Microsoft

Architecting for Resiliency

Andrej Kasnik – Sr FastTrack Engineer
Barney Gwyther – Sr FastTrack Engineer

What is FastTrack for Azure?

Provides you with technical guidance from subject matter experts in Azure engineering

Collaborates with your team to help accelerate and de-risk implementation of workloads in Azure, regardless of your level of cloud experience

Enables you to correctly and confidently continue your Azure journey – at no additional cost

Learn more at aka.ms/fta

What is FastTrack for Azure Live?

A series of multi-customer live sessions delivered by FastTrack for Azure PMs and engineers in an interactive format allowing you, our customers, to directly engage and have your questions answered

Learn more at aka.ms/ftalive

Why is Reliability Important?

Failures happen.

Reliable applications require *resilience*

Reliability

Reliability is the ‘**what**’.

It is the goal for production systems, to ensure availability of their services.

The goal is to maintain reliable systems, with the appropriate level of availability/uptime.

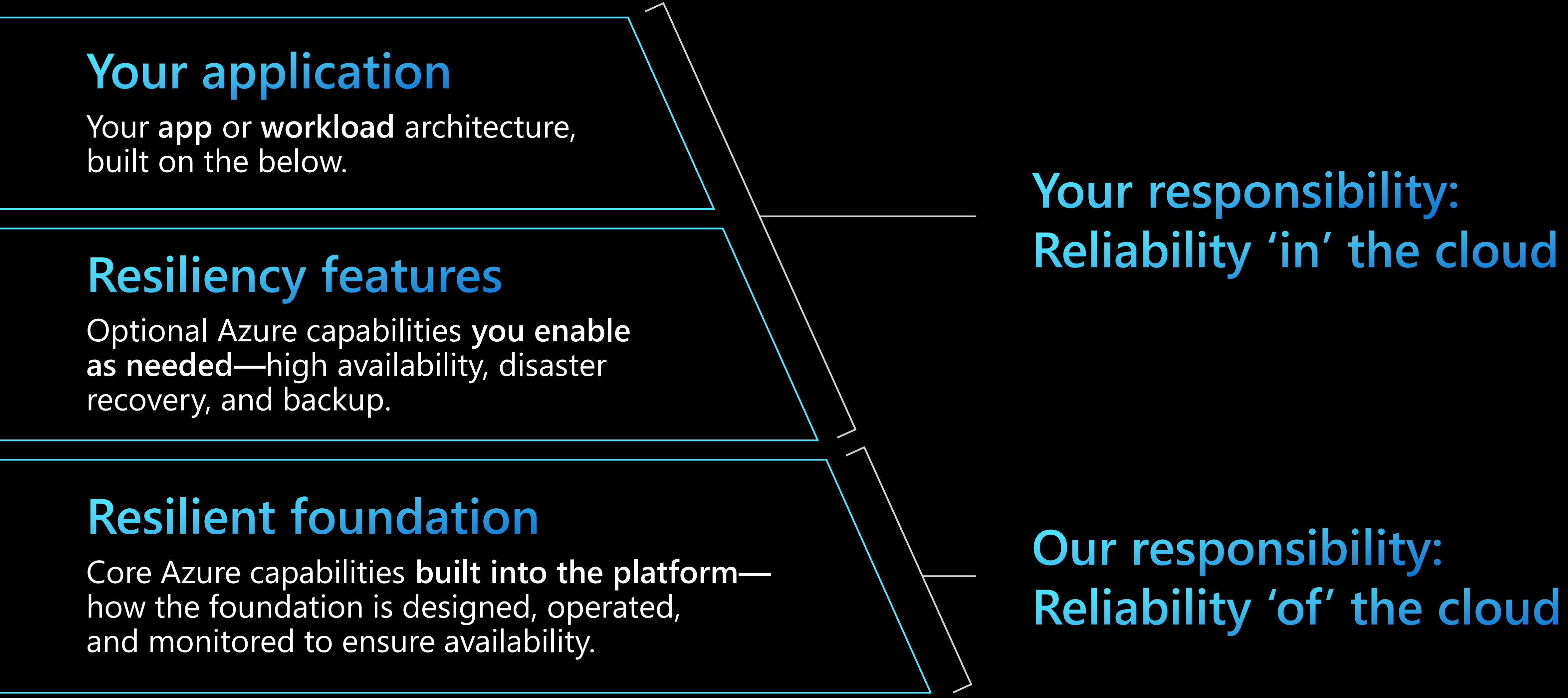
Resilience

Resilience is the ‘**how**’.

It is the way in which production systems can achieve reliability.

The objective is not to avoid any and all failures – it is to ***respond to failure in a way that avoids downtime and data loss***.

Building reliable systems is a shared responsibility



Your application

Your **app** or **workload** architecture, built on the below.

Resiliency features

Optional Azure capabilities **you enable as needed**—high availability, disaster recovery, and backup.

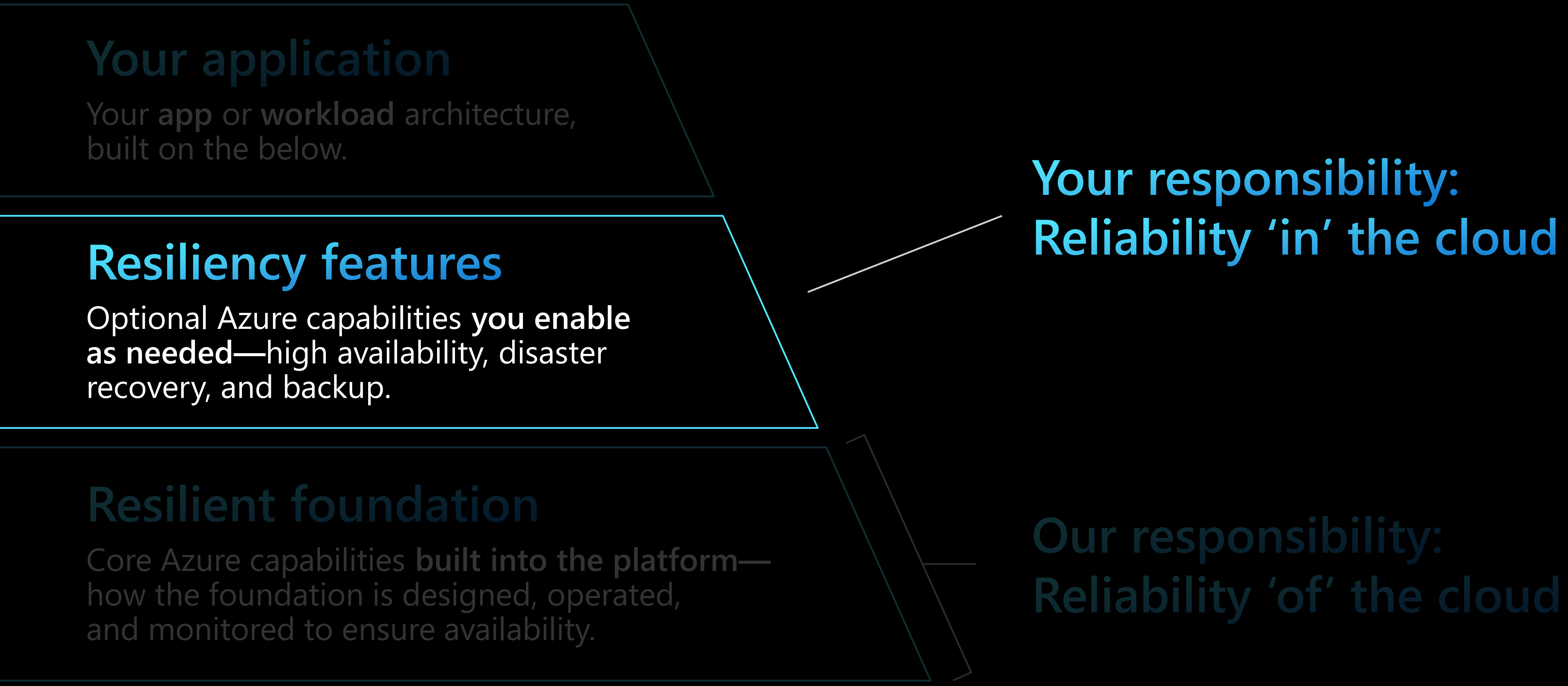
Resilient foundation

Core Azure capabilities **built into the platform**—how the foundation is designed, operated, and monitored to ensure availability.

Your responsibility:
Reliability ‘in’ the cloud

Our responsibility:
Reliability ‘of’ the cloud

Building reliable systems is a shared responsibility



Your application

Your **app** or **workload** architecture, built on the below.

Resiliency features

Optional Azure capabilities **you enable as needed**—high availability, disaster recovery, and backup.

Resilient foundation

Core Azure capabilities **built into the platform**—how the foundation is designed, operated, and monitored to ensure availability.

Your responsibility: Reliability ‘in’ the cloud

Our responsibility: Reliability ‘of’ the cloud

Customer need

Improved availability

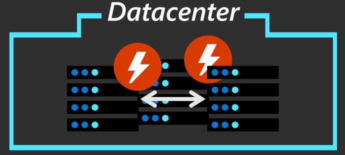
Build and run *highly-available* applications with near-zero RPO/RTO

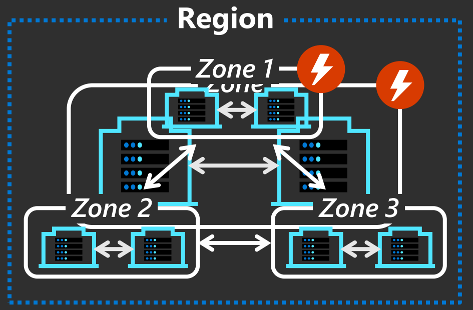
Implement *disaster recovery plans* with data residency and minimal RPO/RTO

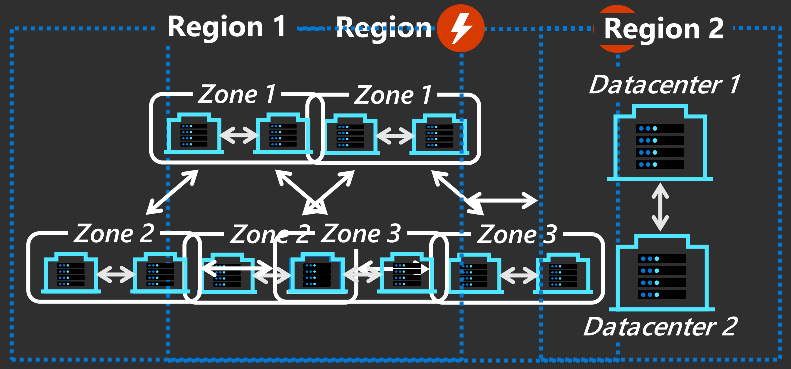
Premium Storage | Availability Sets | Availability Zones | Azure Site Recovery/Region Pairs

Infrastructure (applications and data)

Single VM







Scope of Impact...

SLA 99.9%

SLA 99.95%

SLA 99.99%

Industry-leading RPO/RTO

Isolated VM failure
e.g., OS disk HDD issue

Hardware failure
e.g., server rack issue

Entire datacenter failure
e.g., power/network issue

Entire region failure
e.g., natural disaster

Data (stateful)

Accidental data loss | Data corruption | Ransomware | Rogue administrator

Backup

Go back to *restore* a healthy version of the data

The Microsoft Azure Well-Architected Framework

Architecture guidance and best practices created for architects, developers, and solution owners, to improve the quality of their workloads, based on five aligned and connected pillars...

Cost Optimization

Operational Excellence

Performance Efficiency

Reliability

Security

Learn more: aka.ms/WellArchitected/Framework

Your responsibility: Reliability 'in' the cloud

Aligned to the Azure Well-Architected Framework: aka.ms/WellArchitected/Framework

Design

recommendations

- Availability needs
- Composite SLAs
- Failure Mode Analysis
- Availability Zones (AZs)
- PaaS service highlights

Testing

recommendations

- Testing checklist
- Chaos engineering
- Fault injection
- Azure Chaos Studio

Monitoring

recommendations

- Monitoring checklist
- Alerting disambiguation
- Service Health alerts
- Scheduled Events

Service level acronyms

Understanding your uptime requirements informs your priorities for monitoring & resilience

S.L.I.

Service Level Indicator

...any **measurement.**

e.g., What percentage of this system's user requests are processed within 5 seconds?

S.L.O.

Service Level Objective

...any SLI with a **target.**

e.g., 99% of user requests processed within 5 seconds, over a trailing 1-hour period.

S.L.A.

Service Level Agreement

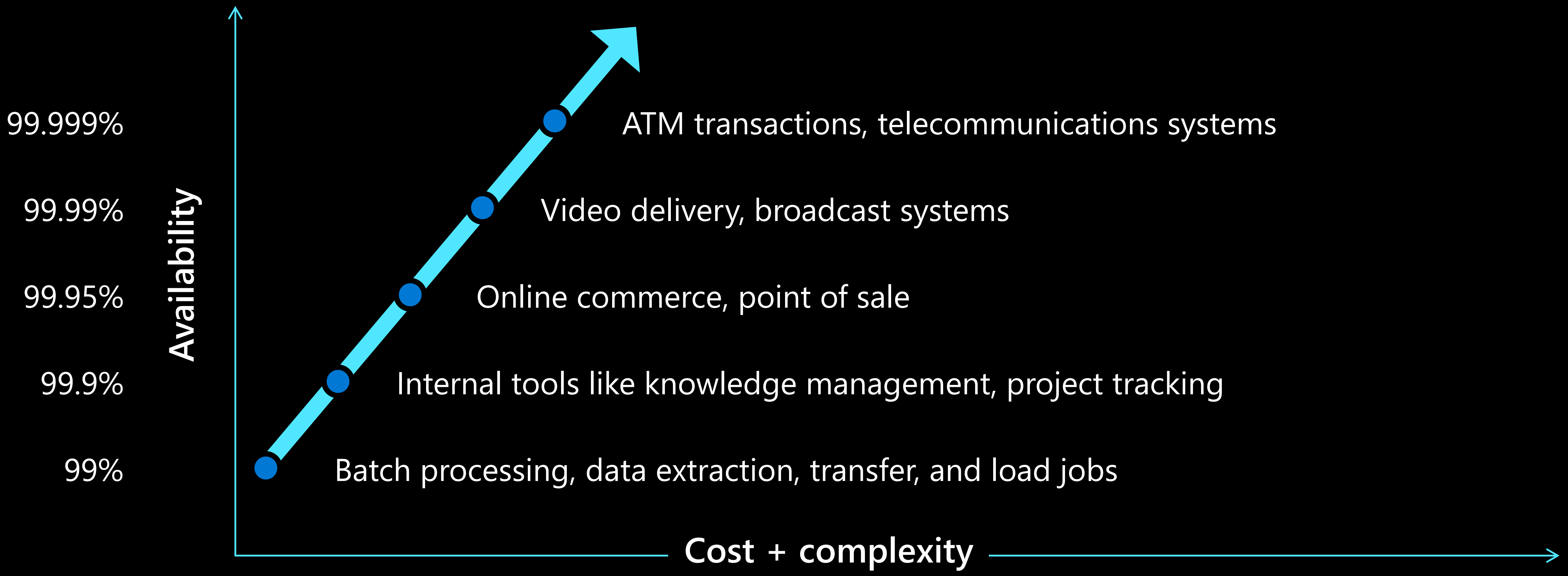
...any SLO in the **contract.**

e.g., We guarantee >99% of user requests will be processed within 5 seconds, OR [credit policy].

* Understand Composite SLA

Application availability needs

Examples of applications commonly seen at each availability tier



Availability

99.999% ATM transactions, telecommunications systems

99.99% Video delivery, broadcast systems

99.95% Online commerce, point of sale

99.9% Internal tools like knowledge management, project tracking

99% Batch processing, data extraction, transfer, and load jobs

Cost + complexity

Service Level Agreements Summary | Microsoft Azure

Azure SLA Board (azurecharts.com)

Failure Mode Analysis (FMA)

A process for building resiliency into a system, by identifying possible failure points

FMA should be part of the architecture/design phases, to build failure recovery in from the outset.

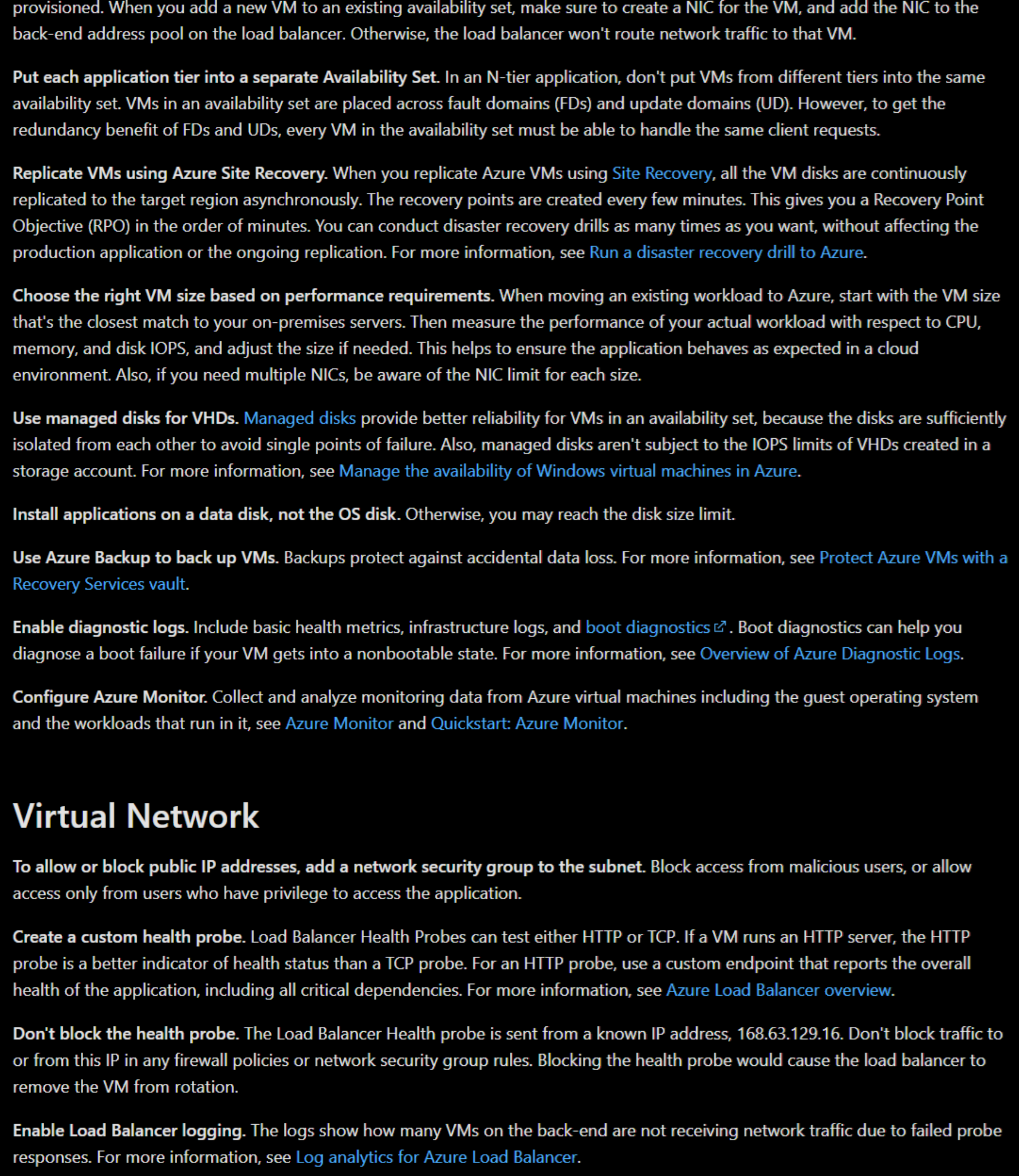
Here is the general process to conduct an FMA:

1. Identify all of the components in the system.
2. For each component, identify potential failures that could occur.
3. Rate each failure mode according to its overall risk.
4. For each failure mode, determine how the application will respond and recover.

*The **Azure Architecture Center** includes a catalog of potential failure modes and their mitigation steps. The catalog is organized by technology or Azure service, plus a general category for application-level design. The catalog is not exhaustive, but covers many of the core Azure services.*

Resiliency checklist for specific Azure services

Resiliency checklist for Azure services - Azure Design Review Framework | Microsoft Docs



provisioned. When you add a new VM to an existing availability set, make sure to create a NIC for the VM, and add the NIC to the back-end address pool on the load balancer. Otherwise, the load balancer won't route network traffic to that VM.

Put each application tier into a separate Availability Set. In an N-tier application, don't put VMs from different tiers into the same availability set. VMs in an availability set are placed across fault domains (FDs) and update domains (UD). However, to get the redundancy benefit of FDs and UDs, every VM in the availability set must be able to handle the same client requests.

Replicate VMs using Azure Site Recovery. When you replicate Azure VMs using Site Recovery, all the VM disks are continuously replicated to the target region asynchronously. The recovery points are created every few minutes. This gives you a Recovery Point Objective (RPO) in the order of minutes. You can conduct disaster recovery drills as many times as you want, without affecting the production application or the ongoing replication. For more information, see Run a disaster recovery drill to Azure.

Choose the right VM size based on performance requirements. When moving an existing workload to Azure, start with the VM size that's the closest match to your on-premises servers. Then measure the performance of your actual workload with respect to CPU, memory, and disk IOPS, and adjust the size if needed. This helps to ensure the application behaves as expected in a cloud environment. Also, if you need multiple NICs, be aware of the NIC limit for each size.

Use managed disks for VHDs. Managed disks provide better reliability for VMs in an availability set, because the disks are sufficiently isolated from each other to avoid single points of failure. Also, managed disks aren't subject to the IOPS limits of VHDs created in a storage account. For more information, see Manage the availability of Windows virtual machines in Azure.

Install applications on a data disk, not the OS disk. Otherwise, you may reach the disk size limit.

Use Azure Backup to back up VMs. Backups protect against accidental data loss. For more information, see Protect Azure VMs with a Recovery Services vault.

Enable diagnostic logs. Include basic health metrics, infrastructure logs, and boot diagnostics. Boot diagnostics can help you diagnose a boot failure if your VM gets into a nonbootable state. For more information, see Overview of Azure Diagnostic Logs.

Configure Azure Monitor. Collect and analyze monitoring data from Azure virtual machines including the guest operating system and the workloads that run in it, see Azure Monitor and Quickstart: Azure Monitor.

Virtual Network

To allow or block public IP addresses, add a network security group to the subnet. Block access from malicious users, or allow access only from users who have privilege to access the application.

Create a custom health probe. Load Balancer Health Probes can test either HTTP or TCP. If a VM runs an HTTP server, the HTTP probe is a better indicator of health status than a TCP probe. For an HTTP probe, use a custom endpoint that reports the overall health of the application, including all critical dependencies. For more information, see Azure Load Balancer overview.

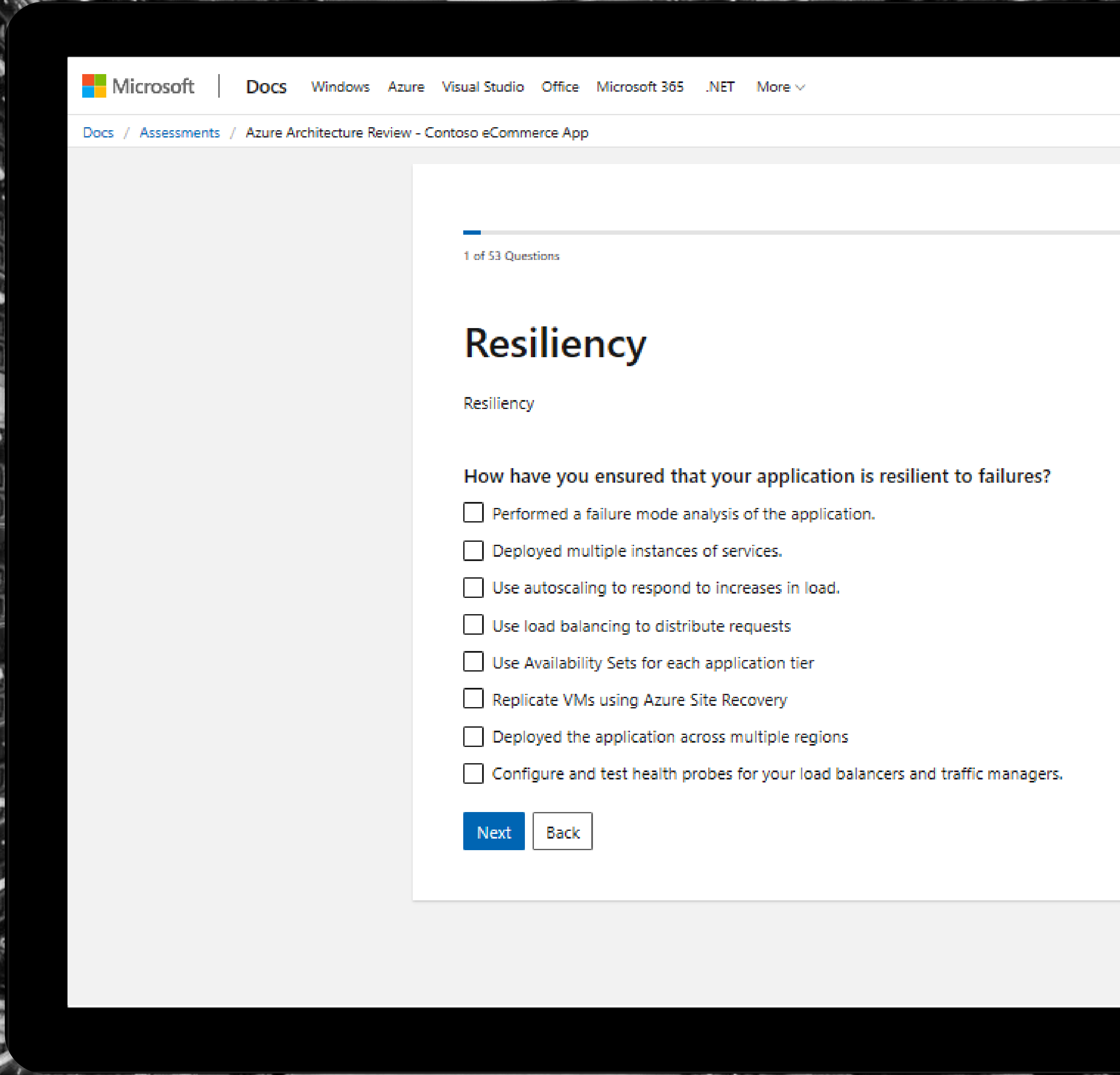
Don't block the health probe. The Load Balancer Health probe is sent from a known IP address, 168.63.129.16. Don't block traffic to or from this IP in any firewall policies or network security group rules. Blocking the health probe would cause the load balancer to remove the VM from rotation.

Enable Load Balancer logging. The logs show how many VMs on the back-end are not receiving network traffic due to failed probe responses. For more information, see Log analytics for Azure Load Balancer.

Microsoft Azure Architecture Review

The Azure Architecture Framework and the associated Azure Architecture Assessment are tools for customers to optimize their workloads across the five pillars—Cost, DevOps, Scalability, Resiliency, and Security.

aka.ms/ArchitectureReview



Docs / Assessments / Azure Architecture Review - Contoso eCommerce App

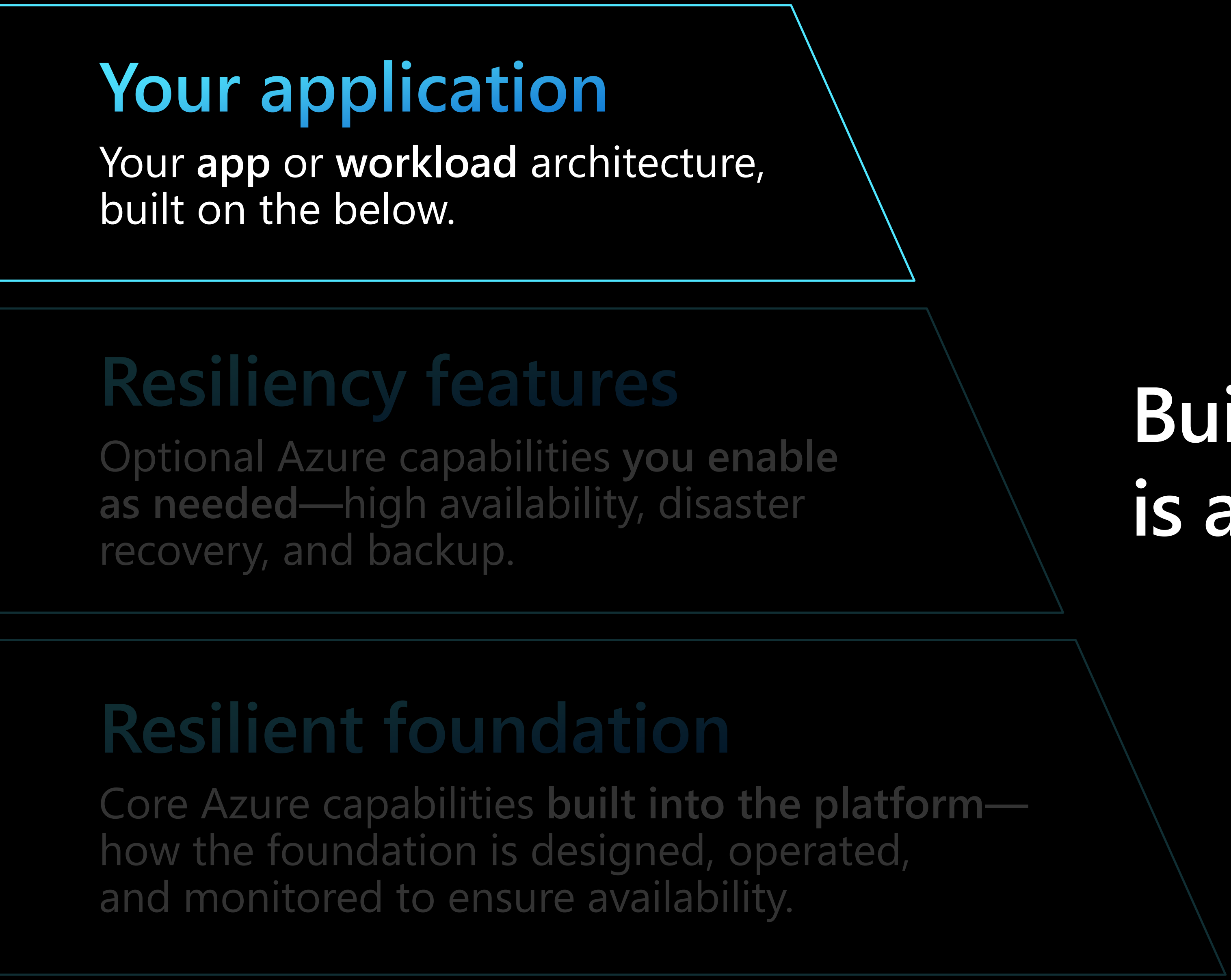
1 of 53 Questions

Resiliency

Resiliency

How have you ensured that your application is resilient to failures?

- □ Performed a failure mode analysis of the application.
- □ Deployed multiple instances of services.
- □ Use autoscaling to respond to increases in load.
- □ Use load balancing to distribute requests
- □ Use Availability Sets for each application tier
- □ Replicate VMs using Azure Site Recovery
- □ Deployed the application across multiple regions
- □ Configure and test health probes for your load balancers and traffic managers.



Your application

Your **app** or **workload** architecture, built on the below.

Resiliency features

Optional Azure capabilities **you enable as needed**—high availability, disaster recovery, and backup.

Resilient foundation

Core Azure capabilities **built into the platform**—how the foundation is designed, operated, and monitored to ensure availability.

Building reliable systems is a shared responsibility

Patterns for resilient cloud applications

Azure Application Architecture Fundamentals - Azure Architecture Center | Microsoft Docs

Resilience pattern: high-availability (99.95% SLA)

Business need

Protect applications and data from hardware and software update failures.

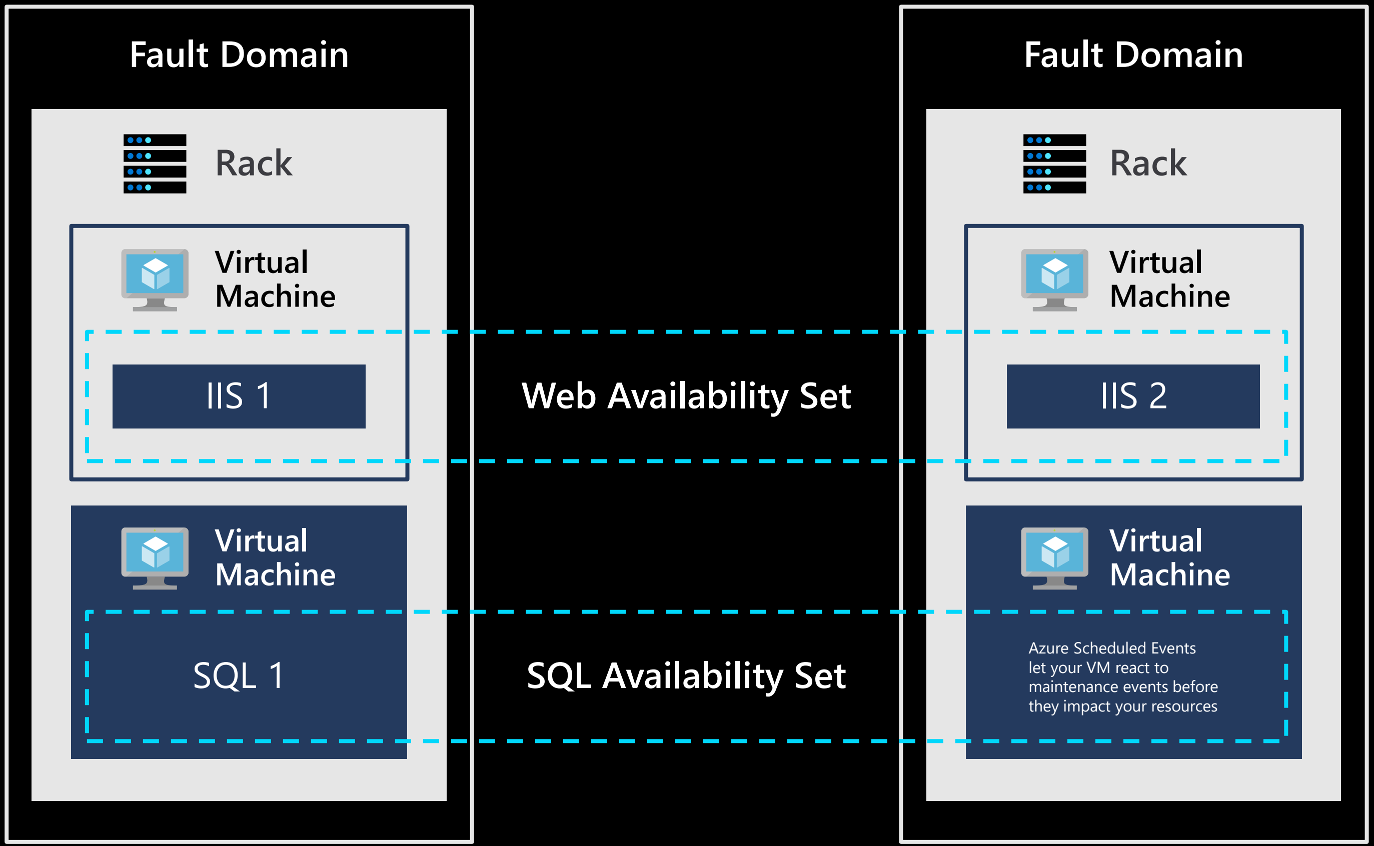
Build and run highly-available active/active applications with synchronous replication.

Latency sensitive applications with <1ms VM-to-VM RTT.

Azure Solution

An Availability Set is a logical grouping to ensure virtual machines are isolated from each other within an Azure datacenter.

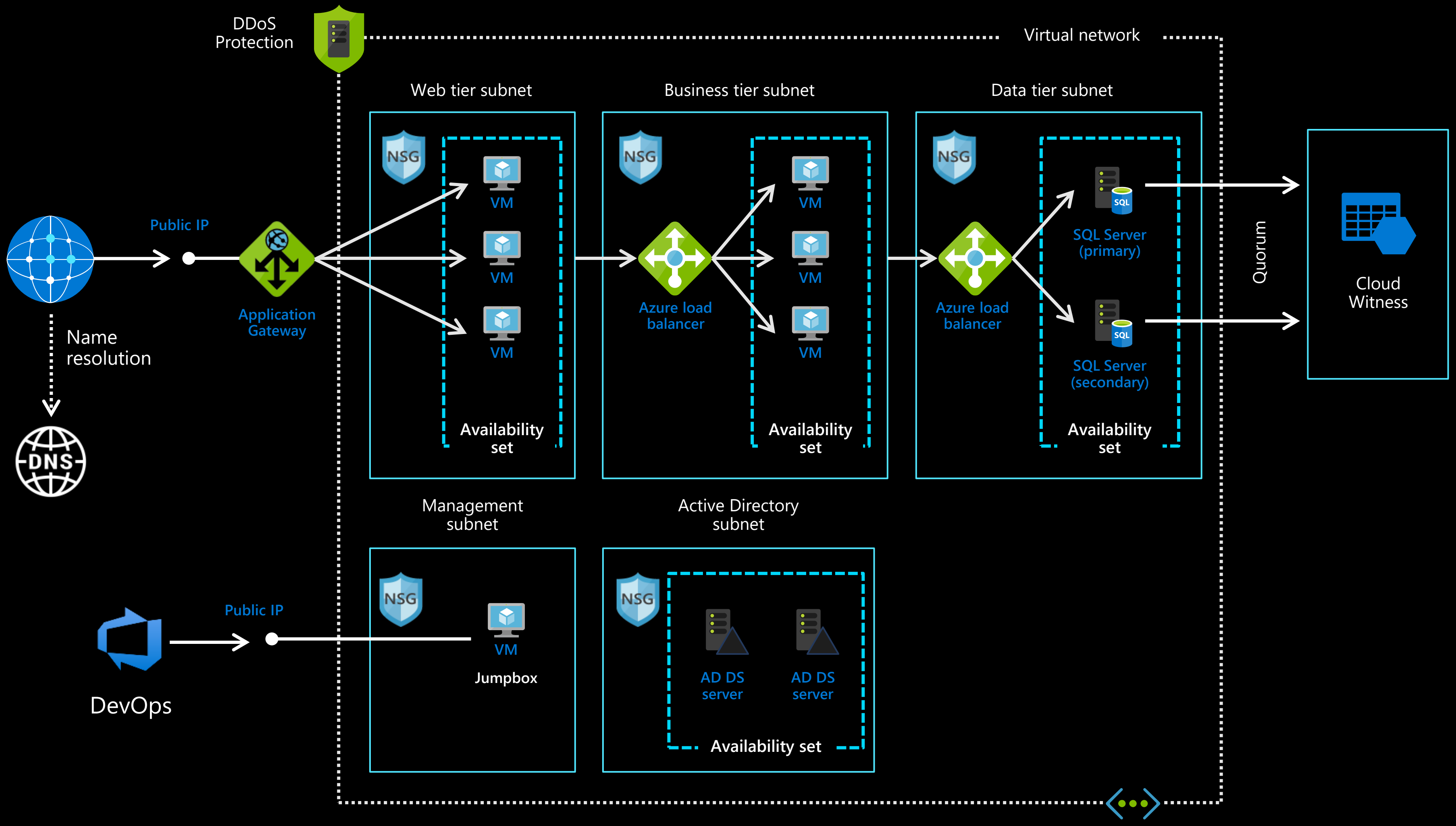
Azure platform distributes VMs within an Availability Set across FDs and UDs providing high-availability.



Fault Domain: a logical group of underlying hardware that share a common power source and network switch, within a datacenter.

Update Domain: a logical group of underlying hardware that can undergo maintenance or be rebooted at the same time.

Resilience pattern: high-availability (99.95% SLA)



Resilience pattern: high-availability (99.99% SLA)

Business need

Protect applications and data from datacenter and software update failures.

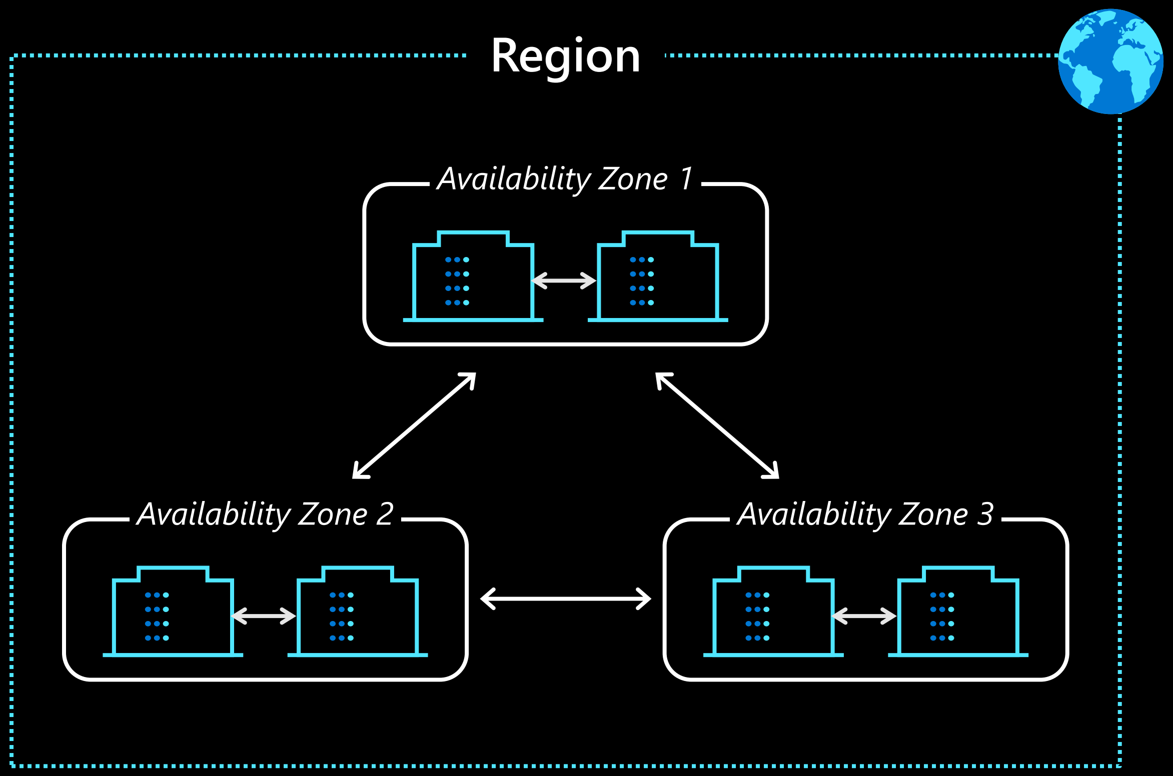
Build and run highly-available active/active applications with synchronous replication.

Azure Solution

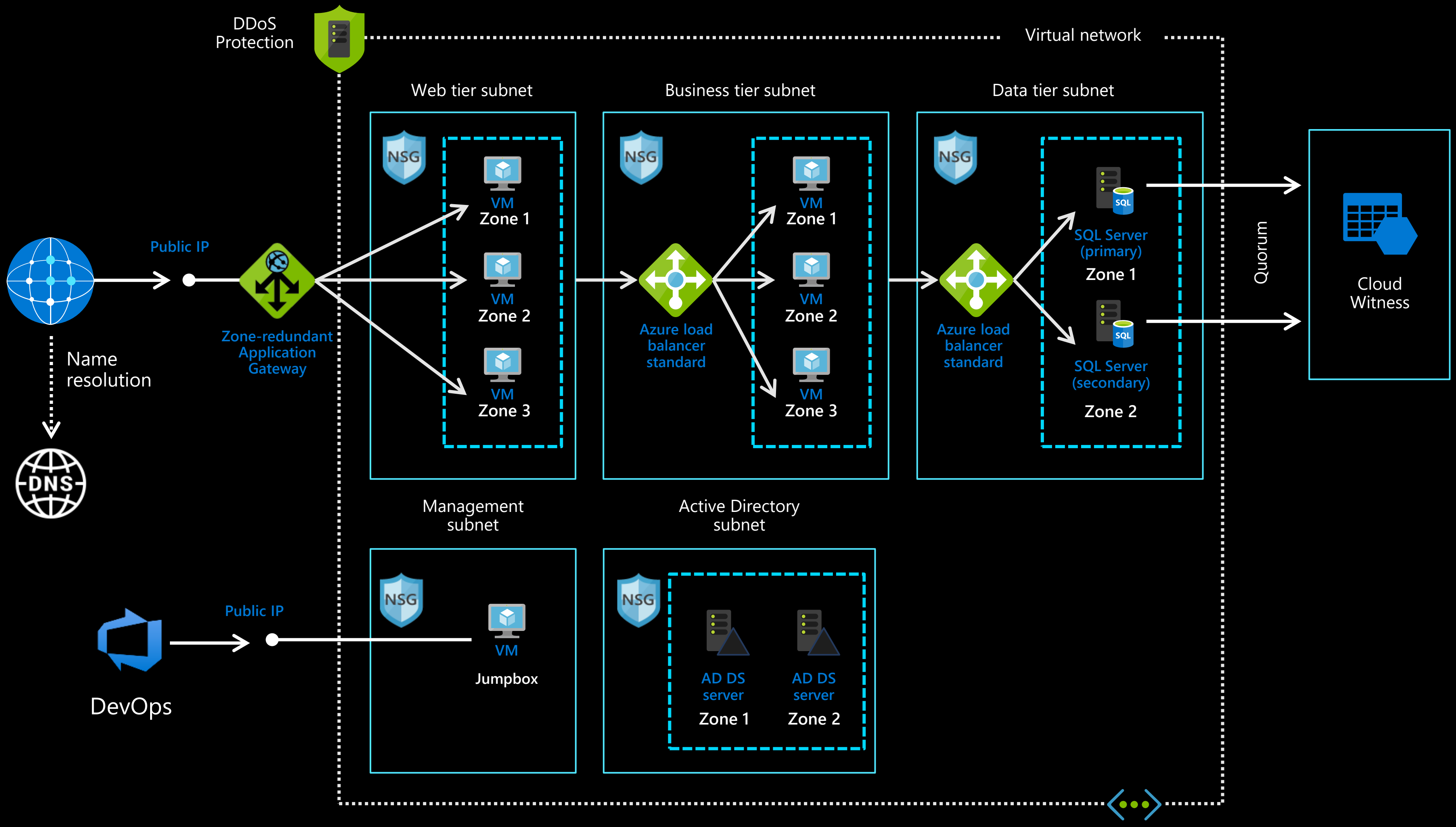
Availability Zones are unique physical locations within an Azure region.

Each Zone consists of one or more datacenters with independent power, cooling and networking.

Availability Zones are designed to meet <2ms VM-to-VM RTT within an Azure region.



Resilience pattern: high-availability (99.99% SLA)



Resilient design pattern:
generic IaaS multi tier application DR

Business need

Protect applications from datacenter and regional failures.

DR should be planned to meet compliance.

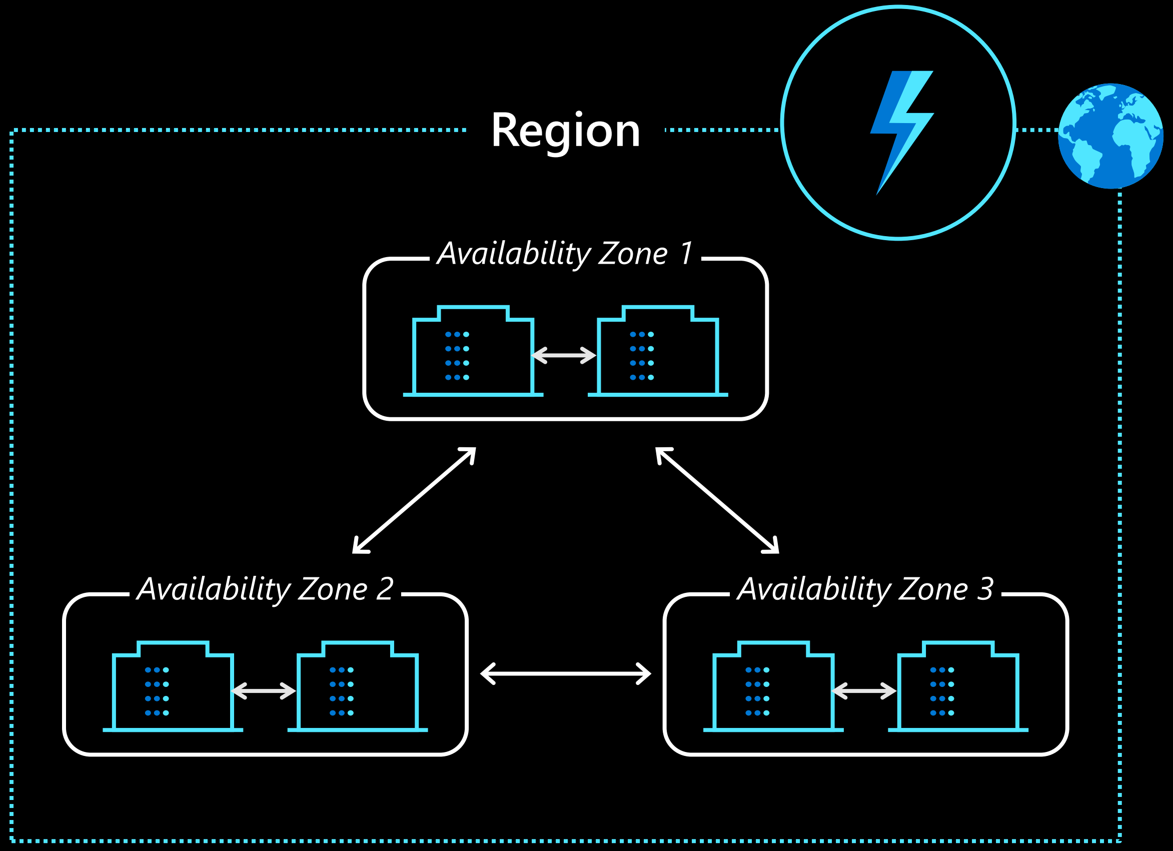
Build highly resilient applications with both high availability and disaster recovery.

Azure Solution

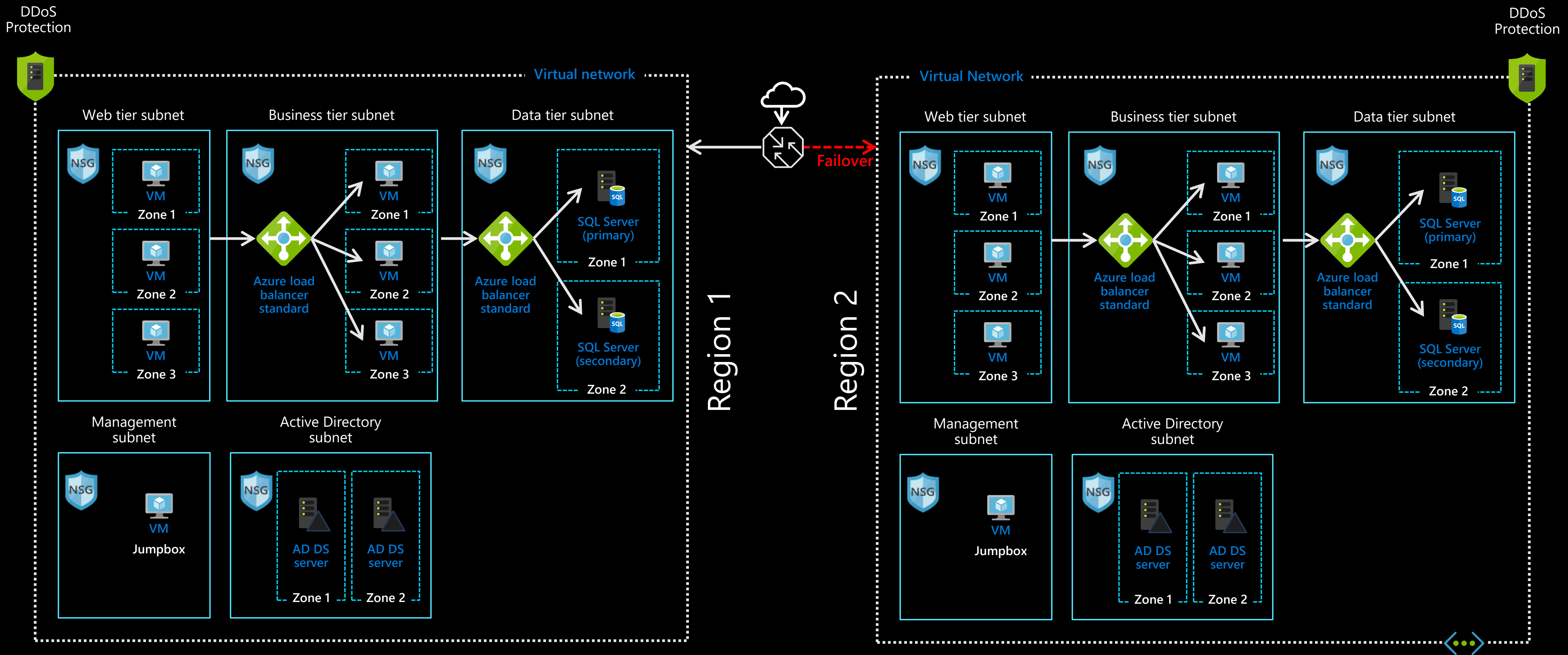
Azure Site Recovery (ASR) replicates VMs to another region within a geographic cluster.

Use database replication to replication data to another region.

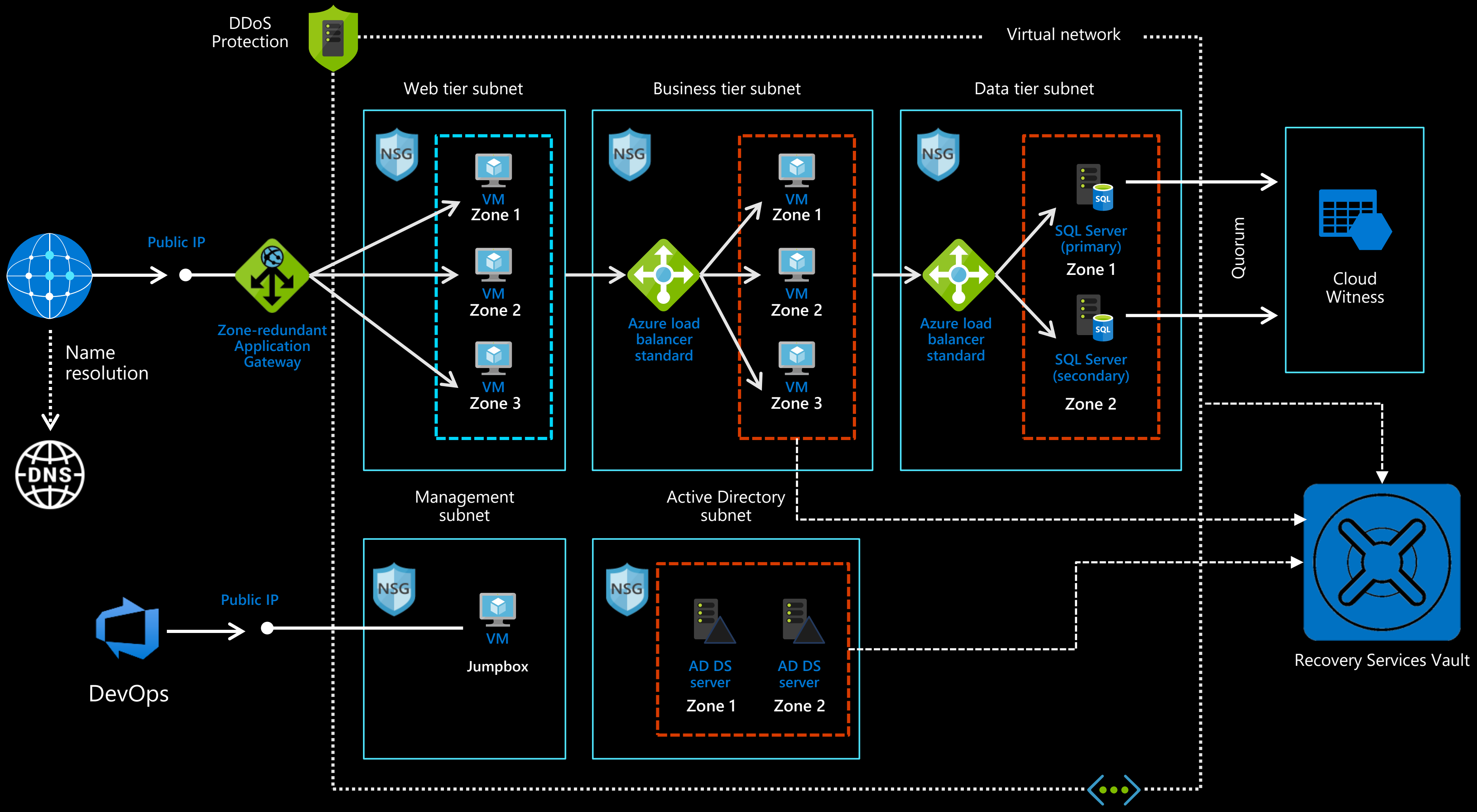
Implement Availability zones for HA in source region to get protection from hardware and datacenter failures.



Use Azure Site Recovery for DR Orchestration and leverage VM replication of ASR and database replication



Use Azure Backup for all data protection scenarios



Designing resilient applications in Azure

Best practices

Method of designing a resilient application
https://docs.microsoft.com/en-us/azure/architecture/Resilience

Constructing a high available application in Azure
https://docs.microsoft.com/en-us/azure/architecture/Resilience/high-availability-azure-applications

Backup and archive your application
https://azure.microsoft.com/en-us/solutions/architecture/backup-archive-cloud-application/

Architecture of designing Disaster recovery
https://azure.microsoft.com/en-us/solutions/architecture/disaster-recovery-smb-azure-site-recovery/

Best practices in creating SAP/HANA with high availability and Disaster recovery in place
https://azure.microsoft.com/en-us/solutions/architecture/sap-s4-hana-on-hli-with-ha-and-dr/

Backup, high availability, and disaster recovery services

Build high availability applications with Availability Zones

Visit the Azure regions page for availability:
http://aka.ms/AzureRegions

Learn more about Availability Zones:
http://aka.ms/AzureAZs

Build a comprehensive Resilience strategy:
http://aka.ms/Resilience
http://aka.ms/AZoverview

Protect your data with Azure Backup

Azure Backup landing page:
https://aka.ms/azure-backup

Azure Backup's Cloud-First approach:
https://aka.ms/azure-backup-cloud-first

Azure Backup blogs:
https://aka.ms/azure-backup-blogs

Azure Backup videos:
https://aka.ms/azurebackupvideos

Azure Backup documentation:
https://aka.ms/azure-backup-documentation

Azure Backup support forum:
https://aka.ms/azure-backup-support-forum

Feedback (user voice
https://aka.ms/azure-backup-user-voice

Ensure application availability with Azure Site Recovery

Support matrix for replicating one Azure region to another

Site Recovery documentation:
https://aka.ms/siterecovery_documentation

Site Recovery blogs:
https://aka.ms/siterecovery_blogs

Site Recovery Academy Course:
https://aka.ms/siterecovery_mva

Support forum:
https://aka.ms/asrforum

Feedback (user voice):
https://aka.ms/ASRuservoice

Application capabilities

PaaS Application/Compute/ Integration resilience

- Auto Scale in App Services
- High density hosting on Azure App Service using per-app scaling
- Azure Service Fabric Reliable Services
- Auto Scale in API Management
- Service Bus Geo-Disaster Recovery
- Service Bus High Availability
- Geo Distributed Scale with App Service Environments
- Azure Web App Backups
- Deployment Slots in Azure App Service
- IoT Hub High Availability and Disaster Recovery

Compute capabilities

IaaS resilience

- Availability Sets
- Availability Zones
- Virtual Machine Scale Sets
- Managed Disks for Virtual Machines in Availability Sets
- Understanding Virtual Machines Reboots Maintance vs downtime
- Designing, building, and operating microservices on Azure
- Azure Site Recovery
- Azure Backup

Storage capabilities

Storage resilience

- Azure Storage Replication
- Locally redundant storage (LRS)
- Zone-redundant storage (ZRS)
- Geo-redundant storage (GRS)

Databases capabilities

Database Service resilience

- Cosmos DB High Availability
- Cosmos DB Global Distribution
- SQL Database High Availability
- Active Geo-Replication and Auto-Failover Groups Azure SQL Database
- Automatic SQL Database Backups
- Business Continuity with Azure Database for MySQL
- Backup and Restore in Azure Database for MySQL
- Business Continuity with Azure Database for PostgreSQL
- Backup and restore in Azure Database for PostgreSQL
- Business Continuity with Azure Database for MariaDB
- Backup and Restore in Azure Database for MariaDB
- Redis Clustering for a Premium Azure Redis Cache

Networking capabilities

Network resilience

- Azure Load Balancer
- Highly Available Network Virtual Appliances
- Highly Available Cross-Premises and VNet-to-VNet Connectivity
- ExpressRoute
- Disaster Recovery using Azure DNS and Traffic Manager
- Autoscaling, Zone Redundant Application Gateway
- Azure Firewall
- Azure Virtual WAN
- Azure Front Door and Load Balancing
- Protecting DNS Zones and Records

Other capabilities

Security/Regional/Other resilience

- Azure Key Vault Disaster Recovery
- Azure Scheduler for High Availability
- Azure Regions
- Availability Paired Regions
- Design for resilience
- Role Based Access
- Azure Monitor
- Azure Monitor and Autoscaling Based on Performance or Schedule
- Azure Advisor High Availability Recommendations
- Azure Service Health
- Azure Policy
- Azure Blueprints