Table of Contents

# About this Guide

Use this guide to define and implement disaster recovery capabilities for your Azure services. This guide will focus on the technical solution implementation of disaster recovery capabilities in Azure as part of the customers larger disaster recovery plan.

## Audience

Use this guide to design, set up and configure Azure Disaster Recovery for your application or service.

The content in this guide is appropriate for use by (but not strictly limited to) individuals with the following areas of responsibility:

* Network Architects
* Enterprise Architects
* IT Architects
* Systems/Network Administrators
* CISO
* Security Architect

Use the following activities to evaluate your needs in terms of business continuity and implement appropriate disaster recovery capabilities:

* [Disaster Recovery Planning](1.0-Disaster-Recovery-Planning.md): Use the information in this section to define the scope and requirements in terms of business continuity.
* [Azure Disaster Recovery Implementation](2.0-Azure-Disaster-Recovery-Implementation.md): Use the information in this section to define the disaster recovery strategies for each cloud service.
* [Azure Disaster Recovery Simulation and Gap Analysis]3.0-Azure-Disaster-Recovery-Simulation-and-Gap-Analysis.md): Use the information in this section to define and execute a disaster recovery simulation and identify gaps and mitigation approaches.

## Next Steps

* [Disaster Recovery Planning](1.0-Disaster-Recovery-Planning.md)

# Disaster Recovery Planning

Disaster recovery relates to measures taken to ensure that operations can be resumed in the event of a catastrophic failure such as the loss of a primary data center.

## Guidance

The Business Impact Assessment (BIA) and Risk Assessment (RA) define requirements in terms of people, process, and technology in support of business continuity and disaster recovery.

Establish a cross-functional disaster recovery Team. Key stakeholders participation during DR planning is critical to understanding and weighing business, compliance, risk and technical considerations when planning for Disaster Recovery. Stakeholders should include, at a minimum: Business Stakeholders, Risk & Compliance, and IT Application and Infrastructure.

## Next Steps

### 1. Conduct a [Business Impact and Risk Assessment](1.1-Business-Impact-and-Risk-Assessment.md)

* Conduct a Business Impact and Risk Assessment to define recovery time objectives and recovery point objectives for key business functions and processes.
* Conduct a [Technical Dependency Analysis](1.2-Technical-Dependency-Analysis.md) to identify the technology services and applications used to delivery the business functions and processes in scope and their existing recovery capabilities, and gaps to the stated business recovery objectives.
* Conduct a [Component Failure Analysis](1.3-Component-Failure-Analysis.md) to identify high impact services and single points of failure.

# Business Impact and Risk Assessment

# Guidance

Disaster recovery planning begin with identifying maximum amount of time a service can be unavailable and the maximum acceptable data loss. The times are expressed as the recovery time objective recovery point objective, respectively:

* Recovery Time Objective (RTO): measures the duration of the outage between the time the outage is declared and full restoration of the service to the point that new transactions can take place.
* Recovery Point Objective (RPO): the time gap or latency between the last committed data transaction before the failure and the most recent data recovered after the failure. This is often referred to as a measure of acceptable data loss.
* As part of Disaster Recovery (DR) the RPO and RTO meaningful and realistic values need to be set reflecting both the business implication and technical of invoking disaster recovery plans.
* RPO and RTO are business driven numbers, that rollup from the RPO and RTO for the technical components that make up the business application.

## Preparation

Business Unit / Department Scope

|  |  |
| --- | --- |
| Field | Description |
| Business Unit/Department Name: |  |
| Description of Business Unit/Department’s Purpose in the Organization: |  |
| Name of Unit/Department’s Manager/Director: |  |
| Business processes performed by the Business Unit/Department |  |

## Procedure

For each business process identified, complete the following BIA Questionnaire:

|  |  |
| --- | --- |
| Field | Description |
| Business Unit/Department Name: |  |
| Business Process Name: |  |
| Business Function Description: |  |
| Does this Function have to be performed at a specific time of the day/week/month/year? |  |
| Using the Impact categories to classify the type of loss incurred and the Loss ranges (0 through 10) specify your estimated amount of exposure during each time period below: |  |
| Loss of Revenue |  |
| Cumulative Impact and Days <1,3,5,10,20,30> |  |
| Additional Expenses |  |
| Cumulative Impact and Days <1,3,5,10,20,30> |  |
| Regulatory and Legal |  |
| Cumulative Impact and Days <1,3,5,10,20,30> |  |
| Customer Service |  |
| Cumulative Impact and Days <1,3,5,10,20,30> |  |
| Goodwill |  |
| Cumulative Impact and Days <1,3,5,10,20,30> |  |
| Is this function dependent on any technology (hardware or software): |  |
| Does this function depend on any outside services or products for its successful completion? |  |
| What is the maximum amount of time this business process could be unavailable? (RTO) |  |
| What is the maximum accepted amount of data loss? (RPO) |  |

# Technical Dependency Analysis

## Guidance

Technical Dependency Analysis (TDA) is a process to define all technology and processes components and key personnel to keep a specific IT capability operational. The Technical Dependency Analysis (TDA) examines the application(s) and supporting infrastructure that a process depends on to determine, at a minimum, the following:

* **Recovery Time Capability (RTC)**: the technical dependency has been proven through a test and may or may not meet the RTO requirement.
* **Recovery Time Estimate (RTE)**: the technical dependency has not been proven through a test and the RTC has not been validated.
* **Recovery Point Capability (RPC)**: the technical dependency has been proven through a test and may or may not meet the RPO requirement.
* **Recovery Point Estimate (RPE)**: the technical dependency has not been proven through a test and the RPC has not been validated.

## Preparation

|  |
| --- |
| **Field** |
| Recovery Time Capability (RTC), or Recovery Time Estimate (RTE), if they haven’t been tested |
| Recovery Point Capability (RPC), or Recovery Point Estimate (RPE), if they haven’t been tested |
| Identify the Primary Production Site |
| Identify the Failover Site (if exists) |
| Identify the dependent applications to the primary application |
| Identify critical systems that are dependent on the primary application |
| Identify all Single Points of Failure (SPOF) for the primary application |
| Has Disaster Recovery (DR) been implemented (not backups)? |
| Is the Disaster Recovery Plan (DRP) Available? |
| Has the Disaster Recovery Plan (DRP) been tested? |
| Can DR tests temporarily impact production? |
| What is the last Disaster Recovery Plan (DRP) test date? |

## Procedure

### 1. Build Service Dependency Maps

* Service Map can automatically map dependencies between systems to ensure a recovery plan is reliable. This can be accomplished by [configuring service map](https://docs.microsoft.com/en-us/azure/monitoring/monitoring-service-map-configure) in Azure and [using service map](https://docs.microsoft.com/en-us/azure/monitoring/monitoring-service-map) solution in Azure.

### 2. Determine Service Recovery Time Capability and Recovery Point Capability

* Determine dependency RTC, RPC
* Determine aggregate RTC, RTE # Component Failure Analysis

## Guidance

## Preparation

Leverage the [Technical Dependency Analysis](1.2-Technical-Dependency-Analysis.md) to identify the services for each business process.

## Procedure

### 1. Conduct a Component Failure Analysis

* Using a spreadsheet, create a grid with business processes on one axis and the dependent Azure services on the other.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Business Process/Function** | **Service 1** | **Service 2** | **Service 3** | **…** | **Service n** |
| Process 1 |  |  |  |  |  |
| Process 2 |  |  |  |  |  |
| Process 3 |  |  |  |  |  |
| Process … |  |  |  |  |  |
| Process n |  |  |  |  |  |

* Leave a blank when a failure of the Azure service does not impact the business process in any ways;
* Insert an ‘X’ when the failure of the Azure service causes the business process to be inoperative;
* Insert an ‘A’ when there is an alternative to provide the service; and
* Insert an ‘M’ when there is an alternative service, but the service requires manual intervention to be recovered.

### 2. Conduct and Impact Assessment

* Identify Single Points of Failure (SPoF)
* Identify the Business/Customer impact of this service failing in terms of users and / or business cost.
* Identify the probability of failure and mitigation approaches to avoid this impact.
  + Design changes to prevent this impact
  + Redundancy or some form of resiliency
  + Additional cost considerations

# Disaster Recovery Implementation

Traditionally, organizations have taken a ‘one size fits all’ approach and essentially created common DR processes regardless of business priorities, objectives, and business impacts. For example by systematically replicating complete production environments from one datacenter to another, often with considerable hardware and software investments. Invariably this ends up being both expensive and an ineffective use of company resources.

With composite solutions consisting of Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as Service (IaaS) components it is important to clearly delineate between responsibilities of the cloud provider and the consumer. The following summarizes these responsibilities with respects to the Microsoft cloud services:

|  |  |
| --- | --- |
| **Service Type** | **Disaster Recovery Responsabilities** |
| SaaS | Microsoft will maintain the solution according the state SLA. Services will failover to Azure secondary regions without customer involvement. |
| PaaS | Microsoft and Customer may responsibility for service continuity depending on the service. Services will need to be reviewed on a case-by-case basis. |
| IaaS | Customer is responsible for service continuity. IaaS-based will not failover to secondary Azure region unless additional measures are configured by the customer. |

If a region-wide service disruption occurs, the locally redundant copies of your data are not available. If you have enabled geo-replication, there are three additional copies of your blobs and tables in a different region. If Microsoft declares the region lost, Azure remaps all of the DNS entries to the geo-replicated region.

## Guidance

* Leverage the business continuity capabilities of the SaaS service provided by the cloud provider. Focus business continuity efforts on PaaS and IaaS components of the solution.
* Services such as DNS, Active Directory have built-in mechanisms for replicating the state that should be used when feasible.
* Leverage Azure Traffic Manager if services are already deployed and dormant in the secondary region
* Leverage reference architectures to achive business continuity objectives:
  + App Service [Run a web application in multiple regions](https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/app-service-web-app/multi-region)
  + N-Tier Web Application [Multi-region N-tier application for high availability](https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/n-tier/multi-region-sql-server)
* Weigh business and compliance requirements, cost, and complexity as inputs to DR strategy by business function. The following table summarizes the high-level patterns for the PaaS and IaaS services in addition to their implications in terms of RTO, Complexity, and Cost.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **DR Pattern** | **Description** | **RTO** | **Complexity** | **Cost** |
| [Azure Site Recovery](https://docs.microsoft.com/en-us/azure/architecture/resiliency/disaster-recovery-azure-applications#failover-using-azure-site-recovery) | Azure Site Recovery, it creates several resources in the secondary region: Resource group, Virtual network (VNet), Storage account, Availability sets to hold VMs after failover. | Medium | Low | High |
| [Redeploy to Secondary Region](https://docs.microsoft.com/en-us/azure/architecture/resiliency/disaster-recovery-azure-applications#redeployment-to-a-secondary-azure-region) | Only the primary region has applications and databases running. The secondary region is not set up for an automatic failover. So when a disaster occurs, you must spin up all the parts of the service in the new region. This includes uploading a cloud service to Azure, deploying the cloud service, restoring the data, and changing DNS to reroute the traffic. | High | Medium | Low |
| [Active/Passive (Database Only)](https://docs.microsoft.com/en-us/azure/architecture/resiliency/disaster-recovery-azure-applications#database-only) | All traffic goes to the active site. The data is active on both regions with synchronization mechanisms in place. If a disaster occurs, the virtual machines, services and applications are restored on the DR site. Traffic is routed to the DR site. | Medium | Medium | Medium |
| [Active/Passive (Full Replica)](https://docs.microsoft.com/en-us/azure/architecture/resiliency/disaster-recovery-azure-applications#full-replica) | All traffic goes to the active site. The data, virtual machines, services and applications are active on both regions with synchronization mechanisms in place. If a disaster occurs, the DR environment is scaled-out as necessary. Traffic is routed to the DR site. | Low | Low | High |
| [Active/Active](https://docs.microsoft.com/en-us/azure/architecture/resiliency/disaster-recovery-azure-applications#active-active) | The data, virtual machines, services and applications are deployed and active on both primary production and secondary production site. Traffic is load balanced between the sites. If a disaster occurs at either site, the traffic is routed exclusively to the active site. The active site is scaled-out as necessary. | Low | High | Low |

## Next Steps

* Implement [Secondary Region Prerequisites](2.2-Azure-Secondary-Region-Prerequisites.md)
* Define DR strategy for [Azure Database Workloads](2.3-Azure-Database-Workloads.md) such as Azure SQL, Cosmos DB, Redis Cache
* Define DR strategy for [Azure Stateful Workloads](2.4-Azure-Stateful-Workloads.md) such as Virtual Machines and VDI such as Citrix.
* Define DR strategy for [Azure Stateless Workloads](2.5-Azure-Stateless-Workloads.md)
* Define DR strategy for [Azure Storage](2.6-Azure-Storage.md)
* Define DR strategy for [D365](2.7-D365.md)
* Conduct [Azure Disaster Recovery Simulation and Gap Analysis](3.0-Azure-Disaster-Recovery-Simulation-and-Gap-Analysis.md) to identify gaps between the business process recovery requirements (RPO, RTO) and the recovery capabilities of the applications and supporting infrastructure (RPE, RTE)

# Non-Regional Services and Secondary Failover

## When to use

Use the procedure described in this section to understand secondary region failover for non-regional and management services.

## Guidance

### Azure Non-Regional Services

Non-regional services are not dependent on any single region and are designed as highly available services managed by Azure.

|  |  |
| --- | --- |
| **Category** | **Name** |
| Identity | Azure Active Directory |
|  | Multi-Factor Authentication |
|  | Azure Active Directory \* B2C |
| Management Tools | Activity Logs & Alerts |
|  | Diagnostic Logs |
|  | Action Groups |
|  | Azure Policy |
|  | Cloud Shell |
| Networking | Azure DNS |
|  | Traffic Manager |
| Securityy | Azure Security Center |

### Azure Key Vault

* In the event that an entire Azure region is unavailable, the requests made to Azure Key Vault in that region are automatically routed (failed over) to a secondary region in read-only mode.

### Azure Recovery Service Vault

* By default, the Recovery Services vault has geo-redundant storage.
* If the Recovery Services vault is the primary backup, set storage replication option to geo-redundant storage.
* If virtual machines are deployed in multiple regions, a Recovery Services vault should be created in each region.

### Automation Account

* Geo-replication, standard in Azure Automation accounts, backs up account data to a secondary geographical region for redundancy. The secondary data, copied from the primary region, is continuously updated in case of data loss.

### Log Analytics Workspace

* Log analytics is support by the primary and secondary region pairing for failover scenarios. However, Log Analytics is not available in all regions and the service may not be delivered from your primary region. Current regional availability includes (East US, South Central US, Canada Central) \* June 2018

### Security Centre Workspace

* Azure Security Center is non-regional and not subject to availability in any given region. Azure Security Center uses the Microsoft Monitoring Agent, also used by the Log Analytics service, to collect security data from your virtual machines. [Data collected and stored](https://docs.microsoft.com/en-us/azure/security-center/security-center-planning-and-operations-guide#data-collection-and-storage) from this agent will be stored in your Log Analytics workspace(s).

### Application Insights

* Application Insights is support by the primary and secondary region pairing for failover scenarios. However, Log Analytics is not available in all regions and the service may not be delivered from your primary region. Current regional availability includes (East US, South Central US, West US 2). \* June 2018

## Procedure

## 1. Select the Automation Account Primary Region

* You can choose a primary region, or location, when [setting up your account](https://docs.microsoft.com/en-us/azure/automation/automation-quickstart-create-account#create-automation-account), and then a secondary region is assigned to it automatically.

## 2. Select Log Analytics Workspace Primary Region

* You can choose a primary region, or location, when [setting up your workspace](https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-quick-create-workspace#create-a-workspace), and then a secondary region is assigned to it automatically.

## 3. Select Key-Vault Primary Region

* You can choose a primary region, or location, when [creating a key vault](https://docs.microsoft.com/en-us/azure/key-vault/quick-create-portal#create-a-vault), and then a secondary region is assigned to it automatically.

## 4. Select Recovery Service Vault Primary Region and Geo-Replication

* You can choose a primary region, or location, [when creating a recovery services vault](https://docs.microsoft.com/en-us/azure/backup/backup-azure-vms-first-look-arm#create-a-recovery-services-vault-for-a-vm), and then a secondary region is assigned to it automatically. Set [storage replication](https://docs.microsoft.com/en-us/azure/backup/backup-azure-vms-first-look-arm#set-storage-replication).

## 5. Selection Application Insight Resource Region

* You can choose a primary region, or location, [when creating an Application Insights Resource](https://docs.microsoft.com/en-us/azure/application-insights/app-insights-create-new-resource#create-an-application-insights-resource-1), and then a secondary region is assigned to it automatically.

# Secondary Region Prerequisites

## When to use

Use the procedure described in this section to prepare Azure secondary site for disaster recovery of PaaS and IaaS services

## Guidance

* The simplest approach, requiring no action, is to wait until the region is restored. This is recommended for short term outages and for workloads with less stringent availability requirements. The current service status on the [Azure Service Health Dashboard](https://azure.microsoft.com/en-us/status/).
* For workloads with more demanding continuity requirements, preparing the secondary data center is necessary. A number of ancillary services and configurations are expected to be pre-defined, configured and running in Lowes’s subscription in the secondary region to facilitate failover activities and testing.
* Azure Traffic Manager automates the failover of user traffic to another region if the primary region fails. Traffic Manager detects a failure in the primary site and rolls over to the failover site, regardless of whether that site is currently serving users.
* The following services should be predefined and configured ahead of time: Azure Virtual Networks, Azure RBAC Assignment, Active Directory Domain Services, Domain Name Services, JumpBox VMs, Systems Center Configuration Manager, Certificate Services (PKI)

## Procedure

### 1. Azure RBAC Assignment

* Security & Access of Azure subscriptions to be maintained with same governance as primary datacenter.

### 2. Azure Virtual Networks

* Continuously deploy and maintain Virtual Networks, Subnets, S2S VPN and any other network components. Note: Two VNets using the same private IP address space and resources in two different regions ahead of time.

### 3. Active Directory and Internal Domain Name Services

* An availability set of virtual machines (2) to be replicated from the primary region and/or the on-premises domain controllers. Running on AD Domain Controllers, AD-integrated DNS will provide internal name resolution. See [Use Azure Site Recovery to protect Active Directory and DNS](https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-active-directory)

### 4. Jumpbox VMs

* For workstations that will be used for system administration see Citrix information under [Azure Stateful Workloads](2.3-Azure-Database-Workloads.md)

### 5. System Center Configuration Manager

* [Configuration Manager on Azure](https://docs.microsoft.com/en-us/sccm/core/understand/configuration-manager-on-azure)
* If Configuration Manager cloud-based distribution points are to be used, Public key infrastructure (PKI) certificates must be installed on the site server for authentication.
* Any task sequences deployed to Azure virtual machines configured to use SCCM must be configured as Download all content locally.
* PXE and multicast, streamed applications, Apple and Unix clients, Windows and third-party updates are not supported features of cloud-based distribution points

### 6. Integration Account

* Identify a secondary region and [create an integration account](https://docs.microsoft.com/en-us/azure/logic-apps/logic-apps-enterprise-integration-create-integration-account) in the secondary region.

### 7. Batch Account

* Identify a secondary region and [create a batch account](https://docs.microsoft.com/en-us/azure/batch/batch-account-create-portal#create-a-batch-account) in the secondary region.

### 8. Azure Traffic Manager

* Azure Traffic Manager provides multiple [routing methods](https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-routing-methods), so you can choose whether to manage your deployments using a primary/backup model or to split traffic between them. Service failover to a set of identical backup services can be done through [configuring the priority traffic routing method](https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-configure-priority-routing-method)

### 9. Virtual Team Scale Set Images

* Ensure Marketplace or custome VM scale set images are available from the secondary region.

# Database Workloads

## When to use

Use the procedure described in this section to implement disaster for PaaS database workloads. This scenario includes Azure SQL, Cosmos DB, and Data Lake.

## Guidance

### Azure SQL

* Leverage Azure SQL Database and Cosmos DB geo-replication to configure secondary database replicas in other regions. Secondary databases are available for querying and for failover in the case of a data center outage or the inability to connect to the primary database.
* [Azure SQL Business Continuity](https://docs.microsoft.com/en-us/azure/sql-database/sql-database-business-continuity) capabilities support standard geo-replication or active-geo-replication.
* **Standard geo-replication:** designed for applications that are using geo-replication to achieve disaster recovery SLA.
* **Active geo-replication:** designed for the applications with high-volume read-oriented workload could benefit from read-scale load balancing in addition to fast disaster recovery.
* To achieve RPO of < 5 seconds and recovery times of less than 30 seconds active geo-replication is required.

### Azure SQL Data Warehouse

* By default, SQL Data Warehouse performs a geo-backup once per day to a paired data center. The RPO for a geo-restore is 24 hours. You can restore the geo-backup to a server in any other region where SQL Data Warehouse is supported. A geo-backup ensures SQL data warehouse can be restored in case the snapshots cannot be accessed in your primary region.

### Redis Cache

* The disaster recovery posture of Redis Cache depends on its usage pattern. When used for web user session caching, geo-replication is generally not required. However, messaging and distributed transaction scenarios may require geo-replication to ensure recoverability requirements can be met.

### Cosmos DB

* Cosmos DB failover handling is automatic without requiring code change of any kind.
* SDK is auto-homing and will failover to next available region in the chosen list of regions.
* There is no availability, performance loss during a manual failover. During DR-based failover potential unreplicated changes can be merged when the region returns to normal database situation.
* see [How to distribute data globally with Azure Cosmos DB](https://docs.microsoft.com/en-us/azure/cosmos-db/distribute-data-globally) and [Automatic regional failover for business continuity in Azure Cosmos DB](https://docs.microsoft.com/en-us/azure/cosmos-db/regional-failover)

## Procedure

## 1. Azure SQL Geo-Replication and Failover Groups

* [Failover groups and active geo-replication](https://docs.microsoft.com/en-us/azure/sql-database/sql-database-geo-replication-overview)

## 2. Azure Redis Cache Geo-Replication

* [How to configure Geo-replication for Azure Redis Cache](https://docs.microsoft.com/en-us/azure/redis-cache/cache-how-to-geo-replication)

## 3. Azure Cosmos DB Geo-Replication

[Add global database regions for Cosmos D](https://docs.microsoft.com/en-us/azure/cosmos-db/tutorial-global-distribution-sql-api) and [How to distribute data globally with Azure Cosmos DB](https://docs.microsoft.com/en-us/azure/cosmos-db/distribute-data-globally)

## 4. Restore Azure SQL Data warehouse

* [Restoring from restore points](https://docs.microsoft.com/en-us/azure/sql-data-warehouse/backup-and-restore) and [Geo-redundant restore](https://docs.microsoft.com/en-us/azure/sql-data-warehouse/backup-and-restore)

# Stateful Workloads

Use the procedure described in this section to enable ***Azure Site Recovery*** for stateful workloads.

## When to Use

This pattern is useful when you want to failover and recover stateful virtual machines from the primary Azure data centre to the secondary Azure data centre in the same region.

Replication is handled by replicating the disk configuration to a secondary set of storage accounts via the Site Recovery Agent Service that is automatically installed once the service has been configured.

In case of an outage, failover of specific workloads to the secondary region can be triggered. Failback to the primary site is also possible when running from the secondary site.

RPOs are usually 30 seconds or less.

|  |  |
| --- | --- |
| **Advantages** | **Disadvantages** |
| The configuration, failover and recovery are all managed from the Azure portal | Windows & Linux Red Hat virtual machines are supported, for the exhaustive list consult this [document](https://docs.microsoft.com/en-us/azure/site-recovery/azure-to-azure-support-matrix) |
| This method can work with any workload supported in Azure VMs. Application specific testing in this [workload summary](https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-workload#workload-summary). | Replicating Virtual Machines is only supported within the same subscription |
| App-agnostic, app-consistent, near-synchronous replication. |  |
| Can integrate with SQL Always On to handle snapshots and app consistency |  |
| Disaster drills can take place without impacting production or replication |  |
| Integration with Azure Automation capabilities |  |
| Seamless connection with currently planned Azure services, including network management, load balancers and Traffic Manager |  |

## Guidance

* Azure Site Recovery RPO will be dependent on the amount of churn in the environment and the network bandwidth.  For example, if a system that is changing frequently (IOPS on the disk), replication of the changes to that environment will be rather high.  If the connectivity from that environment is so poor that the bandwidth can’t transmit all of those changes, the RPO probably will not be achieved.
* With Azure Backup, the RPO is dependent on the frequency of your backups, but the RTO will again be dependent on bandwidth and capacity (i.e. a single file restore is much faster than an entire system).

## Preparation

* **Capacity Planning**
  + Use the [Capacity Planner for Azure Site Recovery DR Solution](https://gallery.technet.microsoft.com/Azure-Recovery-Capacity-d01dc40e) to analyze the source environment (workloads) on Hyper-V or VMware or Physical server, bandwidth requirements, resource requirements (VMs, storage) on the target and any additional server resources that are required on the source side (SC VMMs, Configuration Servers, Process Servers etc).
  + Use the [Site Recovery Deployment Planner for Hyper-V to Azure](https://docs.microsoft.com/en-us/azure/site-recovery/hyper-v-deployment-planner-overview) to profile the environment and allocate sufficient bandwidth based on your daily data-change rate to meet your desired Recovery Point Objective (RPO)

## Procedure

### 1. Azure Site Recovery for Stateful Web Tier

* [Replicate a multi-tier IIS-based web application](https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-iis)

### 2. Azure Site Recovery for SQL Server Instance

* [Protect SQL Server using SQL Server disaster recovery and Azure Site Recovery](https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-sql)

### 3. Azure Site Recovery for Citrix

* [Replicate a multi-tier Citrix XenApp and XenDesktop deployment using Azure Site Recovery](https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-citrix-xenapp-and-xendesktop) \* **Note: Link is Broken**

# Azure Stateless Workloads

Use the procedure described in this section to implement disaster for stateless workloads.

## When to use

This scenario could apply to the following: stateless app servers running on Virtual Machines, Platform Services such as Logic Apps and Functions that use storage accounts as back-end storage

## Guidance

* Consider Re-Deployment through automation over replication when feasible for stateless layers.
* Stateless servers should be redeployed using Infrastructure as Code (ARM templates) when feasible. Leverage template parameters to minimize the changes required to the templates.
* Asynchronously replicate the data stores (such as SQL Azure database, Blob Storage, or CosmosDB) using the respective features of these services such as using Geo-Redundant Storage or other Platform services
* If RTO does not allow time for redeployment, the recommendation is to deploy all primary region resources in a secondary region also. Primary region resources include:
  + Azure Service Bus
  + Azure Event Hubs
  + Azure API Management
  + Azure Logic Apps
  + Azure Functions and Function Proxies
* Access to stateless workload data sets can be insured by replicating the data layer using Geo-Redundant Storage or other Platform services.

|  |  |
| --- | --- |
| **Advantages** | **Disadvantages** |
| Read-access geo-redundant storage (RA-GRS) maximizes availability for your storage account. RA-GRS provides read-only access to the data in the secondary location, in addition to geo-replication across two regions. | Applications manage which endpoint it is interacting with when using RA-GRS. ( The secondary endpoint is similar to the primary endpoint, but appends the suffix –secondary to the account name) |
| Azure Storage typically has an RPO of less than 15 minutes | The proposed solution assumes that it is acceptable to return potentially stale data to the calling application. Because data in the secondary region is eventually consistent, it is possible the primary region may become inaccessible before an update to the secondary region has finished replicating. |

### Service Bus

* The disaster recovery feature implements metadata disaster recovery, and relies on primary and secondary disaster recovery namespaces. Note that the Geo-disaster recovery feature is available for the [Premium SKU](https://docs.microsoft.com/en-us/azure/service-bus-messaging/service-bus-premium-messaging) only.
* By pairing azure service bus namespaces in different regions an alias can be created. The alias provides a single stable Fully Qualified Domain Name (FQDN) connection string. Applications use this alias connection string to connect to a namespace.
* Consider creating a durable client-side queue as a backup.

### Event Hubs

* Event Hub, much like Service Bus, requires the pairing of namespaces across regions as described in [Azure Event Hubs Geo-disaster recovery](https://docs.microsoft.com/en-us/azure/event-hubs/event-hubs-geo-dr). The Geo-disaster recovery feature is globally available for the Event Hubs Standard SKU.
* By pairing Azure Event Hub namespaces in different regions an alias can be created. The alias provides a single stable Fully Qualified Domain Name (FQDN) connection string. Applications use this alias connection string to connect to a namespace.

### API Management

* The service “backup and restore” feature provides the necessary building block for implementing your disaster recovery strategy. Backup is a long running operation that may take multiple minutes to complete.
* Restore is a long running operation that may take up to 30 or more minutes to complete.

### Function Apps

* With Azure Durable Functions all state is persisted in Azure Storage.

### Logic Apps

* Deploy Logic Apps can be deployed through ARM templates in multiple regions to achieve redundancy in either active, or passive (disabled) mode.
* *Note that Logic Apps endpoints are not supported by Traffic Manager, therefore traffic cannot be redirected dynamically. Options includes:*
  + Making the calling or subscribing application aware of the primary and secondary endpoints so they can call the correct endpoint in the event of a failover.
  + Use API Management to provide an endpoint traffic manager can reach and have API Management can then relay requests to Logic Apps.
  + Use Function App Proxy as a light-weight API management layer.
* For B2B scenarios involving X12, AS2, and EDIFACT, see [Logic Apps B2B cross-region disaster recovery](https://docs.microsoft.com/en-us/azure/logic-apps/logic-apps-enterprise-integration-b2b-business-continuity)

### Data Factory

* Infrastructure as code: ADF deployment code should be placed under source control. The source control system must of course be geo-replicated so as to have a copy of the deployment scripts ready to go on case of a failure.
* Dependencies availability: maintain a list of all dependencies such as data sources and sinks used in the data pipelines and commit that list to a document that is placed under geo-replicated source control. Ideally, you should have a dependency check script to accelerate the validation.
* Trigger reset automation scripts: During a failover event, pipelines will either crash, or miss their scheduled execution. Develop a script developed that will reset all the pipeline to a “ready” state so that the workload that should have executed do so in a timely manner to avoid any potential data loss.
* Post-Failover ADF restore checklist
  + Confirm Deployment scripts and documentation is available in geo-replicated source control.
  + Execute deployment script
  + Confirm successful deployment of the ADF service as well as all the pipelines
  + Run the dependencies check script or perform manual validation.
  + If check is successful, execute the trigger reset automation script Once in ready state, manually restart those pipeline that have crashed or missed their scheduled execution. Later, perform a manual validation that ensure those that were scheduled post failover did indeed execute.

### Azure Batch

* The default number of batch accounts per subscription is 1-3. For production workloads requiring a DR posture, that limit may need to be raised using a customer [support request](https://docs.microsoft.com/en-us/azure/batch/batch-quota-limit#increase-a-quota).
* Manage all the Azure Batch code through a Visual Studio project and parametrize the following configuration items:
  + Batch account credentials: Batch Account Name, Batch Account Key, Batch, Account URL
  + Storage account credentials: Storage Account Name, Storage Account Key

### Virtual Machine Scale Set

* Certain workloads, such as web front ends, do not persist state and can be considered stateless. Business continuity for these workloads is achieved by redeploying the scale set and allowing it autoscale to the required configuration.

## Preparation

* Complete the [secondary region pre-requisites](2.2-Azure-Secondary-Region-Prerequisites.md) related to the Azure Integration Account.
* Harden your application by using [Best practices for insulating applications against Service Bus outages and disasters](https://docs.microsoft.com/en-us/azure/service-bus-messaging/service-bus-outages-disasters). Azure Service Bus patterns recommended [active](https://docs.microsoft.com/en-us/azure/service-bus-messaging/service-bus-outages-disasters#active-replication) or [passive](https://docs.microsoft.com/en-us/azure/service-bus-messaging/service-bus-outages-disasters#passive-replication) replication rely on the client sending the message to service bus queues

## Procedure

### 1. Azure Service Bus

* [Azure Service Bus Setup and Failover Flow](https://docs.microsoft.com/en-us/azure/service-bus-messaging/service-bus-geo-dr#setup-and-failover-flow)
* Initiate pairing through Azure Portal Azure Service Bus blade or pair Azure Service Bus namespaces and create a namespace alias with the following: [Enable Service Bus Geo-DR configurations using PowerShell](https://blogs.msdn.microsoft.com/servicebus/2018/02/16/enable-service-bus-geo-dr-configurations-using-powershell/)

### 2. Azure API Management

* Use API Management as the endpoint for Traffic Manager with PowerShell [Add-AzureTrafficManagerEndpoint](https://docs.microsoft.com/en-us/powershell/module/azure/add-azuretrafficmanagerendpoint?view=azuresmps-4.0.0)
* Backup API Management with PowerShell [Backup-AzureRmApiManagement](https://docs.microsoft.com/en-us/powershell/module/azurerm.apimanagement/backup-azurermapimanagement?view=azurermps-1.7.0&redirectedfrom=msdn)
* Restore API Management in secondary region with PowerShell [Restore-AzureRmApiManagement](https://docs.microsoft.com/en-us/powershell/module/Azure/?view=azuresmps-4.0.0)

### 3. Azure Functions

* This pattern consists of deploying a backup (passive) function app to a different region. Traffic Manager will monitor the primary (active) function app for availability. It will fail over to the backup function app if the primary fails.
* For durable functions, use Read-access geo-redundant storage (-RAGRS), which replicates your data to a secondary region and provides read-only access to the data in the secondary location.

### 4. Azure Logic Apps

* Import Logic App into API Management with [Import a Logic App as an API](https://docs.microsoft.com/en-us/azure/api-management/import-logic-app-as-api)

### 5. Azure Data Factory

* Set up a development data factory with VSTS and [continuous integration lifecycle](https://docs.microsoft.com/en-us/azure/data-factory/continuous-integration-deployment#continuous-integration-lifecycle) to author Data Factory resources such as pipelines, datasets, and so forth. Redeploy to secondary regions in the event of a primary data center failure.

### 6. Azure Batch

* Execute batch jobs in secondary regions leveraging parameterized configuration items

### 7. Virtual Machine Scale Set

* Redeploy Virtual Machine Scale Set to secondary region using [Virtual Machine Scale Set templates](Learn%20about%20virtual%20machine%20scale%20set%20templates). # Azure Storage

Microsoft Azure Storage is the Microsoft-managed cloud service that provides storage in the Azure cloud. It consists of three data services: Blob Storage, File Storage and Queue Storage.

Azure Storage can be used as a discreet service, or it can underpin other Azure services that you are consuming. Data is stored in storage accounts.

At the region level, this is referred to as Locally-Redundant storage (LRS) which means that multiple copies of your data are maintained in a given region.

## When to Use

For Disaster Recovery in case of a region outage, Geo-Redundant Storage is designed to provide 16 9s durability by maintaining the local copies of your data in the primary region plus another set of copies of your data in the secondary region (ex: Canada Central is replicated to Canada East)

When a regional disaster affects a primary region, Microsoft will try to restore the service in that region. Dependent upon the nature of the disaster and its impacts, in some rare occasions we may not be able to restore the primary region. At that point, we will perform a geo-failover.

|  |  |
| --- | --- |
| **Advantages** | **Disadvantages** |
| At all times, Azure will keep and manage multiple copies of your data. | Before and during the geo-failover, you won’t have write access to your storage account due to the impact of the disaster but you can still read from the secondary if your storage account has been configured as RA-GRS |
| Storage geo-failover will only be triggered by the Azure Storage team – there is no customer action required. |  |
| Existing storage service endpoints for blobs, tables, queues, and files will remain the same after the failover; the Microsoft-supplied DNS entry will need to be updated to switch from the primary region to the secondary region. Microsoft will perform this update automatically as part of the geo-failover process. |  |
| Azure Active Directory Credentials |  |

## Guidance

### Azure Blob Storage

* When the geo-failover has been completed and the DNS changes propagated, read and write access storage accounts will be resumed if GRS or RA-GRS configured for the storage account.
* Query [“Last Geo Failover Time” of your storage account](https://msdn.microsoft.com/library/azure/ee460802.aspx) to get more details noting the value of the following fields: StatusOfPrimary, LastGeoFailoverTime
* After the failover, a storage account will be fully functioning, but in a “degraded” status, as it is actually hosted in a standalone region with no geo-replication possible. To mitigate this risk, Microsoft will restore the original primary region and then do a geo-failback to restore the original state. If the original primary region is unrecoverable, we will allocate another secondary region.
* For more details on the infrastructure of Azure Storage geo replication, please refer to the article on the Storage team blog about [Redundancy Options and RA-GRS](https://blogs.msdn.microsoft.com/windowsazurestorage/2013/12/11/windows-azure-storage-redundancy-options-and-read-access-geo-redundant-storage/).

### Azure Data Lake

* Critical Data is Azure Data Lakes should be copied to another Data Lake Store account in another region with a frequency aligned to the needs of the disaster recovery plan.
* Understand the different capabilities between storage offerings: [Comparing Azure Data Lake Store and Azure Blob Storage](https://docs.microsoft.com/en-us/azure/data-lake-store/data-lake-store-comparison-with-blob-storage)

## Procedure

### 1. Azure Blob Storage

* Enable Read-access geo-redundant storage (RA-GRS) Replication on storage account. See replication options under [create a general purpose storage account](https://docs.microsoft.com/en-us/azure/storage/common/storage-quickstart-create-account?toc=%2Fazure%2Fstorage%2Fblobs%2Ftoc.json&tabs=portal#create-a-general-purpose-storage-account)

### 2. Azure Data Lake

* Azure Data Factory is a useful service for creating and deploying data moveeverage [ADLCopy](https://docs.microsoft.com/en-us/azure/data-lake-store/data-lake-store-copy-data-azure-storage-blob), [Azure PowerShell](https://docs.microsoft.com/en-us/azure/data-lake-store/data-lake-store-get-started-powershell) or [Azure Data Factory](https://docs.microsoft.com/en-us/azure/data-factory/connector-azure-data-lake-store)ment pipelines on a recurring basis.

# D365 Disaster Recovery

The Dynamics 365 for Finance and Operations production environments are configured with disaster recovery support that includes disaster recovery capabilities of stateful and stateless workloads:

* Azure SQL active-geo replication for primary databases, with a Recovery Point Estimate (RPO) of < 5 seconds.
* Geo-redundant copies of Azure blob storage (containing document attachments) in other Azure regions.
* Same secondary region for the Azure SQL and Azure blob storage replications.

## Stateful D365 Components

The primary data stores are supported for replication. This means that Dynamics 365 for Finance and Operations application components, such Management Reporter and Entity store, use transformed data from the primary database, which need to be generated after the recovery site has been set up and the service has started.

## Stateless D365 Components

Customer code artifacts and recovered data stores is used to re-deploy the site, with a Recovery Time Objective (RTO) of up to 10 hours. This will enable state replication of the compute nodes along with networking and other components to set up the secondary site using the recovered data stores. Refer to Table 6 for more information about the roles and responsibilities for disaster recovery

## API Integration

Applications that do not link to the Microsoft Dynamics 365 SDK assemblies, for example Java applications that access the web services by using SOAP or ODATA, can try accessing the failover URL for the target organization.

  The URL for a failover alternate organization is the same as the URL for the primary organization with “–s” added to the organization name. For example, an organization named Contoso would have the primary and alternate URLs shown below:

* **Primary Organization URL:** https://contoso.api.crm.dynamics.com
* **Alternate Organization URL:**: https://contoso-secondary.api.crm.dynamics.com

For non.NET-connected applications, there is no notification event to which your application can subscribe to receive notice of a service interruption and failover. Your application will begin to receive a variety of fault exceptions, as listed previously, during the service interruption. At that point, the application can attempt to connect to the failover alternate URL for the target organization. After the disaster has been corrected, a fail back to the primary URL for the organization occurs as part of planned organization maintenance.

# Disaster Recovery Simulation

Use this guide to plan and execute disaster recovery simulations to confirm recovery point and recovery time estimate, identify gaps, and mitigation plans.

## Guidance

* The intent of this testing is to evaluate the feasibility of the recovery plan and highlight any issues that were inadequately addressed.
* Execute simulations so that the created scenarios don’t disrupt actual business, while still simulating real situations.
* The simulated scenarios must be completely controllable such that services can be restored even if the tested recovery plan fails.
* Ensure any regulatory reporting requirements related to DR are considerer
* Common Failure Scenarios
  + Shut down VM instances.
  + Pressure resources such as CPU and memory.
  + Disconnect/delay network.
  + Crash processes.
  + Expire certificates.
  + Simulate hardware faults.
  + Shut down the DNS service on the domain controllers.
* Refer to [disaster simulation](https://docs.microsoft.com/en-us/azure/architecture/resiliency/disaster-recovery-azure-applications#disaster-simulation) in Disaster recovery for Azure applications.

## Preparation

* Determine the tolerance for production downtime during DR testing affects the design. There are three basic scenarios:
* Zero tolerance for production downtime – the DR test must be executed without bringing down production.
* Regular Maintenance Window – the DR test must be executed during a regular maintenance window.
* Extended Maintenance Window – special allowance is made for an extended outage during the DR test
* Define the level of integration testing that will be required during the DR test. This covers integration into existing 3rd systems and 3rd party systems
* Define data consistency requirements on how data consistency (between DR and Prod) is confirmed.
* Define the scope of DR testing process: full regression testing of the entire system, functional testing, or smoke testing.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Cloud Service** | **Used In** | **RTO** | **RPO** | **RTE** | **RPE** | **Workload Type** | **DR Approach** | **Test** | **Gap** |
| Microsoft Cloud Service 1 | Dependency | Hours | Minutes | Hours | Minutes | SaaS, PaaS, IaaS | Database, Stateful, Stateless, Storage |  |  |
| Microsoft Cloud Service 2 | Dependency | Hours | Minutes | Hours | Minutes | SaaS, PaaS, IaaS | Database, Stateful, Stateless, Storage |  |  |
| Microsoft Cloud Service 3 | Dependency | Hours | Minutes | Hours | Minutes | SaaS, PaaS, IaaS | Database, Stateful, Stateless, Storage |  |  |
| … |  |  |  |  |  |  |  |  |  |
| Microsoft Cloud Service n | Dependency | Hours | Minutes | Hours | Minutes | SaaS, PaaS, IaaS | Database, Stateful, Stateless, Storage |  |  |

## Procedure

### 1. Azure Stateful Workload Disaster Recovery Simulation

* [Run a disaster recovery drill for Azure VMs to a secondary Azure region](https://docs.microsoft.com/en-us/azure/site-recovery/azure-to-azure-tutorial-dr-drill)

### 2. Azure Database Workload Disaster Recovery Simulation

* [Fail over to a geo-replicated secondary server using the Azure portal](https://docs.microsoft.com/en-us/azure/sql-database/sql-database-geo-replication-portal)
* [Fail over to the secondary server using PowerShell](https://docs.microsoft.com/en-us/azure/sql-database/scripts/sql-database-setup-geodr-and-failover-database-powershell)

## 3. Azure Stateless Workload Disaster Recovery Simulation

* Azure Storage Disaster Recovery Simulation
* [Simulate a failure in accessing read-access redundant storage](https://docs.microsoft.com/en-us/azure/storage/blobs/storage-simulate-failure-ragrs-account-app?tabs=windows)