple storage. Azure Site Recovery can protect both physical and virtual deployments to either a secondary site or to Azure. This document covers details of a DR solution with Azure as the recovery site for a file server VM hosted on Hyper-V and with file shares on StorSimple storage. Other scenarios in which the file server VM is on a VMware VM or a physical machine can be implemented similarly.

## Prerequisites

Implementing a one-click disaster recovery solution that uses Azure Site Recovery for file shares hosted on StorSimple storage has the following prerequisites:

- On-premises Windows Server 2012 R2 File server VM hosted on Hyper-V or VMware or a physical machine
- StorSimple storage device on-premises registered with Azure StorSimple manager
- File shares hosted on the volumes configured on the StorSimple storage device

---

<sup>1</sup> [Azure Site Recovery documentation](#)

- Azure Site Recovery services vault created in a Microsoft Azure subscription<sup>2</sup>

In addition, if Azure is your recovery site, run the Azure Virtual Machine Readiness Assessment tool<sup>3</sup> on VMs to ensure that they are compatible with Azure VMs and Azure Site Recovery services.

To avoid latency issues (which might result in higher costs), make sure that you create your StorSimple virtual device, automation account, and storage account(s) in the same region.

## Enable Disaster Recovery (DR) using Azure Site Recovery for file shares hosted on StorSimple

Each component of the on-premises environment needs to be protected to enable complete replication and recovery. This section describes how to:

- [Set up Active Directory and DNS replication \(optional\)](#)
- [Use Azure Site Recovery to enable protection of the file server VM](#)
- [Enable protection of StorSimple volumes](#)
- [Configure the network](#)

### Set up Active Directory and DNS replication (optional)

If you want to protect the machines running Active Directory and DNS so that they are available on the DR site, you need to explicitly protect them (so that the file servers are accessible after fail over with authentication). There are two recommended options based on the complexity of the customer's on-premises environment.

#### Option 1

If the customer has a small number of applications, a single domain controller for the entire on-premises site, and will be failing over the entire site, then we recommend using Azure Site Recovery replication to replicate the domain controller machine to a secondary site (this is applicable for both site-to-site and site-to-Azure).

#### Option 2

If the customer has a large number of applications, is running an Active Directory forest, and will be failing over a few applications at a time, then we recommend setting up an additional domain controller on the DR site (either a secondary site or in Azure).

Please refer to the companion guide<sup>4</sup> for instructions when making a domain controller available on the DR site. For the remainder of this document, we will assume a domain controller is available on the DR site.

---

<sup>2</sup> [Create Azure Site Recovery vault](#) in Microsoft Azure subscription

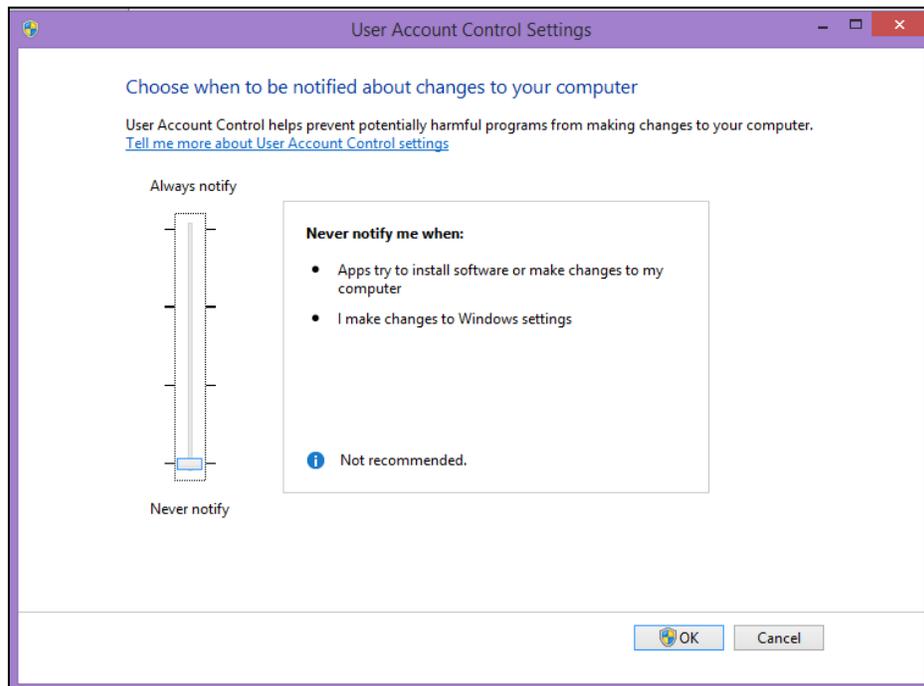
<sup>3</sup> [Azure Virtual Machine Readiness Assessment](#)

## Use Azure Site Recovery to enable protection of the file server VM

This step requires that you prepare the on-premises file server environment, create and prepare an Azure Site Recovery vault, and enable file protection of the VM.

### To prepare the on-premises file server environment

1. Set the **User Account Control** to **Never Notify**. This is required so that you can use Azure automation scripts to connect the iSCSI targets after fail over by Azure Site Recovery.
  - a. Press the Windows key +Q and search for **UAC**.
  - b. Select **Change User Account Control settings**.
  - c. Drag the bar to the bottom towards **Never Notify**.
  - d. Click **OK** and then select **Yes** when prompted.



2. Install the VM Agent on each of the file server VMs. This is required so that you can run Azure automation scripts on the failed over VMs.
  - a. Download the agent from <http://aka.ms/vmagentwin> to C:\Users\\Downloads.
  - b. Open Windows PowerShell in Administrator mode (Run as Administrator), and then enter the following command to navigate to the download location:

```
cd
C:\Users\\Downloads\WindowsAzureVmAgent.2.6.1198.718.rd_art_s
table.
150415-1739.fre.msi
```

**Note:** The file name may change depending on the version.

---

<sup>4</sup> [Automated DR solution for Active Directory and DNS using ASR](#)

- c. Click **Next**.
  - d. Accept the Terms of Agreement and then click **Next**.
  - e. Click **Finish**.
3. Create file shares using volumes carved out of StorSimple storage.<sup>5</sup>
    - a. On your on-premises VMs, press the Windows key +Q and search for **iSCSI**.
    - b. Select **iSCSI initiator**.
    - c. Select the **Configuration** tab and copy the initiator name.
    - d. Log on to the Azure management portal, <https://manage.windowsazure.com/>.
    - e. Select the **StorSimple** tab and then select the StorSimple Manager Service that contains the physical device.
    - f. Create volume container(s) and then create volume(s). (These volumes are for the file share(s) on the file server VMs) Copy the initiator name and give an appropriate name for the Access Control Records when you create the volumes.
    - g. Select the **Configure** tab and note down the IP address of the device.
    - h. On your on-premises VMs, go to the **iSCSI initiator** again and enter the IP in the Quick Connect section. Click **Quick Connect** (the device should now be connected).
    - i. Open the Azure Management Portal and select the **Volumes and Devices** tab. Click **Auto Configure**. The volume that you just created should appear.
    - j. In the portal, select the **Devices** tab and then select **Create a New Virtual Device**. (This virtual device will be used if a failover occurs). This new virtual device can be kept in an offline state to avoid extra costs. To take the virtual device offline, go to the **Virtual Machines** section on the Portal and shut it down.
    - k. Do back to the on-premises VMs and open Disk Management (press the Windows key + X and select **Disk Management**).
    - l. You will notice some extra disks (depending on the number of volumes you have created). Right-click the first one, select **Initialize Disk**, and select **OK**. Right-click the **Unallocated** section, select **New Simple Volume**, assign it a drive letter, and finish the wizard.
    - m. Repeat step l for all the disks. You can now see all the disks on **This PC** in the Windows Explorer.
    - n. Use the File and Storage Services role to create file shares on these volumes.

#### To create and prepare an Azure Site Recovery vault

- Refer to the detailed documentation<sup>6</sup> to get started with Azure Site Recovery before protecting the file server VM.

#### To enable protection

1. Disconnect the iSCSI target(s) from the on-premises VMs that you want to protect through Azure Site Recovery:
  - a. Press Win+Q and search for **iSCSI**.
  - b. Select **Set up iSCSI initiator**.
  - c. Disconnect the StorSimple device that you connected previously. Alternatively, you can switch off the file server for a few minutes when enabling protection.

---

<sup>5</sup> For more information, see [Use the StorSimple Manager service to manage volumes.](#)

<sup>6</sup> For more information, see the [Azure Site Recovery documentation.](#)

**Note:** This will cause the file shares to be temporarily unavailable

2. [Enable virtual machine protection](#) of the file server VM from the Azure Site Recovery portal.
3. When the initial synchronization begins, you can reconnect the target again. Go to the iSCSI initiator, select the StorSimple device, and click **Connect**.
4. When the synchronization is complete and the status of the VM is **Protected**, select the VM, select the **Configure** tab, and update the network of the VM accordingly (this is the network that the failed over VM(s) will be a part of). If the network doesn't show up, it means that the sync is still going on.

## Enable protection of StorSimple volumes

If you have not selected the **Enable a default backup for this volume** option for the StorSimple volumes, go to **Backup Policies** in the StorSimple Manager service, and create a suitable backup policy for all the volumes. We recommend that you set the frequency of backups to the recovery point objective (RPO) that you would like to see for the application.

## Configure the network

For the file server VM, configure network settings in Azure Site Recovery so that the VM networks are attached to the correct DR network after failover.

You can select the VM in the **VMM Cloud** or the **Protection Group** to configure the network settings, as shown in the following illustration.

The screenshot shows the configuration page for a virtual machine named 'sp-webvm1'. The page is divided into two main sections: 'source and target properties' and 'source and target network properties'.

**source and target properties**

PROPERTIES	ON-PREMISES	MICROSOFT AZURE
Name	SP-WebVM1	SP-WebVM1
Size	1 CPU, 4 GB RAM	A3 (4 cores, 7 GB memory)

**source and target network properties**

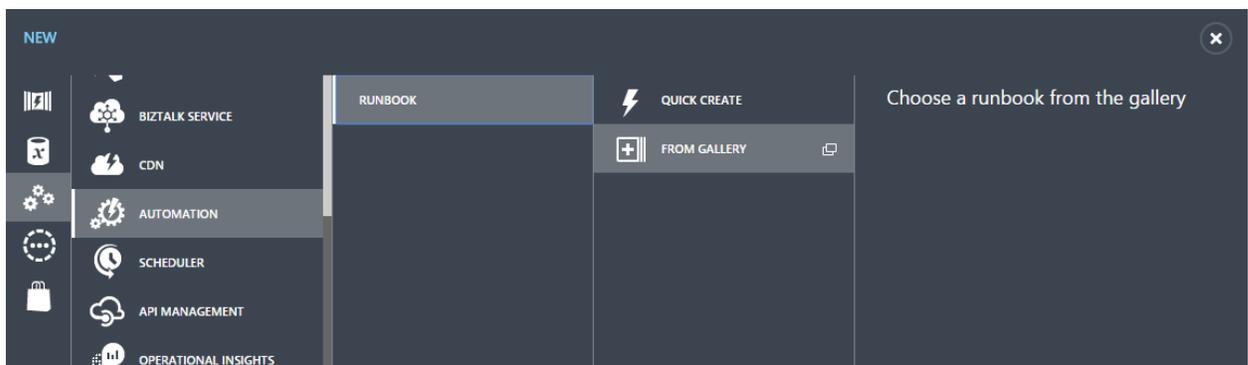
ON-PREMISE NETWORK		MICROSOFT AZURE NETWORK	
Frontend Network		AzureNetwork	
SUBNET	IP TYPE	SUBNET	TARGET IP ADDRESS
Frontend Network	Static	Subnet-1(10.0.0.0/25)	TARGET IP ADDRESS

## Create a recovery plan

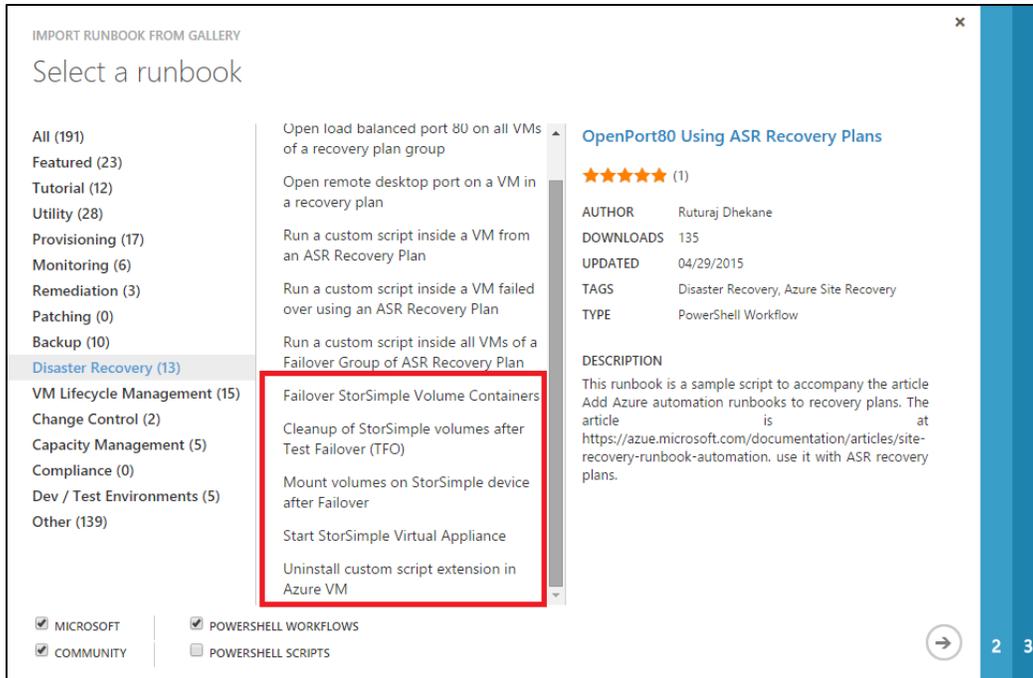
You can create a recovery plan in ASR to automate the failover process of the file shares. If a disruption occurs, you can bring the file shares up in a few minutes with just a single click. To enable this automation, you will need an Azure automation account.

### To create the account

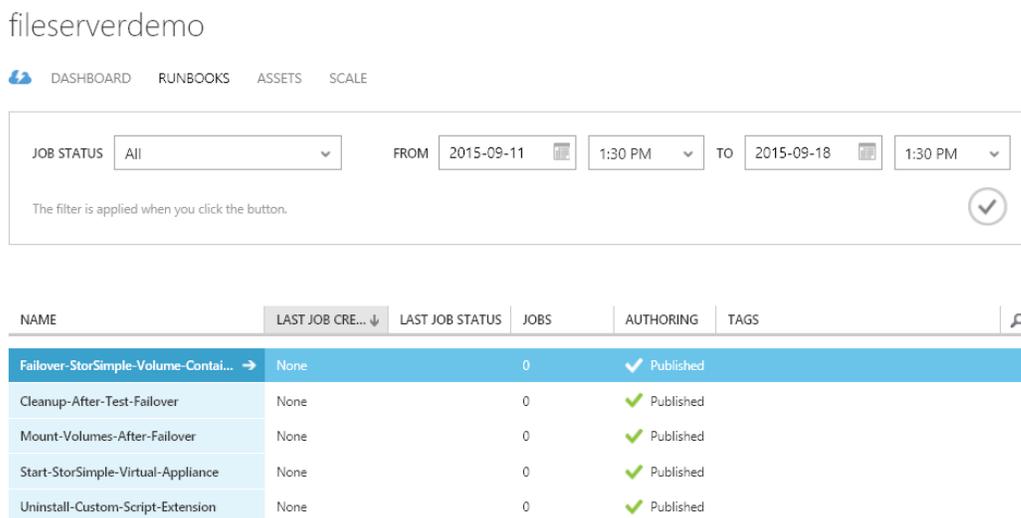
1. Go to the Azure classic portal and go to the **Automation** section.
2. Create a new automation account. Keep it in the same geo/region in which the StorSimple virtual device and storage accounts were created.
3. Click **New > App Services > Automation > Runbook > From Gallery** to import all the required runbooks into the automation account.



4. Add the following runbooks from the **Disaster Recovery** pane in the gallery:
  - Fail over StorSimple volume containers
  - Cleanup of StorSimple volumes after Test Failover (TFO)
  - Mount volumes on StorSimple device after failover
  - Start StorSimple Virtual Appliance
  - Uninstall custom script extension in Azure VM



5. Publish all the scripts by selecting the runbook in the automation account and going to **Author** tab. After this step, the **Runbooks** tab will appear as follows:



6. In the automation account go to the **Assets** tab, click **Add Setting > Add Credential**, and add the Azure credential.

Use the Windows PowerShell Credential. This should be a credential that contains an Org ID user name and password with access to this Azure subscription and with multi-factor authentication disabled. This is required to authenticate on behalf of the user during the failovers and to bring up the file server volumes on the DR site.

7. In the automation account, select the **Assets** tab and then click **Add Setting > Add variable** and add the following variables. You can choose to encrypt these assets. These variables are recovery plan-specific. If your recovery plan (which you will create in the next step) name is TestPlan, then your variables should be TestPlan-StorSimRegKey, TestPlan-AzureSubscriptionName, and so on.
- *RecoveryPlanName-StorSimRegKey*: The registration key for the StorSimple Manager service.
  - *RecoveryPlanName-AzureSubscriptionName*: The name of the Azure subscription.
  - *RecoveryPlanName-ResourceName*: The name of the StorSimple resource that has the StorSimple device.
  - *RecoveryPlanName-DeviceName*: The device that has to be failed over.
  - *RecoveryPlanName-TargetDeviceName*: The device on which the containers are to be failed over.
  - *RecoveryPlanName-VolumeContainers*: A comma-separated string of volume containers present on the device that need to be failed over; for example, volcon1,volcon2, volcon3.
  - *RecoveryPlanName-TargetDeviceDnsName*: The service name of the target device (this can be found in the **Virtual Machine** section: the service name is the same as the DNS name).
  - *RecoveryPlanName-StorageAccountName*: The storage account name in which the script (which has to run on the failed over VM) will be stored. This can be any storage account that has some space to store the script temporarily.
  - *RecoveryPlanName-StorageAccountKey*: The access key for the above storage account.
  - *RecoveryPlanName-ScriptContainer*: The name of the container in which the script will be stored in the cloud. If the container doesn't exist, it will be created.
  - *RecoveryPlanName-VMGUID*: Upon protecting a VM, Azure Site Recovery assigns every VM a unique ID that gives the details of the failed over VM. To obtain the VMGUID, select the **Recovery Services** tab and then click **Protected Item > Protection Groups > Machines > Properties**. If you have multiple VMs, then add the GUIDs as a comma-separated string.
  - *RecoveryPlanName-AutomationAccountName* – The name of the automation account in which you have added the runbooks and the assets.

For example, if the name of the recovery plan is fileServerpreedayRP, then your **Assets** tab should appear as follows after you add all the assets.

NAME	↑	TYPE	LAST I
Azure	→	Module	9/12/20
AzureCredential		Credential	9/7/20
FileserverpredayRP-AutomationAccountName	→	Variable	9/7/20
FileserverpredayRP-AzureSubscriptionName		Variable	9/7/20
FileserverpredayRP-DeviceName		Variable	9/7/20
FileserverpredayRP-DummyVMGUID		Variable	9/10/20
FileserverpredayRP-ResourceName		Variable	9/7/20
FileserverpredayRP-ScriptContainer		Variable	9/7/20
FileserverpredayRP-StorageAccountKey		Variable	9/7/20
FileserverpredayRP-StorageAccountName		Variable	9/7/20
FileserverpredayRP-StorSimRegKey		Variable	9/7/20
FileserverpredayRP-TargetDeviceDnsName		Variable	9/7/20
FileserverpredayRP-TargetDeviceName		Variable	9/7/20
FileserverpredayRP-VMGUIDS		Variable	9/7/20
FileserverpredayRP-VolumeContainers		Variable	9/7/20
Microsoft.PowerShell.Core		Module	9/12/20
Microsoft.PowerShell.Diagnostics		Module	9/12/20
Microsoft.PowerShell.Management		Module	9/12/20
Microsoft.PowerShell.Security		Module	9/12/20
Microsoft.PowerShell.Utility		Module	9/12/20
Microsoft.WSMan.Management		Module	9/12/20
Orchestrator.AssetManagement.Cmdlets		Module	9/12/20

8. Go to the **Recovery Services** section and select the Azure Site Recovery vault that you created earlier.
9. Select the **Recovery Plans** tab and create a new recovery plan as follows:
  - a. Specify a name and select the appropriate **Protection Group**.
  - b. Select the VMs from the protection group that you want to include in the recovery plan.
  - c. After the recovery plan is created, select it to open the Recovery plan customization view.
  - d. Select **All groups shutdown**, click **Script**, and choose **Add a primary side script before all Group shutdown**.
  - e. Select the automation account (in which you added the runbooks) and then select the **Fail over-StorSimple-Volume-Containers** runbook.

- f. Click **Group 1: Start**, choose **Virtual Machines**, and add the VMs that are to be protected in the recovery plan.
- g. Click **Group 1: Start**, choose **Script**, and add all the following scripts in order as **After Group 1** steps.
  - Start-StorSimple-Virtual-Appliance runbook
  - Fail over-StorSimple-volume-containers runbook
  - Mount-volumes-after-failover runbook
  - Uninstall-custom-script-extension runbook
- h. Add a manual action after the iSCSI script in the same **Group 1: Post-steps** section. This action is the point at which you can verify that everything is working correctly. This action needs to be added only as a part of test failover (so only select the **Test Failover** checkbox).
- i. After the manual action, add the Cleanup runbook using the same procedure that you used for the other runbooks. Save the recovery plan.

**NOTE:** When running a test failover, you should verify everything at the manual action step because the StorSimple volumes that had been cloned on the target device will be deleted as a part of the cleanup after the manual action is completed.

## fileserverpredayrp

### CUSTOMIZE

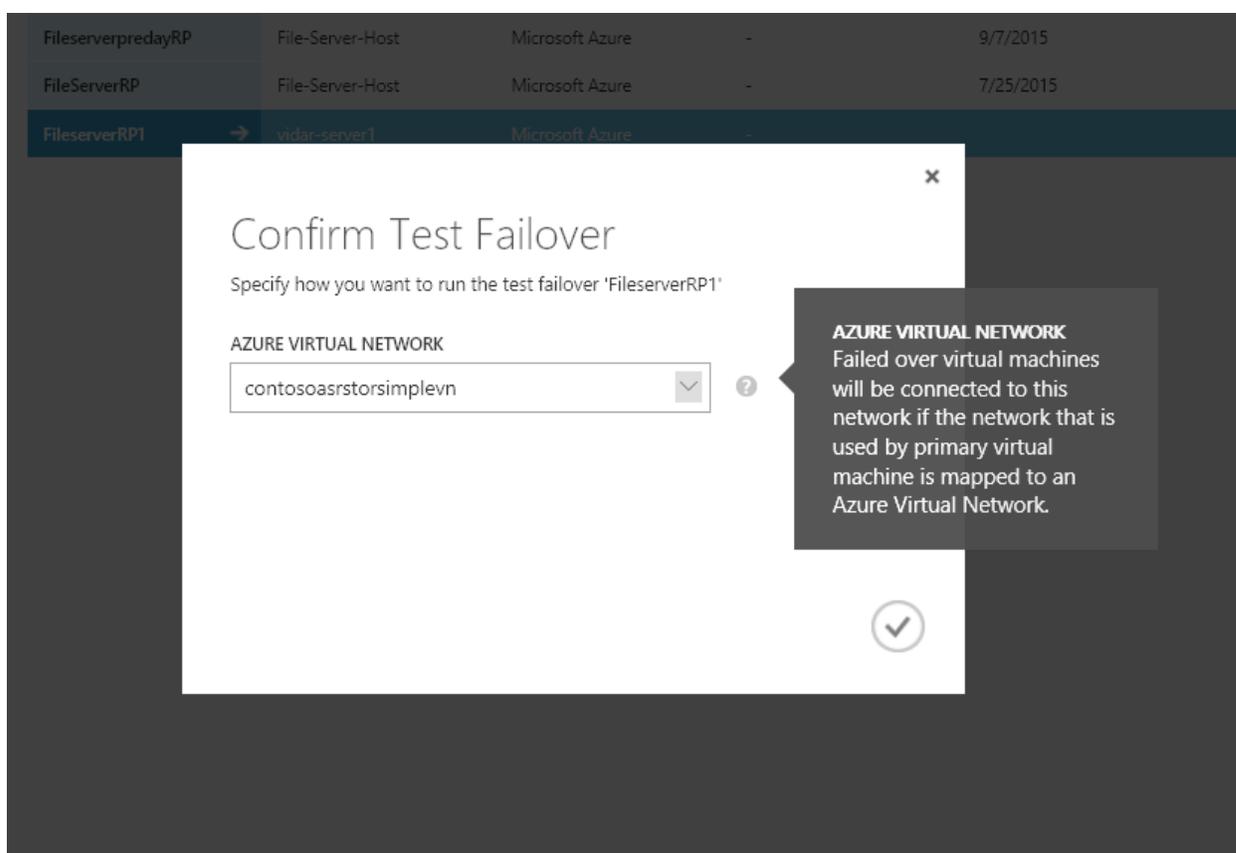
STEP	DETAILS
▲ All groups shutdown : Pre-steps Script : 'Failover-StorSimple-Volume-Containers'	1 step
▲ All groups shutdown Script : 'Start-StorSimple-Virtual-Appliance'	1 virtual machine in 1 group
▲ All groups failover Script : 'Failover-StorSimple-Volume-Containers'	1 virtual machine in 1 group
▲ Group 1 : Start Script : 'Mount-Volumes-After-Failover'	1 virtual machine
FileserverPreDay Manual action : 'TFO testing'	
▲ Group 1 : Post-steps Script : 'Uninstall-Custom-Script-Extension'	6 steps
Script : 'Failover-StorSimple-Volume-Containers'	
Script : 'Mount-Volumes-After-Failover'	
Script : 'Uninstall-Custom-Script-Extension'	
Manual action : 'TFO testing'	
Script : 'Cleanup'	

## Perform a test failover

Refer to the Active Directory DR Solution<sup>7</sup> companion guide for considerations specific to Active Directory during the test failover. The on-premises setup is not disturbed at all when the test failover occurs. The StorSimple volumes that were attached to the on-premises VM are cloned to the StorSimple virtual device on Azure. A VM for test purposes is brought up in Azure and the cloned volumes are attached to the VM.

### To perform the test failover

1. In the Azure Management Portal, select your site recovery vault.
2. Click the recovery plan created for the file server VM.
3. Click **Test Failover**.
4. Select the virtual network to start the test failover process.



5. When the secondary environment is up, you can perform your validations.
6. After the validations are complete, click **Validations Complete**. The test failover environment will be cleaned, and the TFO operation will be completed.

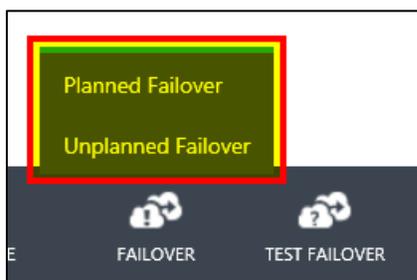
<sup>7</sup> [Automated DR solution for Active Directory and DNS using ASR](#)

## Perform an unplanned failover

During an unplanned failover, the StorSimple volumes are failed over to the virtual device, a replica VM will be brought up on Azure, and the volumes are attached to the VM.

### To perform an unplanned failover

1. In the Azure Management Portal, select your site recovery vault.
2. Click the recovery plan created for file server VM.
3. Click **Failover** and then select **Unplanned Failover**.



4. Select the target network and then click the check icon ✓ to start the failover process.

## Perform a planned failover

During a planned failover, the on-premises file server VM is shut down gracefully and a cloud backup snapshot of the volumes on StorSimple device is taken. The StorSimple volumes are failed over to the virtual device, a replica VM is brought up on Azure, and the volumes are attached to the VM.

### To perform a planned failover

1. In the Azure Management Portal, select your site recovery vault.
2. Click the recovery plan created for the file server VM.
3. Click **Failover** and then select **Planned Failover**.
4. Select the target network and then click the check icon ✓ to start the failover process.

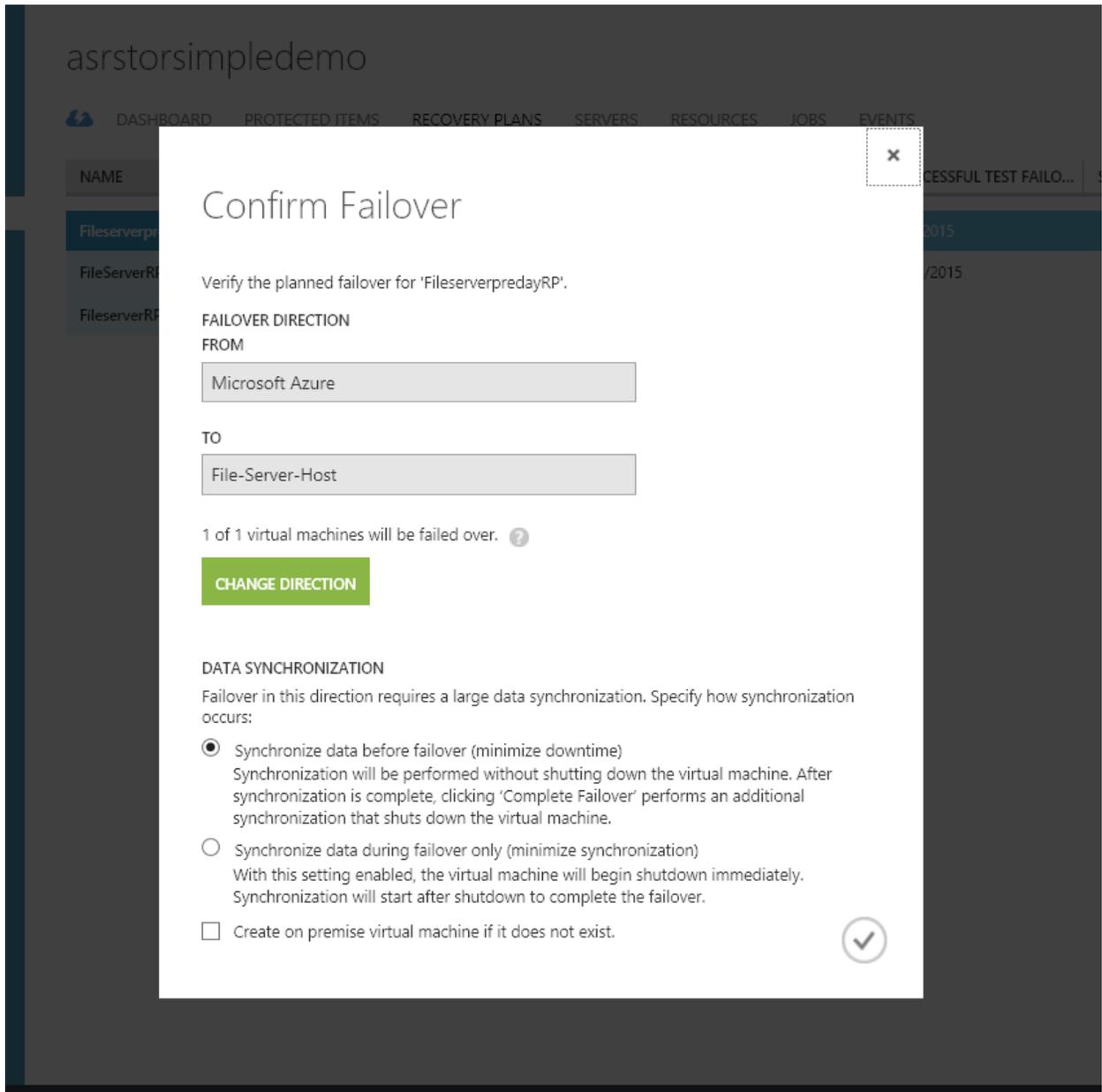
## Perform a failback

During a failback, StorSimple volume containers are failed over back to the physical device after a backup is taken.

### To perform a failback

1. In the Azure Management Portal, select your site recovery vault.
2. Click the recovery plan created for the file server VM.
3. Click **Failover** and select **Planned failover** or **Unplanned failover**.
4. Click **Change Direction**.

5. Select the appropriate data synchronization and VM creation options.
6. Click the check icon ✓ to start the failback process.



# Best Practices

## Capacity planning and readiness assessment

### Hyper-V site

Use the User Capacity planner tool<sup>8</sup> to design the server, storage, and network infrastructure for your Hyper-V replica environment.

### Azure

You can run the Azure Virtual Machine Readiness Assessment tool<sup>9</sup> on VMs to ensure that they are compatible with Azure VMs and Azure Site Recovery Services. The Readiness Assessment Tool checks VM configurations and warns when configurations are incompatible with Azure. For example, it issues a warning if a C: drive is larger than 127 GB.

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

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

## Limitations

1. Currently, only 1 StorSimple device can be failed over (to a single StorSimple virtual device). The scenario of a file server that spans several StorSimple devices is not yet supported.
2. If you get an error while enabling protection for a VM, make sure that you have disconnected the iSCSI targets.
3. All the volume containers that have been grouped together because of backup policies spanning across volume containers will be failed over together.
4. All the volumes in the volume containers you have chosen will be failed over.
5. Volumes that add up to more than 30 TB can't be failed over because the capacity of a single SVA is 30 TB.
6. If the planned/unplanned failover fails and the VMs are created in Azure, then do not clean up the VMs. Instead, do a failback. If you delete the VMs then the on-premises VMs cannot be turned on again.
7. After a failover, if you are not able to see the volumes, go to the VMs, open Disk Management, rescan the disks, and then bring them online.
8. Failover job timeout: The StorSimple script will time out if the failover of volume containers takes more time than the Azure Site Recovery limit per script (currently 20 minutes).
9. In some instances, the drive letters in the DR site might be different than the letters on-premises. If this occurs, you will need to manually correct the problem after the failover is finished.

---

<sup>8</sup> [Hyper-V Replica Capacity Planner tool](#)

<sup>9</sup> [Azure Virtual Machine Readiness Assessment tool](#)

10. Backup job timeout: The StorSimple script times out if the backup of volumes takes more time than the Azure Site Recovery limit per script (currently 10 minutes).

**RECOMMENDATION:** Run the backup manually from the Azure portal and then run the recovery plan again.

11. Clone job timeout: The StorSimple script times out if the cloning of volumes takes more time than the Azure Site Recovery limit per script (currently 10 minutes).
12. Multi-factor authentication should be disabled for the Azure credential that is entered in the automation account as an asset. If this authentication is not disabled, scripts will not be allowed to run automatically and the recovery plan will fail.
13. Time synchronization error: The StorSimple scripts errors out saying that the backups were unsuccessful even though the backup is successful in the portal. A possible cause for this might be that the StorSimple appliance's time might be out of sync with the current time in the time zone.

**RECOMMENDATION:** Sync the appliance time with the current time in the time zone.

14. Appliance failover: The StorSimple script might fail if there is an appliance failover when the recovery plan is running.

**RECOMMENDATION:** Rerun the recovery plan after the appliance failover is complete.

## Summary

Using Azure Site Recovery, you can create a complete automated disaster recovery plan for a file server VM having file shares hosted on StorSimple storage. You can initiate the failover within seconds from anywhere in the event of a disruption and get the application up and running in a few minutes.