Disaster Recovery Playbook

Feb 2020

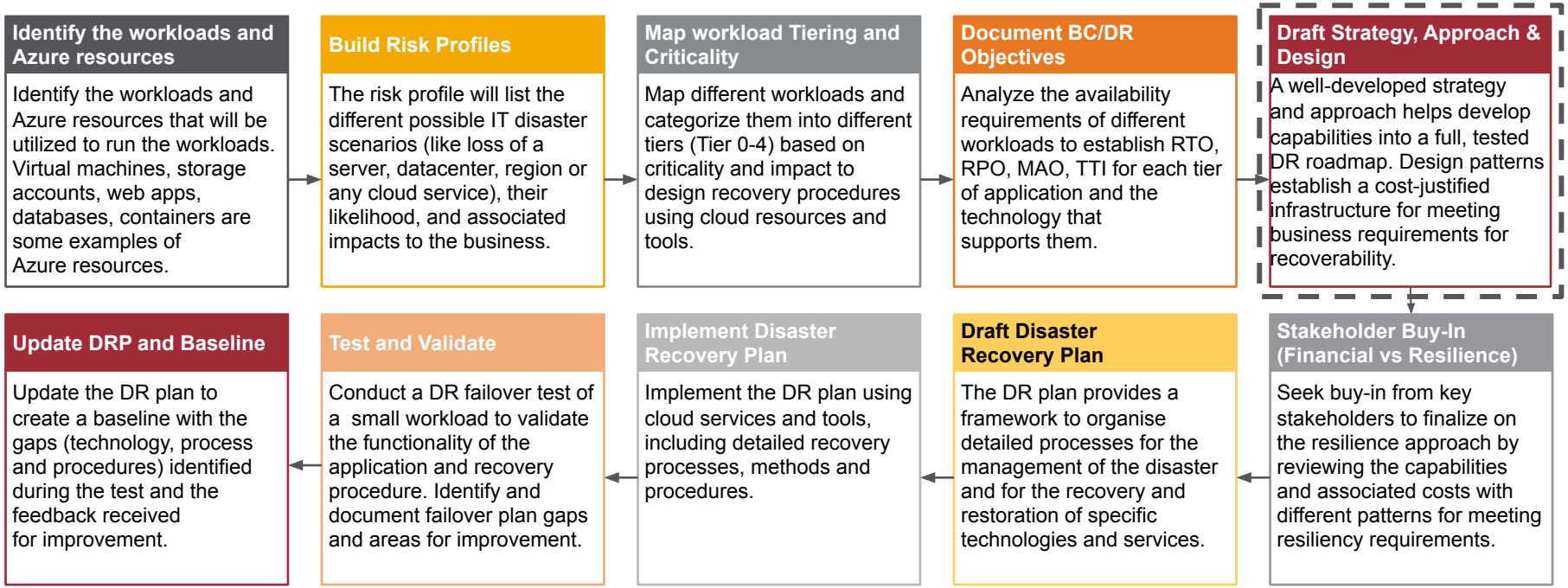
DRAFT

Table of Contents

Roadmap for Resiliency in Azure

Roadmap for Resiliency in Azure

Roadmap for designing and implementing high availability and disaster recovery capabilities in the cloud.

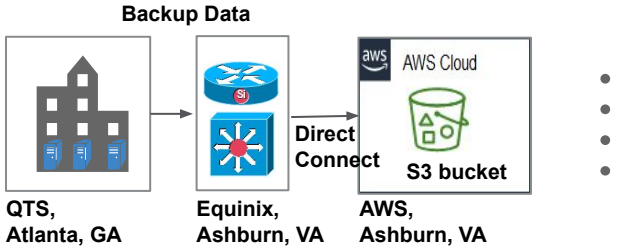


Current State Baseline

Current State Baseline

As part of the initial discovery, we worked with 3 CDOs (MedExpress, USMD, NAMM) to understand the current IT infrastructure and application landscape and the disaster recovery solution implemented by each of the 3 CDOs. Below are some of the the key observations for disaster recovery capabilities for the 3 CDOs.

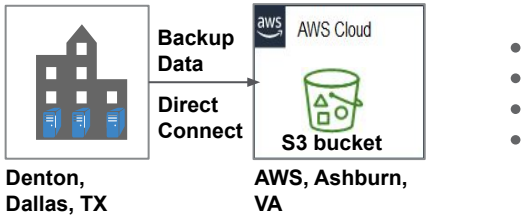
MedExpress



DR Solution: Backup & Restore - Backup data is replicated to S3 buckets in AWS public cloud. In case of a disaster, the environment is restored manually from the backup data.

Tools Used: Netbackup

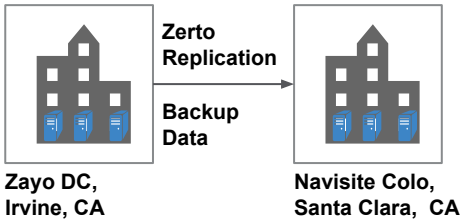
USMD



DR Solution: Backup & Restore - Backup data is replicated to S3 buckets in AWS public cloud. In case of a disaster, the environment is restored manually from the backup data.

Tools Used: Veeam

NAMM



DR Solution: Backup & Restore - Backup data is replicated to Navisite Colo using Zerto replication. In case of a disaster, the environment is restored manually from the backup data..

Tools Used: Zerto

CDO Workload Tiering and RTO/RPO

Different workloads across the 3 CDO's (MedExpress, USMD, NAMM) have been categorized into different tiers and have defined RTO requirements to support the business continuity in case of a disaster.

MedExpress

Restoration Priority/Tier	Applications	Overall RTO	RPO
1	Active Directory, DNS	1 - 4 hours	0.25-3 hours
2	Citrix	25 - 50 hours	0.25-3 hours
3	DocuTAP	49 - 100 hrs	0.25-3 hours
4	Great Plains	57 - 124 hrs	0.25-3 hours
5	Kronos	61 - 136 hrs	0.25-3 hours
6	Portal	68 - 139 hrs	0.25-3 hours

USMD*

Restoration Priority/Tier	Applications	Overall RTO
1	NextGen	72 hours
2		
3		
4		
5		
6		

NAMM

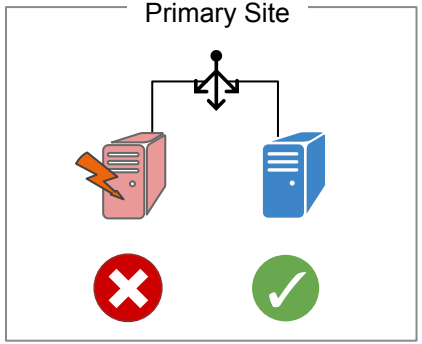
Priority	Applications	Overall RTO
1	Xcelys, Nammnet Express, Secure Provider Portal	8 hours
2	Citrix	48 hours
3	Biztalk, Business Objects, Claims Editing Systems, Common Data Platform, ImageNet, Peoplesoft	72 hours
4	eVIPS	168 hours

* Pending further inputs from USMD IT team, requested 2/5/2020

High Availability or Disaster Recovery

High Availability or Disaster Recovery

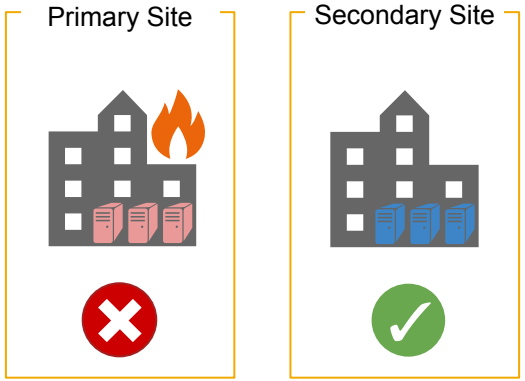
It's not about avoiding failures. It's about responding to failures, with High Availability and Disaster Recovery. High availability is configured to provide fault tolerance for a service/application within the same site. DR is recovery of service/application to an alternate site in case of a significant app-level failure or a catastrophic failure of a data center.



High availability

When one node of the application encounters a catastrophic failure, the other node(s) handle the workload

What does 'High' mean?



Disaster Recovery

When applications encounter a catastrophic failure, workloads are failed over to the secondary site

How quick does the recovery need to be?

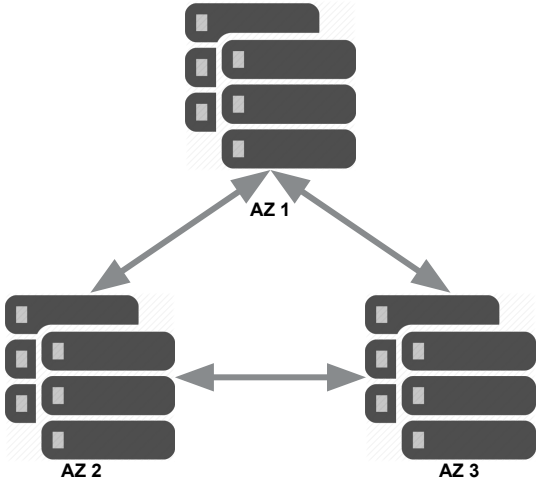
High Availability and Scalability in Azure

High Availability and Scalability in Azure

There are three solutions available in Azure to design high availability for applications.

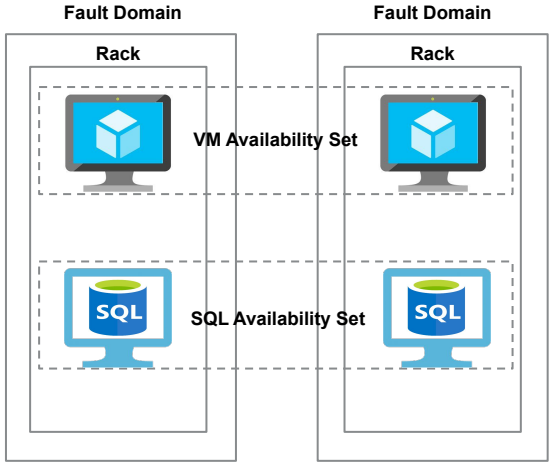
Availability Zones

Protection from datacenter failure



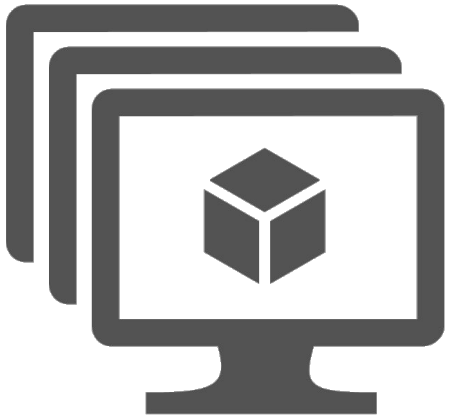
Availability sets

Protection from VM level failure



Virtual Machine Scale Sets (VMSS)

Deploy hundreds of identical virtual machines in minutes and autoscale as per your requirement

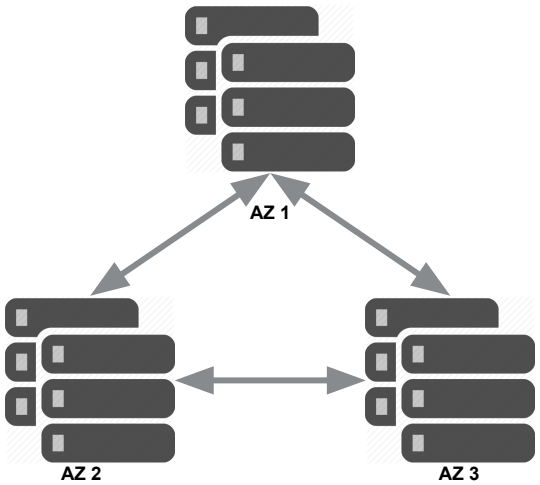


High Availability

Scalability

Availability Zones

Allows workloads to be spread over multiple locations, no concern on which host the workload will run. VM SLA 99.99%

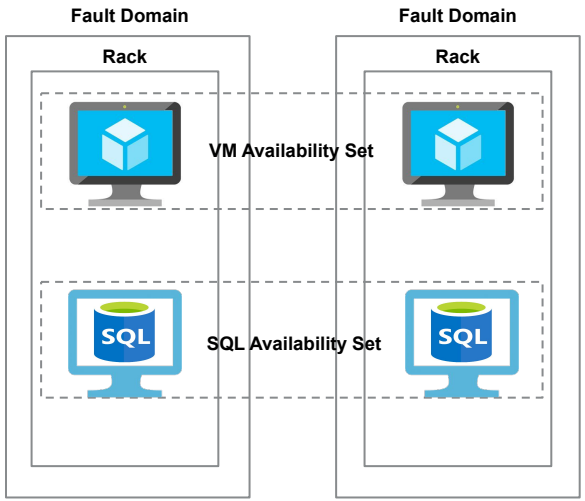


High Availability using Availability Zones

- Deploying resources in Availability Zones protects application from datacenter-level failures
- Each Availability Zone has its own independent power source, network, and cooling; the physical and logical separation of Availability Zones within a region protects applications and data from zone-level failures
- To ensure resiliency, there's a minimum of three separate zones in all enabled regions
- Availability Zones protect mission-critical applications from failures of entire datacenter with low latency and high availability
- There is no cost for Availability Zones, the cost incurred is for every VM instance that is created and running.
- Availability Zones should be used for achieve high availability for applications in case of data center failure in an Azure region. This can be implemented by distributing VMs across multiple Availability Zones, behind a load balancer, so that if one VM or Availability Zone incurs a failure, the VM in the other Availability Zone will take all traffic.

Availability Sets

Allows workloads to be spread over multiple hosts, racks but still remain at the same data center. VM SLA 99.95%

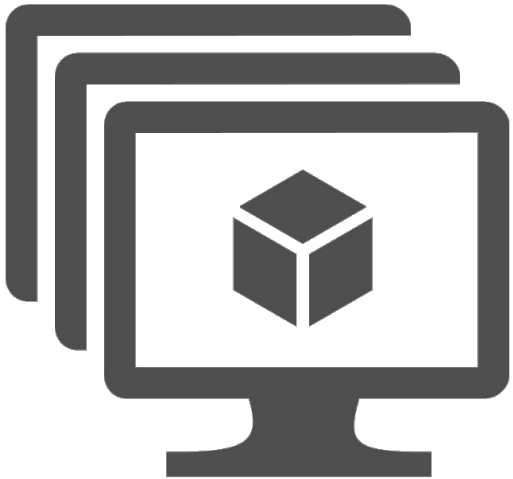


High Availability using Availability Sets

- An Availability Set is a logical grouping capability for isolating VM resources from each other when they're deployed. Azure makes sure that the VMs we place within an Availability Set run across multiple physical servers, compute racks, storage units, and network switches.
- Each availability set is assigned:
  - Update domain – Represents group of resources that will be updated together in case of planned and unplanned maintenance event
  - Fault domain - Represents group of resources anticipated to fail together as they consume same network, power, cooling etc.
- When two or more VMs are configured in an Availability Set, connectivity SLA for VMs is 99.95%. There is no cost for Availability Set, the cost incurred is for every VM instance that is created and running.
- Availability Sets should be used for achieve high availability for applications in case of physical host failure in any Azure data center. This can be implemented by distributing VMs across multiple fault domains, behind a load balancer, so that if one physical host incurs a failure, the VM in the other fault domain will take all traffic.

Virtual Machine Scale Sets

Allows you to create and manage a group of load balanced VMs. VM SLA is 99.95% when two or more VM's created.



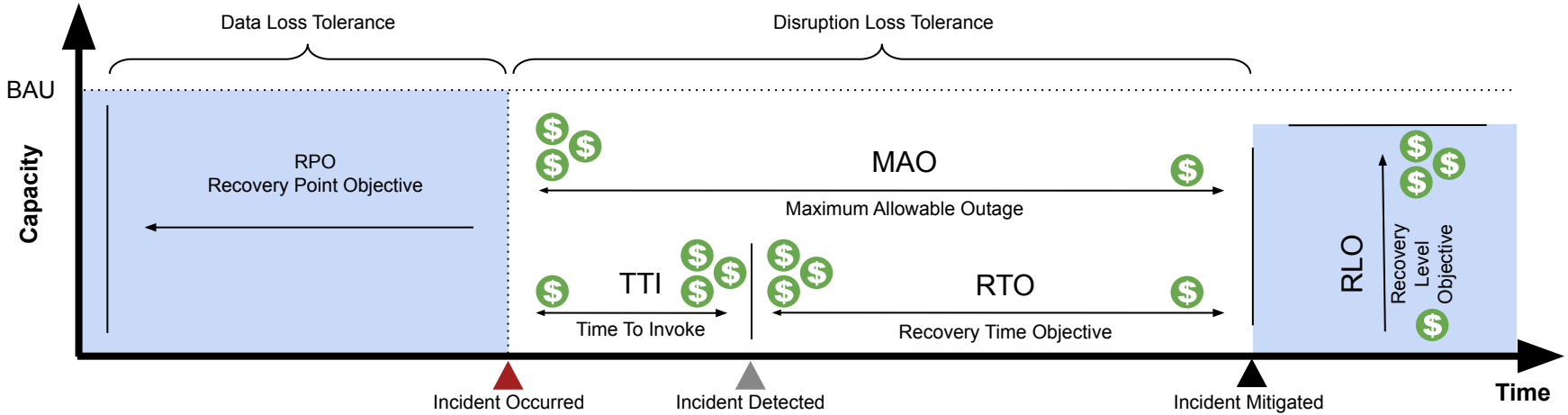
Scalability using VM Scale Sets

- Azure Virtual machine scale sets allow you to create and manage a group of load balanced and identically configured VMs. It automatically scales as resource demand changes.
- Easy to create and manage multiple VMs.
- It provides high availability and application resiliency. Scale sets runs multiple instances of the application, if one of the VMs instances has a problem, users can access the application through one of the other instances with minimal interruption..
- Virtual Machine Scale Sets should be used for applications that have significant swings in traffic throughout the day or week. To match end user demand, scale sets will automatically increase the number of VM instances as application demand increases, and then reduce the number the number of VM instances as demand decreases.

Disaster Recovery

Deconstructing Disaster Recovery Objectives

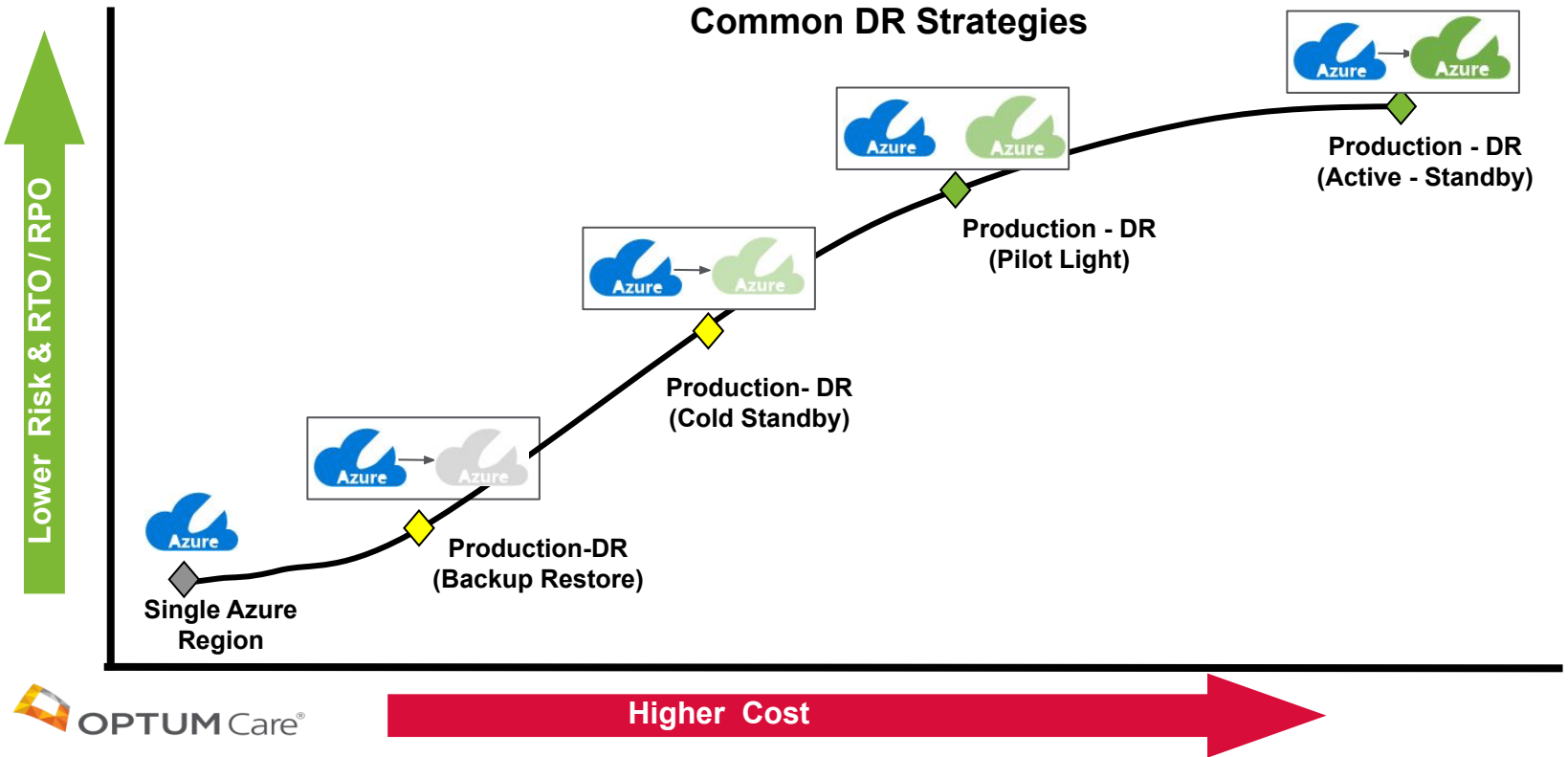
Planning, designing, and testing need to account for more than just RPOs and RTOs



Terminology		
MAO	Maximum Allowable Outage	Time it would take for adverse impacts, which might arise as a result of not providing a product/service or performing an activity, to become unacceptable. (I.e., the elapsed time between an outage and the achievement of the RLO. This must be greater than or equal to the sum of the TTI and RTO)
RLO	Recovery Level Objective	Also referred to as Minimum Business Continuity Objective (MBCO). Minimum level of product/service/activity that is acceptable to the organization to achieve its business objectives during a disruption.
RPO	Recovery Point Objective	Point to which information used by a product/service/activity must be restored to enable the product/service/activity to operate on resumption.
RTO	Recovery TIme Objective	Period of time following an incident within which a product/service/activity/resources must be recovered/resumed.
TTI	Time to Invoke	The elapsed time between point of failure and the invocation of recovery activities. (The recovery activities must be achieved within the stated RTO).
BAU	Business As Usual	The normal services availability and regular execution of operations, as opposed to an exceptional state induced by an unplanned outage or other disruptive event.

Disaster Recovery Strategies

Disaster Recovery architecture strategies are a balance of business risk tolerance to cost; aligned to financial impact of down time. Azure provides a number of options with varying degrees of resiliency.



Disaster Recovery Patterns

Disaster Recovery Design Patterns

DR patterns presented below can be leveraged to develop a disaster recovery system architecture for meeting business requirements for recoverability.

Use Case	DR Pattern	RTO/RPO	TTI	MAO	Implementation Effort	Running Cost (DR)**	Testing Complexity	Skillset Required	Recovery Complexity
Compute	VMs - Hot Standby of Compute Resources w/ CI/CD Parallel Code Deployment	2 - 4 hours	1 - 2 hours	3 - 6 hours	Low	$189 - $741 /month /VM	Low	Manage CI/CD Pipeline	Low (DNS changes required to route traffic to DR region)
	VMs - Hot Standby of Compute Resources w/ Manual Parallel Code Deployment	2 - 4 hours	1 - 2 hours	4 - 7 hours	Med	$189 - $741 /month /VM	Med	Manage Manual Deployment	Low (DNS changes required to route traffic to DR region)
	VMs- Pilot Light Compute Resources w/ CI/CD Parallel Code Deployment	4 - 6 hours	1 - 2 hours	5 - 8 hours	Low	$97 - $373 /month /VM	Low	Manage CI/CD Pipeline	Med (DR VM needs to be scaled up and DNS changes required to route traffic)
	VMs- Pilot Light Compute Resources w/ Manual Parallel Code Deployment	4 - 6 hours	1 - 2 hours	6 - 9 hours	Med	$97 - $373 /month /VM	Med	Manage Manual Deployment	Med (DR VM needs to be scaled up and DNS changes required to route traffic)
	VMs- Cold Standby of Compute Resources using Azure Site Recovery	6 - 8 hours	1 - 2 hours	9 - 11 hours	Med	$25 /month /VM	High	Manage ASR Setup and Failover	High (Manual Failover to replicated VMs and DNS changes)

** Prices are indicative based on the time of writing, and cover a range based on the type of VM selected

Disaster Recovery Design Patterns (cont..)

DR patterns presented below can be leveraged to develop a disaster recovery system architecture for meeting business requirements for recoverability.

Use Case	DR Pattern	RTO/RPO	TTI	MAO	Implementation Effort	Running Cost (DR)**	Testing Complexity	Skillset Required	Recovery Complexity
Database	MS SQL VM - SQL Always on VMs in Azure	4 - 6 hours	1 - 2 hours	6 - 9 hours	High	$1329 - $2882 /month /SQL VM	Med	Manage SQL Always on cluster	High (Promote DR SQL VMs as primary DB copies and application connection string changes)
	Azure SQL DB - Azure SQL DB Geo Redundancy	2 - 4 hours	1 - 2 hours	3 - 6 hours	Low	$368 - $1472 /month /SQL DB	Low	Manage Azure SQL DB Failover Process	Med (Failover to secondary and application connection string changes)
Storage	Azure Storage - Azure Blob Storage Geo Replication	2 - 4 hours	1 - 2 hours	3 - 6 hours	Low	$100 /month /1000 GB	Low	Manage Azure Blob Failover Process	Low (DNS changes to connect to DR Blob storage)
Authentication/ Authorization	Utilize resilient Active Directory deployment	2 - 4 hours	1 - 2 hours	3 - 6 hours	Low	$189 - $741 /month /AD	Low	Manage AD Replication	Low (application to connect to AD instance in DR)

** Prices are indicative based on the time of writing, and cover a range based on the type of VM selected

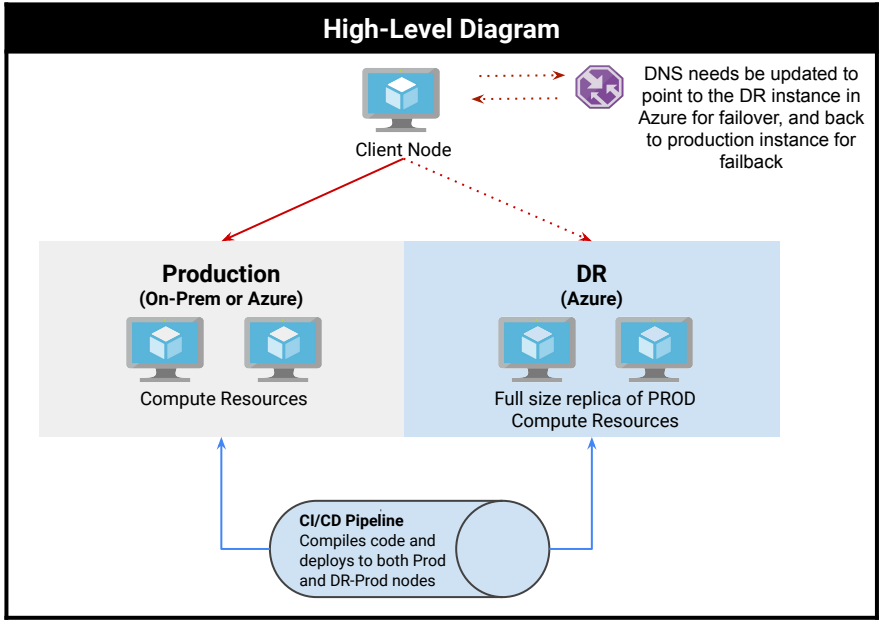
VMs - Hot Standby of Compute Resources w/ CI/CD Parallel Code Deployment

DR Pattern		
Category: Compute	**ID: Compute 1**	**Hot Standby of Compute Resources w/ CI/CD Parallel Code Deployment**
SubCategory: VMs		

Features	
Applicability	On-Prem to Azure Azure to Azure
Protection Method	The DR VMs are left powered on and scaled up (full size). The CI/CD pipeline updates both PROD and DR environment VMs simultaneously
Recovery Method	Update DNS or global load balancing to point to the DR systems
Failback Method	Redeploy compute resources in PROD (if needed) and update DNS or global load balancing to point back to PROD systems

Capabilities (estimated)	
Recovery Time: Low	**Data Loss:** Low

High-Level Diagram



Limitations and Challenges

- Automated deployment pipelines need to be adjusted to accommodate additional nodes in the DR.
- Applications or deployment tools must be capable of deploying to another VM or keeping it in sync.
- Higher cost as a result of additional VMs running in the DR region.

VMs - Hot Standby of Compute Resources w/ Manual Parallel Code Deployment

DR Pattern

Category: Compute	**ID: Compute 2**	**Hot Standby of Compute Resources w/ Manual Parallel Code Deployment**
SubCategory: VMs		

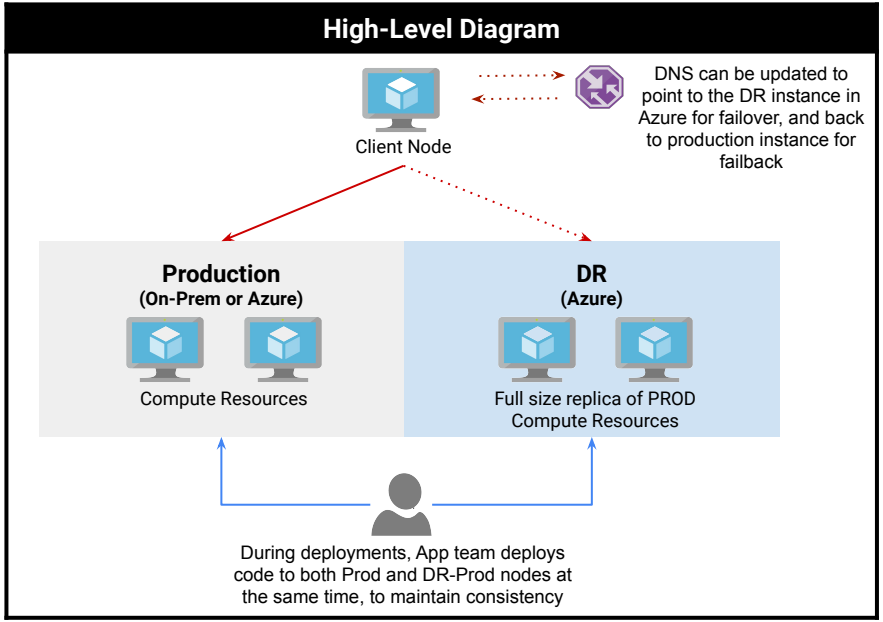
Features

Applicability	On-Prem to Azure Azure to Azure
Protection Method	The DR VMs are left powered on and scaled up (full size). Code updates are manually pushed to the VMs in both the PROD and the DR environments, simultaneously
Recovery Method	Update DNS or global load balancing to point to the DR systems
Failback Method	Redeploy compute resources in PROD (if needed) and update DNS or global load balancing to point back to PROD systems

Capabilities (estimated)

Recovery Time: Low	**Data Loss:** Low

High-Level Diagram



Limitations and Challenges

- Higher cost as a result of additional VMs running in DR region
- Manual deployments are error-prone so end to end functional testing is required.

VMs- Pilot Light Compute Resources w/ CI/CD Parallel Code Deployment

DR Pattern

Category: Compute	**ID: Compute 3**	**Pilot Light Compute Resources w/ CI/CD Parallel Code Deployment**
SubCategory: VMs		

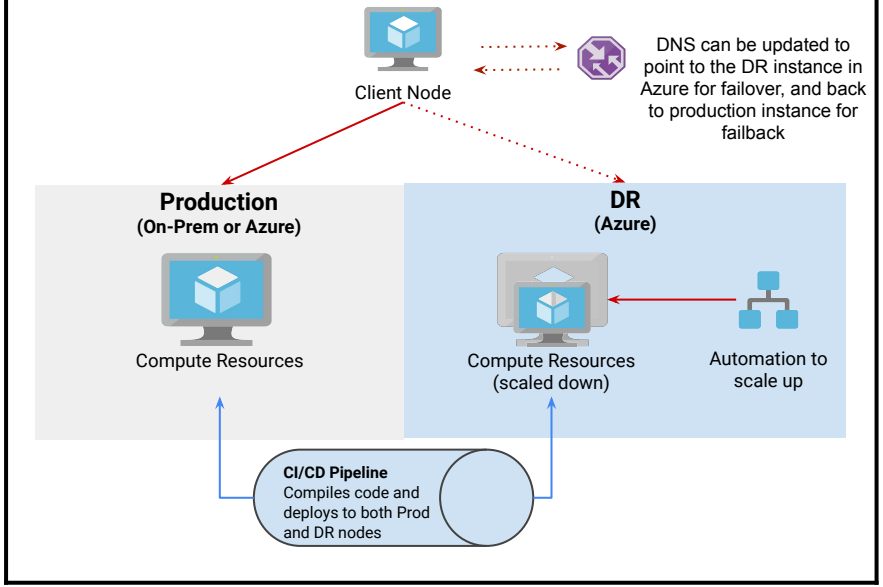
Features

Applicability	On-Prem to Azure Azure to Azure
Protection Method	Deploy a scaled down instance of all compute resources in DR-Prod - then configure the CI/CD pipeline to update nodes in both environments simultaneously
Recovery Method	Utilize automation to scale up DR-Prod footprint to match Production - then update DNS or global load balancing to point to DR-Prod
Failback Method	Redeploy compute resources in Production (if needed) and update DNS or global load balancing to point back to Production

Capabilities (estimated)

Recovery Time: Medium	**Data Loss:** Low

High-Level Diagram



Limitations and Challenges

- Automated deployment pipelines need to be adjusted to accommodate additional nodes in the DR.
- Applications or deployment tools must be capable of deploying to another VM or keeping it in sync.

VMs- Pilot Light Compute Resources w/ Manual Parallel Code Deployment

DR Pattern

Category: Compute	**ID: Compute 4**	**Pilot Light Compute Resources w/ Manual Parallel Code Deployment**
SubCategory: VMs		

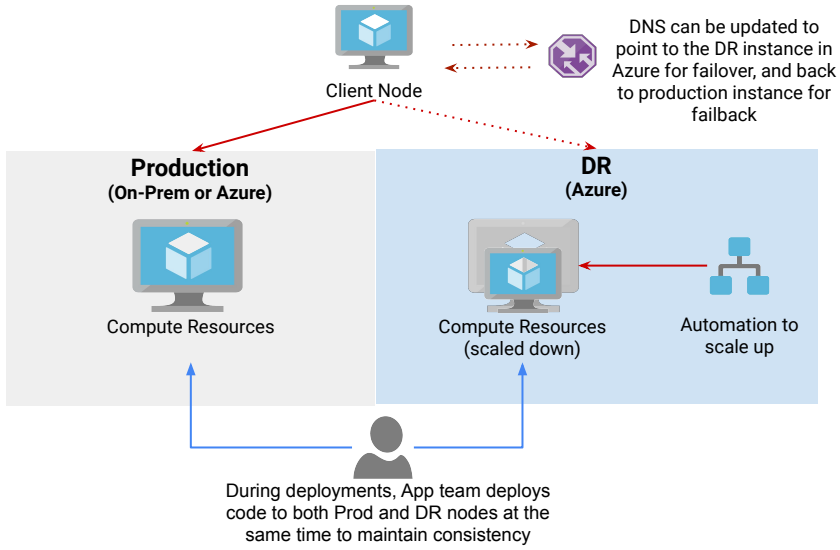
Features

Applicability	On-Prem to Azure Azure to Azure
Protection Method	Deploy a scaled down instance of all compute resources in DR-Prod - for any new deployments, push the code to the nodes in both environments simultaneously
Recovery Method	Utilize automation to scale up DR-Prod footprint to match Production - then update DNS or global load balancing to point to DR-Prod
Failback Method	Redeploy compute resources in Production (if needed) and update DNS or global load balancing to point back to Production

Capabilities (estimated)

Recovery Time: Medium	**Data Loss:** Low

High-Level Diagram



Limitations and Challenges

- Manual deployments are error-prone so end to end functional testing is required.
- The DR environment needs to be scaled up to support the production load.

VMs- Cold Standby of Compute Resources using Azure Site Recovery

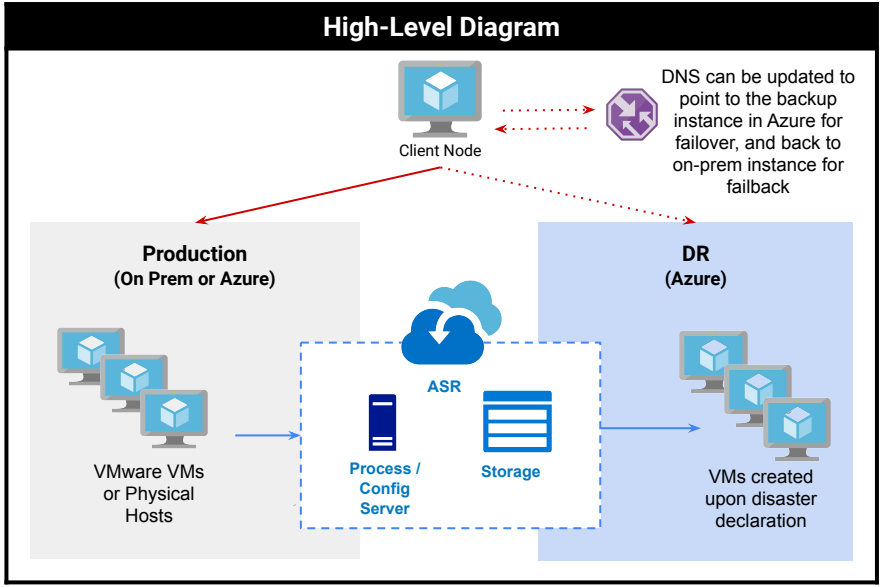
DR Pattern		
Category: Compute	**ID: Compute 5**	**Cold Standby of Compute Resources using Azure Site Recovery**
SubCategory: VMs		

Features	
Applicability	On-Prem to Azure Azure to Azure
Protection Method	Asynchronous Replication: VM snapshots are saved periodically to an Azure Storage account
Recovery Method	VMs are built in the recovery site using the backups saved in Azure. Then DNS is updated to point to the DR environment
Failback Method	Stable-state image replicated back to production VM. Then DNS is updated to point back to production

Capabilities (estimated)	
Recovery Time: Medium	**Data Loss:** Medium

Replication
Failover
Prod resources (On-prem / Azure)
DR resources (Azure)

High-Level Diagram



Limitations and Challenges

- Application Team/IT need to have ASR technical know-how on how to use it
- Restored copies are crash consistent
- ASR automatically configures new resource groups and vnets in DR region, however with Cisco ACI network orchestration we need to change ASR config to use pre-defined resource groups and vnets in DR region

OPTUM Care®

MS SQL VM - SQL Always on to VMs in Azure

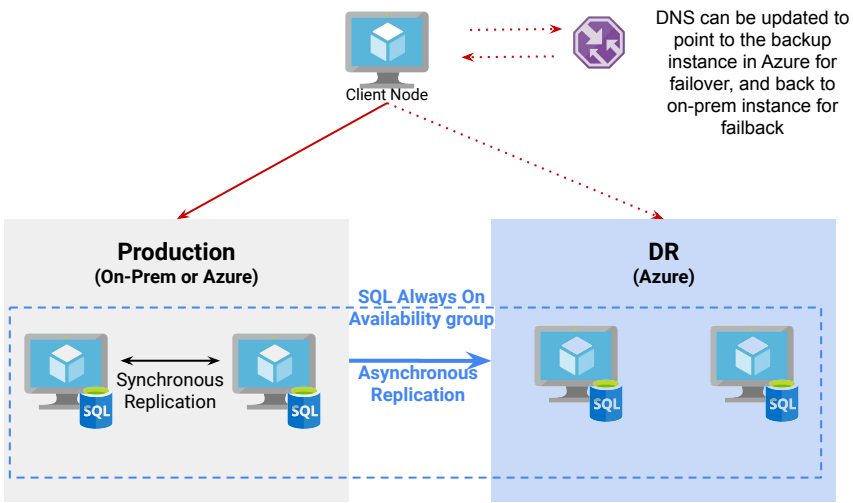
DR Pattern		
Category: Databases	**ID:** **Database 1**	**SQL Always on VMs in Azure**
SubCategory: MS SQL VM		

Features	
Applicability	On-Prem to Azure Azure to Azure
Protection Method	Synchronous or Asynchronous Replication with SQL Always On
Recovery Method	Upon declaration of disaster, DNS is will update to redirect traffic to DR-Prod cluster in Azure
Failback Method	Re-establish production cluster and allow data to resync, then perform a planned failback

Capabilities (estimated)	
Recovery Time: Low	**Data Loss:** Low

Replication
Failover
Prod resources (On-prem / Azure)
DR resources (Azure)

High-Level Diagram



Limitations and Challenges

- A node in Azure would likely be too latent for synchronous replication
- Higher cost to run additional SQL VMs in DR region.

OPTUMCare

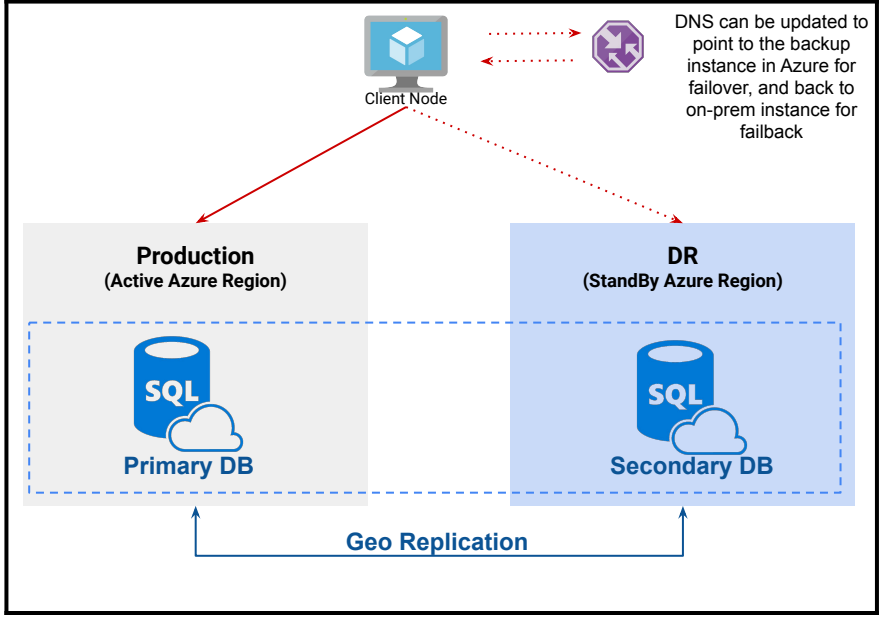
Azure SQL DB - Azure SQL DB Geo Redundancy

DR Pattern		
Category: Databases	**ID-Database 2**	**Azure SQL DB Geo Redundancy**
SubCategory: Azure SQL DB		

Features	
Applicability	Azure to Azure
Protection Method	Create a readable secondary replica in a different region
Recovery Method	Fail over to a secondary database when primary database fails or needs to be taken offline. Active Geo-Replication can be configured for any database in any elastic database pool.
Failback Method	Re-establish production cluster and allow data to resync, then perform a planned failback

Capabilities (estimated)	
Recovery Time: Low	**Data Loss:** Low

High-Level Diagram



Limitations and Challenges

- Additional cost to run a secondary instance of Azure SQL DB in DR region.

Privileged and Confidential | DRAFT

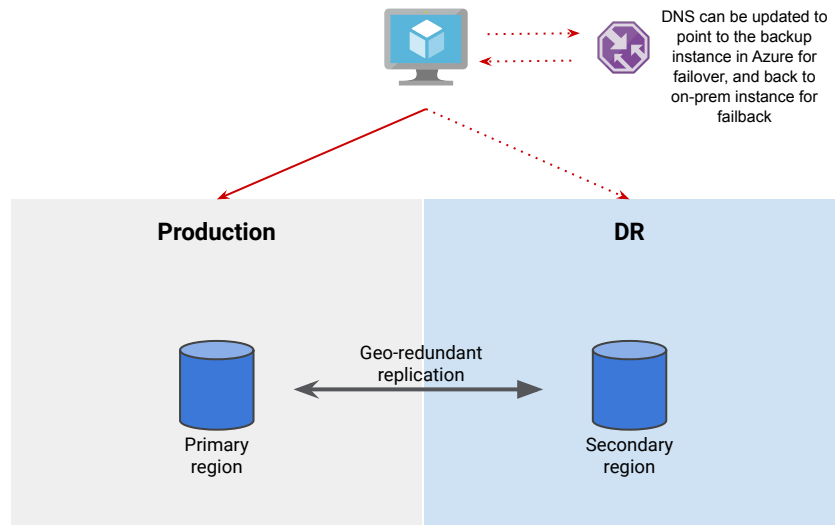
Azure Storage - Azure Blob Storage Geo Replication

DR Pattern		
Category: Storage	**ID-Storage 1**	**Azure Blob Storage Geo Replication**
SubCategory: Azure Storage		

Features	
Applicability	Azure to Azure
Protection Method	Geo-redundancy: Asynchronously replicates the data to DR region. Secondary endpoint can be used for read access to ensure replication is successful and reduce load on primary region
Recovery Method	In case of primary region outage, failover is initiated to transform the secondary endpoint to primary endpoint
Failback Method	Initiate replication from the secondary region blob to primary region once its operational, connect to primary.

Capabilities (estimated)	
Recovery Time: Low	**Data Loss:** Low

High-Level Diagram



Limitations and Challenges

- Additional cost to run a secondary copy of Azure Blob storage in DR region.

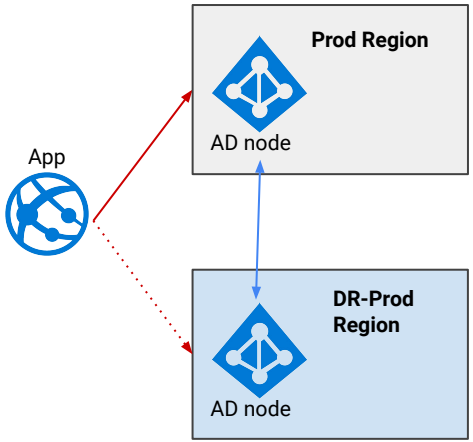
Utilize resilient Active Directory deployment

DR Pattern		
Category: Authentication / Authorization	**ID: AD 1**	**Utilize resilient Active Directory deployment**
SubCategory: AD		

Features	
Applicability	Any application that requires Active Directory
Protection Method	Configure applications to reference AD by DNS name (e.g. domain1.com) and not individual domain controller IPs
Recovery Method	The application will continue to seamlessly communicate with AD without manual changes
Failback Method	The application will continue to seamlessly communicate with AD without manual changes

Capabilities (estimated)	
Recovery Time: Low	**Data Loss:** Not Applicable - Applications typically poll AD periodically and retry as needed

High-Level Diagram



Challenges	
Limitations	- Application **must** support locating AD services by DNS
Supportability	- Industry standard deployment - Fully supported by Microsoft

Replication
Failover
Prod resources (On-prem / Azure)
DR resources (Azure)

Thank You