Azure Standards

Public cloud Architecture

Gerry Lopez

FIS

Contents

[Introduction 2](#_Toc140739734)

[Purpose 3](#_Toc140739735)

[Summary 3](#_Toc140739736)

[Azure Services Allowed in Production 3](#_Toc140739737)

[Approved Azure Services for Production Environments 3](#_Toc140739738)

[Internet-Based Services 3](#_Toc140739739)

[Code Deployment Guidelines 4](#_Toc140739740)

[Continuous Integration and Continuous Deployment (CI/CD) 4](#_Toc140739741)

[Exception Handling for Manual Deployment 4](#_Toc140739742)

[Network Best Practices 4](#_Toc140739743)

[Private Link 4](#_Toc140739744)

[VNet 4](#_Toc140739745)

[NSG 4](#_Toc140739746)

[Azure Firewall & WAF 4](#_Toc140739747)

[Ingress Traffic Best Practices 4](#_Toc140739748)

[Benefits of Using Akamai External Load Balancer 5](#_Toc140739749)

[ Distributed Denial of Service (DDoS) Mitigation: 5](#_Toc140739750)

[ High Availability and Redundancy: 5](#_Toc140739751)

[ Perf 5](#_Toc140739752)

[ SSL Termination: 5](#_Toc140739753)

[Traffic Ingress Guidelines 5](#_Toc140739754)

[DNS Configuration 5](#_Toc140739755)

[SSL Certificate Management 5](#_Toc140739756)

[Compliance Requirements 5](#_Toc140739757)

[Payment Card Industry Data Security Standard (PCI DSS) Compliance 5](#_Toc140739758)

[Personally Identifiable Information (PII) Compliance 5](#_Toc140739759)

[Data Encryption and Privacy 5](#_Toc140739760)

[Data Anonymization 5](#_Toc140739761)

[Common Data Anonymization Techniques 6](#_Toc140739762)

[Data Aggregation 6](#_Toc140739763)

[Data Perturbation 6](#_Toc140739764)

[Data Masking 6](#_Toc140739765)

[Data Generalization 6](#_Toc140739766)

[De-identification and Pseudonymization 6](#_Toc140739767)

[De-identification 6](#_Toc140739768)

[Pseudonymization 6](#_Toc140739769)

[Data Masking and Tokenization 6](#_Toc140739770)

[Data Masking 6](#_Toc140739771)

[Tokenization 6](#_Toc140739772)

[Automation 6](#_Toc140739773)

[Terraform Environments 6](#_Toc140739774)

[Terraform Versioning and State Management 7](#_Toc140739775)

[DNS Resolution and Advanced DNS Configurations 7](#_Toc140739776)

[DNS Resolver in Azure 7](#_Toc140739777)

[Conditional Forwarders 7](#_Toc140739778)

[Pinned DNS Entries 7](#_Toc140739779)

[Control over Private Endpoint IPs 7](#_Toc140739780)

[Design across Multiple DNS Servers 7](#_Toc140739781)

[High Availability for DNS Servers 7](#_Toc140739782)

[Geo-Redundancy and Load Balancing 7](#_Toc140739783)

[Private DNS Zones for Cross-VNet Resolution 7](#_Toc140739784)

[Risk Management 7](#_Toc140739785)

[Vendor Risk Assessment 8](#_Toc140739786)

[Risk Mitigation for Approved Vendors 8](#_Toc140739787)

[Risk Mitigation for Unapproved Vendors 8](#_Toc140739788)

[SIEM Logging 8](#_Toc140739789)

[QRadar 8](#_Toc140739790)

[Key Log Sources for QRadar Integration 8](#_Toc140739791)

[Integration best practices 8](#_Toc140739792)

# Introduction

## Purpose

The purpose of this document is to provide our clients with comprehensive guidelines and best practices for securely and efficiently leveraging the Azure cloud environment. By adhering to these standards, clients can ensure the successful adoption of Azure services while focusing on security, compliance, and scalability.

# Summary

The sections that follow detail the standards and best practices for adopting the Azure cloud, including production-ready services, code deployment methods, network configurations, compliance requirements, and available tools.

By adhering to these Azure Cloud Standards and Best Practices, our clients can effectively harness the power of the Azure cloud environment while ensuring data security, compliance, and seamless deployments. Regularly review and update your infrastructure and applications in line with industry trends and evolving Azure services to optimize your cloud environment continuously.

# Azure Services Allowed in Production

Prior to deploying services in a production environment, it is essential to confirm that they satisfy specific performance, availability, security, and support criteria. The services being contemplated for deployment in production environments should be subjected to rigorous testing and validation.

## Approved Azure Services for Production Environments

* Virtual Machines (VMs) with specific VM sizes for different workloads.
* Azure Kubernetes Service (AKS) for container orchestration.
* Azure SQL Database for managed relational databases.
* Azure App Service for web applications.
* Azure Cosmos DB for globally distributed databases.
* Azure Front Door for global load balancing and security.
* Azure Application Gateway for application-level routing and load balancing.
* Azure Key Vault for secure key management.
* Azure Monitor for proactive monitoring and alerting.
* Azure Backup for data protection and disaster recovery.
* JFrog Artifactory for container registries
* Hashicorp key vault

## Internet-Based Services

The following Azure services are internet-based only and should be used with caution:

* Azure Active Directory (Azure AD): Provides identity and access management services.
* Azure B2B/B2C: Enables external collaboration and customer identity management.
* Azure Multi-Factor Authentication (MFA): Adds an extra layer of security to user authentication.
* Azure API Management: Facilitates API management and exposure to external consumers.
* Azure Logic Apps: Automates workflows across applications and services.

## Code Deployment Guidelines

### Continuous Integration and Continuous Deployment (CI/CD)

Pipelines for continuous integration and continuous delivery (CI/CD) must be utilized by any and all applications and services that are going to be deployed in Microsoft's Azure cloud. This will ensure that deployments are automated, consistent, and reliable. Continuous Integration and Continuous Deployment (CI/CD) pipelines encourage version control, automated testing, and seamless rollbacks in the event that there are problems with deployment.

### Exception Handling for Manual Deployment

In exceptional cases where manual deployments are necessary, clients must request approval from the designated authority. Manual deployments should be well-documented, follow strict change management procedures, and adhere to security best practices.

## Network Best Practices

### Private Link

Private Link should be used to securely access Azure services privately over the Microsoft backbone network. It is especially recommended when accessing services like Azure Storage, Azure SQL Database, and Azure Cosmos DB from on-premises networks or virtual networks.

### VNet

Design VNets with proper IP address planning and subnet allocation. Utilize peering and Network Security Groups (NSGs) for traffic isolation and granular access control.

### NSG

NSGs should be used to control inbound and outbound traffic to subnets and individual resources. Define explicit rules to restrict unnecessary access and apply the principle of least privilege.

### Azure Firewall & WAF

Leverage Azure Firewall to protect Virtual Networks and control outbound internet access. Additionally, deploy Azure WAF to safeguard web applications from common web exploits and attacks.

## Ingress Traffic Best Practices

All incoming traffic should be routed through Akamai's External Load Balancer (ELB) to improve the security, efficacy, and dependability of our web services. The robust content delivery network (CDN) and load balancing capabilities of Akamai ensure that our applications can handle high volumes of traffic while maintaining low-latency responses for users around the globe.

### Benefits of Using Akamai External Load Balancer

* Global Load Distribution: Akamai's vast network of servers located strategically around the world enables efficient load distribution. Incoming requests are automatically routed to the nearest Akamai edge server, reducing latency, and ensuring a smoother user experience.
* Distributed Denial of Service (DDoS) Mitigation: Akamai's DDoS protection capabilities provide a strong defense against malicious traffic and cyberattacks. The CDN intelligently filters and blocks harmful traffic at the network edge, safeguarding our infrastructure and applications from disruptions.
* High Availability and Redundancy: Akamai's ELB is designed for high availability and fault tolerance. It provides redundant, geographically dispersed endpoints, reducing the risk of single points of failure and ensuring service continuity.
* Performance Optimization: Akamai's CDN caches static and dynamic content, optimizing delivery and reducing the load on our origin servers. Accelerated content delivery leads to faster load times, minimizing user wait times and improving overall website performance.
* SSL Termination: Akamai supports SSL termination at the edge, reducing the computational burden on our servers. This enables efficient handling of secure connections without compromising security or performance.

## Traffic Ingress Guidelines

### DNS Configuration

Update the DNS settings to point to Akamai's ELB as the primary entry point for all web services. Akamai's authoritative DNS ensures that users are directed to the closest edge server for optimal performance.

### SSL Certificate Management

Upload valid SSL certificates to Akamai's SSL Certificate Management system to enable secure communication between Akamai's edge servers and our infrastructure.

# Compliance Requirements

## Payment Card Industry Data Security Standard (PCI DSS) Compliance

For handling payment card data, clients must ensure compliance with PCI DSS requirements. Sensitive cardholder data should be encrypted, and access to this data must be strictly controlled.

### Personally Identifiable Information (PII) Compliance

Handling PII data requires adherence to data protection regulations, including encryption at rest and during transit. Access to PII data should be restricted on a need-to-know basis.

### Data Encryption and Privacy

All sensitive data, regardless of compliance requirements, should be encrypted at rest and during transit. Clients are responsible for implementing and managing encryption keys securely, as per policy.

# Data Anonymization

Data anonymization is the process of deleting or encrypting personally identifying information (PII) from datasets. This is done to preserve the privacy of individuals and to ensure compliance with any data protection rules. The utility of the data is meant to be preserved through the process of data anonymization, which also ensures that the data cannot be traced back to any particular individuals.

## Common Data Anonymization Techniques

### **Data Aggregation**

Combine individual data points into groups or categories to prevent identification.

### Data Perturbation

Add random noise to the data, making it harder to link data points to specific individuals.

### Data Masking

Replace sensitive information with fake or masked data while preserving data format and structure.

### Data Generalization

Reduce the level of detail in data, such as replacing precise ages with age groups.

## De-identification and Pseudonymization

### De-identification

Remove or modify PII from the dataset so that the data can no longer be associated with a specific individual.

### Pseudonymization

Replace PII with pseudonyms or tokens to prevent direct identification. Pseudonymized data can be re-identified using a separate key.

## Data Masking and Tokenization

### Data Masking

Replace sensitive data with fictitious values or hashed representations to protect sensitive information during development and testing processes.

### Tokenization

Substitute sensitive data with randomly generated tokens that can be used to retrieve the original data from a secure token vault.

# Automation

Terraform makes it possible to implement Infrastructure as Code, which offers a variety of advantages including version control, repeatability, and consistency in the provisioning of resources.

## Terraform Environments

Implement distinct Terraform environments (e.g., development, staging, production) to segregate infrastructure changes and minimize risk.

## Terraform Versioning and State Management

Maintain version control for Terraform configurations and store state files securely to ensure proper collaboration and tracking of changes.

# DNS Resolution and Advanced DNS Configurations

## DNS Resolver in Azure

Configure Azure Virtual Networks to use Azure-provided DNS resolver by default. This resolver ensures name resolution for Azure resources within the same VNet and across peered VNets.

## Conditional Forwarders

Implement conditional forwarders when specific DNS zones require resolution through external DNS servers, such as on-premises DNS servers or DNS servers in a different cloud.

## Pinned DNS Entries

Use pinned DNS entries to override the default DNS resolution for specific domain names or IP addresses. This feature is useful when specific applications or services require custom DNS configurations.

## Control over Private Endpoint IPs

To maintain control over private endpoint IP addresses, reserve a private IP address range in the subnet where the private endpoints are deployed. This approach ensures consistent IP assignment across restarts and scaling events.

## Design across Multiple DNS Servers

### High Availability for DNS Servers

Implement DNS server redundancy by deploying multiple DNS servers in different Availability Zones to ensure high availability and fault tolerance.

### Geo-Redundancy and Load Balancing

For DNS resolution across multiple regions, deploy DNS servers in different Azure regions with DNS traffic load balancing for improved performance and fault tolerance.

### Private DNS Zones for Cross-VNet Resolution

Use Azure Private DNS Zones for DNS resolution between VNets without exposing DNS records to the public internet.

# Risk Management

## Vendor Risk Assessment

Conduct a thorough risk assessment for all vendors that interact with the Azure cloud environment through procurement. Assess potential risks related to data security, compliance, service availability, and financial stability, if any please reach out to John Marandola.

### Risk Mitigation for Approved Vendors

For approved vendors, establish clear contractual agreements that outline security requirements, data handling practices, and incident response procedures. Periodically review vendor performance and adherence to security standards.

### Risk Mitigation for Unapproved Vendors

If a vendor fails to meet the established risk criteria, consider alternative vendors with a proven track record of security and compliance. In cases where an unapproved vendor is essential, implement additional security controls and closely monitor their activities.

# SIEM Logging

Security Information and Event Management (SIEM) logging is a crucial component of an organization's security posture. It involves the collection, analysis, and correlation of security event data from various sources to detect and respond to security incidents.

## QRadar

QRadar is a leading SIEM solution that enables real-time threat detection and response. To integrate Azure resources with QRadar, use Azure Monitor's Diagnostic Logs and Azure Sentinel, the cloud-native SIEM from Microsoft.

### Key Log Sources for QRadar Integration

* Azure Activity Logs: Monitor operational data generated by Azure resources.
* Azure Security Center Alerts: Receive security alerts for potential threats.
* Azure Firewall and Application Gateway Logs: Analyze network traffic and web application traffic.
* Azure AD Sign-In and Audit Logs: Monitor sign-in and audit events in Azure AD.

### Integration best practices

* Centralize log collection: Use Azure Monitor to send logs to a central log analytics workspace for QRadar integration.
* Enable Log Analytics agent: Install the Log Analytics agent on VMs and other resources to collect additional data for analysis.
* Define correlation rules: Create custom correlation rules in QRadar to detect specific threats and anomalies.
* Continuous tuning: Regularly review and tune QRadar rules to reduce false positives and enhance detection accuracy.