1200 XP

Protect your Azure infrastructure with Azure Site Recovery

59 min • Module • 9 Units

V V V V W 4.6 (189) Rate it

Intermediate Solutions Architect Azure

Provide disaster recovery for your Azure infrastructure by managing and orchestrating replication, failover, and failback of Azure virtual machines with Azure Site Recovery.

In this module, you will:

Protect Azure virtual machines with Azure Site Recovery
Run a disaster recovery drill to validate protection
Failover and failback your virtual machines

- Basic understanding of Azure virtual machines
- Basic understanding of Azure virtual networking

This module is part of these learning paths
Architect migration, business continuity, and disaster recovery in Azure

100 XP

Introduction

2 minutes

Natural or human-made disasters may affect the continuity of your organization's cloud infrastructure. Planning for disaster and making sure recovery and business continuity plans are in place to deal with such an event is key to any organization's longevity.

Azure Site Recovery provides disaster recovery for Azure infrastructure by managing and orchestrating replication, failover, and failback of Azure virtual machines.

Assume you're working at a medical care organization with multiple facilities across the country. Your organization has recently suffered an outage because of building damage in your datacenter from a hurricane. You want to move this infrastructure to Azure and take advantage of the replication and recovery features available in Azure. You have several virtual machines running in Azure already, and now wish to configure protection for them to fail over to a secondary Azure region if there's a disaster.

In this module, you'll learn about **Azure Site Recovery** and explore the features applicable to a business continuity and disaster recovery (BCDR) plan.

Learning objectives

In this module, you'll:

- Protect Azure virtual machines with Azure Site Recovery
- Run a disaster recovery drill to validate protection
- Failover and failback your virtual machines

Prerequisites

- Basic understanding of Azure virtual machines
- Basic understanding of Azure virtual networking

> **Note**
>
> For this module, you will need use your own subscription to complete the optional exercises. This can be a free trial subscription, or a subscription that you already have access to.

Next unit: What is Azure Site Recovery

Continue

100 XP

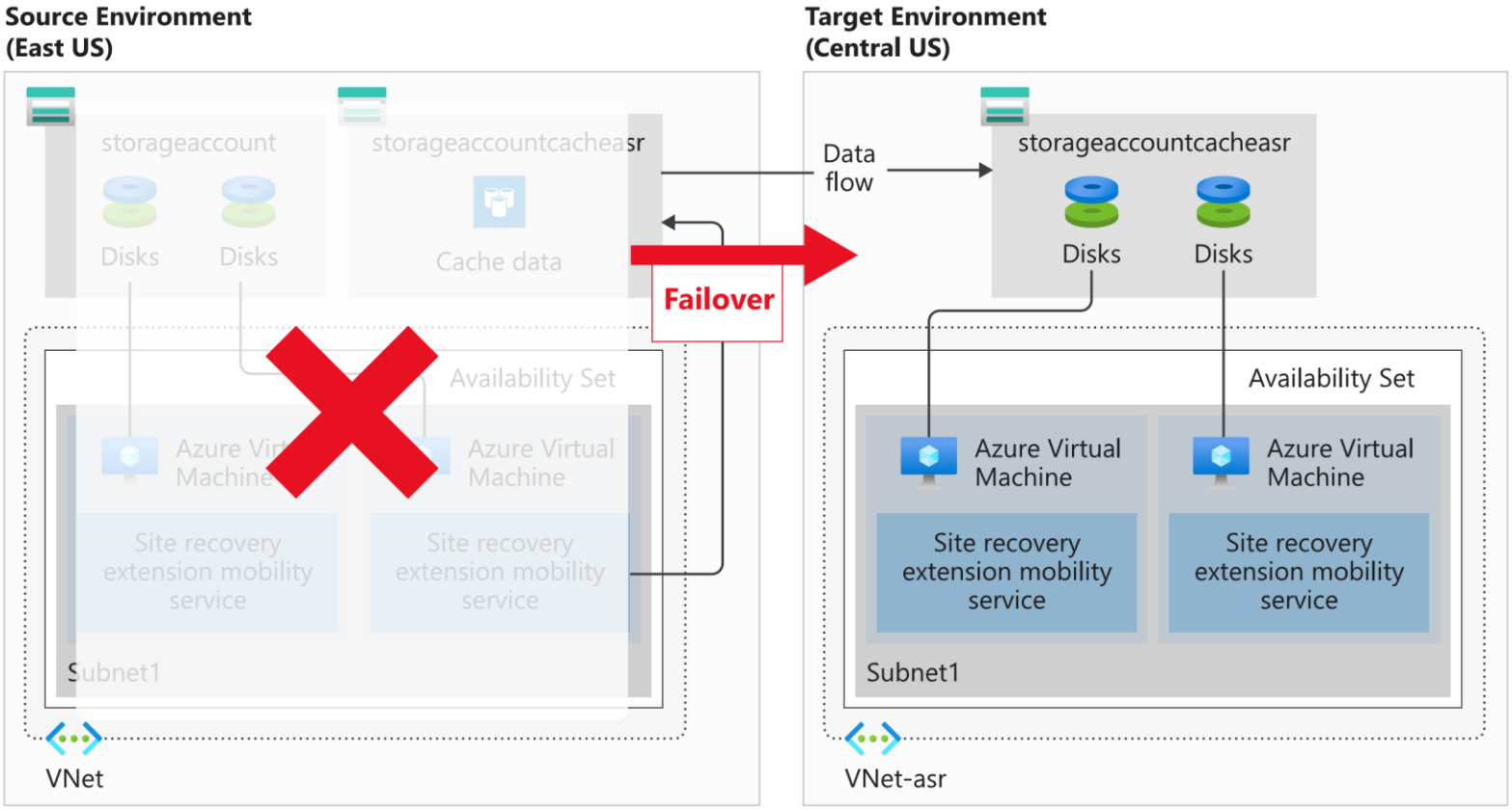
What is Azure Site Recovery

4 minutes

Azure Site Recovery replicates your virtual machine workloads between Azure regions. You can also use Site Recovery to migrate VMs from other environments, such as on-premises infrastructure, to Azure. You'll see that Site Recovery does much more than just backing up and restoring infrastructure.

Let's assume your organization recently suffered an outage caused by a hurricane. Here, we'll learn about the Azure Site Recovery features that help handle future interruptions. We'll also identify the Site Recovery features required to protect your Azure virtual machines (VMs) by enabling failing over to a secondary Azure region.

Site Recovery features



Site Recovery manages the orchestration of disaster recovery in Azure. It's designed to replicate workloads from a primary site or region, to a secondary site. If the primary site has an issue, Site Recovery can replicate protected VMs to another Azure region.

Site Recovery manages the replication of Azure VMs between regions, or the replication of on-premises VMs to Azure and back again. Because it's built natively into Azure, Site Recovery can run seamless tests (disaster recovery drills) without affecting production workloads.

Azure virtual machine protection

Site Recovery protects your VM instances in Azure automatically. Site Recovery mirrors the source VM configuration and creates required or associated resource groups, storage accounts, virtual networks, and availability sets to a secondary Azure region. The resources created are appended with a Site Recovery suffix.

Snapshots and recovery points

Site Recovery has customizable replication policies that allow you to define the retention history of recovery points and the frequency of snapshots. You create a recovery point from a snapshot of a VMs' disk. The two types of snapshots available are **App-consistent** and **Crash-consistent**.

- **Crash-consistent** recovery represents the data on-disk at the time the snapshot is taken. The default for capturing snapshots is every five minutes.

- **App-consistent** recovery captures the same data as crash-consistent but also includes all in-memory data and in-process transactions. Including the in-memory data means Site Recovery can restore a VM and any running apps without any data loss. The default for capturing snapshots is every 60 minutes.

All recovery points are kept for 24 hours by default, although you can extend this period to 72 hours.

Replication to a secondary region

Installing the Site Recovery mobility service happens when you enable replication for an Azure VM. The installed extension registers the VM with Site Recovery. Continuous replication of the VM then begins, with any writes to the disk immediately transferred to a local storage account. Site Recovery uses this account, replicating the cache to a storage account in the destination environment.

Site Recovery copies data stored in the cache and syncs it with either the target storage account or replicated managed disks. After the data is processed, crash-consistent recovery points are created. If app-consistent recovery points are enabled, they'll be generated on a schedule as set in the Site Recovery replication policy.

Site Recovery can use accelerated networking for Azure virtual machines, reducing jitter, and reduce CPU usage.

Disaster recovery (DR) drills

Site Recovery allows you to do disaster recovery drills after all the pre-requisite configuration tasks are complete. Running a DR drill enables you to validate the replication strategy for your environment without losing data, having downtime, or compromising your production environment. Drills don't affect your production environment and are a way to test that you have correctly configured everything.

Flexible failover and failback

Site Recovery failover and failback can be quickly started using the Azure portal. When running a failover, you select a recovery point, then let Site Recovery take care of the failover. Failback is simply a reverse of this process. When a failover is successfully committed, it's available to failback.

Next unit: Prepare for disaster recovery with Azure Site Recovery

Continue

200 XP

Prepare for disaster recovery with Azure Site Recovery

9 minutes

In the previous unit, we explore the capabilities of Azure Site Recovery. Our next step is to prepare for disaster recovery in our Azure environment.

Using our organization's business continuity and disaster recovery (BCDR) plan, we can run through the Azure Site Recovery configurations and set a preparation plan in motion that fits with our organization's BCDR goals. Let's assume we're using the East US Azure region for our existing solution, and we've decided to use the West US region for replication.

Here, we'll explore how to take advantage of Azure Site Recovery's automated features to prepare for a disaster recovery scenario.

Environment setup

We need to set up our environment for our later exercises. As this setup takes a few minutes to complete, we'll start the process now, and then we can work through some of the theory while the configuration completes in the background.

> **Note**
>
> If you want to complete the following set up, but you don't have an Azure subscription, or prefer not to use your account, you will need to create a free account before you begin.

Let's assume, we have two VMs configured in the organization. We'll configure the following services in the East US region to simulate this configured VMs.

- A virtual network
- Two VMs
- A storage account

We'll also configure a resource group in West US. We'll later configure Azure Site Recovery to use the West US region as our target environment.

Our first step is to create our exercise environment. We'll run a script that creates our companies infrastructure in Azure. Once the script completes, we'll have a virtual network, two VMs, and a storage account that we'll use for our Recovery Services Vault.

1. Sign in to the Azure portal with your credentials, and start a Cloud Shell session.
2. Make sure you're running a Bash session in Cloud Shell.
3. Copy the Azure Resource Manager JSON templates to create your company's infrastructure.

```bash
curl https://raw.githubusercontent.com/MicrosoftDocs/mslearn-protect-infrastructure-with-azure-site-recovery/master/deploy.json > deploy.json
```

4. Run the following command to create resource groups and the company's infrastructure.

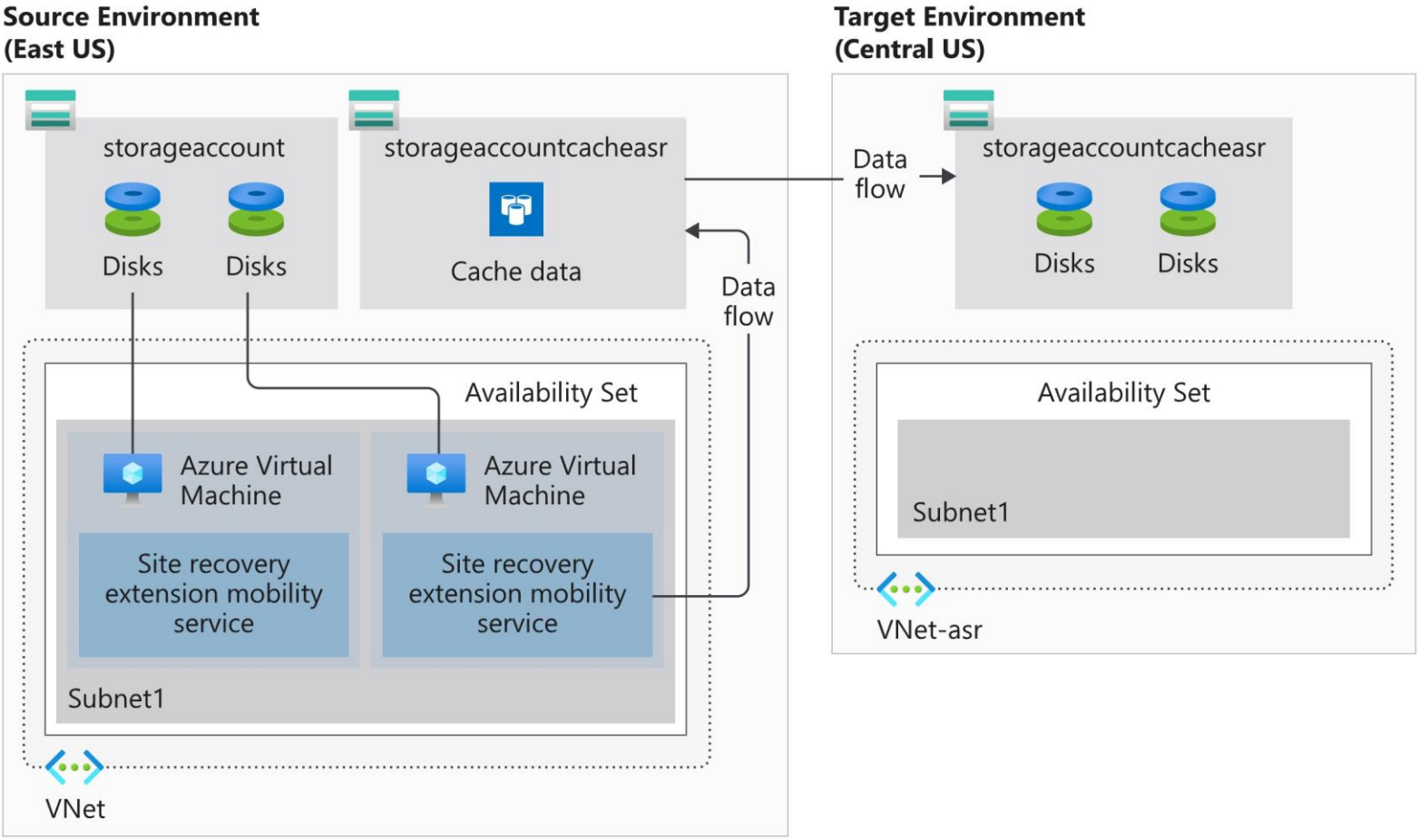
```bash
az group create --name west-coast-rg --location westus2
az group create --name east-coast-rg --location eastus2

az group deployment create \
    --name asrDeployment \
    --template-file deploy.json \
    --parameters storageAccounts_asrcache_name=asrcach$RANDOM \
    --resource-group west-coast-rg
```

Keep in mind that configuring the environment can take up to five minutes to complete. We're now ready to continue with the rest of this unit while the deployment completes.

Disaster recovery preparation with Azure Site Recovery

Azure Site Recovery will manage and orchestrate our DR process for Azure VMs or on-premises machines. However, to enable it, there are several components we need to configure. We'll need to:

- Add a Recovery Services Vault
- Organize target resources
- Configure outbound network connectivity
- Set up replication on existing VMs



What is a Recovery Services vault?

A Recovery Services vault enables Azure Site Recovery to complete disaster recovery replication. These vaults use storage accounts to store data backups, VM configuration settings, and workloads. To meet Azure Site Recovery requirements, provision a recovery services vault using the portal or the Azure CLI.

What are the target resources?

Target resources are all the Azure services that are created once our existing resources replicate. In our scenario, the West US region is the region where all our target resources get created. There are a few considerations to keep in mind when selecting the target resources region.

- The target resources for Azure Site Recovery replication have to be in a different Azure region.
- The storage account that stores the backed-up data must also be in a different region to the resources being protected.
- The target region allows the creation of virtual machines and has enough resources to match the size of the existing VMs.

Configure Outbound network connectivity & URLs

Azure Site Recovery requires outbound connectivity on the virtual machines that we wish to replicate.

The required network connectivity is set up for us automatically when using Virtual Machines created in Azure. However, when we migrate on-premises VMs to Azure, we may need to update your network connectivity.

Azure Site Recovery doesn't support controlling network connectivity via an authentication proxy. If our organization is using a URL-based firewall proxy to restrict outbound connectivity, we'll need to add access to several URLs.

URL	Description
login.microsoftonline.com	For the Azure Site Recovery URLs to authenticate

URL	Description
*.blob.core.windows.net	To write VM data to the source storage account cache
*.hypervrecoverymanager.windowsazure.com	For Azure Site Recovery to communicate with the VM
*.servicebus.windows.net	For Azure Site Recovery monitoring and diagnostic data from the VM

If you prefer to control the connectivity using IP addresses instead, then you need to add the IP address ranges for:

- The Azure Datacenters
- The Azure Site Recovery endpoints

Update Azure VM root certificates

Every Azure VM we wish to replicate has to register with Azure Site Recovery. For a VM to register, Azure Site Recovery requires the latest root certificates installed on the VM. On a Windows VM, we'll need to make sure we install all the latest windows updates. The process for updating root certificates on Linux VM varies from distribution to distribution. We'll need to follow the guidance published by the distributor.

Configure Account permissions

Azure Site Recovery uses Role-Based Access Control (RBAC) in Azure by default. RBAC enables fine-grained access control and allows us to use several built-in Azure Site Recovery roles:

Role	Description
Site Recovery Contributor:	A contributor has full permissions for Azure Site Recovery operations in a recovery services vault, suitable for disaster recovery admins.
Site Recovery Operator:	An operator has Permissions to run and administer Azure Site Recovery failover and failback operations, suitable for disaster recovery operators.
Site Recovery Reader:	A Reader has permissions to view Azure Site Recovery operations, suitable for IT monitoring executives.

To enable replication on a VM, a user must have permission to create a VM in both the virtual network and resource group.

What is Azure Mobility Service?

Every VM that is to be replicated needs the Azure Mobility Service to be installed. This client is available for Windows and Linux VMs and will be installed and configured automatically by Site Recovery. If the automatic installation fails, you can install the service manually.

The mobility service works in partnership with Azure Site Recovery to keep an up-to-date cache of the VMs' data. The cache is replicated to the target environment's storage account. The replicated data will be used if Azure Site Recovery fails over the environment.

Check your knowledge

1. How are storage accounts used by Site Recovery to store data backups?

- [?] Site Recovery creates recovery services vaults.

  Recovery services vaults are used to store backup data, VM configuration settings, and workloads.

- [?] Site Recovery creates docker containers using storage accounts.
- [?] Site Recovery creates and stores managed disks.

2. Which four ways does Site Recovery protect virtual machine infrastructure?

- [?] Implements an organizations BCDR, enables automatic failover and recovery, failed over machines are automatically protected, automatically manages backup storage
- [?] Creates snapshots and recovery points, replicates VMs to a secondary region, supports DR drills, and enables flexible failover / failback

These are the four main features of Site Recovery that will protect your virtual machines.

- Backs up VM disks locally and to a different region, automatically manages backup storage, creates a Microsoft Azure Backup Server (MABS), mirrors workloads between primary and secondary regions

---

Next unit: Exercise - Set up disaster recovery with Azure Site Recovery

Continue

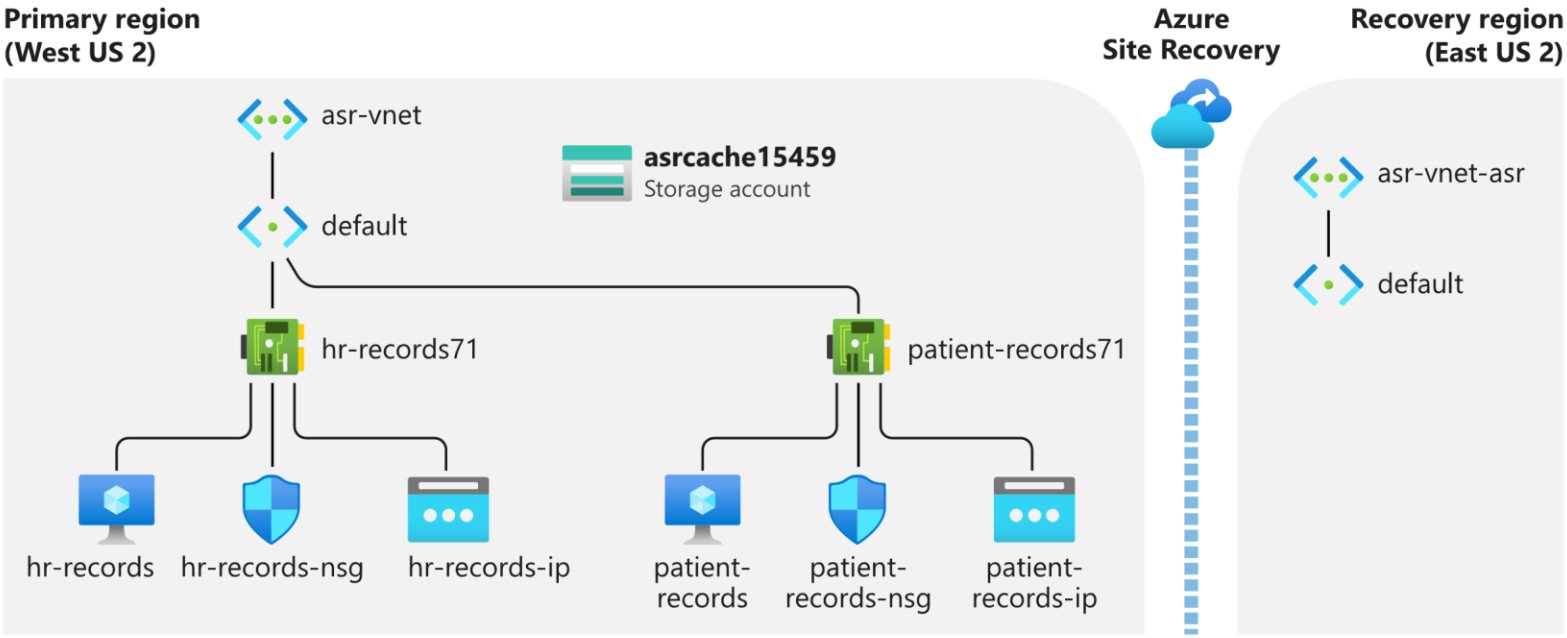
100 XP

Exercise - Set up disaster recovery with Azure Site Recovery

10 minutes

Azure Site Recovery automates the setup of recovery from one region to another. The setup process will install the Mobility Service on to the VMs, create the required infrastructure in the recovery region, and give us a way to monitor the progress.

We currently have two virtual machines running the companies patient and employee systems. These systems are running in the West US region. You've been asked to protect the infrastructure by enabling it to be recovered to the East US region. Using Azure Site Recovery, you'll enable a Recovery Services vault to replicate the current workloads.



In this exercise, we'll complete the setup of Azure Site Recovery using the portal.

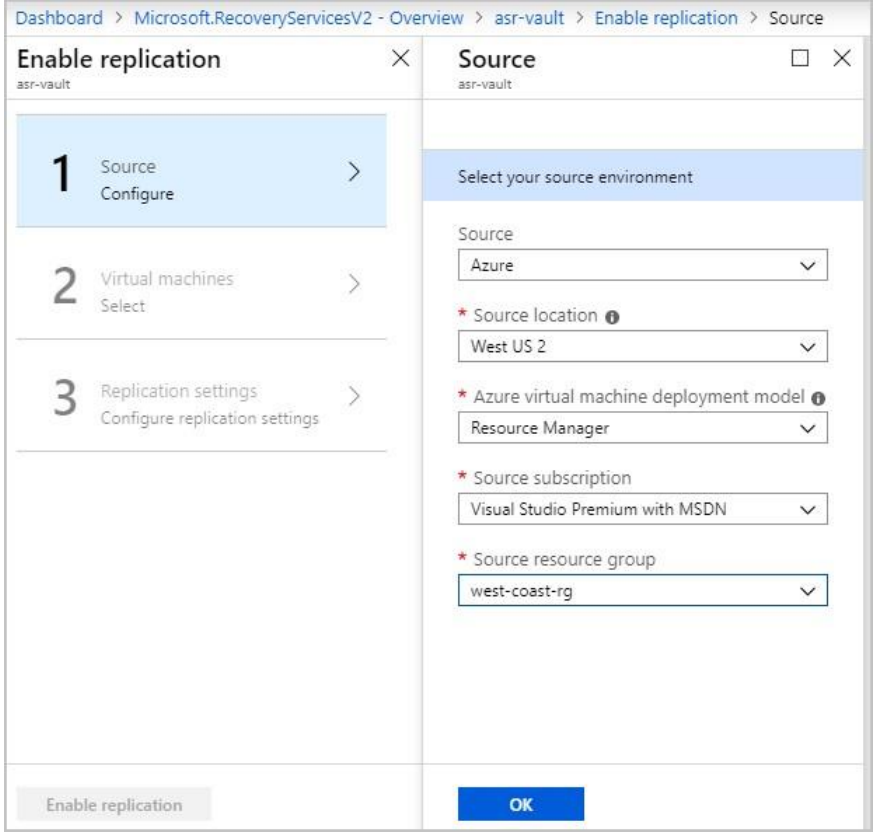
> **Note**
>
> This exercise is optional. If you don't have an Azure account, you can read through the instructions to understand how to use backup virtual machines with Azure Backup. If you want to complete this exercise, but you don't have an Azure subscription, or prefer not to use your account, you will need to create a free account before you begin.

Create a recovery services vault

1. Sign into the Azure portal with your own credentials.
2. Select **+ Create a resource** option on the top-left hand side of the portal.
3. Under the **Azure Marketplace**, select **IT & Management Tools**, then select **Backup and Site Recovery**.
4. Select **east-coast-rg** for the **Resource Group**.
5. Set the **Vault name** to **asr-vault**.
6. Set the **Region** to **East US 2**.
7. Select. **Review + create**, and then on the Summary page, select **Create**.
8. Once deployed, view the resource.

Enable replication

1. In the Recovery Services vault pane, select **+ Replicate**.



2. Select **Azure** as your source in the pane that opens.

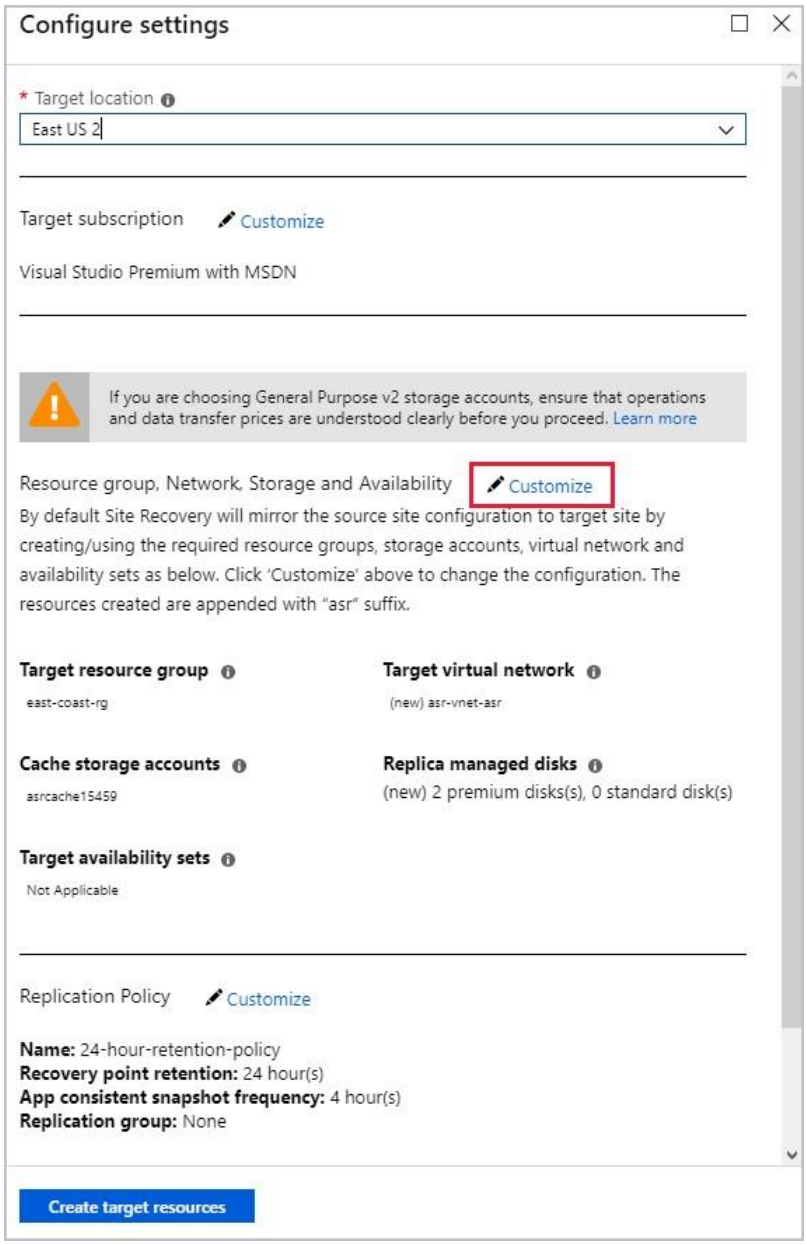
3. Select **West US 2** in the source location to select the original location.

4. Select **west-coast-rg** in the **Source resource group**.

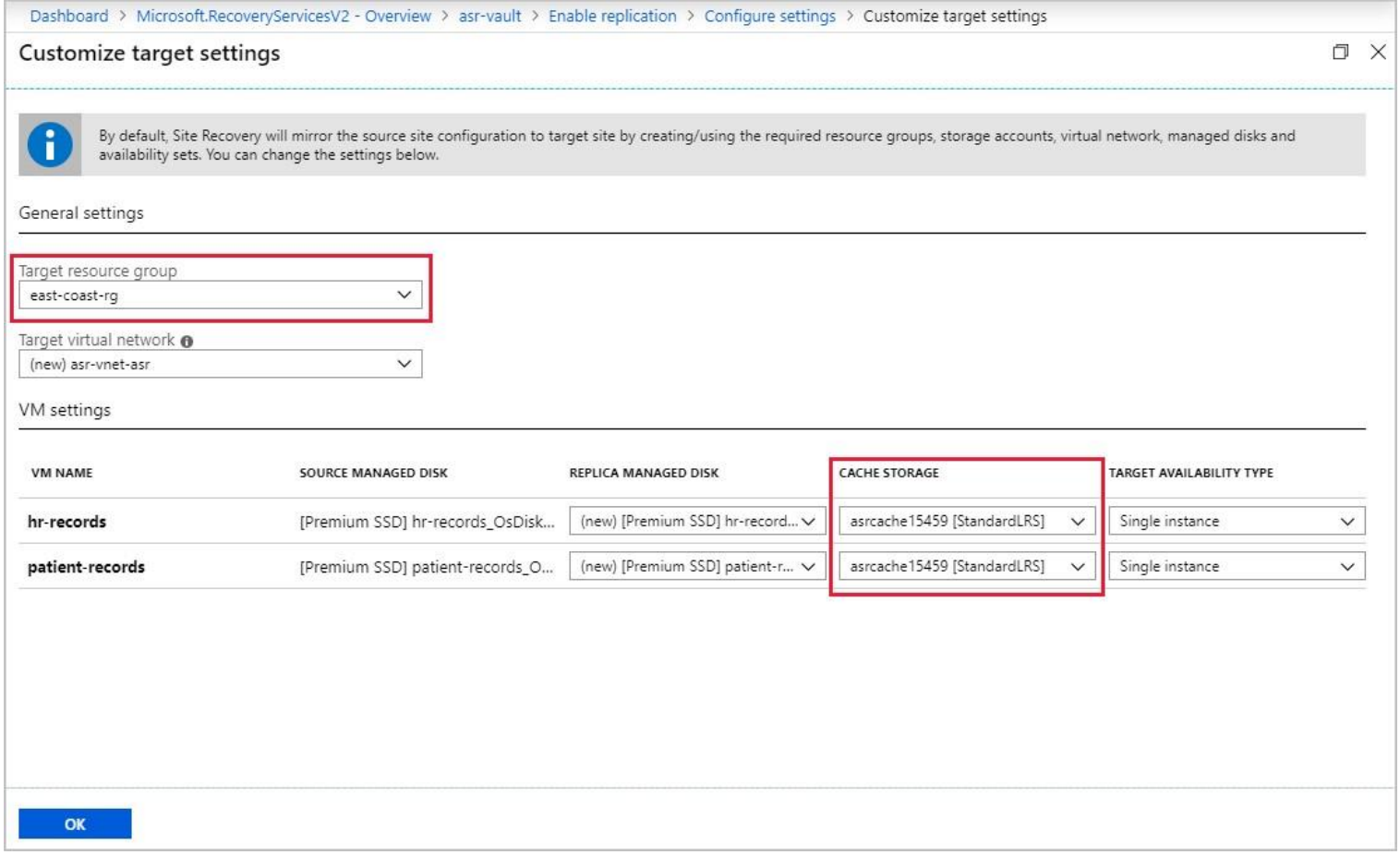
5. Select **OK** at the bottom of the pane.

6. On the **Select virtual machines** pane, select both virtual machines.

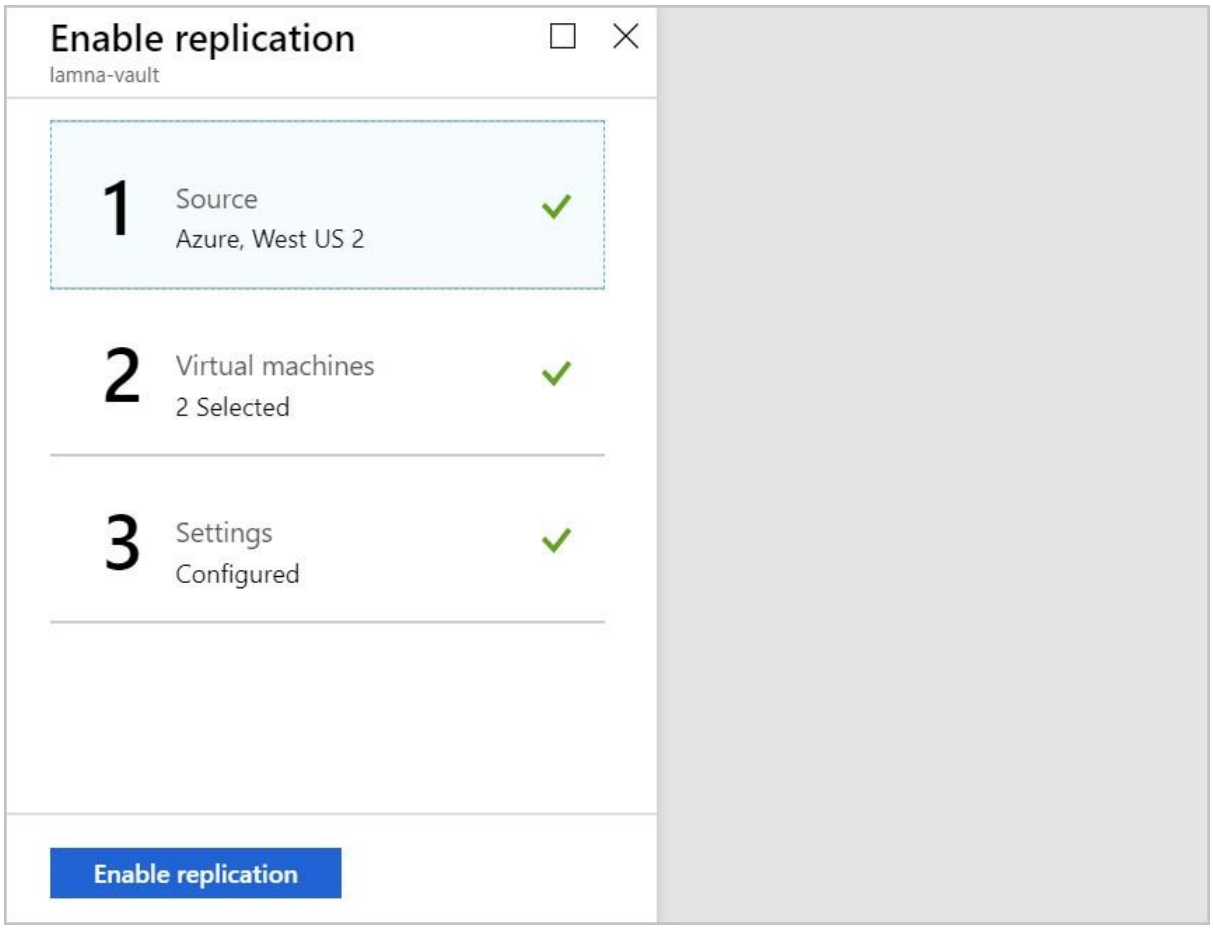
7. Select **OK**.



8. Select **Customize**.



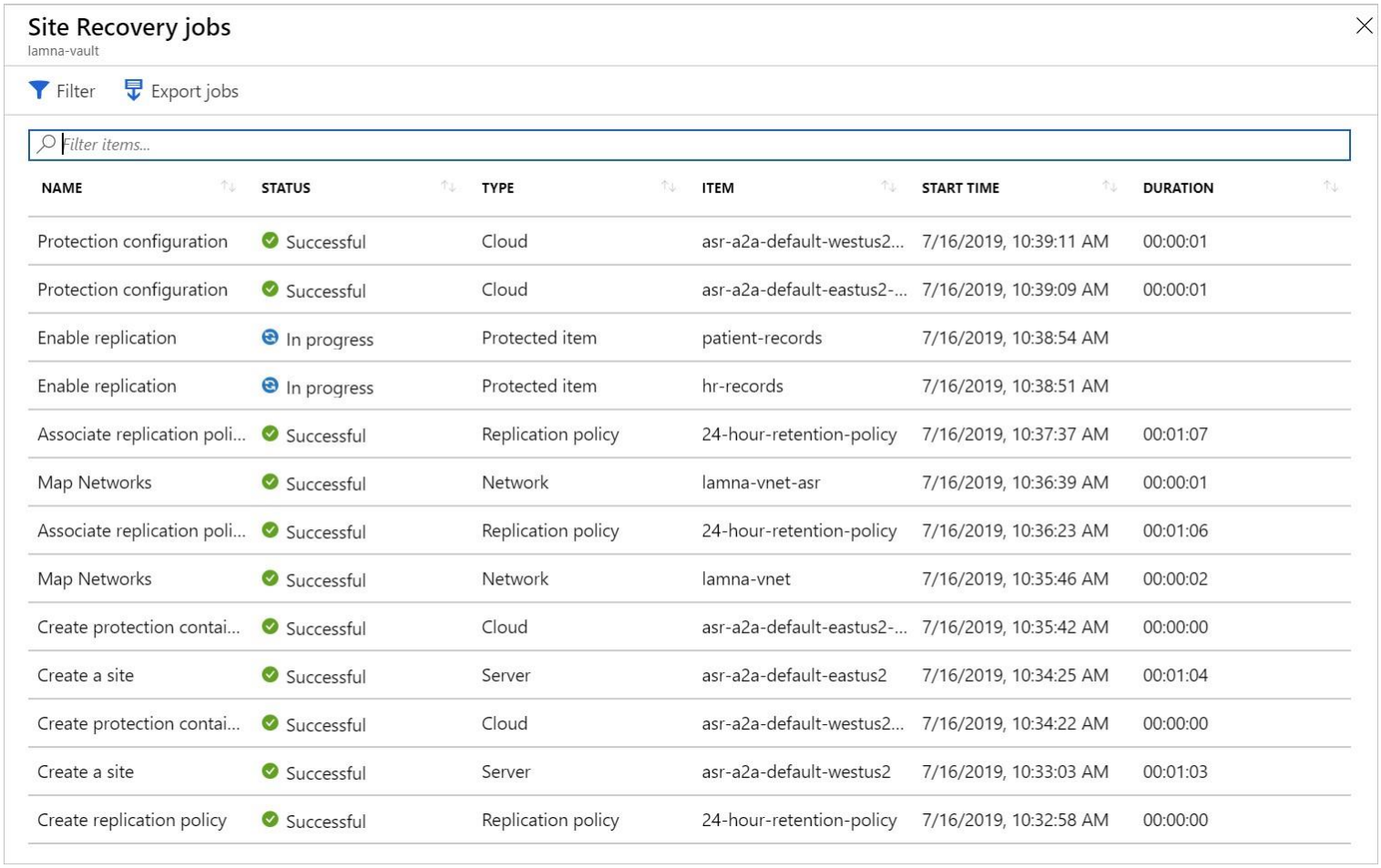
9. In the **Target resource group** change it to **east-coast-rg**
10. For each VM, change the cache storage to **asrcacheXXXX**, where **XXXX** is a random number.
11. Select **OK**.
12. Select **Create target resources**. Wait for the target resources to be created.



13. Once the resources have been created, you can select **Enable replication**. This step can take up to 15 minutes. Continue to the next steps to monitor the progress.

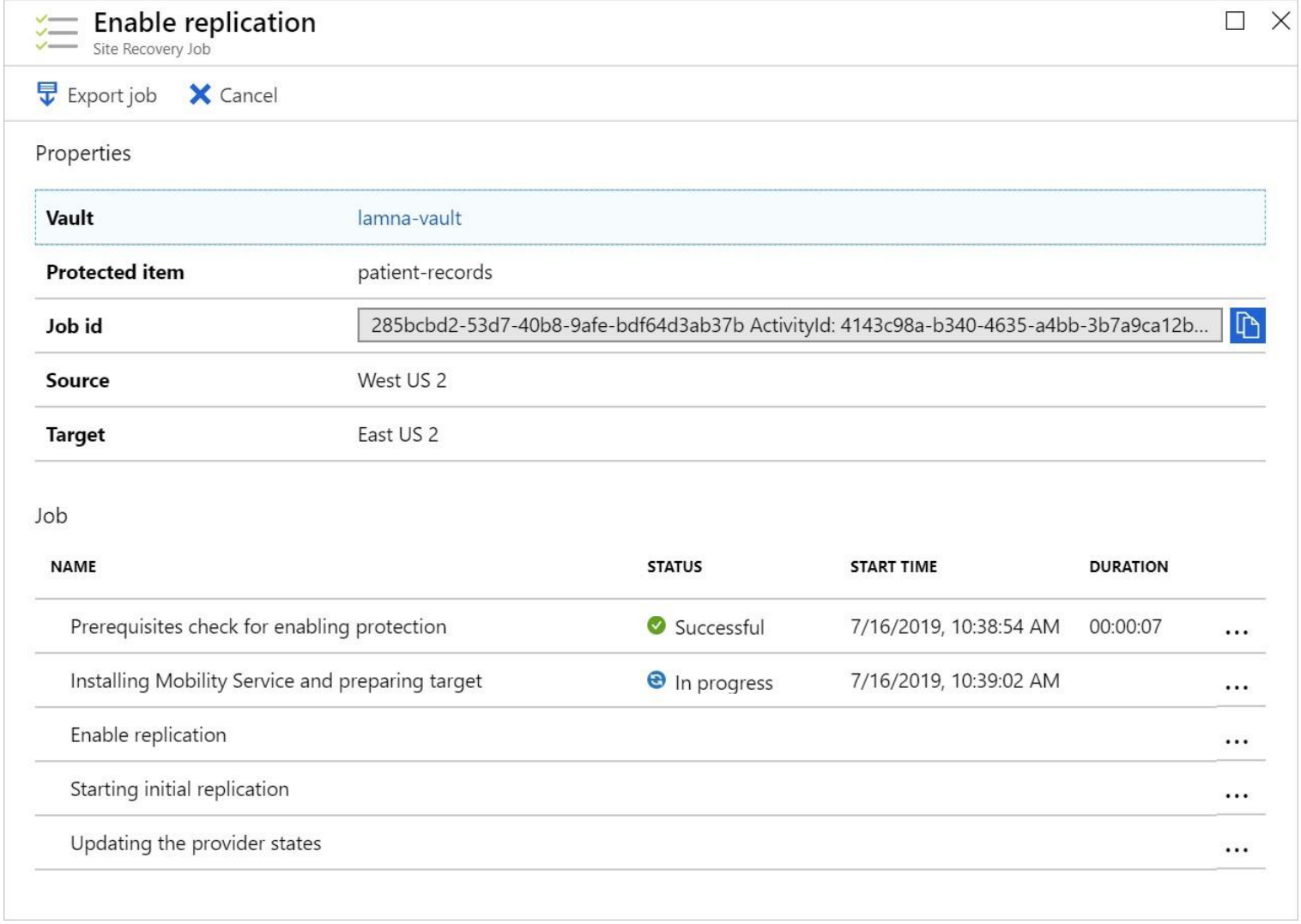
Monitor replication progress

1. Select **Home** on the top breadcrumb menu of the page to return to the portal's home page.
2. Select **All resources**.
3. In the list of resources, select the **Recovery Services vault** named **asr-vault**
4. On the left under **Monitoring**, select **Site Recovery jobs**.
5. In the jobs list, select the **In progress** link to view how the replication setup is progressing.



NAME	STATUS	TYPE	ITEM	START TIME	DURATION
Protection configuration	Successful	Cloud	asr-a2a-default-westus2...	7/16/2019, 10:39:11 AM	00:00:01
Protection configuration	Successful	Cloud	asr-a2a-default-eastus2-...	7/16/2019, 10:39:09 AM	00:00:01
Enable replication	In progress	Protected item	patient-records	7/16/2019, 10:38:54 AM	
Enable replication	In progress	Protected item	hr-records	7/16/2019, 10:38:51 AM	
Associate replication poli...	Successful	Replication policy	24-hour-retention-policy	7/16/2019, 10:37:37 AM	00:01:07
Map Networks	Successful	Network	lamna-vnet-asr	7/16/2019, 10:36:39 AM	00:00:01
Associate replication poli...	Successful	Replication policy	24-hour-retention-policy	7/16/2019, 10:36:23 AM	00:01:06
Map Networks	Successful	Network	lamna-vnet	7/16/2019, 10:35:46 AM	00:00:02
Create protection contai...	Successful	Cloud	asr-a2a-default-eastus2-...	7/16/2019, 10:35:42 AM	00:00:00
Create a site	Successful	Server	asr-a2a-default-eastus2	7/16/2019, 10:34:25 AM	00:01:04
Create protection contai...	Successful	Cloud	asr-a2a-default-westus2...	7/16/2019, 10:34:22 AM	00:00:00
Create a site	Successful	Server	asr-a2a-default-westus2	7/16/2019, 10:33:03 AM	00:01:03
Create replication policy	Successful	Replication policy	24-hour-retention-policy	7/16/2019, 10:32:58 AM	00:00:00

6. You can select any of the listed jobs to view more details.



Two of these jobs will take the most time to complete. If you select either of the **Enable replication** jobs, you'll see that the **Installing Mobility Service and preparing target** step can take between five to 10 minutes to finish.

Next unit: Run a disaster recovery drill

Continue

Run a disaster recovery drill

6 minutes

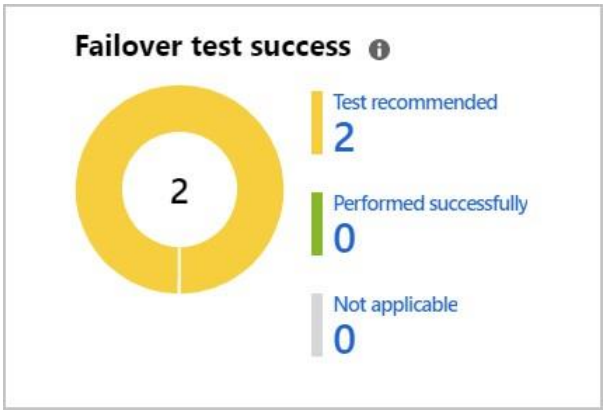
We use Disaster recovery (DR) drills test our organization's ability to recover from an outage, without impacting any production service.

We finished setting up Azure Site Recovery, and now need to test our infrastructure replication. The way we test our configuration is to run a disaster recovery drill. Azure Site Recovery allows us to do these drills in a safe manner that won't impact our production environment. We'll run some quality assurance on the configuration to ensure our DR solution is working.

Here, we'll learn about Azure Site Recovery disaster drills. What we need to consider, and how to run a test to check the configuration is correct.

What is a disaster recovery drill?

A disaster recovery (DR) drill is a way to check if we configured our solution correctly. The drill should give us, and our company, confidence that our data and services are available even if a disaster hits. Typically organizations set a recovery time objective (RTO) that indicates how long it takes to recover infrastructure. Alongside the RTO, our company should define a recovery point objective (RPO). The RPO defines the amount of data loss that is acceptable as a function of time. For example, if our company's RPO is a day, we'll need to create at least a backup of all our data each day. We'll also need to make sure it takes less than a day to restore this backup.



To ensure that we run our DR tests, Azure Site Recovery actively prompts us to run them on the Site Recovery dashboard.

Why should you run a DR drill?

A DR drill is vital to ensure the solution implemented meets the business continuity and disaster recovery (BCDR) requirements, and to check the replication works appropriately. Our DR drill, combined with RTO and RPO, needs to be tested thoroughly to ensure replication, failover, and recovery happen in the required timeframe.

For example, assume our RTO is an hour, and RPO is six hours. Our systems backed up every hour, that's an hour of lost data plus the additional hour to recover our systems.

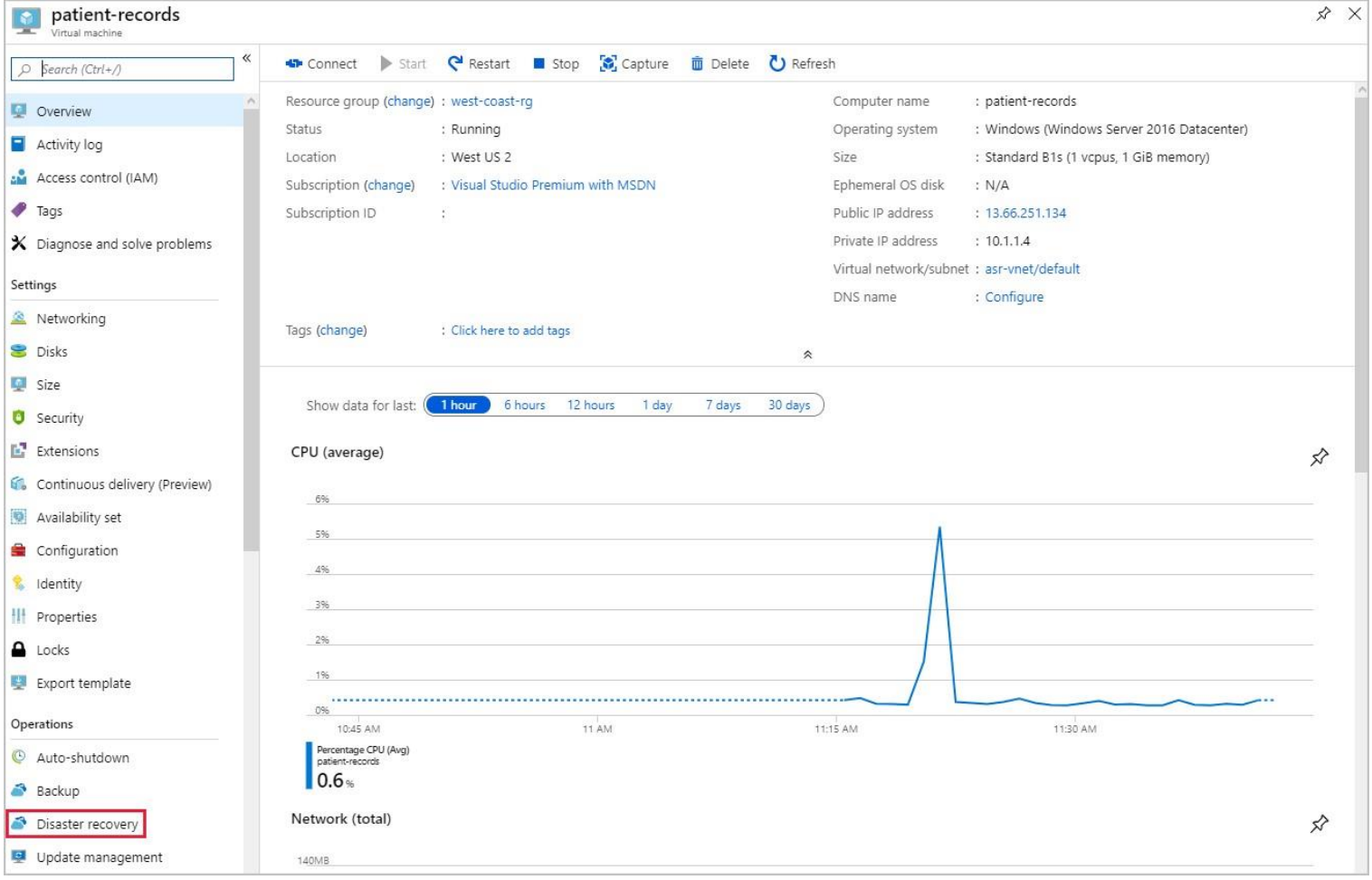
Imagine our actual recovery time is five hours. Our systems are now close to being over six hours out of date, which means we'll be in breach of the BCDR RPO objective. Testing the actual time it takes to recover from failures can give us confidence that our systems follow our BCDR plans.

Test failover of individual machines

A test failover allows you to simulate a disaster and see its effects. Failover tests can be started from the Site Recovery dashboard, or directly from the disaster recovery menu on a specific VM. We'll start by choosing a recovery point. We can choose from either the last processed, the latest app-consistent point, or a custom recovery point.

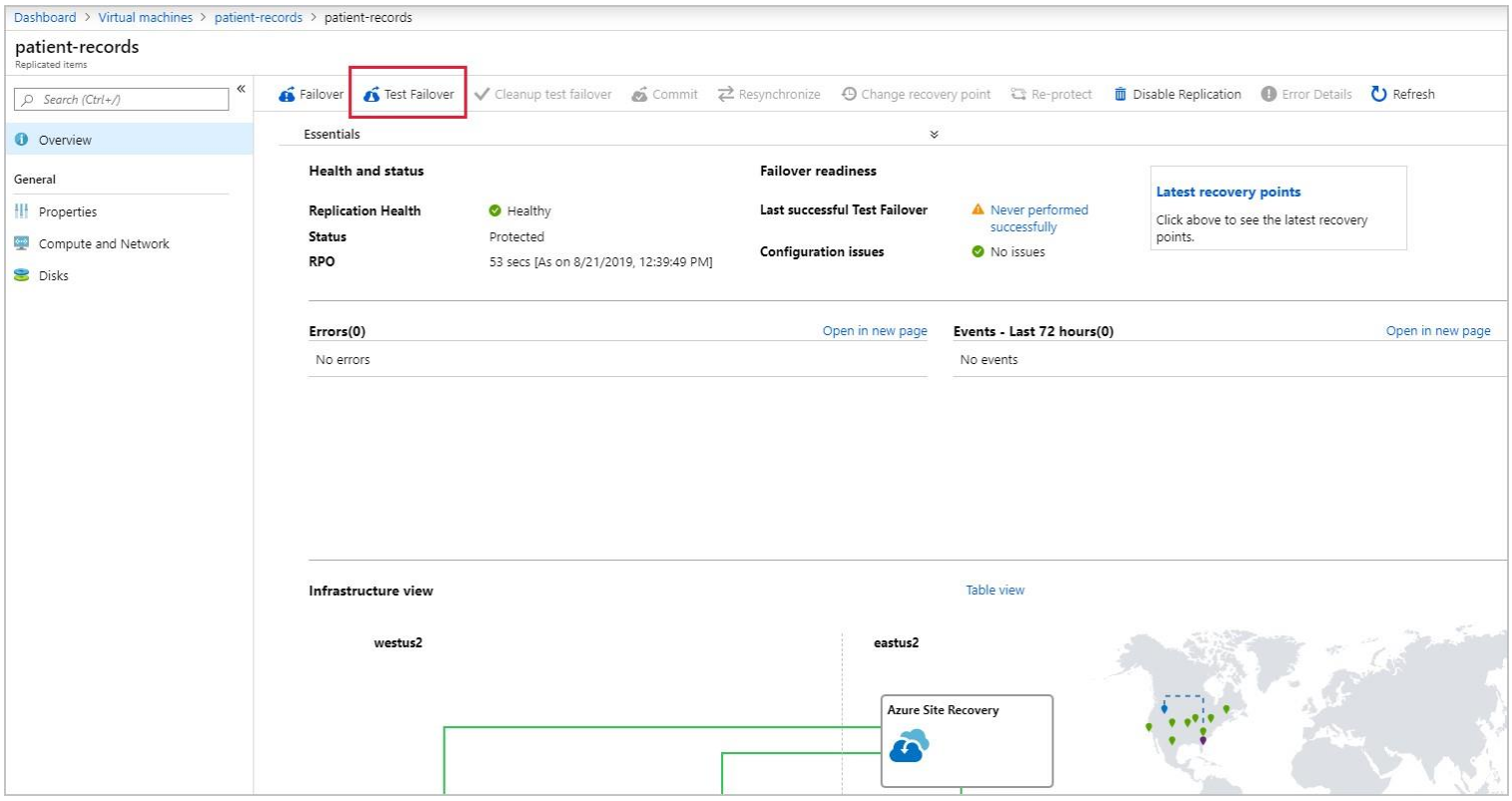
The steps are as follows:

1. We'll create an isolated virtual network so that our production infrastructure isn't affected.



2. On the target VMs' overview, select **Disaster recovery**.

3. This option opens a new **Replicated items** pane.



4. Select **Test Failover** at the top of the pane.

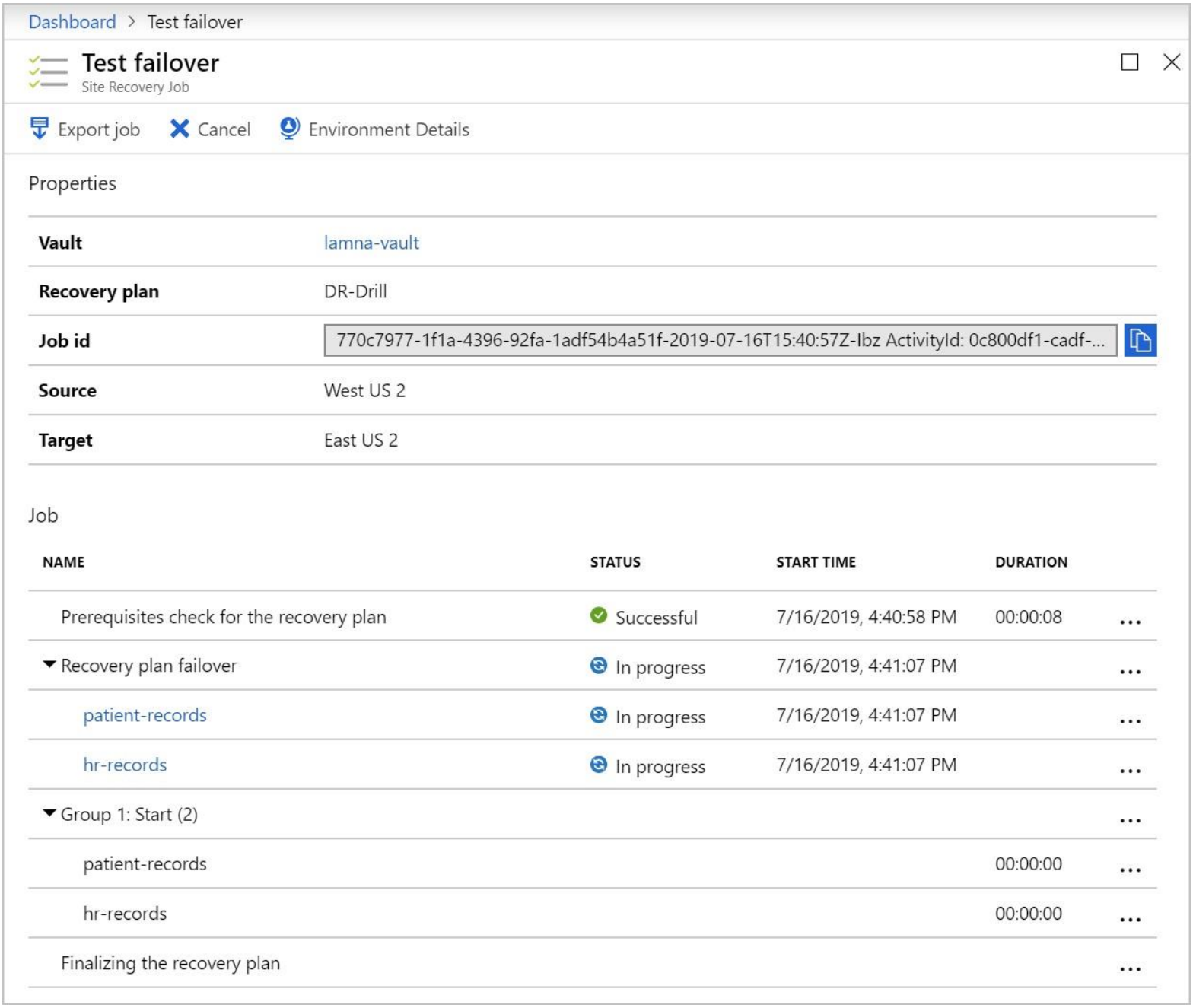
5. This option will run a test failover of the VM, and allow us to track its progress through the Site Recovery jobs page.

6. Once complete, the failed over VM appears in the portal under Virtual Machines, in the recovery region. We can then check the VM is running, is sized and connected correctly, and is mirroring the source VM but in a different Azure region.

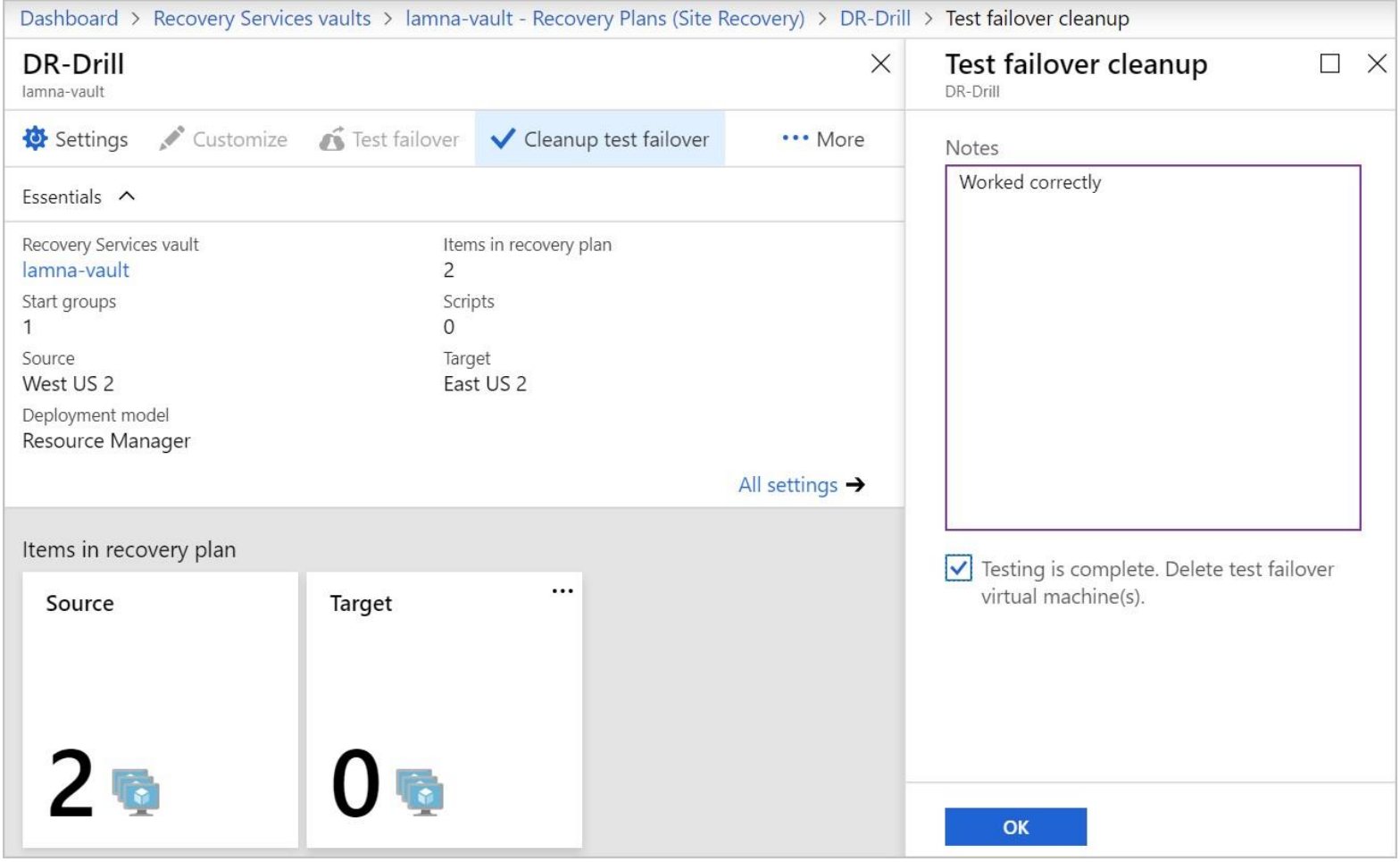
7. After we've validated everything has worked as expected, the replicated VM is deleted by selecting **Cleanup test failover**. It's a good idea to add notes about the test outcome at this point.

Flexible failover of multiple machines

Azure Site Recovery gives us the flexibility to run a full DR test scenario for all our virtual machines. We can create recovery plans that include one or more of our VMs. Failovers are runnable as many times as we like, and allow for a flexible policy to test different combinations of infrastructure.



Just like testing the single VMs, the same test cleanup is available for everything included in the recovery plan.



Difference between a drill and production failover

Running a production failover in Azure Site Recovery is similar to that of a test drill. There are some exceptions, the first being tha**Failover** is selected, instead of Test failover. We can choose to shut down the source VM before starting the failover so that no data is lost during the switch. Azure Site Recovery doesn't clean up the source environment once the failover is complete.

When the failover completes, validate the VM is working as expected. Azure Site Recovery gives us the ability to change the recovery point at this stage. If we're happy the failover works, we'll**Commit** the failover. Azure Site Recovery deletes all the source VM recovery points and finishes the failover. With our replicated infrastructure and data in the secondary region, we need to keep in mind that the new VM in the secondary region also needs protection.

Check your knowledge

1. How does Site Recovery support grouping of machines and workloads?

- Site Recovery Mobility service.
- Recovery plans.

  Recovery plans allow you to group VMs around workloads. For example, a recovery plan protecting a company's e-commerce website would include the web server, database server, and API server.
- Azure Automation.

Next unit: Exercise - Run a disaster recovery drill

Continue

100 XP

Exercise - Run a disaster recovery drill

10 minutes

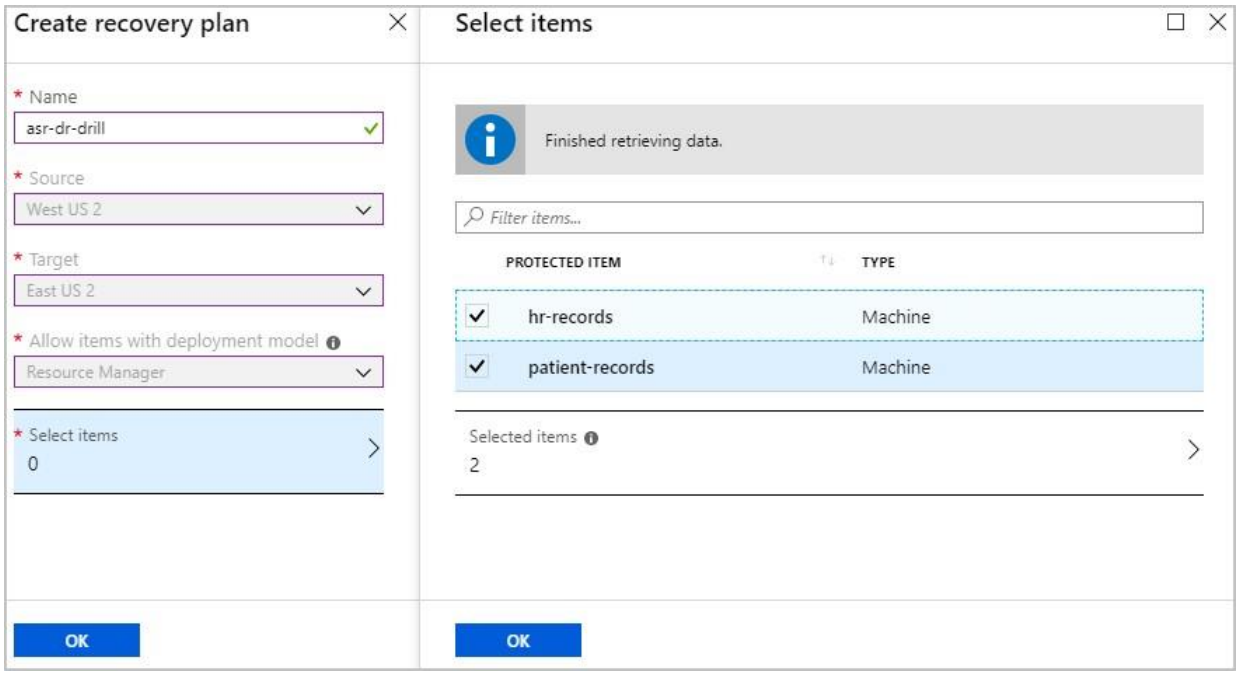
Azure Site Recovery is flexible enough to support many different recovery scenarios. We can choose to failover individual machines or our entire infrastructure with recovery plans. The flexibility allows us to simulate various disasters, like losing only part of our infrastructure. Multiple recovery plans can be defined to allow for all the different kinds of disaster drills you want to run.

With Azure Site Recovery in place, the head of Ops has asked you to test how long it takes to failover all your infrastructure. You've investigated the different options and decided to create a recovery plan so that you can failover all the VMs. With the plan in place, you'll run a test failover, and monitor its progress.

In this exercise, we'll complete the steps needed to run a disaster recovery drill using a recovery plan on the portal.

Create a recovery plan

1. Sign into the Azure portal with your credentials.
2. On the left of the portal, select **All resources**.
3. From the list of resources, select the Recovery Services vault,**asr-vault**
4. Under **Manage**, select **Recovery Plans (Site Recovery)**.
5. Select **+ Recovery Plan**.
6. Enter **asr-dr-drill** in the **Name** field on the *Create recovery plan* pane.
7. Select **West US 2** as the **Source** value.
8. Select **East US 2** as the **Target** value.
9. Select **Resource Manager** as the **Allow items with deployment model**



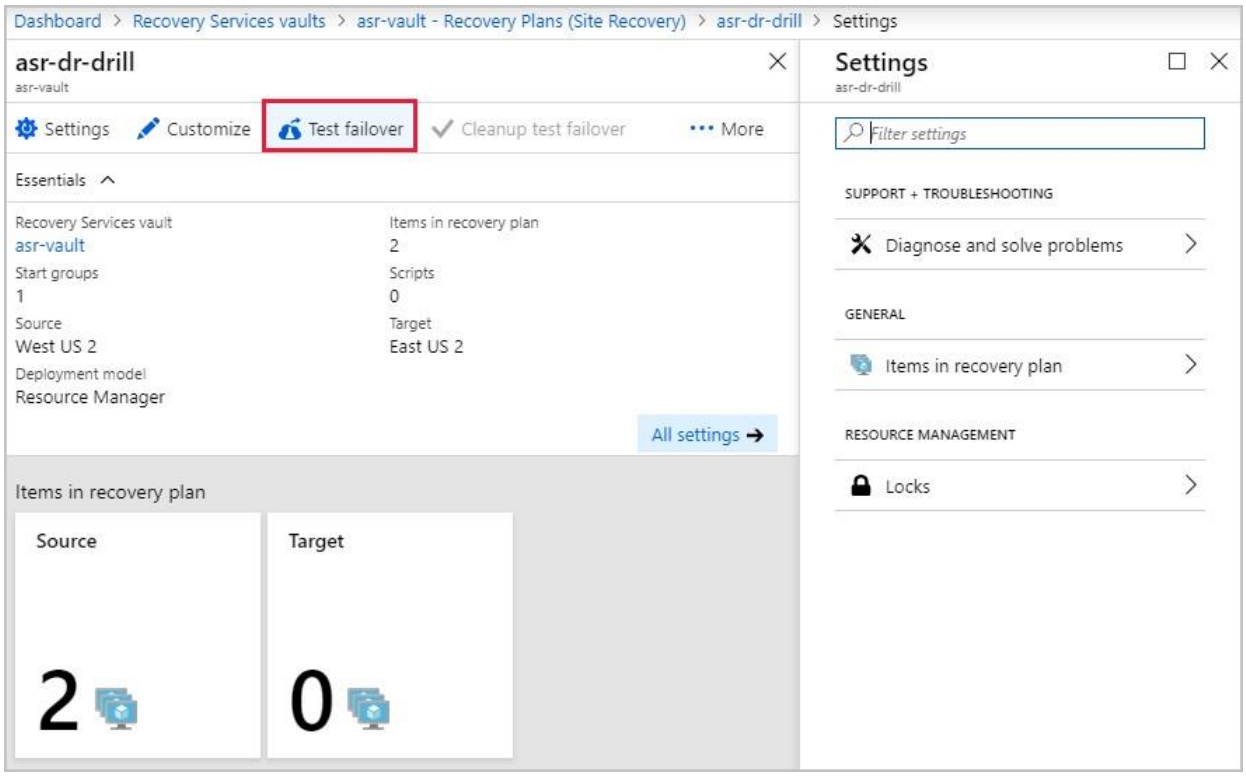
10. Click on **Select items** and choose your company's two VMs, then select **OK**.
11. Select **OK** at the bottom of the pane.

> **Note**
>
> It can happen that the configuration fails. If the configuration fails, delete the plan and create a new plan.

Run a test failover using a recovery plan

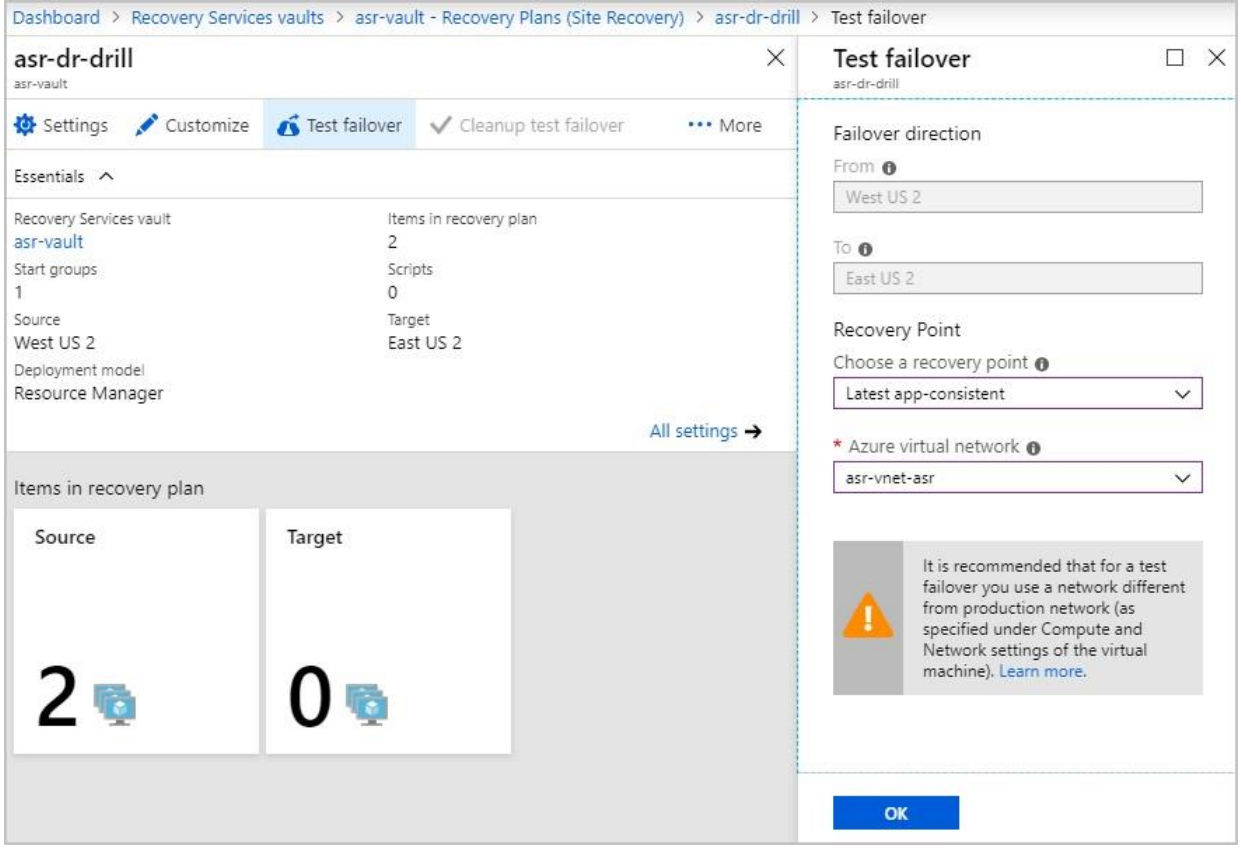
1. View the details of the recovery plan you created above by selecting**asr-dr-drill**

2. On the recovery plan details pane, at the top, select**Test failover**.



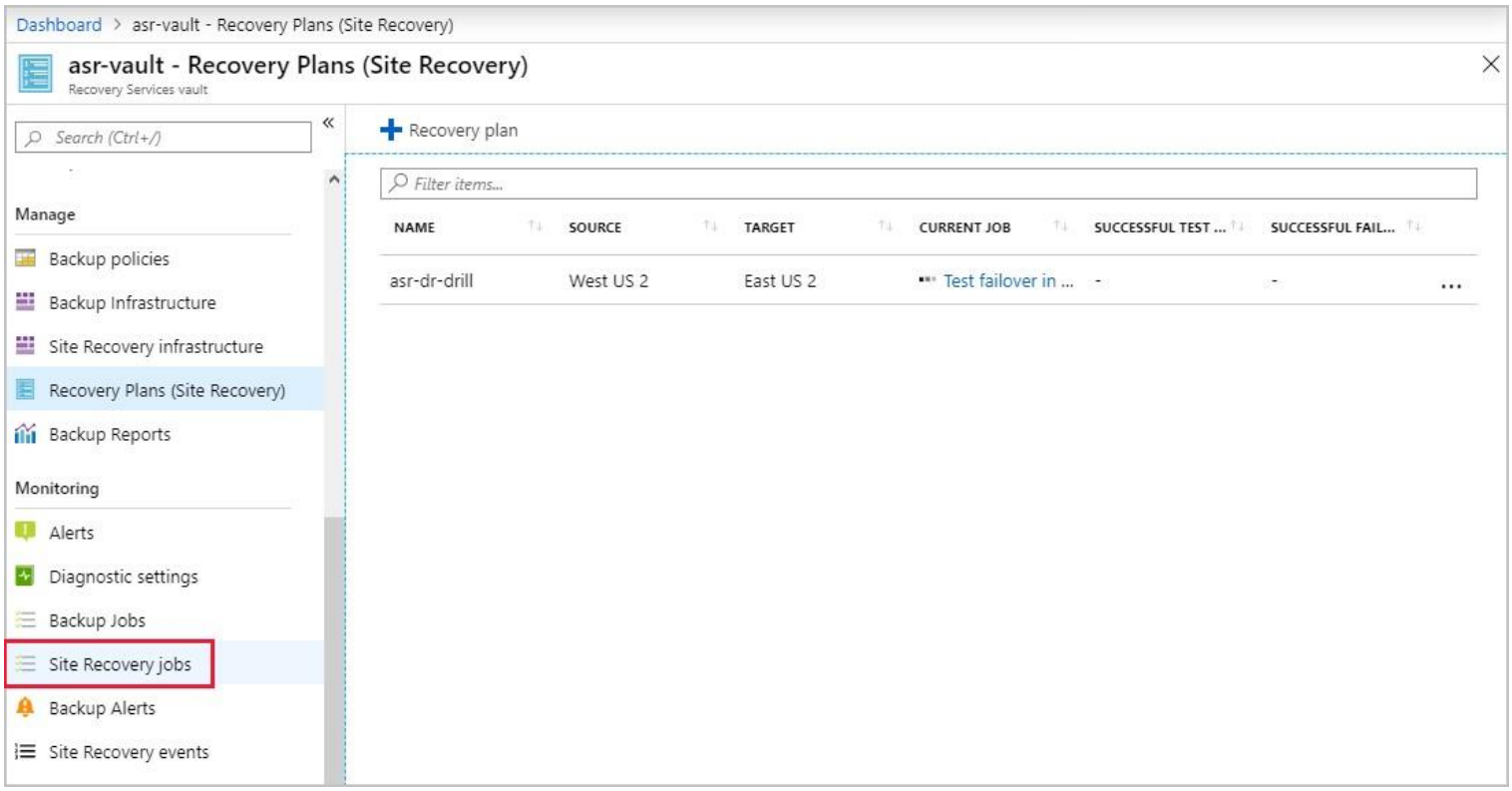
Important: The network configuration failover support for each VM can take several minutes to auto configure as each VM also needs to complete an initial synchronization. Running a failover test may not be available immediately.

3. Select **West US 2** as the **From** region value.
4. Select **East US 2** as the **To** region value.
5. Select **Latest app-consistent** as the **Recovery Point** value.
6. Select **asr-vnet-asr** as the **Azure virtual network** value.
7. Select **OK** to begin the failover.

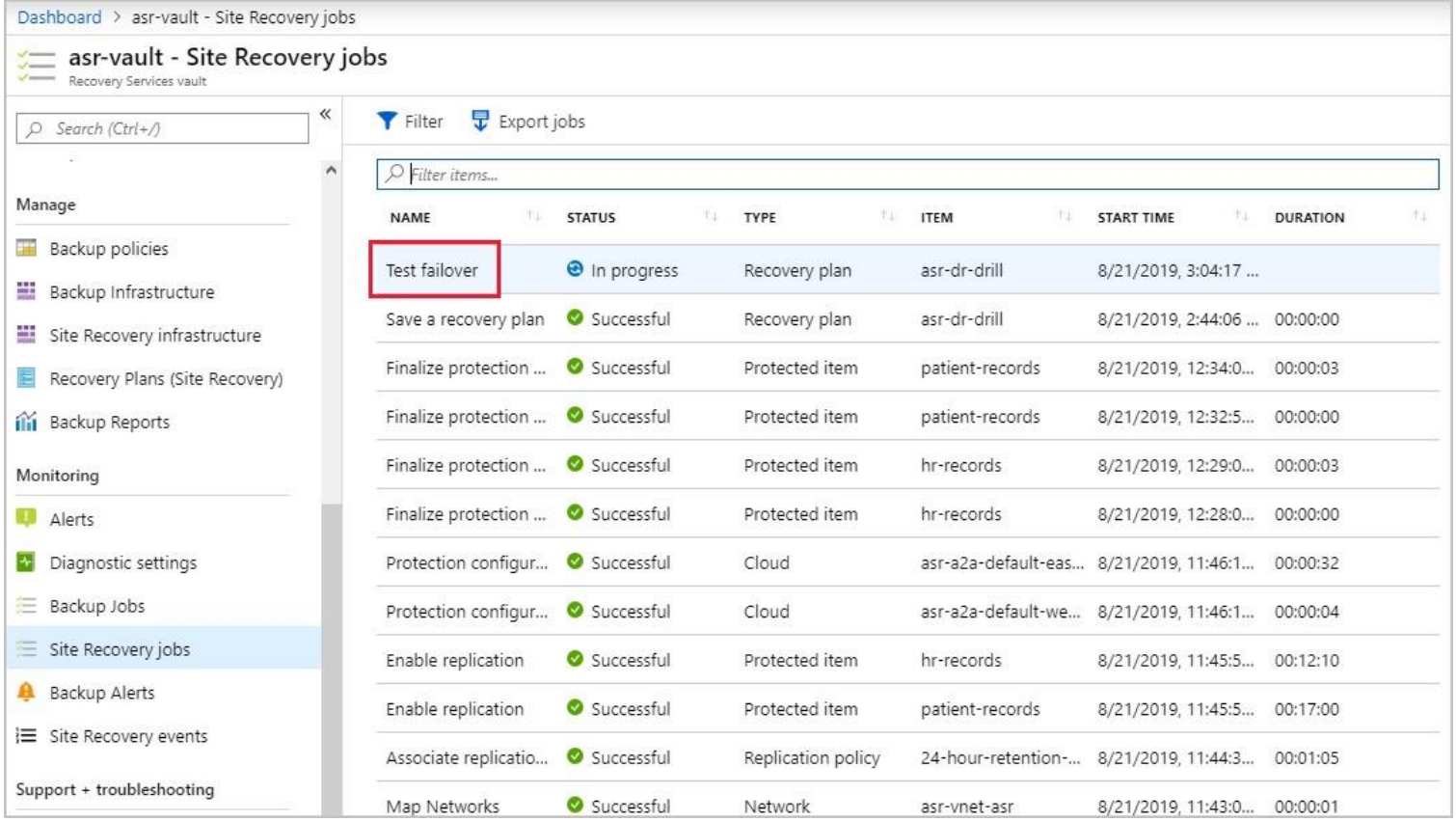


Monitor failover progress

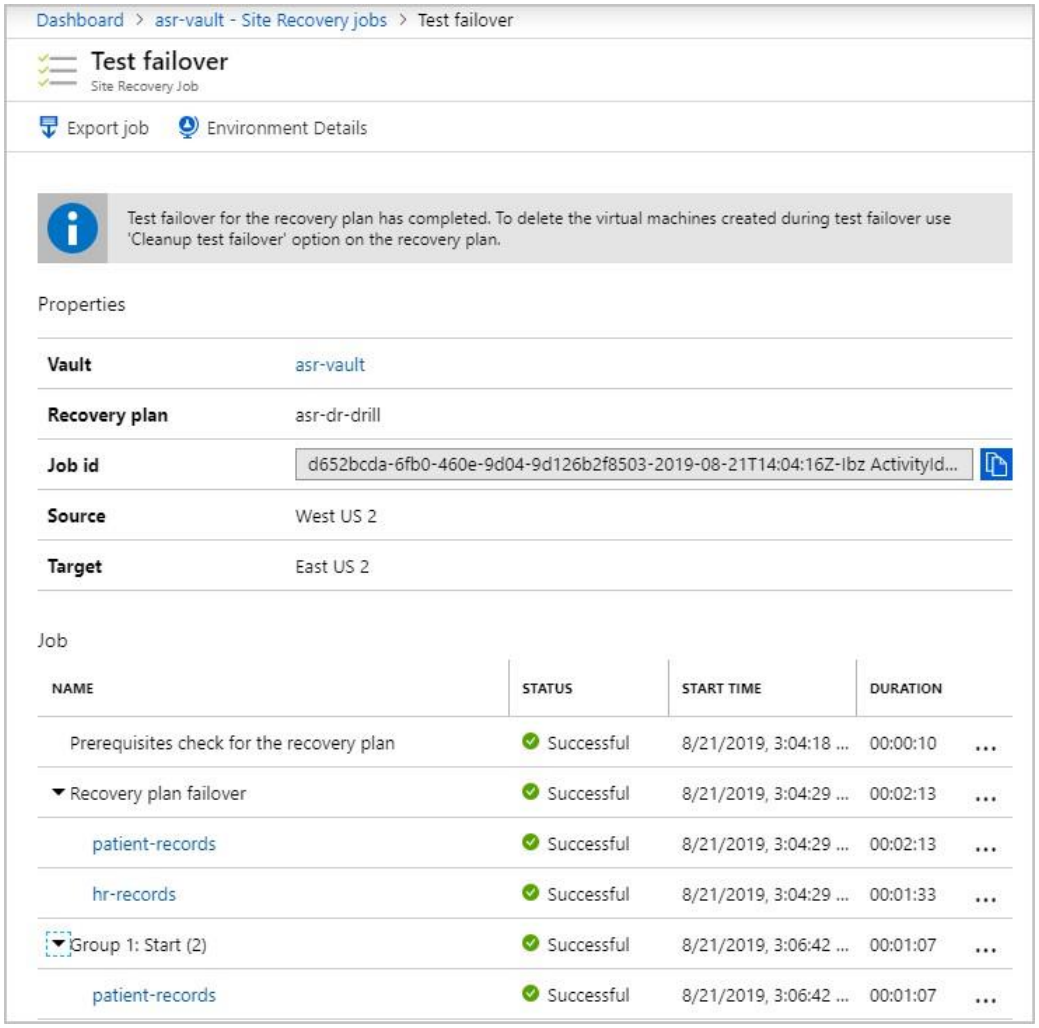
1. In the navigation slug at the top of the pane, select**asr-vault - Recovery Plans (Site Recovery)**



2. Under Monitoring, select **Site Recovery jobs**.

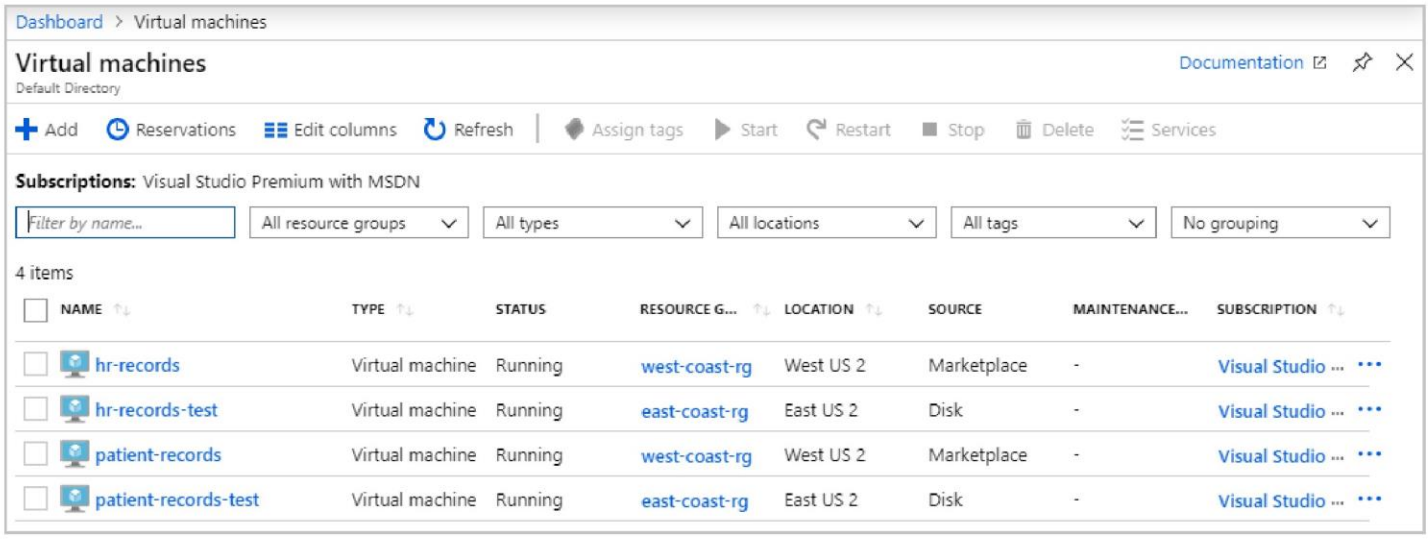


3. Select **Test failover** to view the status of the jobs.

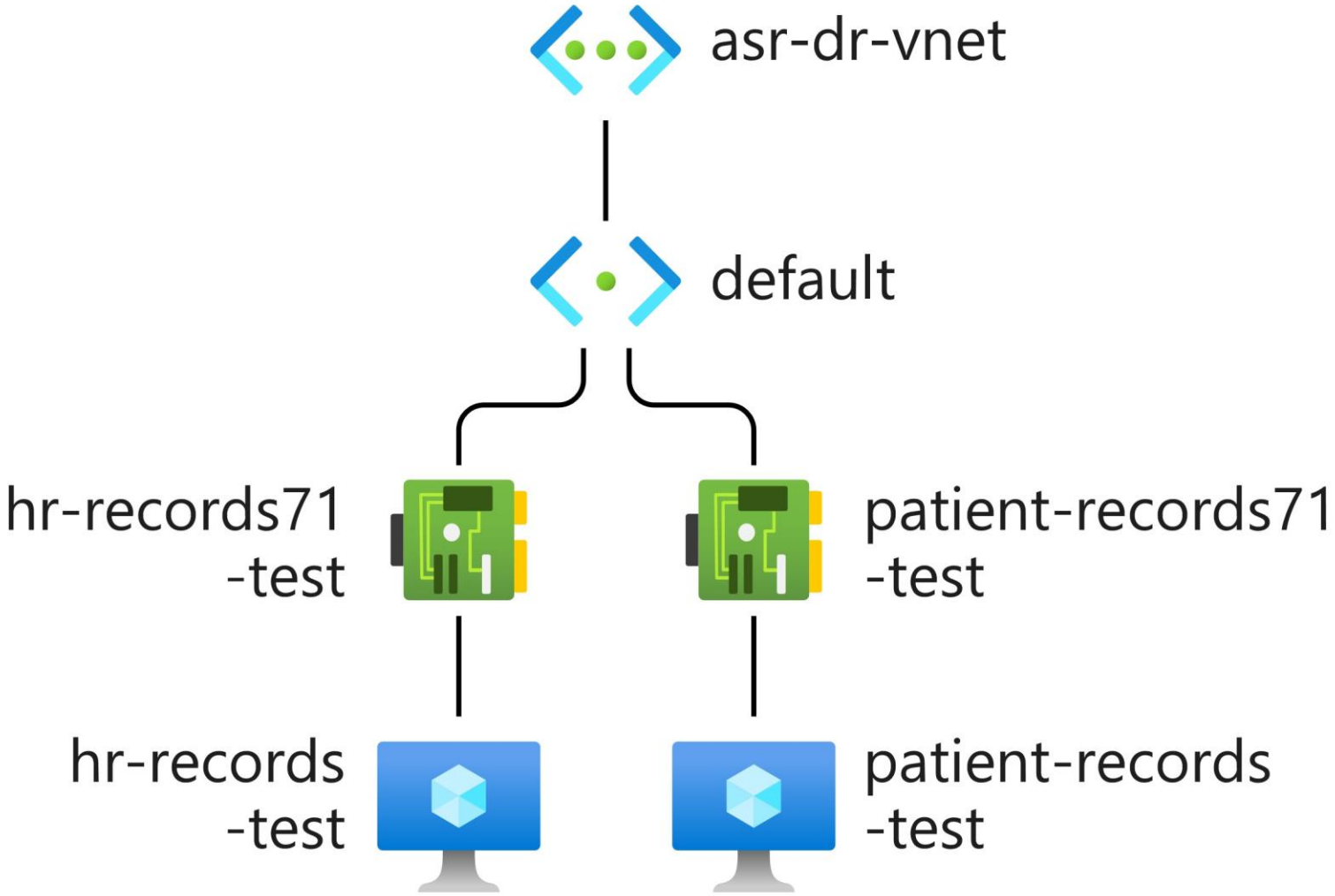


We'll use the information on this page to report back to the Ops manager that an Azure failover for our company's current infrastructure will take less than three minutes to complete. These jobs are running in parallel, so it isn't a simple sum of all of them to work out the total the time taken.

4. Once all the jobs have finished successfully, on the far left select **Virtual machines**.

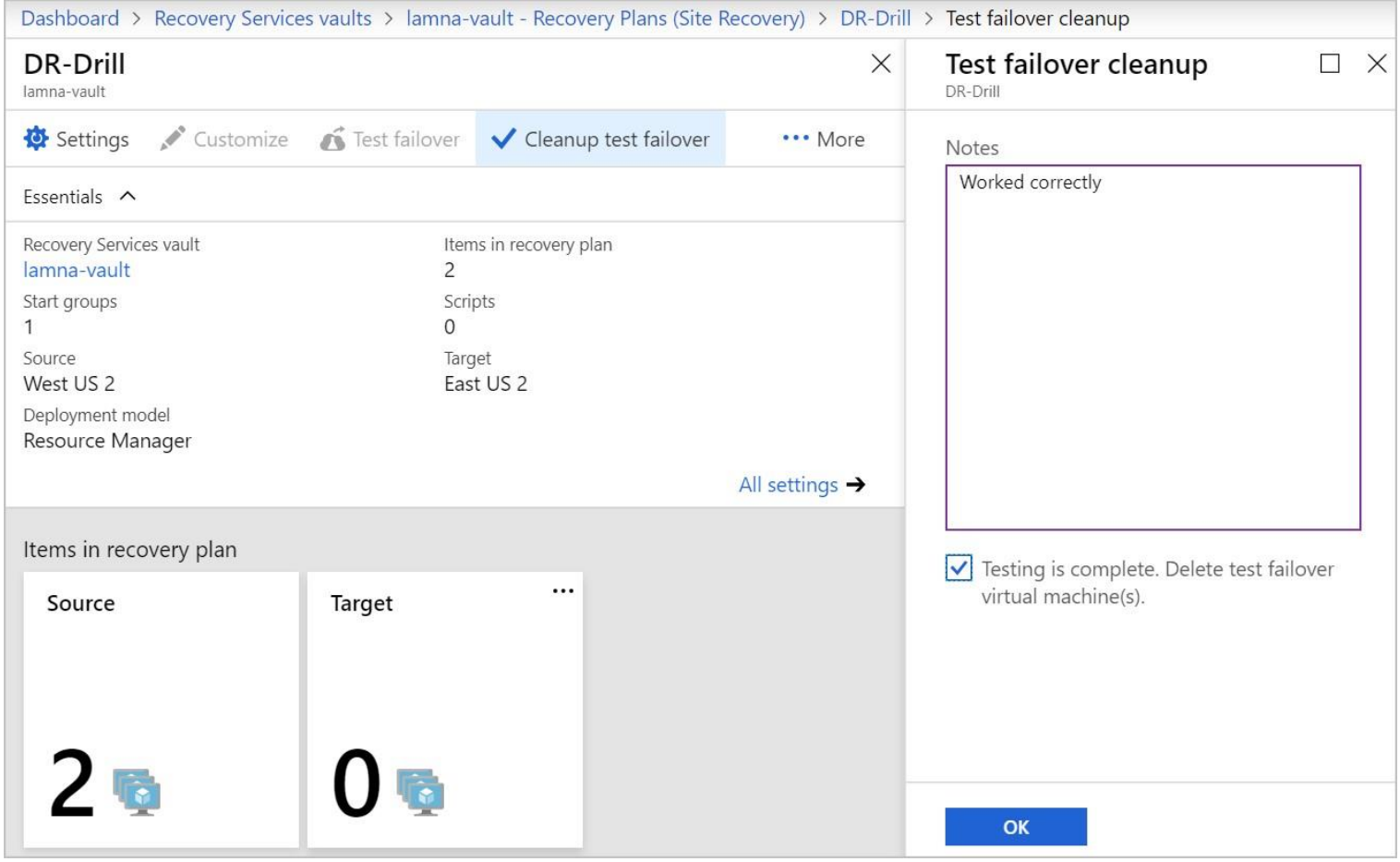


5. Select one of the new test VMs, then on the left under **Settings**, select **Networking**, then select **Topology**.



> ⓘ Note
>
> Both the patient-records and hr-records VMs have been failed over by Azure Site Recovery. The machines are running in their own disaster recovery virtual network.

6. Once we're satisfied with the test results, make sure to capture any notes about the test outcome. We'll now switch back to our **asr-dr-drill** site recovery plan and select the **Cleanup test failover** option to delete the replicated VMs.



7. Select the **Testing is complete** checkbox and then select the **OK** button to complete the cleanup process. This step can take up to three minutes to complete.

Next unit: Failover and failback using Azure Site Recovery

Continue

200 XP

Failover and failback using Azure Site Recovery

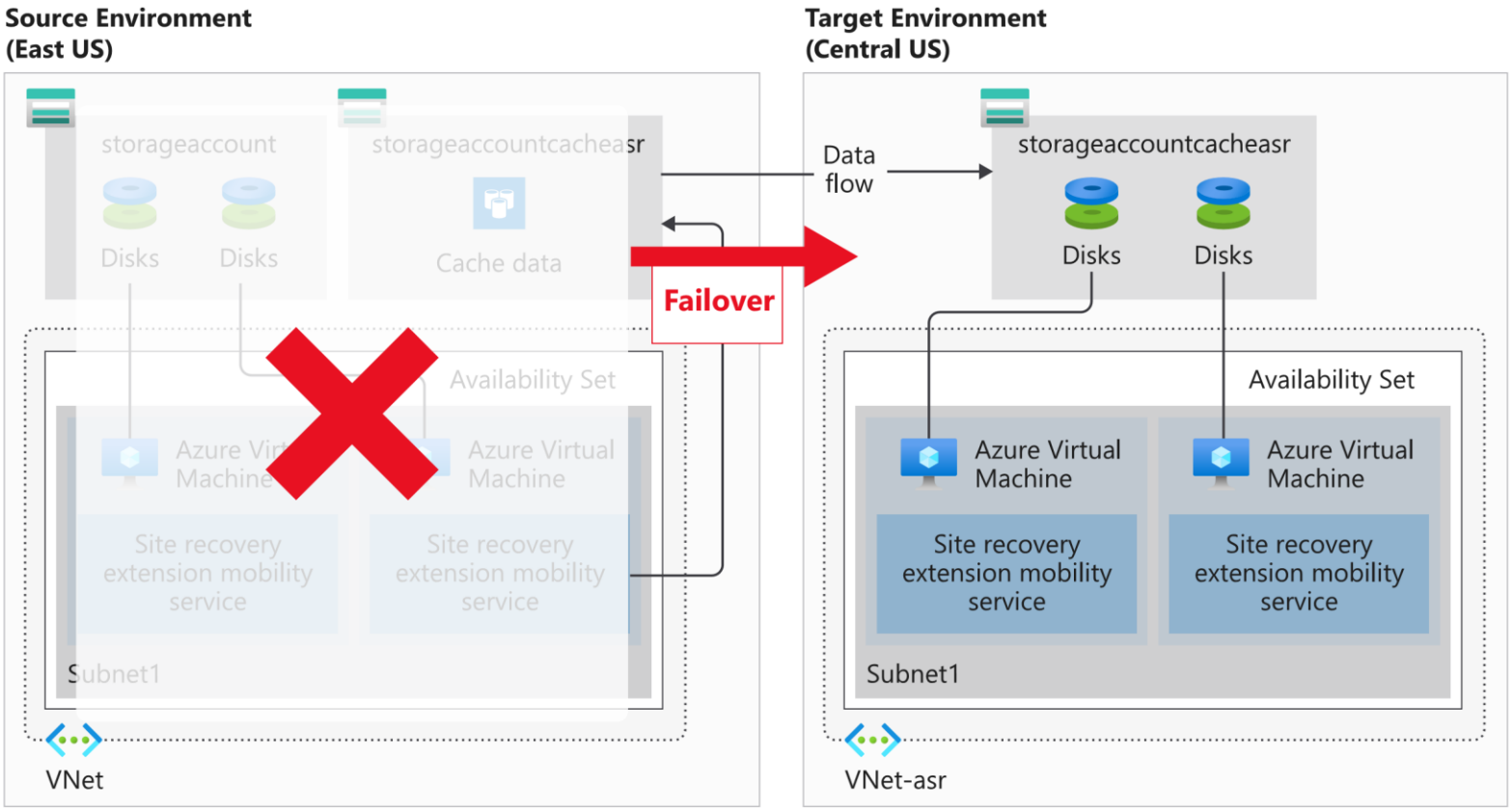
6 minutes

Azure Site Recovery enables your organization to have flexibility. Either manually failing over to a secondary Azure region, or falling back to a source virtual machine. The simplest way to manage this process is manually on the Azure portal. You do have other options to enable automation if your company wants to automate triggering a failover. These options include technologies like scripting via PowerShell, or setting up runbooks in Azure Automation to orchestrate failovers.

You would now like to run through a full failover of a protected VM to a secondary region in your subscription. Once the failover has completed successfully, you'll then failback that virtual machine.

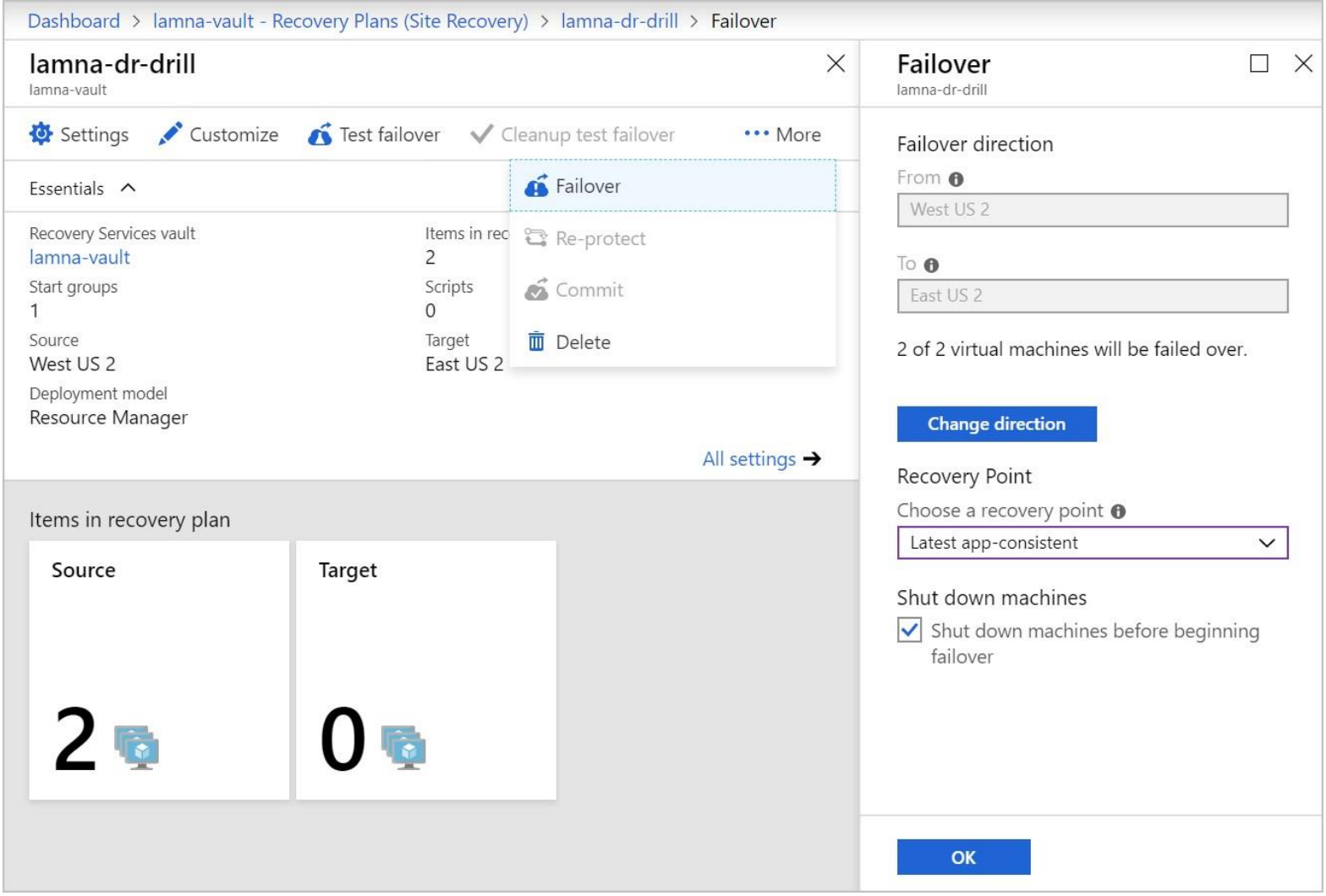
In this unit, you'll explore failover and failback, how to reprotect a failed over VM, and monitor the status of the reprotection.

What is failover?



A failover happens when a decision is made to execute a DR plan for our organization. The existing production environment, protected by Azure Site Recovery, is replicated to a different region. The target environment becomes the de facto production environment and becomes the environment our organization's production services run on. Once the target region is active, and the source environment should no longer be used. We enforce this by leaving the source VMs stopped.

There's another advantage to shutting down the source VMs. Using a shutdown VM results in minimal data loss, as Azure Site Recovery waits until all the data is written to disk before triggering the failover. To use this data and have the lowest possible RPO, we select the **Latest (lowest RPO)** recovery point.

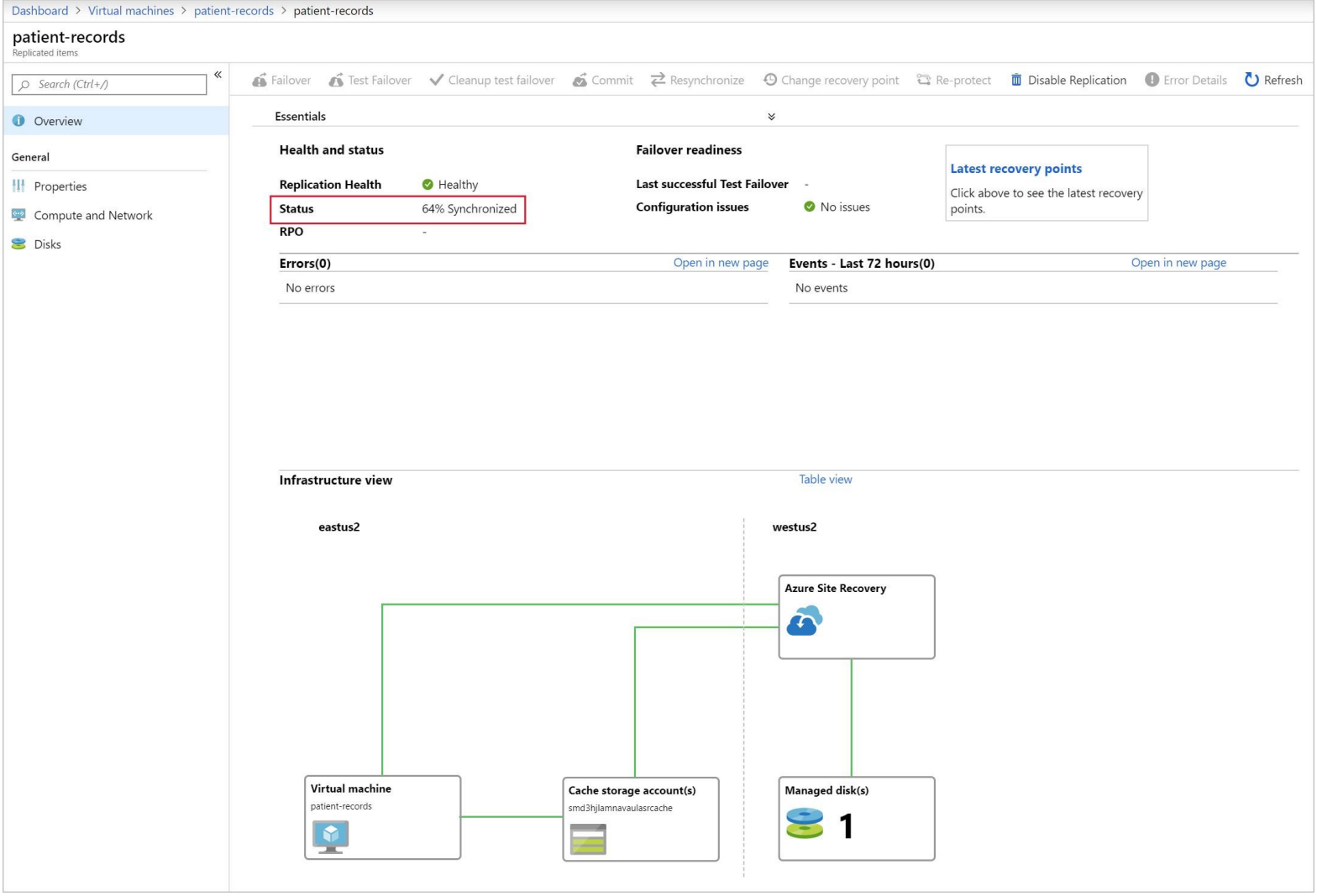


What is reprotection, and why is it important?

When a VM is failed over, the replication performed by Azure Site Recovery is no longer happening. We have to re-enable the protection to start protecting the failed over VM. As we already have the infrastructure in a different region, we can start replication back to the source region. Reprotection enables Azure Site Recovery to start replicating our new target environment back to the source environment where it started.

The flexibility of failing over single VMs, or failover using a recovery plan, can be used to reprotect our failed over infrastructure. We can reprotect each VM individually, or we can reprotect multiple VMs using a recovery plan.

Reprotecting takes anywhere between 45 minutes to 2 hours, dependent on the size and type of VM. Unlike the other Site Recovery processes that can be monitored by watching the progress of the jobs, reprotection progress has to be viewed at the VM level. This requirement is because the synchronization phase isn't listed as a site recovery job.



The above image shows the status of the protected item, with the percentage synchronized highlighted.

What is failback?

Failback is the reverse of a failover. It's where a completed failover to a secondary region has been committed and is now the production environment. Reprotection has completed for the failed over environment, and the source environment is now its replica. In a failback scenario, Azure Site Recovery will fail over back to the source VMs.

The process to complete a failback is the same as a failover, even down to reusing the recovery plan. Selecting failover on your recovery plan has **from** set to the target region and the **to** set to the source region.

Managing failovers

Azure Site Recovery can run failovers on demand. Test failovers are isolated, meaning they don't impact production services. This flexibility allows us to run a failover without interrupting the users of that system. The flexibility works the other way too, allowing failback on-demand either as part of a planned test or as part of a fully invoked DR process.

The recovery plans in Azure Site Recovery also allow for the customization and sequencing of failover and failback. The plans allow you to group machines and workloads.

Flexibility can also apply to how you trigger the failover process. Manual failovers are easy to do via the Azure portal. PowerShell scripting or using runbooks in Azure Automation gives you automation options.

Fixing issues with a failover

Even though Azure Site Recovery is automated, errors can still happen. Below is a list of the three most common issues we may see. For a full list of issues and how to troubleshoot them see the link in the summary unit.

Azure resource quota issues

Azure Site Recover needs to create resources in different regions. If our subscription isn't able to do this, the replication fails. This error also happens if our subscription doesn't have the right quota limits to create VMs that match the size of the source VMs.

The fix is to contact Azure billing support and ask them to enable creating the correct size VMs in the needed target region.

One or more disk(s) are available for protection

This error happens if you've finished setting up Azure Site Recovery for your VMs. Then you've added or initialized, additional disks.

To fix this error, you can add replication for the newly added disks, or you can choose to ignore the disk warning.

Trusted root certificates

Check that the latest root certificates are installed to allow Azure Site Recovery to communicate and authenticate VMs for replication securely. You could see this error if your VMs don't have the latest updates applied. Update Both Windows and Linux VMs before Azure Site Recovery can enable replication.

The fix is different for each OS. Windows is as simple as ensuring automatic Windows update is switched on, and updates are applied. For each Linux distribution, you'll need to follow the guidance provided by the distributor.

Check your knowledge

1. Site Recovery is being used to reprotect a failed over VM, which PowerShell command allows you to monitor the progress?

- Get-AzRecoveryServicesAsrFabric
- Get-AzRecoveryServicesAsrRecoveryPlan
- Get-AzRecoveryServicesAsrJob

Gets the details of the specified Site Recovery job or the list of recent Site Recovery jobs in the Recovery Services vault. Specifying the job that started the reprotection will show its status.

Next unit: Exercise - Failover and failback using Azure Site Recovery

Continue

100 XP

Exercise - Failover and failback using Azure Site Recovery

10 minutes

We can fail over protected resources in three ways. Using the portal, using PowerShell, or automating the failover with an Azure Automation runbook.

With all our resources protected, we'd like to run a real failover of our patient-records VM. With the disaster recovery drill complete, we'll do the failover with PowerShell and the portal. Once completed, we'll be in a better position to recommend which approach our company should use.

In this exercise, we'll complete failover for a VM using PowerShell, and failback the VM using the Azure portal.

Fail over a VM to a secondary region using PowerShell

1. Sign into the Azure portal with your own credentials.

2. Start a Cloud Shell and switch it to PowerShell.

3. Run the following commands.

```powershell
    $vault = Get-AzRecoveryServicesVault -Name "asr-vault"
    Set-AzRecoveryServicesAsrVaultContext -Vault $vault
    $PrimaryFabric = Get-AsrFabric -Name "asr-a2a-default-westus2"
    $PrimaryProtContainer = Get-ASRProtectionContainer -Fabric $PrimaryFabric
    $ReplicationProtectedItem = Get-ASRReplicationProtectedItem -ProtectionContainer $PrimaryProtContainer -FriendlyName "patient-records"
    $RecoveryPoints = Get-ASRRecoveryPoint -ReplicationProtectedItem $ReplicationProtectedItem
    $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
    $CommitFailoverJob = Start-ASRCommitFailoverJob -ReplicationProtectedItem $ReplicationProtectedItem
    Get-ASRJob -Job $CommitFailoverJob
```

The PowerShell commands above:

- Store the Azure Site Recovery vault in a variable
- Set the context for the session to your vault
- Store the protected patient-records from the vault
- Get a list of all the recovery points
- Trigger a failover for the latest recovery point
- Show the result of the failover

4. The failover can take a couple of minutes. While the script is running, leave the cloud shell open and navigate to the *asr-vault*.

5. On the left, under **Monitoring**, select **Site Recovery jobs**.

> **Note**
>
> You can view the progress of the failover job at the same time as the script is running.

6. In the portal, select **Virtual machines** to check that the patient-record VM has been failed over to the east coast region.

7. There are now three VMs, with two named **patient-records**.

Reprotect the VM using PowerShell

1. Once the failover has completed successfully, we can reprotect the VM.

2. Run the following commands.

```powershell
$RecoveryFabric = Get-AsrFabric -Name "asr-a2a-default-eastus2"
$RecoveryProtContainer = Get-ASRProtectionContainer -Fabric $RecoveryFabric
$ProtectionContainerMapping = Get-AzRecoveryServicesAsrProtectionContainerMapping -ProtectionContainer $RecoveryProtContainer -Name eastus2-westus2-24-hour-
retention-policy
$StorageAccount = New-AzStorageAccount -ResourceGroupName "east-coast-rg" -AccountName "reprotectcache" -Location eastus2 -SkuName Standard_GRS
$ResourceGroup = Get-AzResourceGroup -Name "west-coast-rg"
```

```
$ReprotectJob = Update-AzRecoveryServicesAsrProtectionDirection -AzureToAzure -ProtectionContainerMapping $ProtectionContainerMapping -ReplicationProtectedItem
$ReplicationProtectedItem -LogStorageAccountId $StorageAccount.ID -RecoveryResourceGroupId $ResourceGroup.ResourceId
```

The PowerShell commands above:

- Setup variables that will be used by the Update-AzRecoveryServicesAsrProtectionDirection command
- A storage account is needed to store the reprotected logs and data. This storage needs to be in the same region as the VM that is being protected
- The last line starts the reprotect job, and stores a reference to it

Monitor and test using PowerShell

The job to reprotect the VM can take around approximately 10 minutes to complete.

1. We can monitor the job using this PowerShell command:

```
PowerShell
Copy

Get-AzRecoveryServicesAsrJob -Job $ReprotectJob
```

2. This command will return the status of the job. The output will look like this example:

```
PowerShell
Copy

Name             : 0993fa3c-6ac1-4d96-920d-df06830d49f2
ID               : /Subscriptions/3dd370ad-858c-49f0-8f7a-ee6cc0d841de/resourceGroups/east-coast-rg/providers/Microsoft.RecoveryServices/vaults/asr-
vault/replicationJobs/0993fa3c-6ac1-4d96
                   -920d-df06830d49f2
Type             : Microsoft.RecoveryServices/vaults/replicationJobs
JobType          : SwitchReplicationGroupProtection
DisplayName      : Reprotect
ClientRequestId  :
State            : Succeeded
StateDescription : Completed
StartTime        : 7/22/19 10:25:49 AM
EndTime          : 7/22/19 10:35:07 AM
TargetObjectId   : 28542035-9d78-58c9-a3ec-0ad29b0a88d8
TargetObjectType : ProtectionEntity
TargetObjectName : patient-records
AllowedActions   :
Tasks            : {}
Errors           : {}
```

> **Note**
>
> The State is **Succeeded**, and the StateDescription is **Completed**.

Failback to the West US region using the portal

1. Close the Cloud Shell so that we can use the Azure portal more easily.
2. Select **All resources** in the upper left-hand side of the portal.
3. Select the **Recovery Services vault** by selecting **asr-vault**.
4. Under **Protected items**, select **Replicated items**.
5. Select the **patient-records**.

   We can't failback the VM until the replication has completed, and synchronization is 100% completed. Please note that the synchronization process can take several minutes to complete.
6. Once synchronization completes, select **failover**.
7. Select the latest processed (low RTO) for the Recovery Point.
8. Select **OK** to begin the failback.

Monitor the failback

1. Select **All resources** in the upper left-hand side of the portal.
2. Select the **Recovery Services vault** by selecting **asr-vault**.
3. Under **Monitoring**, select **Site Recovery jobs**.
4. Select the in progress **Failover** job.