Azure High Availability Deployment Checklist

A Complete Step-by-Step Guide to Deploy Highly Available Services in Azure

This checklist provides a comprehensive framework for deploying highly available services in Microsoft Azure. Use this guide to ensure your infrastructure is resilient, redundant, and ready for production workloads.

Phase 1: Planning & Architecture

- ■ Define Recovery Time Objective (RTO) - Maximum acceptable downtime

  Example: Can your business tolerate 1 minute, 1 hour, or 4 hours of downtime?

- ■ Define Recovery Point Objective (RPO) - Maximum acceptable data loss

  Example: Can you lose 5 minutes, 1 hour, or 24 hours of data?

- ■ Document all application dependencies (databases, APIs, storage, authentication)

  Map every external service and internal component your application requires

- ■ Select primary Azure region based on user location and latency requirements

  For EU-based users: West Europe (Netherlands), North Europe (Ireland), or Germany

- ■ Select secondary Azure region for disaster recovery (if needed)

  Choose paired regions for automatic geographic replication support

- ■ Verify GDPR and data residency compliance requirements

  Ensure selected regions meet regulatory requirements for your industry

- ■ Calculate budget for redundant infrastructure (typically 30-50% increase)

  Include costs for: duplicate VMs, zone-redundant storage, data transfer, load balancers

- ■ Create architecture diagram showing all components and redundancy paths

  Document: availability zones, load balancers, storage replication, failover routes

Phase 2: Infrastructure Setup

- ■ Create dedicated resource group for high availability deployment

  Use clear naming: [project]-ha-[environment]-rg (e.g., webapp-ha-prod-rg)

- ■ Deploy Virtual Machines across at least 2 availability zones

Minimum: Zone 1 and Zone 2. Recommended: All three zones for maximum resilience

- [ ] Configure Virtual Machine Scale Sets (VMSS) if using multiple identical VMs

VMSS automatically distributes VMs across zones and handles scaling

- [ ] Set up Availability Sets within each zone (if using VMs)

Protects against rack-level failures within the datacenter

- [ ] Choose appropriate VM sizes with sufficient capacity for failover scenarios

Each VM must handle 50% of peak load (for 2-zone) or 33% (for 3-zone with N+1)

- [ ] Enable Accelerated Networking on VMs for reduced latency

Reduces network latency between zones from ~2ms to <1ms

Phase 3: Storage & Data Redundancy

- [ ] Create storage accounts with Zone-Redundant Storage (ZRS)

ZRS replicates data synchronously across 3 availability zones

- [ ] Enable Geo-Redundant Storage (GRS) for critical data requiring regional failover

GRS replicates to secondary region 100s of kilometers away

- [ ] Configure Azure SQL Database with Business Critical or Premium tier

These tiers include built-in zone redundancy and readable replicas

- [ ] Enable geo-replication for Azure SQL Database (if regional failover required)

Creates readable secondary database in different region

- [ ] Set up managed disks with Zone-Redundant Storage (ZRS)

Premium ZRS or Standard ZRS for VM disks

- [ ] Configure automated backups with appropriate retention periods

Minimum: 7 days. Recommended: 30 days for production workloads

- [ ] Test restore procedures from backups

Verify you can actually recover data before you need to in an emergency

Phase 4: Load Balancing Configuration

- [ ] Deploy Azure Load Balancer (Standard tier) in zone-redundant configuration

Standard tier supports zone redundancy; Basic tier does not

- [ ] Create backend pool with VMs from all availability zones

Ensure VMs from each zone are registered in the backend pool

- [ ] Configure health probes to check application health (not just server availability)

Test actual application endpoint (e.g., /health or /api/status), interval: 5-15 seconds

- [ ] Set up load balancing rules for each service port

Common ports: 80 (HTTP), 443 (HTTPS), 3389 (RDP), 22 (SSH)

- [ ] Configure session persistence (sticky sessions) if required by application

Only enable if your app cannot handle distributed sessions

- [ ] Deploy Azure Application Gateway (if using Layer 7 features)

Required for: SSL termination, URL routing, Web Application Firewall

- [ ] Set up Azure Front Door for global load balancing (multi-region deployments)

Provides CDN, SSL, and intelligent routing to closest healthy region

Phase 5: Networking & Connectivity

- [ ] Create Virtual Network (VNet) with subnets in multiple availability zones

VNets span all zones automatically; use separate subnets for organization

- [ ] Configure Network Security Groups (NSGs) with least-privilege access

Only allow necessary inbound traffic; deny by default

- [ ] Set up Azure Firewall or Network Virtual Appliance (if required)

Deploy in zone-redundant configuration for high availability

- [ ] Configure VNet peering for connectivity between environments

Example: Connectivity between production and DR regions

- [ ] Set up Azure Traffic Manager for DNS-based global routing

Automatically routes users to healthy region based on routing policy

- [ ] Configure custom DNS records with appropriate TTL values

Lower TTL (60-300 seconds) enables faster failover but increases DNS queries

Phase 6: Monitoring & Alerting

- [ ] Enable Azure Monitor for all resources

Captures metrics, logs, and diagnostics for your entire infrastructure

- [ ] Create Log Analytics workspace for centralized logging

Required for advanced queries and long-term log retention

- [ ] Configure diagnostic settings to send logs to Log Analytics

Enable for: VMs, Load Balancers, SQL Databases, Storage Accounts, NSGs

- [ ] Set up metric alerts for critical thresholds (CPU >80%, Memory >90%, etc.)

Configure appropriate thresholds based on your baseline performance

- [ ] Create log-based alerts for application errors and exceptions

Example: Alert when error rate exceeds normal baseline by 50%

- [ ] Configure health probe failure alerts

Alert when 1+ instances fail health checks for more than 2 minutes

- [ ] Set up action groups with appropriate notification channels

Use SMS/phone for critical alerts, email for warnings

- [ ] Enable Azure Service Health alerts for platform-level issues

Get notified about Azure outages, planned maintenance, and security advisories

- [ ] Deploy Application Insights for application performance monitoring

Tracks: response times, dependency calls, exceptions, user metrics

Phase 7: Security Configuration

- [ ] Enable Azure Security Center (now Microsoft Defender for Cloud)

Provides security recommendations and threat detection

- [ ] Configure Azure Key Vault for secrets, certificates, and encryption keys

Never store credentials in code or configuration files

- [ ] Enable managed identities for Azure resources

Eliminates need for credentials in code when accessing Azure services

- [ ] Implement Role-Based Access Control (RBAC) with least privilege

Grant minimum permissions necessary for each user/service

- [ ] Enable encryption at rest for all storage accounts and databases

Azure provides this by default, but verify it is enabled

- [ ] Configure TLS/SSL certificates for all public endpoints

Use Azure-managed certificates or upload your own

- [ ] Enable Azure DDoS Protection (Standard tier for production)

Protects public IP addresses from volumetric attacks

Phase 8: Testing & Validation

- [ ] Test application functionality in multi-zone configuration

Verify application works correctly when distributed across zones

- [ ] Measure latency between availability zones

Expect 1-2ms latency between zones in same region

- [ ] Perform load testing to verify capacity during zone failure

Simulate failure of 1 zone and verify remaining zones handle load

- [ ] Test automatic failover by stopping VMs in one availability zone

  Verify: Load balancer stops routing traffic, application stays available

- [ ] Verify health probes correctly detect application failures

  Stop application service (not just VM) and confirm health probe fails

- [ ] Test database failover and verify connection strings handle redirection

  For Azure SQL: Test automatic failover groups

- [ ] Validate backup restoration procedures

  Actually restore a backup to a test environment

- [ ] Review all monitoring alerts fire correctly during tests

  Confirm alerts reach the right people through configured channels

- [ ] Document observed failover times (actual RTO)

  Measure time from failure to full service restoration

Phase 9: Documentation

- [ ] Create architecture documentation with diagrams

  Include: component diagram, network diagram, failover flow

- [ ] Document all configuration settings and design decisions

  Explain WHY choices were made, not just WHAT was configured

- [ ] Write runbook for manual failover procedures

  Step-by-step instructions for forcing failover during emergency

- [ ] Create incident response procedures for common failure scenarios

  Document: zone failure, database failure, network issues, DDoS attack

- [ ] Document monitoring dashboard locations and access procedures

  Ensure on-call engineers know where to check system health

- [ ] Maintain contact list for escalations

  Include: Azure support contacts, internal teams, third-party vendors

- [ ] Create change management procedures for updates

  Define: testing requirements, approval process, rollback procedures

Phase 10: Ongoing Operations

- [ ] Schedule quarterly failover drills

  Test failover procedures every 3 months to ensure they still work

- [ ] Review Azure Service Health notifications weekly

Stay informed about planned maintenance and potential issues

- [ ] Analyze availability metrics and compare to SLA targets monthly

  Track actual uptime vs. commitments; identify improvement opportunities

- [ ] Review and update disaster recovery procedures quarterly

  Ensure documentation reflects current architecture

- [ ] Monitor Azure costs and optimize resource usage

  Use Azure Cost Management; review monthly for unexpected increases

- [ ] Apply security updates and patches on regular schedule

  Establish maintenance windows; use Azure Update Management

- [ ] Review and rotate access keys and certificates before expiration

  Set reminders 30 days before expiration

- [ ] Conduct post-incident reviews after any outage

  Document: what happened, why, how to prevent recurrence

- [ ] Stay current with Azure platform updates and new HA features

  Review Azure updates monthly; evaluate new features for your architecture

About This Checklist

This checklist was created by **Ace Networks**, specialists in Information, Telephony, and Computing (ITC) development and IT consulting for enterprises across Europe. Our team holds advanced Microsoft certifications and has successfully deployed highly available cloud solutions for clients in financial services, healthcare, manufacturing, and professional services.

Need Help?

If you need expert guidance to deploy highly available services in Azure, our team can help you design, implement, and optimize your cloud infrastructure.

Contact us: www.acenetworks.eu
Expertise: Azure Architecture, High Availability, Cloud Migration, IT Consulting