Azure Architect: Design Monitoring

Aligned with Microsoft Certification Exam AZ-304

ine.com

Course Topics

Logging
Auditing
Monitoring

AZ-304 Objective Domains

- **Design monitoring (10-15%)**
- Design identity and security (25-30%)
- Design data storage (15-20%)
- Design business continuity (10-15%)
- Design infrastructure (25-30%)

Exam AZ-304: Microsoft Azure Architect Design

- Design for cost optimization
  - + recommend a solution for cost management and cost reporting
  - + recommend solutions to minimize costs
- Design a solution for logging and monitoring
  - + determine levels and storage locations for logs
  - + plan for integration with monitoring tools including Azure Monitor and Azure Sentinel
  - + recommend appropriate monitoring tool(s) for a solution
  - + choose a mechanism for event routing and escalation
  - + recommend a logging solution for compliance requirements

Pre-requisites

- **Azure Administrator Associate**

Optimize Resource Consumption

Optimize Resource Consumption

Optimize Performance

Demonstration: Verifying Azure Performance

Optimize Costs

Demonstration: Exploring Cost Scenarios

Optimize Performance

- **Infrastructure**
  - VMs
    - Understand workload balance (processor, memory, disk, network)
    - Utilize temp disk appropriately
    - Optimize disk throughput
  - Network
    - Use peering rather than Vnet-to-Vnet
    - Linux – use Azure optimized images
  - Storage
    - Use managed disks
    - Use the appropriate performance tier (Standard HDD, Standard SSD, Premium SSD, Ultra)

Optimize Performance

- **Database**
  - Choose the right performance tier
  - Choose the right platform – SQL Database vs SQL Warehouse vs Data Lake
  - Consider sharding
  - Use design best practices
- **Cosmos DB**
  - Optimize partitioning – avoid partition key hot spots
  - Index wisely
  - Monitor RU/s

Optimize Performance

- **App Services**
  - Scale appropriately – tier, size, count
  - Design for scalability – asynchronous, micro-services
  - Consider Isolated
  - Co-locate resources – storage, data
  - Cache
    - Redis Cache
    - CDN

Optimize Costs

- Choose the right tier and size
- Use autoscale
- User serverless compute
- Be aware of data transfer costs
- Use reservations for VMs, SQL, and Cosmos DB
- Evaluate regional cost differences

Optimize Cost - Workload

- **Virtual Machines**
  - Use burstable tier
  - Utilize Hybrid benefit
  - Provision a scaleset for autoscaling
  - Implement automation to shut down unused VMs
  - Use Azure batch for one-time or scheduled processing
    - Use low priority VMs
- **App Services**
  - Choose the right tier
  - Implement Autoscale
  - Use the included storage

Optimize Cost - Data

- **Relational**
  - Choose the right SQL Server cost method – DTU, vCore, Managed Instance
  - Choose the right tier – General Purpose, Business Critical
  - Factor in geo-redundancy
- **Tabular**
  - Table Storage vs. Cosmos DB
- **Queues**
  - Queue Storage vs. Service Bus
- **Massive Scale**
  - SQL Data Warehouse vs. Data Lake vs. Storage Account

Log Storage - Levels, Locations, and Duration

Log Storage - Levels, Locations, and Duration

- Control Plane and Data Plane
- Standardized Logging Options
- Non-Standardized Logging Options
- **Demonstration**: Configuring Logging

Control Plane and Data Plane

Logging Options

- **Standard**
  - Storage
  - Event Hub
  - Azure Monitor
- **Non-Standard**
  - App service
    - To disk or storage
    - Application insights
  - VM – agent based
    - Storage
    - Azure Monitor
  - Containers - Azure Monitor for containers
- **Log retention**

Monitoring Tools for Azure

Monitoring Tools for Azure

- Azure Monitor
- Network Monitoring
- Third Party Monitoring
- **Demonstration**: Monitoring

Azure Monitoring

- **Azure Monitor**
  - Centralized monitoring for subscription
  - Subsuming Log Analytics
  - Evolving
- **Network Watcher**
  - Monitoring
  - Diagnostics
  - Metrics
- **Third Party**
  - ELK – Elasticsearch, Logstash, Kibana
  - Splunk – Azure Monitor Add-on for Splunk

Azure Event Routing and Escalation

Azure Event Routing and Escalation

- Event Routing Options in Azure
- **Demonstration**: Event Grid

Event Routing in Azure

Auditing Activity in Azure

Auditing Activity in Azure

- Auditing Azure
- Auditing Azure Services
- **Demonstration**: Auditing Azure

Auditing Azure

- Control Plane
  - Activity Log
  - Security Center
  - Policy
- Data Plane
  - SQL Server
  - Key Vault
  - Cosmos DB
  - Data Lake
  - Storage Account*

Designing Audit Policies

Designing Audit Policies

- ARM Policy
- Azure Audit Policy
- **Demonstration**: Auditing with ARM Policy

ARM Policy

- Condition
  - Based on resource attributes
    - Example: Virtual machines without Azure Monitor Extension
  - Conditional logic
    - Multiple conditions
    - Multiple matching criteria
- Effect
  - Deny, Audit, Append, AuditIfNotExists, DeployIfNotExists
- Assign
  - Management Group
  - Subscription
  - Resource Group

Azure Audit Policy

```
"if": {
        "allOf": [
                {"field": "type",  "equals": "Microsoft.Compute/virtualMachines"},
                {"field": "Microsoft.Compute/imagePublisher","in": ["MicrosoftWindowsServer"]},
                {"field": "Microsoft.Compute/imageOffer","in": ["WindowsServer"]}
        ]
},
```

Azure Audit Policy

```
"then": {
        "effect": "auditIfNotExists",
        "details": {
                "type": "Microsoft.Compute/virtualMachines/extensions",
                "existenceCondition": {
                        "allOf": [
                                {"field": "Microsoft.Compute/virtualMachines/extensions/publisher",
                                    "equals": "Microsoft.Azure.Monitoring.DependencyAgent"},
                                {"field": "Microsoft.Compute/virtualMachines/extensions/type",
                                    "equals": "DependencyAgentWindows"}
                        ]
}}}
```

Data Auditing in Azure

Data Auditing in Azure

- Azure SQL Auditing
- **Demonstration**: Auditing an Azure SQL Database

Azure SQL Auditing

Azure Sentinel

Azure Sentinel

- Azure Sentinel
- Data Sources
- Requirements
- Demo: Azure Sentinel

Azure Sentinel

- Security Information Event Management (SEIM)
- Security Orchestration Automated Response (SOAR)
- Collect – Users, devices, apps, infrastructure
- Detect – Microsoft AI and threat intelligence
- Investigate – deep investigation and hunting tools
- Respond – Azure monitor workbooks

Data Sources

- Service to service integration:
  - Amazon Web Services - CloudTrail
  - Office 365
  - Azure AD / Activity / Security Center/ Information Protection / ATP
  - Windows security events / firewall
- External solutions via API
  - Barracuda
  - Symantec
  - Citrix Analytics (Security)
- External solutions via agent
  - Connect using the Syslog protocol via an agent.

Requirements

- Log Analytics workspace
- Subscription contributor role
- Resource group contributor or reader
- Paid service

Demo: Azure Sentinel