<https://www.getorchestra.io/guides/what-is-azure-orchestration-data-orchestration-tooling>

High Availbility

Disaster Recovery

Fault Tolerance

In Azure, fault tolerance refers to a system's ability to continue operating uninterrupted even when components fail, ensuring high availability and resilience. This is achieved through various mechanisms like redundancy, replication, and failover capabilities.

Here's a more detailed explanation:

Key Concepts:

* **Definition:**

Fault tolerance is the property that enables a system to continue operating properly in the event of the failure of (or one or more faults within) some of its components.

* **Importance:**

It's a crucial aspect of building reliable and resilient applications in the cloud, minimizing downtime and ensuring business continuity.

* **Achieving Fault Tolerance in Azure:**

Azure offers several features and services to enable fault tolerance:

* + **Availability Zones:** Deploying resources across multiple, physically isolated zones within a region can protect against datacenter failures.
  + **Availability Sets:** Distributing virtual machines across different fault domains and update domains within a region can prevent failures from affecting all VMs.
  + **Region Pairs:** Replicating data and resources to a secondary region can provide disaster recovery capabilities and protect against regional outages.
  + **Managed Disks:** These provide high availability and durability by replicating data three times within the same region.
  + **Storage Spaces Direct:** This feature provides fault tolerance and storage efficiency for virtualized storage environments.
  + **Azure NetApp Files:** This service offers built-in high availability, RAID technologies, and cross-region replication for fault-tolerant storage.
  + **Azure VMware Solution:** Fault domains in Azure VMware Solution help improve availability in various failure scenarios.
  + **Azure App Service:** Deploy multiple instances of your plan, use deployment slots, and avoid scaling up or down to mitigate transient faults.
  + **Azure Data Factory & Azure Synapse:** Configure fault tolerance in Copy activity in a pipeline.
  + **Azure Relay:** Applications can generally reconnect automatically if they are configured to handle transient faults using retry policies.

Examples:

* **Web Application:**

Deploying a web application across multiple virtual machines in different availability sets ensures that if one VM fails, the others can continue serving traffic.

* **Database Server:**

Using a database service with built-in replication or setting up a failover cluster can ensure that the database remains available even if one instance fails.

* **Disaster Recovery:**

Replicating virtual machines and data to a secondary region allows for quick recovery in the event of a regional outage.

**Disaster recovery in action**

Let’s say a natural disaster, such as a flood, destroys an organization’s primary datacenter. If that organization has a disaster recovery strategy in place, it’s much more likely to recover essential data. There are a few different methods for backup that the organization could have employed ahead of time to quickly recover from this scenario:

* **Replication** of critical data at a secondary datacenter at a different physical location. Replication is when data is perpetually copied to another datacenter. Often, the secondary datacenter is owned by a cloud services provider.
* A **removable drive** stored at the primary datacenter. If removed before a disaster occurs, the drive can be used to restore the data at another datacenter.
* An **offsite** **datacenter**that stores data at a secondary datacenter. A secondary datacenter should be far enough away from the primary datacenter that it wouldn’t be affected by the same disaster. Using this method requires the data to be backed up to the offsite center regularly.
* A**cloud-based backup** service, such as Azure Backup, that automatically backs up the data to the cloud. This method is often more cost-effective than on-premises options.

These backup methods are also effective if your organization’s data is compromised from a security breach. Take, for example, a ransomware attack. During a ransomware attack, a cybercriminal installs malicious software that that locks sensitive data and/or business critical systems and demands a ransom for access. If your organization has securely backed up its critical data using one of the methods outlined above, the potential impact of ransomware and other cyberattacks can be greatly lessened.

**Creating a disaster recovery plan**

Disaster recovery planning starts with the formation of a **disaster recovery team**toidentify critical systems and data. That team should draft the **disaster recovery plan**around ensuring that data is as secure as possible to prevent losses, and corrective measures that ensure access and critical data is regained as soon as possible if it’s lost.

A disaster recovery plan should prioritize two key metrics: **recovery time objective (RTO)** and **recovery point objective (RPO)**:

* **RTO** determines the amount of time that it takes your organization to restore essential access, data, and functionalities after a technology-related disaster.
* **RPO**, on the other hand, refers to the amount of time it can take your organization to restore essential functionalities and access to data before incurring major losses. RPO determines how often you should back up essential data. For example, if your organization’s RPO is four hours, your critical data should be backed up at least every 4 hours.

After you’ve outlined a disaster recovery plan to achieve RPO, you’ll need to fine-tune it. Here are some disaster recovery best practices:

1. Take compliance and regulatory considerations into account when drafting and updating your disaster recovery plans. In many regions, data privacy laws require disaster recovery plans are in place to protect sensitive data. These laws and regulations should be an integral part of your organization’s disaster recovery strategy. Failure to quickly recover compromised data after a disaster can lead to compliance violations and fines.
2. Test your disaster recovery plan regularly and work to identify emerging new threats. It’s not enough to have a disaster recovery plan in place: regularly test the plan and adjust it as new threats emerge. This ensures that you’re not caught off guard by the scale or novelty of a technology-related disaster.
3. Train employees on disaster recovery procedures. Employees that are prepared for a disaster in advance are much more likely to successfully execute their role during disaster recovery.

As outlined in the previous section, there are a few different methods for achieving data redundancy. Your disaster recovery team should determine which of them would be the most effective way to back up essential data based on RPO. There are also several cloud-based solutions that can help. Here are a few to consider while drafting a disaster recovery plan:

* **Backup and disaster recovery solutions** back up data by storing it in the cloud. Cloud services providers like Azure offer end-to-end backup that’s scalable and secure.
* **Virtualization** is a service that backs up data and entire computing environments using virtual machines. This allows employees to quickly access their files and work environments if the primary datacenter fails.
* **VMware backup**solutions help you back up Vmware VMs to the cloud. Vmware VMs can be backed up to Azure using Microsoft Azure Backup Servers.

These represent just a few of the many cloud disaster recovery solutions available. As you outline your disaster recovery plan, you should choose methods and solutions that protect the most important types of data at your organization. That said, regardless of your backup and recovery needs, disaster recovery in the cloud is typically more cost-effective than relying on a second on-premises datacenter.

**How Azure can help with cloud-based disaster recovery**

Azure offers several disaster recovery services and solutions:

* [**Backup and disaster recovery**](https://azure.microsoft.com/en-us/solutions/backup-and-disaster-recovery/)is an end-to-end solution that’s simple, secure, and cost-effective. Azure disaster and backup recovery solutions can be integrated with your on-premises data protection.
* [**Azure Backup**](https://azure.microsoft.com/en-us/products/backup/) helps protect against ransomware and other threats. It’s cost-effective compared to on-premises backup options and scalable based on your needs.
* [**Azure Site Recovery**](https://azure.microsoft.com/en-us/products/site-recovery/)isthe native disaster recovery as a service that’s built into Azure. Azure Site Recovery works by replicating your Azure VMs to a datacenter in a different region.
* **JetStream DR** is a cloud-native disaster recovery solution designed to minimize the downtime of your VMware workloads and virtual machines when there’s a disaster.

Yes, Azure Functions supports zone redundancy when deployed on Premium (Elastic Premium) or Dedicated (App Service) plans, ensuring your function app instances are automatically distributed across three availability zones in the selected region for higher availability.

Here's a more detailed explanation:

* **Zone Redundancy in Azure Functions:**

When you configure your Azure Functions app as zone-redundant, the platform automatically distributes the function app instances across three separate availability zones within the same Azure region.

* **Availability Zones:**

These are physically separate locations within an Azure region, each with independent power, cooling, and networking, designed to withstand failures in one zone without impacting the others.

* **Supported Plans:**

Zone redundancy is available for Azure Functions apps deployed on Premium (Elastic Premium) and Dedicated (App Service) plans.

* **How to Enable:**
  + **Create a new plan:** When creating a new Premium or Dedicated plan, ensure you enable zone redundancy during the configuration process.
  + **Migrate existing app:** You can also migrate an existing function app to a newly created availability zone-enabled Premium plan.
* **Benefits:**
  + **High Availability:** Zone redundancy helps ensure that your function app remains highly available even if one or more zones experience a failure.
  + **Resilience:** Your application is protected from datacenter failures within a region.
  + **Data Durability:** Azure Functions, when configured with zone-redundant storage, ensures data durability across multiple zones.