200 XP

Azure Site Recovery overview

10 minutes

Azure Site Recovery is more than just a tool to help you recover from system outages. Azure Site Recovery replicates workloads between a primary and secondary site. Site Recovery also can be used to migrate VMs from on-premises infrastructure to Azure.

Your first task to protect your workloads from an earthquake, for example, is to review the company's current business continuity and disaster recovery (BCDR) plan. You need to identify the different recovery objectives and scope for the systems that need protection.

In this unit, you'll investigate how Azure Site Recovery can help achieve these goals and make failover and recovery of resources possible in the event of a disaster.

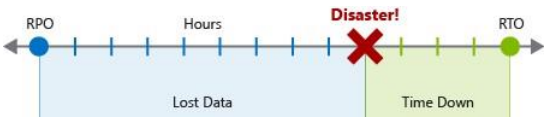
Business continuity and disaster recovery

Loss of service can cause disruption to your staff and users. Every second that systems are unavailable can cause your company lost revenue. Your company also might face financial penalties for breaking agreements written for the availability of services you provide.

BCDR plans are formal documents that companies draw up that cover the scope and actions to be taken when a disaster or large-scale outage happens. Each outage is assessed on its own merit. For example, a disaster recovery plan comes into action when a whole datacenter loses power.

In this example scenario, an earthquake occurred and damaged communications lines made the datacenter useless until it's repaired. A disaster of this size might bring services down for days, not hours, so a full BCDR plan must be invoked to get the service back online.

As part of your BCDR plan, identify the recovery time objectives (RTOs) and recovery point objectives (RPOs) for your applications. Both objectives help to realize the maximum tolerable hours that your business can be without specified services, and what the data recovery process should be. Let's look closer at each one.



Recovery time objective

A recovery time objective is a measure of the maximum amount of time your business can survive after a disaster before normal service is restored. Let's assume your RTO is 12 hours, which means that operations can continue for 12 hours without the business's core services functioning. If the downtime is 24 hours, your business would be seriously harmed.

Recovery point objective

A recovery point objective is a measure of the maximum amount of data loss that's acceptable during a disaster. A business can typically decide to do a backup every 24 hours, 12 hours, or even in real time. If a disaster occurs, there's always some data loss.

For example, if your backup occurred every 24 hours, at midnight, and a disaster happened at 9:00 AM the following day, then nine hours of data would be lost. If your company's RPO was 12 hours, it would be okay because only nine hours passed. If the RPO was four hours, there would be a problem and damage would occur to the business.

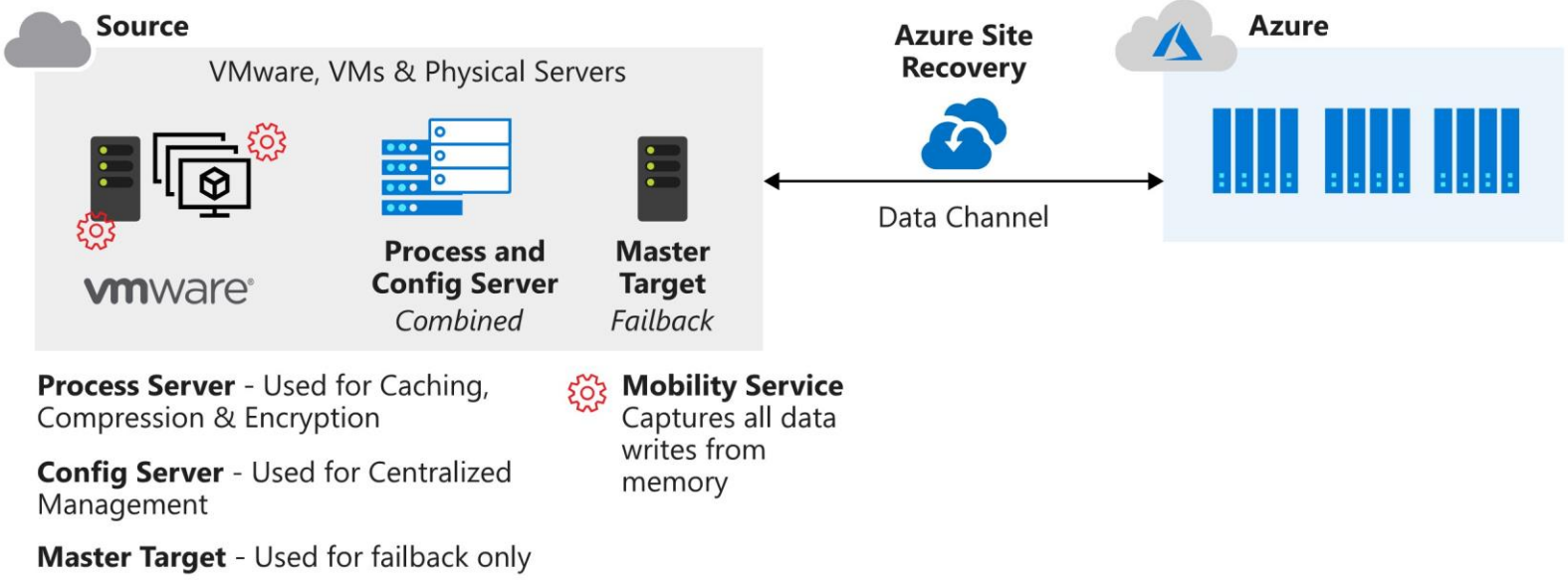
What is Azure Site Recovery?

Azure Site Recovery can contribute to your disaster recovery plan because it can replicate workloads from a primary site to a secondary site. If an issue occurs at the primary site. Site Recovery can be automatically invoked to replicate the protected virtual machines to another location. The failover could be from on-premises to Azure, or it could be from one Azure region to another.

Some notable features of Azure Site Recovery are:

- **Central management** : Replication can be set up and managed and failover and failback can be invoked all from within the Azure portal.
- **On-premises virtual machine replication** : On-premises virtual machines can be replicated to Azure or to a secondary on-premises datacenter, if necessary.
- **Azure virtual machine replication** : Azure virtual machines can be replicated from one region to another.
- **App consistency during failover** : By using recovery points and application-consistent snapshots, virtual machines are kept in a consistent state at all times during replication.
- **Flexible failover** : Failovers can be run on demand as a test or triggered during an actual disaster. Tests can be run to simulate a disaster recovery scenario without interruption to your live service.
- **Network integration** : Site Recovery can manage network management during a replication and disaster recovery scenario. Reserved IP addresses and load balancers are included so that the virtual machines can work in the new location.

Set up Azure Site Recovery

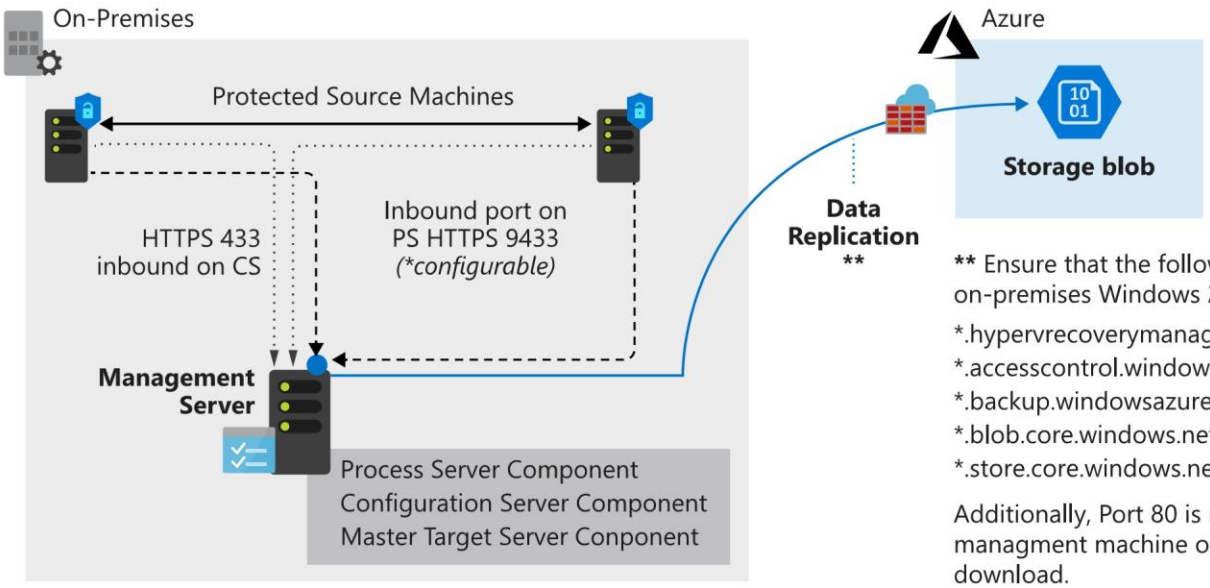


Several components must be set up to enable Azure Site Recovery:

- **Networking**: A valid Azure virtual network is required for the replicated virtual machines to use.
- **Recovery Services vault**: A vault in your Azure subscription stores the migrated VMs when a failover is run. The vault also contains the replication policy and the source and target locations for replication and failover.
- **Credentials**: The credentials you use for Azure must have the **Virtual Machine Contributor** and **Site Recovery Contributor** roles to allow permission to modify both the VM and the storage that Site Recovery is connected to.
- **Configuration server**: An on-premises VMware server fulfills several roles during the failover and replication process. It's obtained from the Azure portal as an open virtual machine appliance (OVA) for easy deployment. The configuration server includes a:
  - **Process server**: This server acts as a gateway for the replication traffic. It caches, compresses, and encrypts the traffic before sending it over the WAN to Azure. The process server also installs the mobility service onto all the physical and virtual machines targeted for failover and replication.
  - **Master target server**: This machine handles the replication process during a failback from Azure.

> **Important**
>
> To fail back from Azure to an on-premises environment, VMware vCenter with a configuration server must be available even if you're only replicating physical machines to Azure. You can't fail back to physical servers.

The replication process



** Ensure that the following URL's are accessible from on-premises Windows 2012 R2 Management machine:

*.hypervrecoverymanager.windowsazure.com
*.accesscontrol.windows.net
*.backup.windowsazure.com
*.blob.core.windows.net
*.store.core.windows.net

Additionally, Port 80 is required to be open on the managment machine only during setup for MySQL download.

After the prerequisite tasks are set up, replication of the machines can begin. They're replicated according to the created replication policy. During the initial stages of the first copy, the server data is replicated to Azure Storage. After the initial replication finishes, a second replication occurs. This time, the delta changes to the virtual machine are replicated to Azure.

Test and monitor a failover

After your environment is set up for disaster recovery, test it to make sure it's configured correctly and that everything works as you expect. Test the configuration by doing a disaster recovery drill on an isolated VM. It's a best practice to use an isolated network for the test so that live services aren't disrupted.

200 XP

Workloads supported for protection with Azure Site Recovery

6 minutes

After you set up Azure Site Recovery, you can use protection at the lower application level with applicationaware replication. Application-level protection is in addition to restoring at the machine level.

After you confirm the company's business continuity and disaster recovery (BCDR) plan with key stakeholders, you now want to investigate the workloads that Azure Site Recovery supports to ensure it fits with your organization's BCDR goals.

In this unit, you'll explore the application-level protection you can take advantage of to protect your company's different workloads.

Azure Site Recovery supported workloads

Site Recovery can replicate any app that runs on a supported machine:

- **Azure VM**: Replication is available for any workload that runs on a supported Azure virtual machine.
- **Hyper-V VM**: Protection is available for any workload that runs on a Hyper-V virtual machine.
- **Physical servers**: Protection is available for Windows and Linux operating systems.
  VMware VM: Protection is available for any workload that runs in a VMware virtual machine.

Site Recovery provides application-aware replication for many types of workloads or applications that run on top of the server operating system. Application replication is supported for many different workloads. Taking advantage of the integration with specific workloads has many benefits during normal replication, and also

during failover. Some of the features offered include:

- **Near synchronous replication** : Data is written to the primary storage and the replica almost simultaneously to allow for low recovery times.
- **App-consistent snapshots** : Snapshots taken for recovery purposes can view information in memory and pending I/O operations, which allows for quick recovery times. The application is ready to go after switching to the replica VM.
- **Integration with SQL Always On** : Always On is an enterprise-level alternative to normal database mirroring techniques.
- **Flexible recovery plans** : The ability to recover an entire application stack with a single click. Both manual and scripted actions can be incorporated into the overall plan.

    - **Network management** : The automated ability to simplify the reservation of IP addresses, configure load balancers, and integrate with Azure Traffic Manager.
    - **Automation library** : Production-ready scripts that can be downloaded and integrated with the recovery plan to provide a fully automated recovery, if needed.

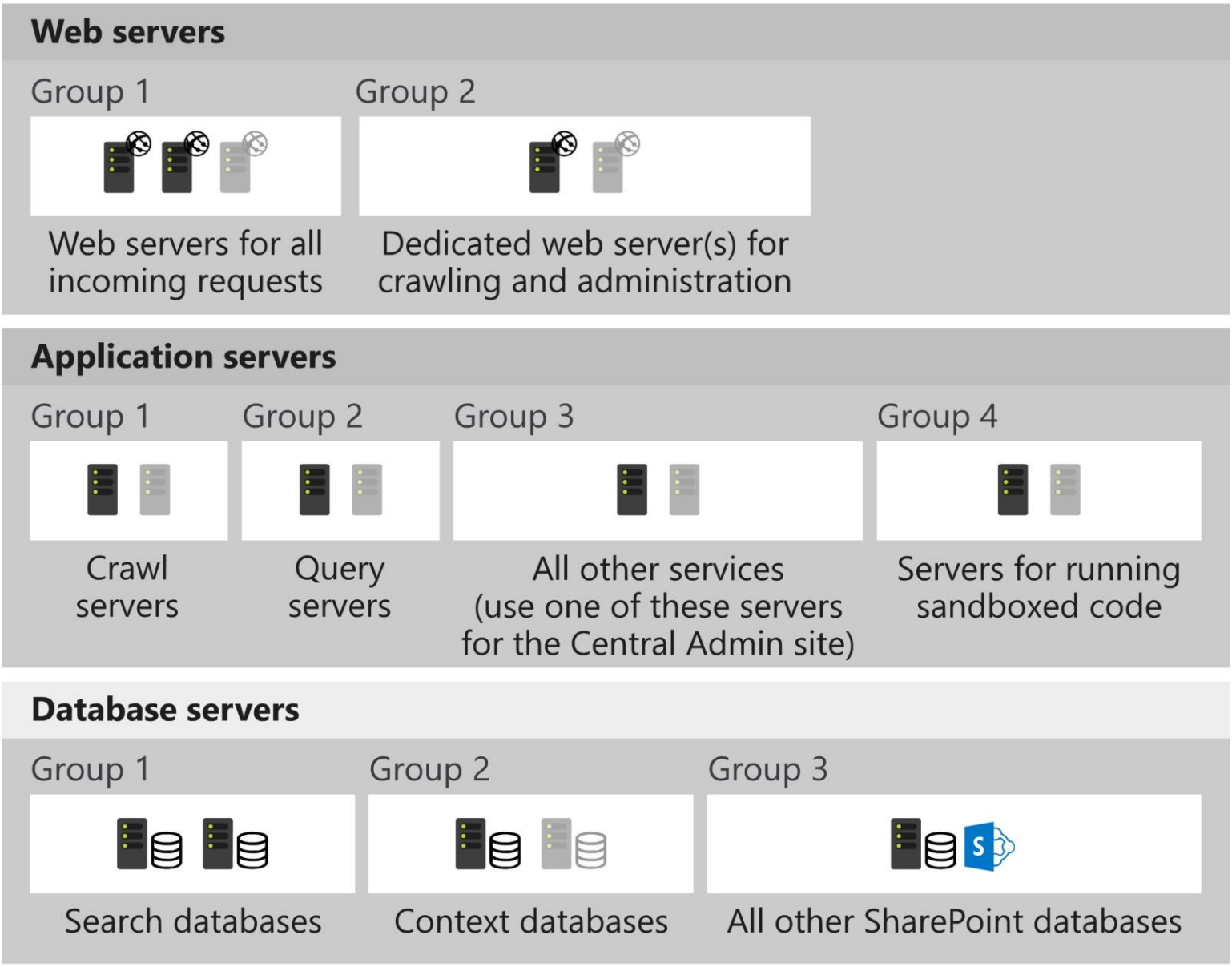
Active Directory and DNS

Active Directory and DNS can be configured for an automated failover. Typically, they're completed first in the scope of the overall recovery plan. In this way, the Active Directory instance and DNS name resolution are available for when the other applications are failed over. You can have Active Directory up and running in a few minutes. Site Recovery protects the virtual machine that hosts your domain controller and DNS.

SQL Server

Site Recovery can be used alongside SQL-specific high-availability technologies, such as Always On availability groups. Standalone servers or clusters are supported for replication to Azure or a secondary site. Azure Site Recovery can also scale peak loads by "bursting" them onto larger VMs in Azure. Test failovers and compliance checks can be run on demand, or can be scheduled, without affecting the live environment.

SharePoint



Protecting SharePoint with Site Recovery allows for all the servers that make up the solution to be failed over at the same time. In the previous example, a high-demand server farm can include web, app, and database server groups. The constant replication to Azure allows any updates deployed to the live environment to be automatically deployed to the replica to allow for patch consistency during a failover.

Dynamics AX

Protecting Dynamics AX involves a similar approach as the one you would take to protect SharePoint because Dynamics consists of web, app, and database tiers. The replica environment could also be used for test and development purposes.

Remote desktop services

Managed or unmanaged pooled virtual desktops, remote applications, and sessions can be replicated to a secondary site or Azure.

Exchange

Small deployments of Exchange, such as those with a single server, can be replicated. For larger deployments, Site Recovery integrates with Exchange database availability groups. This high-availability feature of Exchange 2010 can host up to 16 mailbox servers and automates recovery at the database level.

SAP

SAP NetWeaver and non-NetWeaver production application components can be replicated. The replicated environment can be used as a test bed for project upgrades and testing.

IIS

Protecting IIS allows for full automation of the recovery plan if you need to fail over to the replicated environment. Protection for IIS servers can be easily enabled, and IP addressing can be properly configured by mapping the primary and recovery networks prior to fail over. Scripts can be used during failover to update application dependencies and bindings. This approach enables a one-click failover for multiple web applications on the web servers and eliminates the scope for confusion in the event of a disaster.

Citrix XenApp and XenDesktop

Full protection is available for Citrix by using Site Recovery. You can protect all aspects of your Citrix solution, Active Directory, DNS, SQL Server, and Citrix-specific servers, such as the StoreFront server. They all can be part of the same recovery plan. After replication is in place, you can use the replicated environment as a test platform.

Check your knowledge

1. Which of the following features of Azure Site Recovery aid application workloads in a seamless failover?

App-consistent snapshots, near synchronous replication, SQL Server Always On integration

All three are features within Site Recovery that aid application workloads with failover.

- App-consistent snapshots, flexible recovery plans, database mirroring
- Asynchronous replication, SQL Server Always On integration, database mirroring

2. How does IIS in particular benefit from application replication?

- IIS virtual directory replication, load-balanced site traffic, script integration
- One-click failover, script integration, network mapping

All of the above are features of Site Recovery that support application replication.

- Manual failover and failback only, DHCP network address backup, one-click failover

Next unit: Run a disaster recovery drill

Continue

Run a disaster recovery drill

7 minutes

Disaster recovery drills enable you to test your company's ability to recover from a disaster without affecting production services.

After you produce a business continuity and disaster recovery (BCDR plan), you're asked to explore the options for how the system can be tested without interrupting live service. You want to learn more about recovery drills and how they can verify that your Azure Site Recovery solution is set up and works correctly.

In this unit, you'll gain an understanding of recovery time and recovery point objectives. You'll see how you can then use a recovery drill to test that Azure Site Recovery was configured correctly to meet these objectives.

Disaster recovery drill

With Azure Site Recovery, you can do a full disaster recovery test without affecting your existing live environment. Recovery plans are created within Site Recovery and allow for the automation of recovery tasks, model-specific applications around its dependencies, such as the need for Active Directory or DNS to function. Recovery plans also allow you to test your disaster recovery.

After a recovery plan is created in the Azure portal, it can be executed for test purposes. Follow these steps:

1. In the **Site Recovery** section of the Azure portal, select **Recovery Plans** > your recovery plan name > **Test Failover**.
2. Select the recovery point from the options presented. Options include **Latest processed**, which is the latest recovery point that was processed by Site Recovery.
3. Select the Azure virtual network on which the virtual machine will be created. Use an isolated network from the live environment to prevent any impact to production environments.
4. Track progress in the **Jobs** tab and also in the **Site Recovery** dashboard.

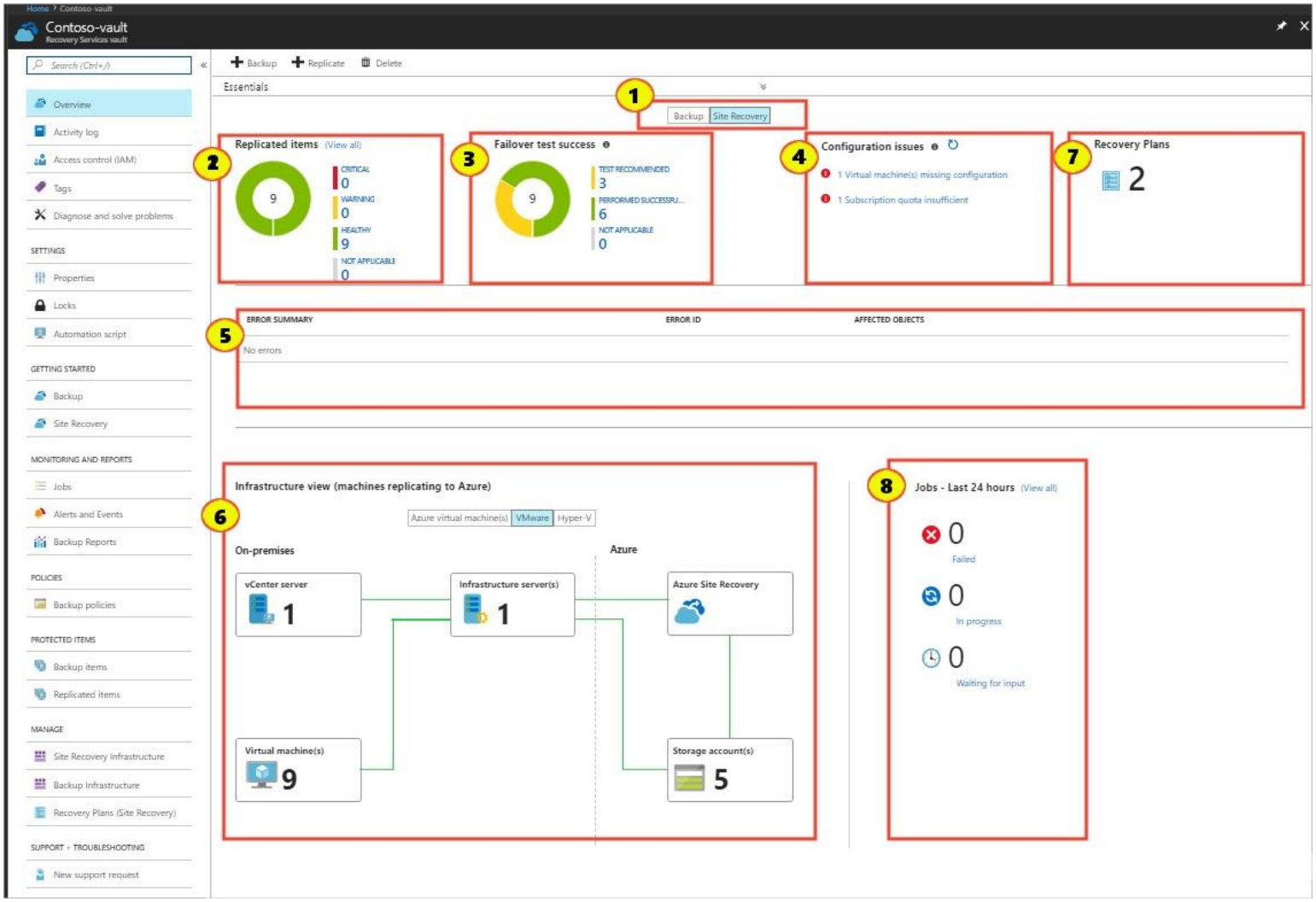
Monitor a test recovery

Use the Site Recovery dashboard to monitor recovery operations, which include recovery drills started under test circumstances. The dashboard is accessed from within the Recovery Services vault by clicking **Overview**.

Tabs are then visible to monitor both Site Recovery and backup operations.

In the dashboard, you can monitor replicated items and test failovers. Each replicated item under both categories is placed into a particular state for easy viewing of a healthy item compared to one with issues.

See the following diagram.



(1) Backup or Site Recovery : Switch between the **Backup** or the **Site Recovery** dashboards. In this example, you're on the **Site Recovery** tab.

(2) Replicated items - **Healthy** : Replication is running normally with no warnings. **Warning** means that one or more issues were identified that could affect replication. **Critical** means that one or more critical replication errors were identified.

(3) Failover test success - **Test recommended** : Specific machines haven't had a failover since Site Recovery protection was enabled. **Performed successfully** means that one or more machines replicated successfully. **Not applicable** means that machines aren't currently eligible for a test failover.

(4) Configuration issues - **Missing configurations** : A necessary setting is missing. **Missing resources** means that a specified resource can't be found or isn't available. An example is a deleted resource such as a virtual network. **Subscription quota** shows the amount of resource available for your subscription and whether there's enough to do a failover. **Software updates** shows the availability of new software updates and information about out-of-date software.

(5) Error summary : Review a summary of errors here for easy access so that you can quickly identify any issues in your environment.

(6) Infrastructure view : See a visualization of your replication infrastructure and a display of health.

(7) Recovery Plans : View recovery plans for your infrastructure.

(8) Jobs - Last 24 hours : See the status of any jobs that are in progress, waiting, or that failed.

Check your knowledge

1. Which of these is the correct meaning of a recovery time objective (RTO)?

- The measure of the maximum amount of data that can be lost during a disaster
- The measure of the time between the disaster starting and the business recovering from the disaster
- The measure of the maximum amount of time the business can survive if a disaster happens

  An RTO is the amount of time that data can be lost via an outage before it impacts the company significantly.
- The measure of the maximum amount of data that's recoverable from a backup

2. When you monitor a recovery from the recovery services vault, which of the following statistics can be viewed on the Site Recovery dashboard?

- Replicated items, monitoring of test failovers, and monitoring of configuration issues

  All of these items can be viewed from the Recovery Services vault dashboard.
- Replicated items, vault status, and network status
- Monitoring of configuration issues, vault status, and DHCP replication status

---

Next unit: Failover and failback

Continue

200 XP

Failover and failback

6 minutes

Azure Site Recovery gives you the flexibility to fail over to Azure if a disaster occurs and fail back to on-premises machines after the event is over.

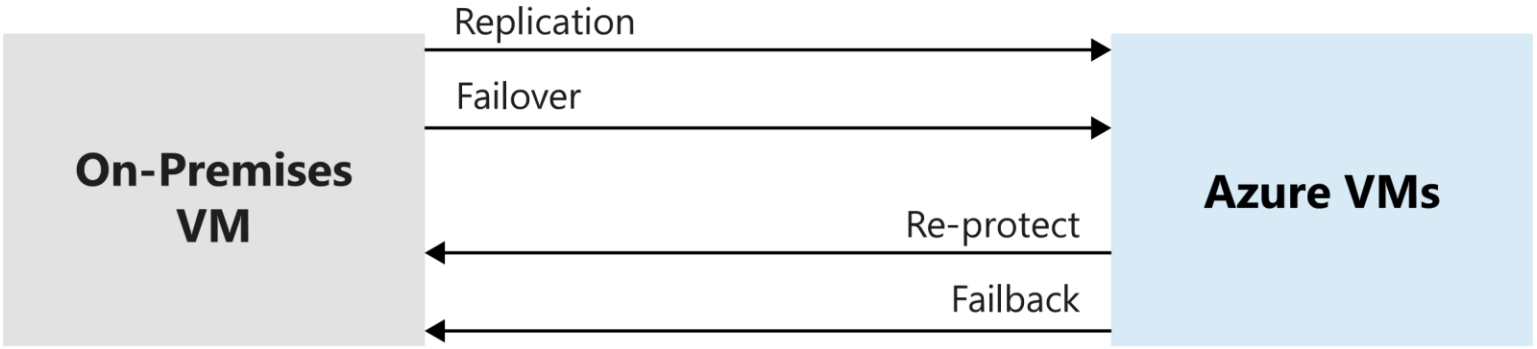
You now want to do a full failover for the rest of the protected environment to Azure. You do a full failover after you successfully run a failover drill on a single test virtual machine. You'll then do the failback after the failover has completed successfully.

In this unit, you'll explore the differences between failover and failback. You'll also learn how you get a failback policy created automatically after you set up a replication policy to Azure.

Failover and failback

A failover is the process that takes place when the decision is made to invoke the disaster recovery plan for the business. Failover happens when the current live environment that's protected by using Azure Site Recovery is moved over to the replica environment. This target replica environment takes the place of the live environment and becomes the primary infrastructure.

A failback is the reverse of a failover. The previous live environment (which is now the replica environment because a failover took place) takes back its original role and becomes the live environment again. After the failover has happened in the first instance, a reprotection phase needs to occur. In this phase, you bring the original environment back into sync with the new live environment. This process allows the failover and failback to happen without any data loss. The reprotection phase is likely to be a lengthy process because you need to establish that the old live environment works correctly after the disaster.



The four stages of failover and failback actions are:

- **Fail over to Azure**: If the on-premises primary site goes down, the decision to fail over to Azure (or your secondary site) is made, which creates virtual machines from the primary replicated data.

Reprotect Azure virtual machines: After the failover occurs, the Azure virtual machines must be reprotected so that they can replicate changes back to the on-premises environment after the disaster is averted. Virtual machines are powered off to ensure data consistency.

Fail back to on-premises: When the on-premises site is back up and running, it's possible to fail over back to that environment. It then becomes the live environment again. You can't fail back to physical servers. All systems must fail back to virtual machines.

Reprotect on-premises virtual machines: Reprotection of the on-premises virtual machines takes place so that they start replicating to Azure after the failback has happened successfully.

Failback policies

When you create an on-premises replication policy to copy your on-premises machines to Azure, an associated failback policy is automatically created for you. The policy has some fixed attributes that can't be changed. These attributes are:

Can only replicate back to your on-premises configuration server.

The recovery point objective is set at 15 minutes.

The recovery point retention is set to 24 hours.

App-consistent snapshots are set to every hour.

Running the failback stops the Azure VMs. After the replication has finished, start your on-premises VM to take over the workloads. Service will be disrupted, so schedule the failback at a time that won't affect your business.

Recovery plans

Recovery plans within Site Recovery allow for the customization and sequencing of failover and failback of virtual machines and the applications that run on them. Machines are grouped together, and recovery actions can be automated with the use of scripts during the failover or failback. You can also add additional manual steps for actions if you need to. If you test the recovery plan before a disaster happens, you can be more confident that you'll have a positive outcome. You'll need to get your infrastructure back up and running again at the secondary location quickly to meet the company's recovery time objective.

Flexible failovers

With the ability to be flexible with failovers, Azure Site Recovery can run failovers on demand for test purposes. Isolating these tests means they won't interrupt live services. This flexibility also allows for a failover to be run during a planned outage of the live service. Users of the system won't notice any interruptions from the outage because they're automatically switched over to the replicated environment. The flexibility works the other way too. Failback on demand can be either as part of a planned test or as part of a fully invoked disaster recovery scenario.

Check your knowledge

1. What is meant by the terms failover and failback in the context of disaster recovery?

- Failover is the transfer of workload from the secondary site to a primary site during a test or disaster recovery scenario. Failback is when the workload gets transferred back to the secondary site.
- Failover is the time taken between discovering there has been a disaster and invoking actual disaster recovery. Failback is the time taken between fixing the disaster and when the environment is running from the primary site again.
- Failover is the transfer of workload to a secondary site during a test or disaster scenario. Failback is when the workload gets transferred back over to the primary site from the secondary site.

These descriptions are correct. A failover is when the primary site fails over to the secondary site, and a failback is the reverse of this.

2. What is the correct order for the four stages of failover and failback when you replicate your on-premises environment to Azure?

- Reprotect Azure virtual machines by replicating back to on-premises. Fail over to the secondary site on Azure. Fail back to the primary on-premises site. Reprotect the on-premises virtual machines by replicating to Azure.
- Fail back to the primary on-premises site. Reprotect the on-premises virtual machines by replicating to Azure. Fail over to the secondary site on Azure. Reprotect the Azure virtual machines by replicating back to on-premises.
- Fail over to the secondary site on Azure. Reprotect the Azure virtual machines by replicating back to on-premises. Fail back to the primary on-premises site. Reprotect the on-premises virtual machines by replicating to Azure.

These are the correct steps in the correct order.

Next unit: Summary

Continue

The first task when you attempt a recovery drill is to verify your test virtual machine properties in the **Protected Items** section of the Azure portal. The latest recovery points are viewed from the **Replicated Item** pane. In the **Compute & Network** section, the virtual machine name, resource group, target size, availability set, and disk settings are adjusted, if needed.

Recovery drills can be started from the **Settings** > **Replicated Items** section of the Azure portal. Select the target virtual machine, and then select the **Test Failover** menu item for the latest processed recovery point. Select the Azure network in the same menu. To start the recovery job, select **OK** on the network selection screen.

The status of the recovery job and the replicated virtual machine is accessed via the **Overview** section of the Recovery Services vault. Replicated items have a status of:

- **Healthy**: Replication is operating normally.
- **Warning**: There's an issue that could impact replication.
- **Critical**: A critical replication error was detected.

If all went well, the replicated VM status is set to **Performed successfully** . If a test hasn't been done, the status is set to **Test recommended** . The VM is also set to **Test recommended** if it's been more than six months since the last test.

Check your knowledge

1. What are the key steps required to set up Azure Site Recovery to protect your on-premises VMs?

- Central management, on-premises virtual machine replication, network integration, app consistency during failover
- Networking, create a Recovery Services vault, give the correct permissions to credentials, install a configuration server in your vCenter via an OVA

  Correct, all of the above are needed to set up Azure Site Recovery correctly.
- Protected Items, Replicated Item, Compute & Network, use an existing Recovery Services vault, Test Failover

2. How should you test the Azure Site Recovery deployment?

- Run a disaster recovery drill for all the protected VMs, on the production network.
- Run a disaster recovery drill for a single isolated VM, on the production network.
- Run a disaster recovery drill for a single isolated VM, on an isolated network.

  Proving the recovery on a single VM, on an isolated network, ensures that live services aren't affected and proves the recoveries are set up correctly.

Next unit: Workloads supported for protection with Azure Site Recovery

Continue