Backup and disaster recovery for Azure IaaS disks

This article explains how to plan for backup and disaster recovery (DR) of IaaS virtual machines (VMs) and disks in Azure. This document covers both managed and unmanaged disks.

First, we cover the built-in fault tolerance capabilities in the Azure platform that helps guard against local failures. We then discuss the disaster scenarios not fully covered by the built-in capabilities. This is the main topic addressed by this document. We also show several examples of workload scenarios where different backup and DR considerations can apply. We then review possible solutions for the DR of IaaS disks.

Introduction

The Azure platform uses various methods for redundancy and fault tolerance to help protect customers from localized hardware failures. Local failures can include problems with an Azure Storage server machine that stores part of the data for a virtual disk or failures of an SSD or HDD on that server. Such isolated hardware component failures can happen during normal operations.

The Azure platform is designed to be resilient to these failures. Major disasters can result in failures or the inaccessibility of many storage servers or even a whole datacenter. Although your VMs and disks are normally protected from localized failures, additional steps are necessary to protect your workload from region-wide catastrophic failures, such as a major disaster, that can affect your VM and disks.

In addition to the possibility of platform failures, problems with a customer application or data can occur. For example, a new version of your application might inadvertently make a change to the data that causes it to break. In that case, you might want to revert the application and the data to a prior version that contains the last known good state. This requires maintaining regular backups.

For regional disaster recovery, you must back up your IaaS VM disks to a different region.

Before we look at backup and DR options, let’s recap a few methods available for handling localized failures.

Azure IaaS resiliency

*Resiliency* refers to the tolerance for normal failures that occur in hardware components. Resiliency is the ability to recover from failures and continue to function. It's not about avoiding failures, but responding to failures in a way that avoids downtime or data loss. The goal of resiliency is to return the application to a fully functioning state following a failure. Azure virtual machines and disks are designed to be resilient to common hardware faults. Let's look at how the Azure IaaS platform provides this resiliency.

A virtual machine consists mainly of two parts: a compute server and the persistent disks. Both affect the fault tolerance of a virtual machine.

If the Azure compute host server that houses your VM experiences a hardware failure, which is rare, Azure is designed to automatically restore the VM on another server. If this happens, your computer reboots, and the VM comes back up after some time. Azure automatically detects such hardware failures and executes recoveries to help ensure the customer VM is available as soon as possible.

Regarding IaaS disks, the durability of data is critical for a persistent storage platform. Azure customers have important business applications running on IaaS, and they depend on the persistence of the data. Azure designs protection for these IaaS disks, with three redundant copies of the data that is stored locally. These copies provide for high durability against local failures. If one of the hardware components that holds your disk fails, your VM is not affected, because there are two additional copies to support disk requests. It works fine, even if two different hardware components that support a disk fail at the same time (which is very rare).

To ensure that you always maintain three replicas, Azure Storage automatically spawns a new copy of the data in the background if one of the three copies becomes unavailable. Therefore, it should not be necessary to use RAID with Azure disks for fault tolerance. A simple RAID 0 configuration should be sufficient for striping the disks, if necessary, to create larger volumes.

Because of this architecture, Azure has consistently delivered enterprise-grade durability for IaaS disks, with an industry-leading zero percent [annualized failure rate](https://en.wikipedia.org/wiki/Annualized_failure_rate).

Localized hardware faults on the compute host or in the Storage platform can sometimes result in of the temporary unavailability of the VM that is covered by the [Azure SLA](https://azure.microsoft.com/support/legal/sla/virtual-machines/) for VM availability. Azure also provides an industry-leading SLA for single VM instances that use Azure Premium Storage disks.

To safeguard application workloads from downtime due to the temporary unavailability of a disk or VM, customers can use [availability sets](https://docs.microsoft.com/en-in/azure/virtual-machines/windows/manage-availability). Two or more virtual machines in an availability set provide redundancy for the application. Azure then creates these VMs and disks in separate fault domains with different power, network, and server components.

Because of these separate fault domains, localized hardware failures typically do not affect multiple VMs in the set at the same time. Having separate fault domains provides high availability for your application. It's considered a good practice to use availability sets when high availability is required. The next section covers the disaster recovery aspect.

Backup and disaster recovery

Disaster recovery is the ability to recover from rare, but major, incidents. This includes non-transient, wide-scale failures, such as service disruption that affects an entire region. Disaster recovery includes data backup and archiving, and might include manual intervention, such as restoring a database from a backup.

The Azure platform’s built-in protection against localized failures might not fully protect the VMs/disks if a major disaster causes large-scale outages. This includes catastrophic events, such as if a datacenter is hit by a hurricane, earthquake, fire, or if there is a large-scale hardware unit failures. In addition, you might encounter failures due to application or data issues.

To help protect your IaaS workloads from outages, you should plan for redundancy and have backups to enable recovery. For disaster recovery, you should back up in a different geographic location away from the primary site. This helps ensure your backup is not affected by the same event that originally affected the VM or disks. For more information, see [Disaster recovery for Azure applications](https://docs.microsoft.com/en-us/azure/architecture/resiliency/disaster-recovery-azure-applications).

Your DR considerations might include the following aspects:

* High availability: The ability of the application to continue running in a healthy state, without significant downtime. By *healthy state*, we mean the application is responsive, and users can connect to the application and interact with it. Certain mission-critical applications and databases might be required to always be available, even when there are failures in the platform. For these workloads, you might need to plan redundancy for the application, as well as the data.
* Data durability: In some cases, the main consideration is ensuring that the data is preserved if a disaster happens. Therefore, you might need a backup of your data in a different site. For such workloads, you might not need full redundancy for the application, but only a regular backup of the disks.

Backup and DR scenarios

Let’s look at a few typical examples of application workload scenarios and the considerations for planning for disaster recovery.

Scenario 1: Major database solutions

Consider a production database server, like SQL Server or Oracle, that can support high availability. Critical production applications and users depend on this database. The disaster recovery plan for this system might need to support the following requirements:

* The data must be protected and recoverable.
* The server must be available for use.

The disaster recovery plan might require maintaining a replica of the database in a different region as a backup. Depending on the requirements for server availability and data recovery, the solution might range from an active-active or active-passive replica site to periodic offline backups of the data. Relational databases, such as SQL Server and Oracle, provide various options for replication. For SQL Server, use [SQL Server AlwaysOn Availability Groups](https://msdn.microsoft.com/library/hh510230.aspx) for high availability.

NoSQL databases, like MongoDB, also support [replicas](https://docs.mongodb.com/manual/replication/) for redundancy. The replicas for high availability are used.

Scenario 2: A cluster of redundant VMs

Consider a workload handled by a cluster of VMs that provide redundancy and load balancing. One example is a Cassandra cluster deployed in a region. This type of architecture already provides a high level of redundancy within that region. However, to protect the workload from a regional-level failure, you should consider spreading the cluster across two regions or making periodic backups to another region.

Scenario 3: IaaS application workload

Let's look at the IaaS application workload. For example, this might be a typical production workload running on an Azure VM. It might be a web server or file server holding the content and other resources of a site. It might also be a custom-built business application running on a VM that stored its data, resources, and application state on the VM disks. In this case, it's important to make sure you take backups on a regular basis. Backup frequency should be based on the nature of the VM workload. For example, if the application runs every day and modifies data, then the backup should be taken every hour.

Another example is a reporting server that pulls data from other sources and generates aggregated reports. The loss of this VM or disks might lead to the loss of the reports. However, it might be possible to rerun the reporting process and regenerate the output. In that case, you don’t really have a loss of data, even if the reporting server is hit with a disaster. As a result, you might have a higher level of tolerance for losing part of the data on the reporting server. In that case, less frequent backups are an option to reduce costs.

Scenario 4: IaaS application data issues

IaaS application data issues are another possibility. Consider an application that computes, maintains, and serves critical commercial data, such as pricing information. A new version of your application had a software bug that incorrectly computed the pricing and corrupted the existing commerce data served by the platform. Here, the best course of action is to revert to the earlier version of the application and the data. To enable this, take periodic backups of your system.

Disaster recovery solution: Azure Backup

[Azure Backup](https://azure.microsoft.com/services/backup/) is used for backups and DR, and it works with [managed disks](https://docs.microsoft.com/en-in/azure/virtual-machines/windows/managed-disks-overview) as well as [unmanaged disks](https://docs.microsoft.com/en-in/azure/virtual-machines/windows/about-disks-and-vhds#unmanaged-disks). You can create a backup job with time-based backups, easy VM restoration, and backup retention policies.

If you use [Premium Storage disks](https://docs.microsoft.com/en-in/azure/virtual-machines/windows/premium-storage), [managed disks](https://docs.microsoft.com/en-in/azure/virtual-machines/windows/managed-disks-overview), or other disk types with the [locally redundant storage](https://docs.microsoft.com/en-in/azure/storage/common/storage-redundancy#locally-redundant-storage) option, it's especially important to make periodic DR backups. Azure Backup stores the data in your recovery services vault for long-term retention. Choose the [geo-redundant storage](https://docs.microsoft.com/en-in/azure/storage/common/storage-redundancy#geo-redundant-storage)option for the backup recovery services vault. That option ensures that backups are replicated to a different Azure region for safeguarding from regional disasters.

For [unmanaged disks](https://docs.microsoft.com/en-in/azure/virtual-machines/windows/about-disks-and-vhds#unmanaged-disks), you can use the locally redundant storage type for IaaS disks, but ensure that Azure Backup is enabled with the geo-redundant storage option for the recovery services vault.

Note

If you use the [geo-redundant storage](https://docs.microsoft.com/en-in/azure/storage/common/storage-redundancy#geo-redundant-storage) or [read-access geo-redundant storage](https://docs.microsoft.com/en-in/azure/storage/common/storage-redundancy#read-access-geo-redundant-storage) option for your unmanaged disks, you still need consistent snapshots for backup and DR. Use either [Azure Backup](https://azure.microsoft.com/services/backup/) or [consistent snapshots](https://docs.microsoft.com/en-in/azure/virtual-machines/windows/backup-and-disaster-recovery-for-azure-iaas-disks#alternative-solution-consistent-snapshots).

The following table is a summary of the solutions available for DR.

| Scenario | Automatic replication | DR solution |
| --- | --- | --- |
| Premium Storage disks | Local ([locally redundant storage](https://docs.microsoft.com/en-in/azure/storage/common/storage-redundancy#locally-redundant-storage)) | [Azure Backup](https://azure.microsoft.com/services/backup/) |
| Managed disks | Local ([locally redundant storage](https://docs.microsoft.com/en-in/azure/storage/common/storage-redundancy#locally-redundant-storage)) | [Azure Backup](https://azure.microsoft.com/services/backup/) |
| Unmanaged locally redundant storage disks | Local ([locally redundant storage](https://docs.microsoft.com/en-in/azure/storage/common/storage-redundancy#locally-redundant-storage)) | [Azure Backup](https://azure.microsoft.com/services/backup/) |
| Unmanaged geo-redundant storage disks | Cross region ([geo-redundant storage](https://docs.microsoft.com/en-in/azure/storage/common/storage-redundancy#geo-redundant-storage)) | [Azure Backup](https://azure.microsoft.com/services/backup/) [Consistent snapshots](https://docs.microsoft.com/en-in/azure/virtual-machines/windows/backup-and-disaster-recovery-for-azure-iaas-disks#alternative-solution-consistent-snapshots) |
| Unmanaged read-access geo-redundant storage disks | Cross region ([read-access geo-redundant storage](https://docs.microsoft.com/en-in/azure/storage/common/storage-redundancy#read-access-geo-redundant-storage)) | [Azure Backup](https://azure.microsoft.com/services/backup/) [Consistent snapshots](https://docs.microsoft.com/en-in/azure/virtual-machines/windows/backup-and-disaster-recovery-for-azure-iaas-disks#alternative-solution-consistent-snapshots) |

High availability is best met by using managed disks in an availability set along with Azure Backup. If you use unmanaged disks, you can still use Azure Backup for DR. If you are unable to use Azure Backup, then taking [consistent snapshots](https://docs.microsoft.com/en-in/azure/virtual-machines/windows/backup-and-disaster-recovery-for-azure-iaas-disks#alternative-solution-consistent-snapshots), as described in a later section, is an alternative solution for backup and DR.

Your choices for high availability, backup, and DR at application or infrastructure levels can be represented as follows:

| Level | High availability | Backup or DR |
| --- | --- | --- |
| Application | SQL Server AlwaysOn | Azure Backup |
| Infrastructure | Availability set | Geo-redundant storage with consistent snapshots |

Using Azure Backup

[Azure Backup](https://docs.microsoft.com/en-in/azure/backup/backup-azure-vms-introduction) can back up your VMs running Windows or Linux to the Azure recovery services vault. Backing up and restoring business-critical data is complicated by the fact that business-critical data must be backed up while the applications that produce the data are running.

To address this issue, Azure Backup provides application-consistent backups for Microsoft workloads. It uses the volume shadow service to ensure that data is written correctly to storage. For Linux VMs, only file-consistent backups are possible, because Linux does not have functionality equivalent to the volume shadow service.

When Azure Backup initiates a backup job at the scheduled time, it triggers the backup extension installed in the VM to take a point-in-time snapshot. A snapshot is taken in coordination with the volume shadow service to get a consistent snapshot of the disks in the virtual machine without having to shut it down. The backup extension in the VM flushes all writes before taking a consistent snapshot of all of the disks. After taking the snapshot, the data is transferred by Azure Backup to the backup vault. To make the backup process more efficient, the service identifies and transfers only the blocks of data that have changed after the last backup.

To restore, you can view the available backups through Azure Backup and then initiate a restore. You can create and restore Azure backups through the [Azure portal](https://portal.azure.com/), by [using PowerShell](https://docs.microsoft.com/en-in/azure/backup/backup-azure-vms-automation), or by using the [Azure CLI](https://docs.microsoft.com/en-us/cli/azure/).

Steps to enable a backup

Use the following steps to enable backups of your VMs by using the [Azure portal](https://portal.azure.com/). There is some variation depending on your exact scenario. Refer to the [Azure Backup](https://docs.microsoft.com/en-in/azure/backup/backup-azure-vms-introduction) documentation for full details. Azure Backup also [supports VMs with managed disks](https://azure.microsoft.com/blog/azure-managed-disk-backup/).

1. Create a recovery services vault for a VM:

a. In the [Azure portal](https://portal.azure.com/), browse **All resources** and find **Recovery Services vaults**.

b. On the **Recovery Services vaults** menu, click **Add** and follow the steps to create a new vault in the same region as the VM. For example, if your VM is in the West US region, pick West US for the vault.

1. Verify the storage replication for the newly created vault. Access the vault under **Recovery Services vaults** and go to **Settings** > **Backup Configuration**. Ensure the **geo-redundant storage** option is selected by default. This ensures that your vault is automatically replicated to a secondary datacenter. For example, your vault in West US is automatically replicated to East US.
2. Configure the backup policy and select the VM from the same UI.
3. Make sure the Backup Agent is installed on the VM. If your VM is created by using an Azure gallery image, then the Backup Agent is already installed. Otherwise (that is, if you use a custom image), use the instructions to [install the VM agent on a virtual machine](https://docs.microsoft.com/en-in/azure/backup/backup-azure-arm-vms-prepare#install-the-vm-agent-on-the-virtual-machine).
4. Make sure that the VM allows network connectivity for the backup service to function. Follow the instructions for [network connectivity](https://docs.microsoft.com/en-in/azure/backup/backup-azure-arm-vms-prepare#network-connectivity).
5. After the previous steps are completed, the backup runs at regular intervals as specified in the backup policy. If necessary, you can trigger the first backup manually from the vault dashboard on the Azure portal.

For automating Azure Backup by using scripts, refer to [PowerShell cmdlets for VM backup](https://docs.microsoft.com/en-in/azure/backup/backup-azure-vms-automation).

Steps for recovery

If you need to repair or rebuild a VM, you can restore the VM from any of the backup recovery points in the vault. There are a couple of different options for performing the recovery:

* You can create a new VM as a point-in-time representation of your backed-up VM.
* You can restore the disks, and then use the template for the VM to customize and rebuild the restored VM.

For more information, see the instructions to [use the Azure portal to restore virtual machines](https://docs.microsoft.com/en-in/azure/backup/backup-azure-arm-restore-vms). This document also explains the specific steps for restoring backed-up VMs to a paired datacenter by using your geo-redundant backup vault if there is a disaster at the primary datacenter. In that case, Azure Backup uses the Compute service from the secondary region to create the restored virtual machine.

You can also use PowerShell for [restoring a VM](https://docs.microsoft.com/en-in/azure/backup/backup-azure-arm-restore-vms#restore-a-vm-during-an-azure-datacenter-disaster) or for [creating a new VM from restored disks](https://docs.microsoft.com/en-in/azure/backup/backup-azure-vms-automation#create-a-vm-from-restored-disks).

Alternative solution: Consistent snapshots

If you are unable to use Azure Backup, you can implement your own backup mechanism by using snapshots. Creating consistent snapshots for all the disks used by a VM and then replicating those snapshots to another region is complicated. For this reason, Azure considers using the Backup service as a better option than building a custom solution.

If you use read-access geo-redundant storage/geo-redundant storage for disks, snapshots are automatically replicated to a secondary datacenter. If you use locally redundant storage for disks, you need to replicate the data yourself. For more information, see [Back up Azure-unmanaged VM disks with incremental snapshots](https://docs.microsoft.com/en-in/azure/virtual-machines/windows/incremental-snapshots).

A snapshot is a representation of an object at a specific point in time. A snapshot incurs billing for the incremental size of the data it holds. For more information, see [Create a blob snapshot](https://docs.microsoft.com/en-in/azure/storage/blobs/storage-blob-snapshots).

Create snapshots while the VM is running

Although you can take a snapshot at any time, if the VM is running, there is still data being streamed to the disks, and the snapshots might contain partial operations that were in flight. Also, if there are several disks involved, the snapshots of different disks might have occurred at different times. This means these snapshots might not be coordinated. This is especially problematic for striped volumes whose files might be corrupted if changes were being made during backup.

To avoid this situation, the backup process must implement the following steps:

1. Freeze all the disks.
2. Flush all the pending writes.
3. [Create a blob snapshot](https://docs.microsoft.com/en-in/azure/storage/blobs/storage-blob-snapshots) for all the disks.

Some Windows applications, like SQL Server, provide a coordinated backup mechanism via a volume shadow service to create application-consistent backups. On Linux, you can use a tool like fsfreeze for coordinating the disks. This tool provides file-consistent backups, but not application-consistent snapshots. This process is complex, so you should consider using [Azure Backup](https://docs.microsoft.com/en-in/azure/backup/backup-azure-vms-introduction) or a third-party backup solution that already implements this procedure.

The previous process results in a collection of coordinated snapshots for all of the VM disks, representing a specific point-in-time view of the VM. This is a backup restore point for the VM. You can repeat the process at scheduled intervals to create periodic backups. See [Copy the backups to another region](https://docs.microsoft.com/en-in/azure/virtual-machines/windows/backup-and-disaster-recovery-for-azure-iaas-disks#copy-the-snapshots-to-another-region) for steps to copy the snapshots to another region for DR.

Create snapshots while the VM is offline

Another option to create consistent backups is to shut down the VM and take blob snapshots of each disk. Taking blob snapshots is easier than coordinating snapshots of a running VM, but it requires a few minutes of downtime.

1. Shut down the VM.
2. Create a snapshot of each virtual hard drive blob, which only takes a few seconds.

To create a snapshot, you can use [PowerShell](https://docs.microsoft.com/en-in/azure/storage/common/storage-powershell-guide-full), the [Azure Storage REST API](https://msdn.microsoft.com/library/azure/ee691971.aspx), [Azure CLI](https://docs.microsoft.com/en-us/cli/azure/), or one of the Azure Storage client libraries, such as [the Storage client library for .NET](https://msdn.microsoft.com/library/azure/hh488361.aspx).

1. Start the VM, which ends the downtime. Typically, the entire process finishes within a few minutes.

This process yields a collection of consistent snapshots for all the disks, providing a backup restore point for the VM.

Copy the snapshots to another region

Creation of the snapshots alone might not be sufficient for DR. You must also replicate the snapshot backups to another region.

If you use geo-redundant storage or read-access geo-redundant storage for your disks, then the snapshots are replicated to the secondary region automatically. There can be a few minutes of lag before the replication. If the primary datacenter goes down before the snapshots finish replicating, you cannot access the snapshots from the secondary datacenter. The likelihood of this is small.

Note

Only having the disks in a geo-redundant storage or read-access geo-redundant storage account does not protect the VM from disasters. You must also create coordinated snapshots or use Azure Backup. This is required to recover a VM to a consistent state.

If you use locally redundant storage, you must copy the snapshots to a different storage account immediately after creating the snapshot. The copy target might be a locally redundant storage account in a different region, resulting in the copy being in a remote region. You can also copy the snapshot to a read-access geo-redundant storage account in the same region. In this case, the snapshot is lazily replicated to the remote secondary region. Your backup is protected from disasters at the primary site after the copying and replication is complete.

To copy your incremental snapshots for DR efficiently, review the instructions in [Back up Azure unmanaged VM disks with incremental snapshots](https://docs.microsoft.com/en-in/azure/virtual-machines/windows/incremental-snapshots).

Recovery from snapshots

To retrieve a snapshot, copy it to make a new blob. If you are copying the snapshot from the primary account, you can copy the snapshot over to the base blob of the snapshot. This process reverts the disk to the snapshot. This process is known as promoting the snapshot. If you are copying the snapshot backup from a secondary account, in the case of a read-access geo-redundant storage account, you must copy it to a primary account. You can copy a snapshot by [using PowerShell](https://docs.microsoft.com/en-in/azure/storage/common/storage-powershell-guide-full) or by using the AzCopy utility. For more information, see [Transfer data with the AzCopy command-line utility](https://docs.microsoft.com/azure/storage/common/storage-use-azcopy).

For VMs with multiple disks, you must copy all the snapshots that are part of the same coordinated restore point. After you copy the snapshots to writable VHD blobs, you can use the blobs to recreate your VM by using the template for the VM.

Other options

SQL Server

SQL Server running in a VM has its own built-in capabilities to back up your SQL Server database to Azure Blob storage or a file share. If the storage account is geo-redundant storage or read-access geo-redundant storage, you can access those backups in the storage account’s secondary datacenter in the event of a disaster, with the same restrictions as previously discussed. For more information, see [Back up and restore for SQL Server in Azure virtual machines](https://docs.microsoft.com/en-in/azure/virtual-machines/windows/sql/virtual-machines-windows-sql-backup-recovery). In addition to back up and restore, [SQL Server AlwaysOn availability groups](https://docs.microsoft.com/en-in/azure/virtual-machines/windows/sql/virtual-machines-windows-sql-high-availability-dr) can maintain secondary replicas of databases. This greatly reduces the disaster recovery time.

Other considerations

This article has discussed how to back up or take snapshots of your VMs and their disks to support disaster recovery and how to use those to recover your data. With the Azure Resource Manager model, many people use templates to create their VMs and other infrastructures in Azure. You can use a template to create a VM that has the same configuration every time. If you use custom images for creating your VMs, you must also make sure that your images are protected by using a read-access geo-redundant storage account to store them.

Consequently, your backup process can be a combination of two things:

* Back up the data (disks).
* Back up the configuration (templates and custom images).

Depending on the backup option you choose, you might have to handle the backup of both the data and the configuration, or the backup service might handle all of that for you.

Appendix: Understanding the impact of data redundancy

For storage accounts in Azure, there are three types of data redundancy that you should consider regarding disaster recovery: locally redundant, geo-redundant, or geo-redundant with read access.

Locally redundant storage retains three copies of the data in the same datacenter. When the VM writes the data, all three copies are updated before success is returned to the caller, so you know they are identical. Your disk is protected from local failures, because it's extremely unlikely that all three copies are affected at the same time. In the case of locally redundant storage, there is no geo-redundancy, so the disk is not protected from catastrophic failures that can affect an entire datacenter or storage unit.

With geo-redundant storage and read-access geo-redundant storage, three copies of your data are retained in the primary region that is selected by you. Three more copies of your data are retained in a corresponding secondary region that is set by Azure. For example, if you store data in West US, the data is replicated to East US. Copy retention is done asynchronously, and there is a small delay between updates to the primary and secondary sites. Replicas of the disks on the secondary site are consistent on a per-disk basis (with the delay), but replicas of multiple active disks might not be in sync with each other. To have consistent replicas across multiple disks, consistent snapshots are needed.

The main difference between geo-redundant storage and read-access geo-redundant storage is that with read-access geo-redundant storage, you can read the secondary copy at any time. If there is a problem that renders the data in the primary region inaccessible, the Azure team makes every effort to restore access. While the primary is down, if you have read-access geo-redundant storage enabled, you can access the data in the secondary datacenter. Therefore, if you plan to read from the replica while the primary is inaccessible, then read-access geo-redundant storage should be considered.

If it turns out to be a significant outage, the Azure team might trigger a geo-failover and change the primary DNS entries to point to secondary storage. At this point, if you have either geo-redundant storage or read-access geo-redundant storage enabled, you can access the data in the region that used to be the secondary. In other words, if your storage account is geo-redundant storage and there is a problem, you can access the secondary storage only if there is a geo-failover.

For more information, see [What to do if an Azure Storage outage occurs](https://docs.microsoft.com/en-in/azure/storage/common/storage-disaster-recovery-guidance).

Note

Microsoft controls whether a failover occurs. Failover is not controlled per storage account, so it's not decided by individual customers. To implement disaster recovery for specific storage accounts or virtual machine disks, you must use the techniques described previously in this article.