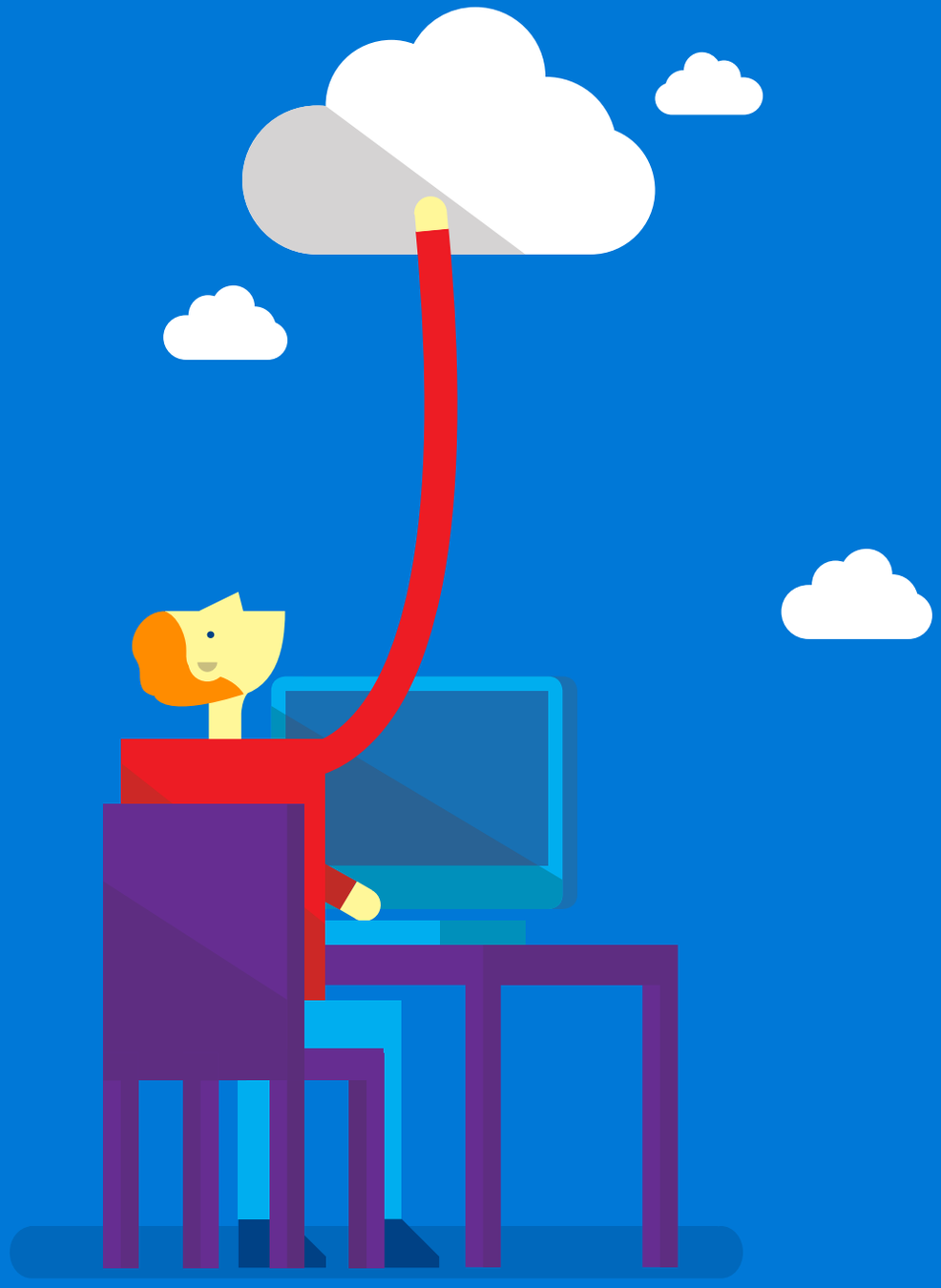
Azure Certification Jump Start

Exam 70-534: Architecting Microsoft Azure Solutions

Microsoft



Architecting Microsoft Azure Solutions

Exam 70-534 is suitable for professionals who:

- want to validate their Microsoft Azure solution design skills
- know the features and capabilities of Azure services
- can identify tradeoffs and make decisions for designing solutions
- can define solutions that meet functional, operational, and deployment requirements through the solution lifecycle

Exam Reference: http://aka.ms/70-534

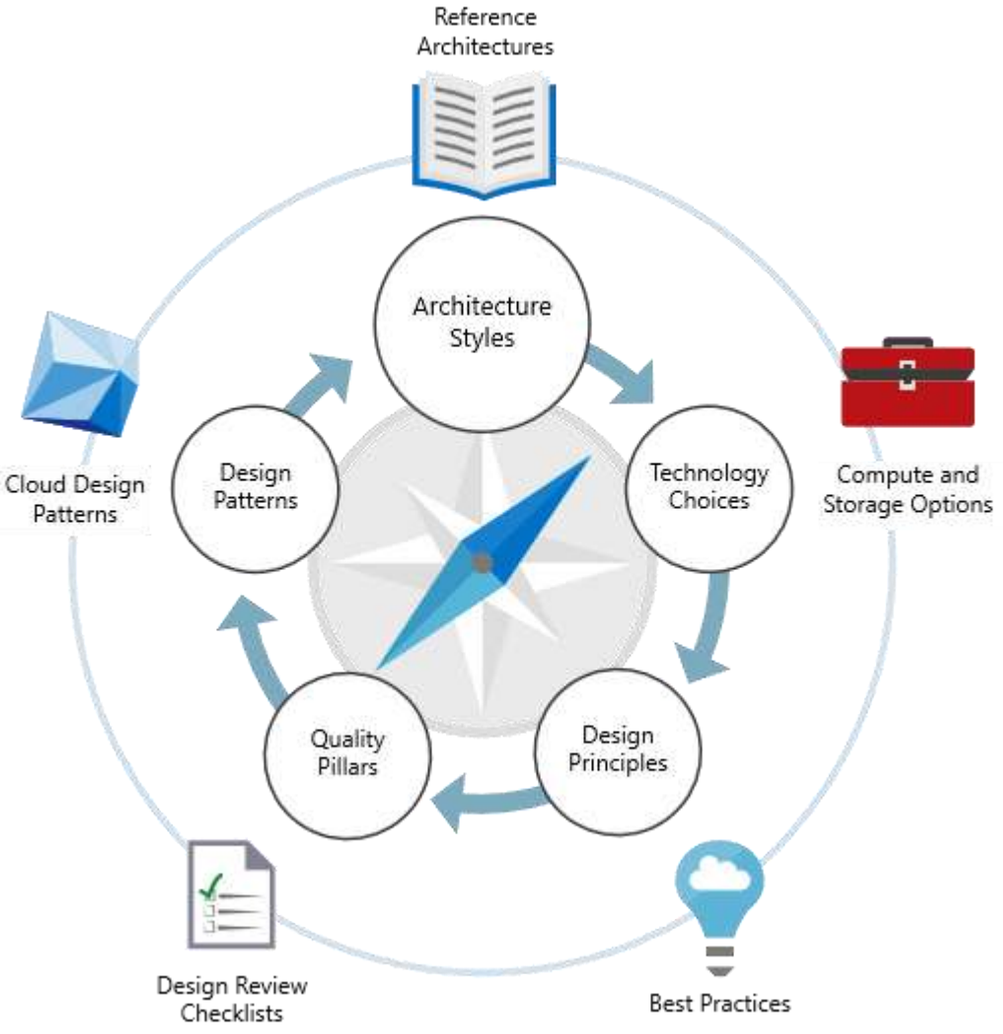
Exam 70-532: Developing Microsoft Azure Solutions and Exam 70-533: Implementing Microsoft Azure Infrastructure Solutions are useful for candidates who want to validate their implementation experience across cloud projects, but they are not prerequisites for this exam.

Session 1:
Solution Architecture

Solution Architecture: Overview

Session Goals

- Understand Azure architectural approach, and recognize different Architecture Styles
- Know when to choose a particular style, based on benefits, challenges, and best practices
- Understand Technology Choices for implementing architecture styles.
- Recognize Azure services that can be used for compute and data services



Reference: https://docs.microsoft.com/en-us/azure/architecture/

Architecture Styles

N-tier

- Traditional enterprise architecture
- Ideal for lift-and-shift

Web-Queue-Worker

- PaaS solutions
- Relies on asynchronous messaging

Microservices

- Many small, independent services
- Requires mature DevOps processes

Event-driven

- Producers publish, consumers subscribe
- Common with large data volumes (e.g. IoT)

Big Data & Big Compute

- Parallel processing of chunks across large dataset
- Parallel computations across large number of cores

Design Considerations:

- Scale
- Complexity
- Cost
- Manageability
- Service-Level Agreement

Technology Choices: Compute

Infrastructure-as-a-Service (IaaS)

- Virtual Machines

Platform-as-a-Service (PaaS)

- App Service
- Service Fabric
- Azure Container Service
- Azure Batch

Functions-as-a-Service (FaaS)

- Azure Functions

Decision Factors

- Hosting model
  - How is the service hosted?
- DevOps
  - What is the deployment model?
- Scalability
  - Can it auto-scale? Based on what metrics?
- Availability
  - What is the service SLA?
- Cost
  - Is there additional cost to manage?
- Supported Application Architectures
- Overall Service limitations

Reference: Compute Comparison

Technology Choices: Data and Storage

Relational

- Azure SQL/MySQL/PostgreSQL

Key/Value

- Cosmos DB, Azure Redis Cache

NoSQL/Document/Graph

- Cosmos DB

Data Analytics

- SQL Data Warehouse, Azure Data Lake

Objects and Files

- Blob Storage, Azure Files

Decision Factors

- Functional Requirements
  - Data model, structure, consistency, schema, data movement, lifecycle
- Non-functional Requirements
  - Performance, scalability, availability, resilience, replication, service limits
- Management and Cost
  - Managed service, licensing, cost
- Security
  - Confidentiality, auditing, networking
- DevOps
  - Skillset, clients

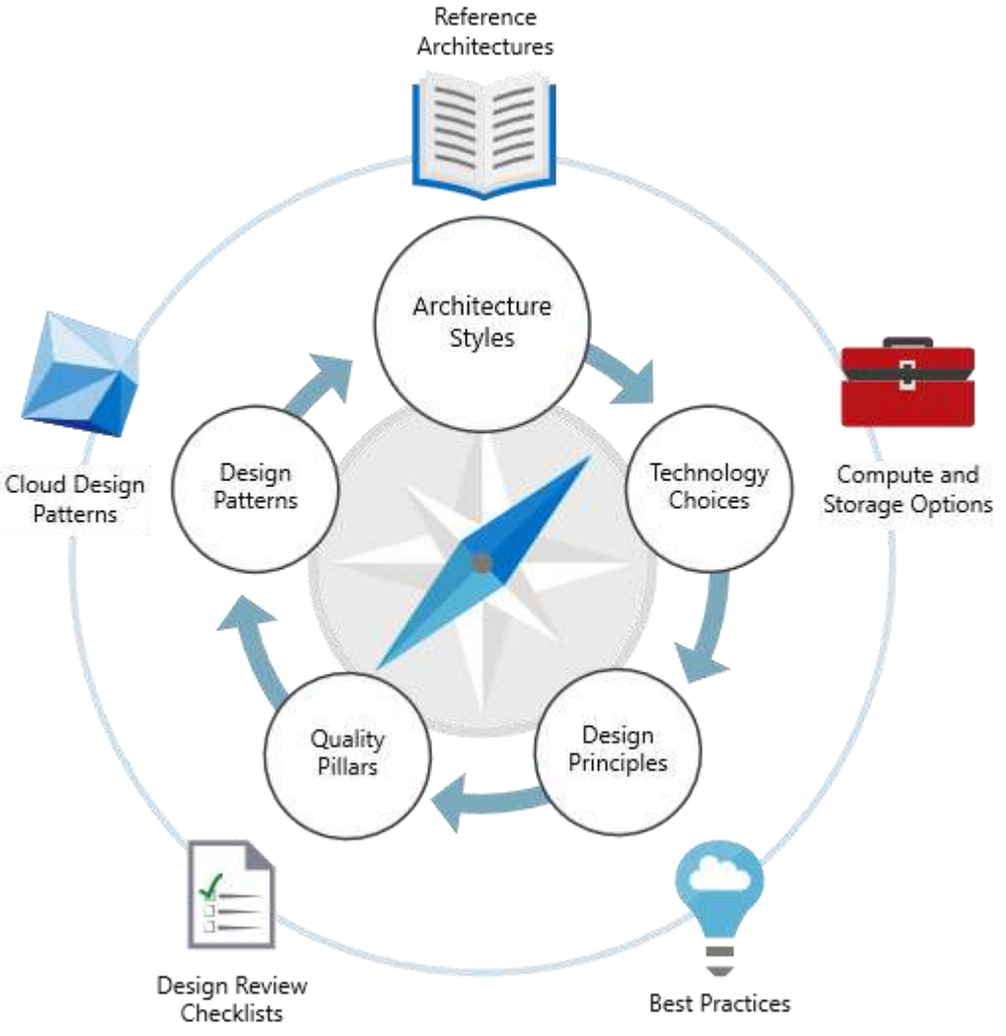
Reference: Data Comparison

Session 2: Quality Pillars

Quality Pillars: Overview

Session Goals

- Understand how design choices can impact the scalability, availability, resiliency, management, and security of a solution



Scalability

- Horizontal vs. Vertical scaling
  - Limits of vertical scaling
  - Complexity of horizontal scaling
- Best Practices
  - Autoscaling
  - Background Jobs
  - Caching
  - CDN
  - Data partitioning

Availability

- Calculating Service-Level Objectives (Uptime)
  - Solutions that use multiple services will often have multiple, per-service SLAs
  - Consider composite SLAs when developing solution uptime objectives

% Uptime	Downtime per week	Downtime per month	Downtime per year
99%	1.68 hours	7.2 hours	3.65 days
99.9%	10 minutes	43.2 minutes	8.76 hours
99.95%	5 minutes	21.6 minutes	4.38 hours
99.99%	1 minute	4.32 minutes	52.56 minutes
99.999%	6 seconds	26 seconds	5.26 minutes

- Best Practices
  - Autoscaling
  - Background Jobs

Resiliency

- High Availability & Disaster Recovery
  - Alphabet soup: RTO, RPO, MTTR, and SLA
- Planning for Failure
  - Design solutions to expect occasional failures and recover from them
  - Take advantage of platform resiliency features
    - Fault Domains (Availability Sets, Managed Disks)
    - Built-in geo-replication (Azure Storage, Azure SQL Database)
    - Load Balancing (Azure Traffic Manager, Load Balancer)
- Best Practices
  - Fault Tolerance
  - Backup
  - Transient Fault Handling

Management

- Monitoring
  - Built-in Capabilities
    - Included: Azure Diagnostics, Azure Monitor, Log Analytics (free tier)
    - Charged: Application Insights and Log Analytics
- Diagnostics
  - Built-in Capabilities
    - Included: Azure Advisor, Log Analytics (free tier)
    - Charged: Desired State Configuration, Log Analytics
- DevOps
  - Automation of testing and deployments
  - Continuous Integration/Continuous Delivery

Security

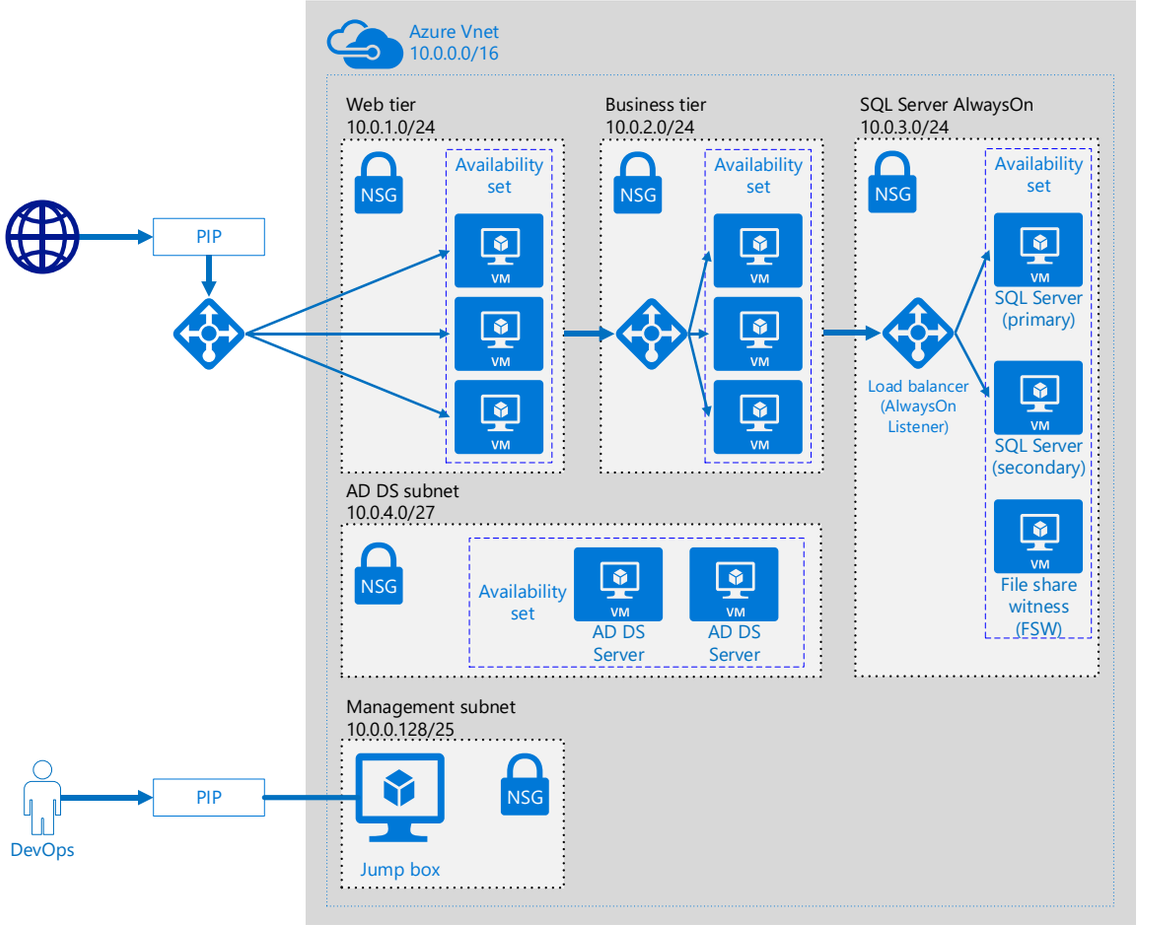
- Access Control
  - Identity Management and Role-based Access Control
    - Azure Active Directory, Azure Resource Manager
- Application Security
  - Plan for application-level threats: XSS, CSRF, SQL injection
    - Azure Security Center, Azure Application Gateway
  - Secure Shared Secrets
    - Azure Key Vault (HSMaaS)
- Confidentiality and Privacy
  - Data sovereignty: ARM Policies and National Clouds
  - At-rest and in-transit encryption: Cosmos DB, Azure SQL DB, encrypted VM disks, storage service encryption

Session 3: Compute Design

Compute Design: Overview

Session Goals

- Recognize Azure compute services
- Become familiar with design choices available for Azure compute services
- Know which Azure Resource Manager features are available for your solution



Azure Resource and Role Hierarchy

Enterprise Administrators manage Enrollments

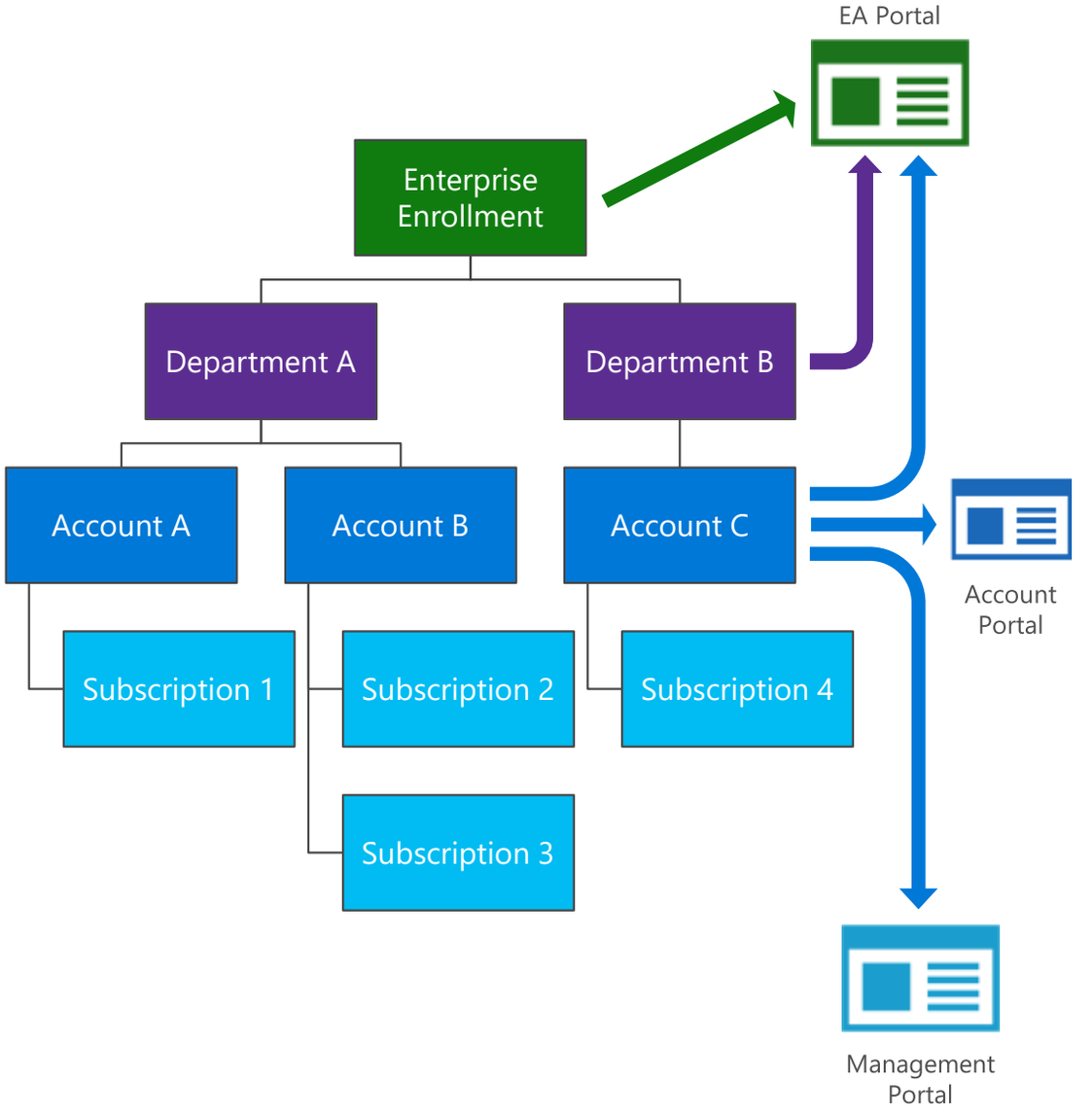
- Add other **Enterprise Administrators, Departments** and **Department Administrators**
- Add or associate **Account Owners** to the Enrollment
- View **monetary commitment** balance associated to the Enrollment and **usage and charges** data across all Accounts and Subscriptions

Department Administrators manage Accounts

- Edit their **department name** and cost center, and manage **department admins**
- **Add and remove accounts** for their departments
- View **Department charges** if enabled by the Enterprise Admin.

Account Owners manage Subscriptions

- Create **Subscriptions** for their Account
- Add **additional Administrators** for an individual Subscription
- View **usage data and account charges** for their Account
- Log into the Azure Account Portal to update **subscription names**
- Log into the Azure Management Portal as **Service Administrator**



Subscription Design Considerations

Business Requirements

- Availability
- Recoverability
- Performance

Technical Requirements

- Network connectivity
- Active Directory

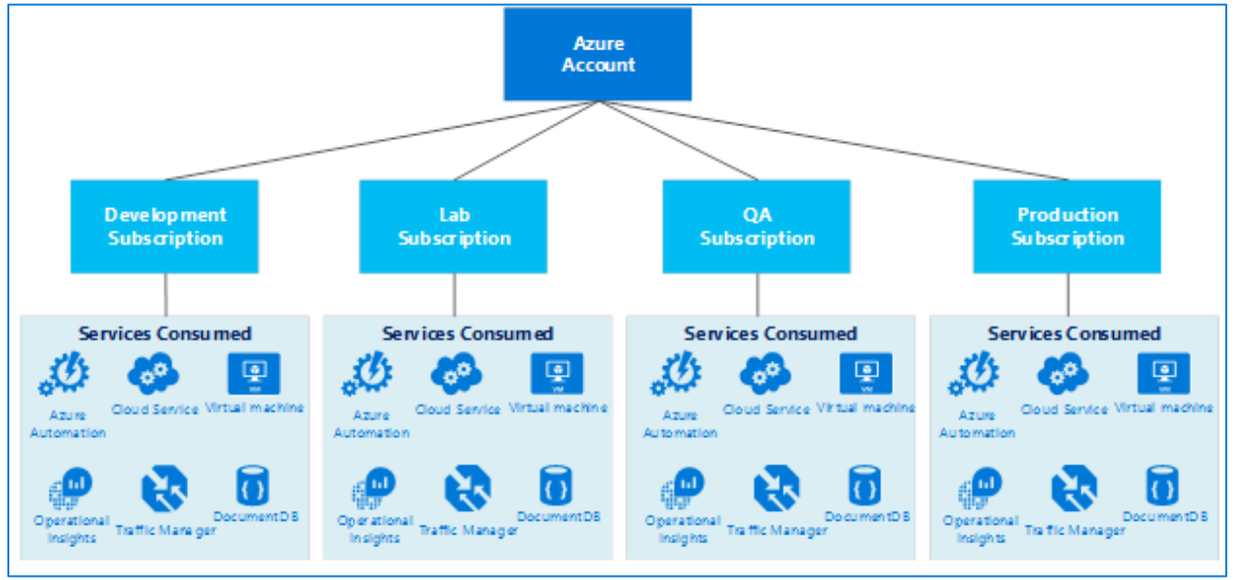
Security Requirements

- Administrative access
- Least privilege

Scalability Requirements

- Growth
- Resource Allocation
- Management overhead

Service (Lifecycle) Subscription Model



Develop the Subscription, Network, Storage, Availability and Administrative models together in order to have a cohesive approach.

Azure Resource Manager Features

Resource Groups

Deploy, manage, and monitor all the resources for your solution as a group

ARM Templates

Manage infrastructure through declarative templates rather than scripts

Role-Based Access Control

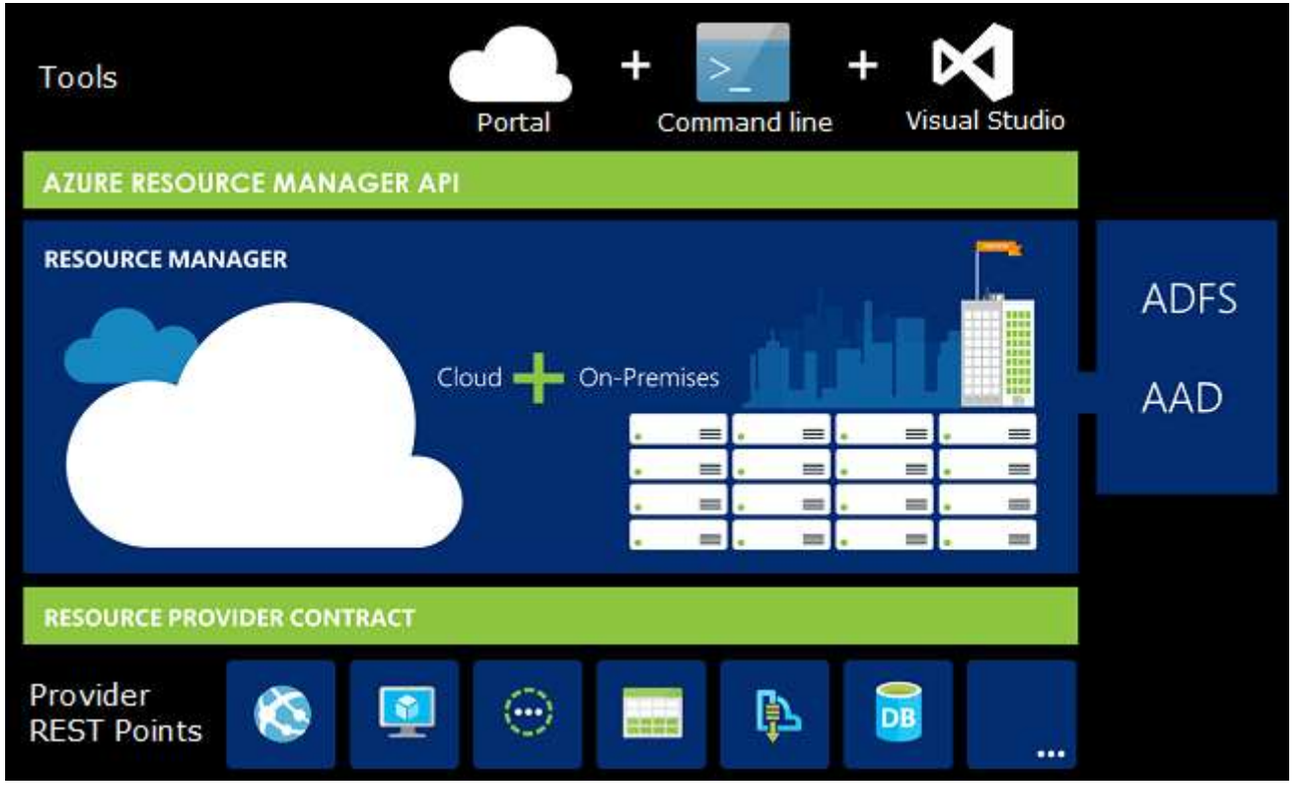
Apply access control to all services in your resource group

Tags

Logically organize all the resources in your subscription

Resource Locks

Protect resources from accidental change or deletion



Azure Resource Manager Templates

- What are they?
  - JSON documents that can be used to deploy resources using declarative statements rather than scripts
  - Can be created in authoring tool or exported from Azure portal
  - ARM Templates can be used to deploy many resources within an environment or solutions
  - Resource Manager Policies can be used to restrict deployment of resources in a resource group to only approved, standardized configurations
- Scenarios
  - Automate Deployments
    - Use Azure Automation to schedule and deploy resources consistently as part of DevOps process
  - Limit Selection of Resources
    - Define templates for standardized resource options (e.g., t-shirt sizes), and enforce with policy

Virtual Machine Design

VM Design Choices

- Regions
- Series and Sizes
- Resource Groups
- Availability Sets
- Images (Custom or Gallery)
- Disks (OS, Data, Temporary)
- Storage Accounts
- Virtual Networks (VNet)
- Network Security Groups
- Public IP Addresses
- Load Balancers
- Diagnostics and Monitoring

Design Considerations

- Scalability
  - Load Balancers
  - VM Scale Sets
  - Stateless VMs
- Availability
  - Azure SLA for VMs
  - Multi-region deployments for HA
- Resiliency
  - Backup
- Management
  - Deployment Runbooks
  - Desired State Configuration
- Security
  - Network virtual appliances
  - Azure Key Vault (HSM)

Examples

- Single VM
- N-Tier Solution

App Service Design

- App Types
  - Web App
    - For hosting web and mobile apps
  - Mobile Apps
    - For hosting mobile app back ends
  - API Apps
    - For hosting RESTful APIs
  - Logic Apps
    - For automating business processes
- Examples
  - Basic Web App
  - Multi-region Web App

- Design Choices
  - App Service Plan/Environment
  - Framework Versions
  - Deployment slots
  - Auto-scale (up and out)
  - Diagnostics & Monitoring
  - Domain names
  - Encryption/SSL
  - Authentication
  - Background tasks/Webjobs

Running Containers in Azure

Service	When To Use	Notes
App Services on Linux with Containers	You want to develop a web app and deploy via containers but get the App Services scaling benefits.	• Does not provide multi-container management or orchestration • Bring your own custom image with web framework/server. • Best for standalone container solutions with a focus on web traffic 80/443.
Container Instances (preview)	Quickly spin up a container with low administration and scaling planning, costs or effort.	• Does not provide its own multi-container management or orchestration. (integrates with Kubernetes, etc.) • Does not provide Docker daemon access • Think of it as rapid containers as a service.
Azure Container Services	You run orchestrated containers in the cloud without having to manage or administer the hosts, networking or storage.	• 3 Choices: Kubernetes, Docker Swarm and DCOS • You have no direct control over the hosts, storage or networking. • Azure is the backbone, and you pick your preferred orchestrator.
Azure Service Fabric	You want to orchestrate both containers and individual processes (exes) in a highly scalable platform.	• Backbone service for many high scale Azure services like Cosmos DB, Azure SQL, etc. • We provide the orchestration engine, networking, etc. • You have no direct control over the hosts, storage or networking.
3rd Party & Containers on Azure IaaS	You want to have direct control over the VM hosts, architecture, etc. OR You want to run a 3rd party container platform/orchestrator that is not directly supported by your PaaS services.	• Some 3rd party providers have officially supported templates and solutions that have been co-developed: OpenShift, Docker on Azure, etc.

Other Compute Options

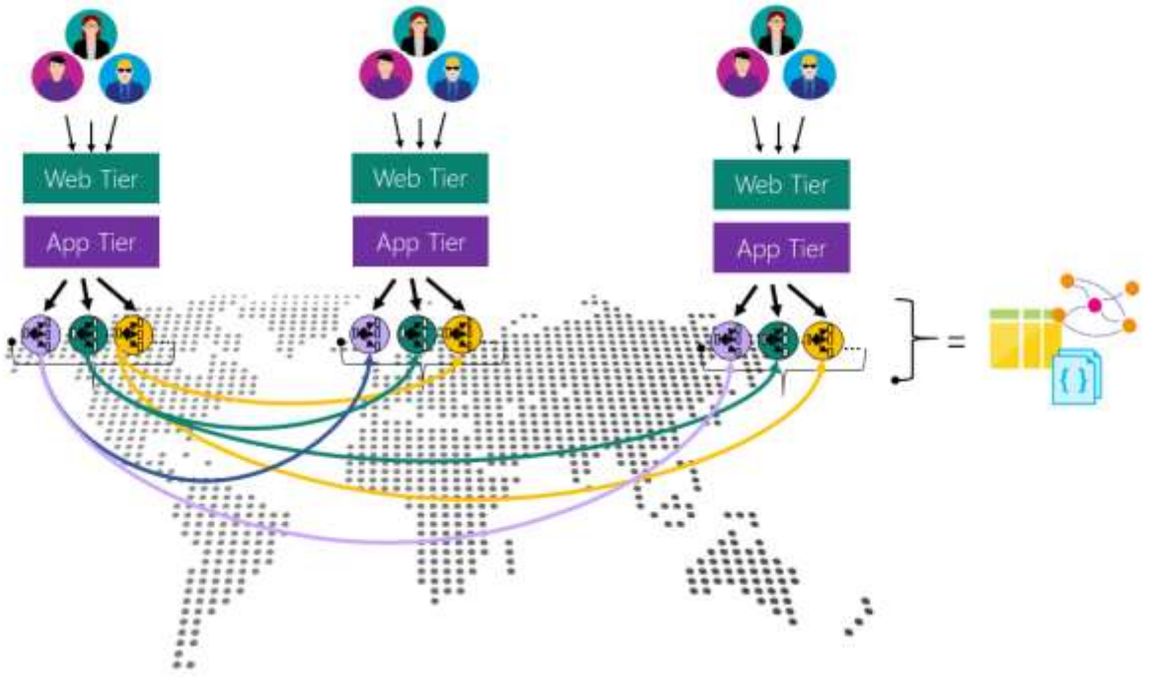
- Serverless Compute
  - Azure Functions
    - Run code on-demand without having to explicitly provision or manage infrastructure
- High-Performance Computing
  - Azure Batch
    - Schedule large-scale parallel and HPC applications to run on a managed collection of VMs
- Web and Worker Roles
  - Cloud Services
    - Similar to App Service, but more control over the OS (e.g., ability to install software).

Session 4: Data Design

Data Design: Overview

Session Goals

- Recognize Azure data and storage services and features
- Become familiar with design choices available for Azure data and storage services



Azure SQL Database Design

- Features
  - PaaS
    - MSFT manages OS and SQL Code base
    - MySQL and PostgreSQL in Preview
  - Data Structures
    - Relational data, JSON, spatial, and XML
  - Scalability
    - Dynamically scalable (DB or pool)
  - Availability
    - Backup, Restore, Geo-replicate, Failover
  - Performance
    - OLTP, In-memory ColumnStore, Automatic tuning & threat detection
  - Security & Compliance
    - Encryption (DIM, DAR, AE), masking, RLS
- Design Choices
  - Subscription, Region, RG
  - Pricing Tier (B, S, P, RS)
  - Database Transaction Units (DTU)
  - Server firewall rules
  - Features/Options
    - Access Control
    - Audit Logging
    - Threat Detection
    - Tuning
    - Backups
    - Replication
    - Scaling

Azure Cosmos DB Design

- Features
  - Global-Distribution
    - No geo-replication required
    - Native Multi-homing APIs
    - 5 levels of consistency choices
  - Multi-modal
    - Document, graph, key-value, table, columnar
    - Access via DocumentDB, MongoDB, Table and Graph APIs
  - Performance
    - Scale throughput and storage
    - End-to-end low latency at 99th percentile
    - 99.99% availability in a single region
- Design Choices
  - Subscription, Region, RG
  - API
  - Collection storage
  - Throughput (RU/s)
  - Features/Options
    - Global Distribution
    - Failover Priority
    - Consistency
    - TTL (collection, document)

Azure Storage Design

- Features
  - Multiple Services
    - Blobs – Massively scalable cloud storage
      - Choose Block, Append, or Page Blobs
      - Choose Access Tier (Hot, Cool)
    - Disks – VM disks stored in page blobs
      - Choose Unmanaged or Managed Disks
    - Files – Managed SMB file share
    - Queues – Managed message queue
    - Tables – Now part of CosmosDB!
  - Other Storage Services
    - StorSimple: Hybrid storage appliance with local iSCSI volumes, and tiered backup to Azure storage
    - File Transfer Service: Ship disks to MSFT
- Design Choices
  - Subscription, Region, RG
  - Storage Account
  - Performance
    - Standard (HDD), Premium (SSD)
  - Replication
    - Locally-Redundant (LRS)
    - Zone-Redundant (ZRS)
    - Geo-Redundant (GRS)
    - Read-Access GRS (RA-GRS)
  - Features/Optiosn
    - Secure Transfer Required
    - Access Keys
    - Encryption (Files, Blobs)

Designing Other Data Options

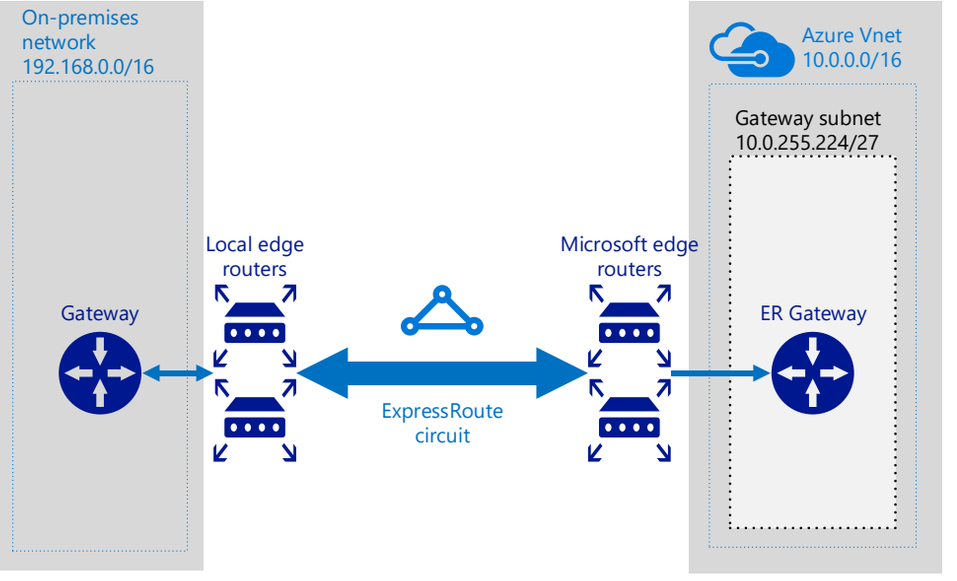
- Azure Redis Cache
  - Low-latency, high-throughput managed Redis cache
    - Offers clustering, persistence, and virtual network support
  - Choose pricing tier (Basic, Standard, Premium)
    - Tiers provide different levels of storage, bandwidth, availability, and SLA
- SQL Data Warehouse
  - Fully-managed elastic data warehouse service
    - Architecture: control node, compute nodes, and the storage layer, spread across 60 distributions
    - Independently scale compute nodes and storage capacity
  - Choose Performance Level using Data Warehouse Units (DWUs)
    - Provides performance objectives for scan, load, and query speeds.
- Data Services on Virtual Machines (IaaS)

Session 5: Network Design

Network Design: Overview

Session Goals

- Understand how to design Azure Virtual networks and recognize services that can be used with Virtual Networks
- Understand how to design hybrid networks using public and private connections



Virtual Network Design

- Features
  - Segmentation/Isolation
    - Use virtual networks (VNets) and subnets to separate environments
    - Connect VNets by VPN or peering
  - Connectivity and Routing
    - Default or custom routing to internet
    - Backhaul traffic to on-premises
  - Filtering
    - Use ACLs to limit traffic
  - Load balancing
    - Internal, external, global
    - Distribute by DNS, Application, Network

- Design Choices
  - Network architecture
  - Address Space
  - Subnets
  - Routing
  - Peering
  - DNS services
  - Internet connectivity
  - DMZ safeguards
  - Network security groups

Reference: Azure Virtual Network

Hybrid Network Design

- Features
  - Public connection: VPN
    - Site-to-site or point-to-site
    - Access to VNets and Virtual Machines
    - Average speeds <100 Mbps
    - SSTP, IPSec protocols supported
    - Policy-based or static routing
  - Private connection: ExpressRoute
    - Various speeds and meters available
    - Access to VNets, VMs, and public Azure services
    - Speeds from 50 Mbps to 10 Gbps
    - Routing via BGP
- Design Choices
  - VPN
    - On-prem VPN termination point
    - Routing type and protocols
    - Throughput
    - Persistence
    - Availability
  - ExpressRoute
    - Provider
    - Peering types
      - Azure Private (VMs, VNet, Cloud Svcs)
      - Azure Public (Azure Public Services)
      - Microsoft Peering (O365, D365)
  - Shared Services

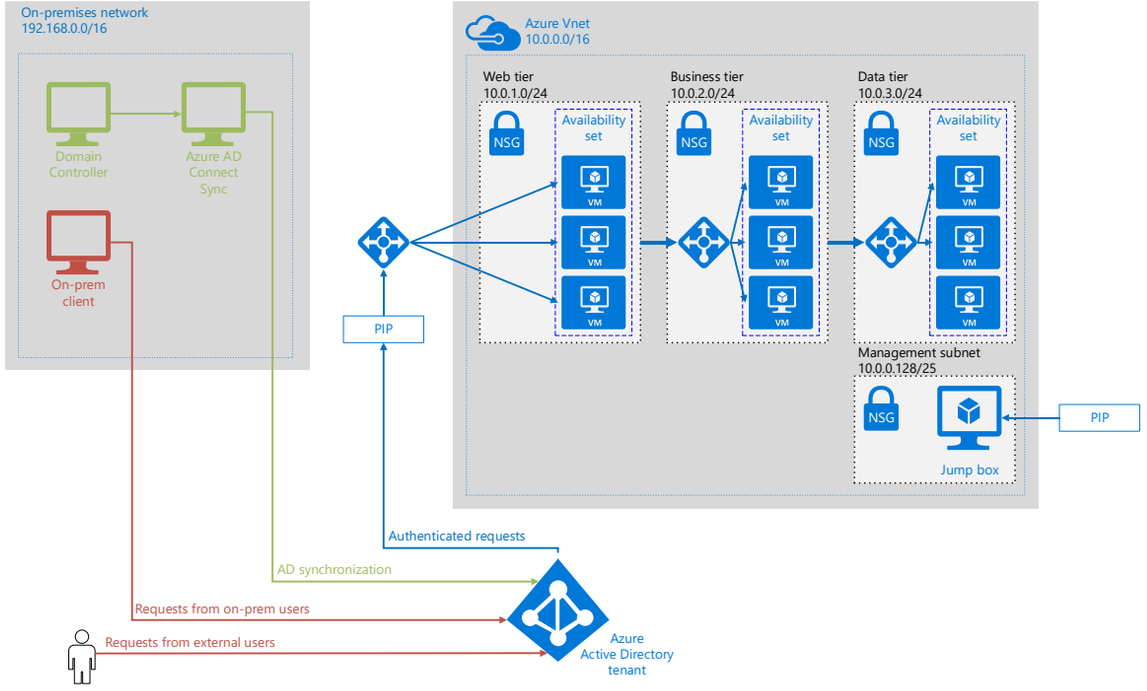
Reference: ExpressRoute

Session 6: Identity Design

Identity Design: Overview

Session Goals

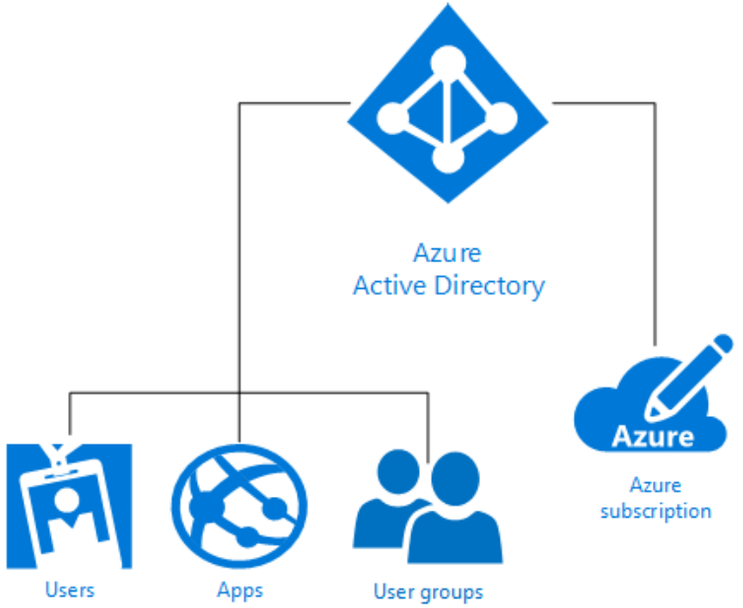
- Understand how to integrate managed and hybrid identities into solutions
- Learn how to design and implement role-based access control
- Recognize options for integrating external identity providers with applications



Azure Active Directory Design

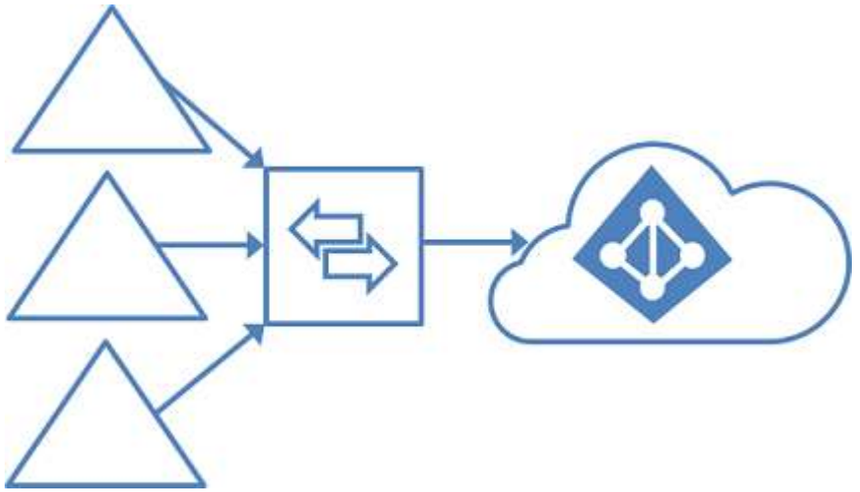
- Features
  - Is NOT Managed Active Directory
    - Is actually Cloud Identity-as-a-Service
  - Provides
    - Azure Portal access and RBAC
    - Single-sign-on to SaaS apps
    - Self-service identity management
  - Premium Features Available
    - Hybrid integration with ADDS
    - Multi-factor Authentication
    - Privilege account management
    - Identity Protection
    - Domain Services (DCaaS)

- Design Choices
  - Hybrid or cloud-only?
  - Cloud-only
    - Directory name
    - Custom domain
    - SKU (Premium Services)



Hybrid Identity Design

- Features
  - Deploy using AAD Connect
    - Synchronized Identity
      - Use same identity as on-premises
      - Password sync is available, but not required
      - Easiest to deploy
    - Federated Identity (ADFS)
      - Auth-N is redirected to on-prem AD
      - Provides support for SSO, on-Prem MFA, and PKI integration
      - Use password sync as backup IdP
      - Most complicated to deploy
    - Pass-through Authentication
      - Agent-based validation using connector
      - No credentials store in Azure
      - Currently in Preview; Not on exam!
- Design Choices
  - Synchronized or Federated
  - ADFS Architecture
  - Password sync
  - Self-service
  - Single Sign-On



Application Identity Integration

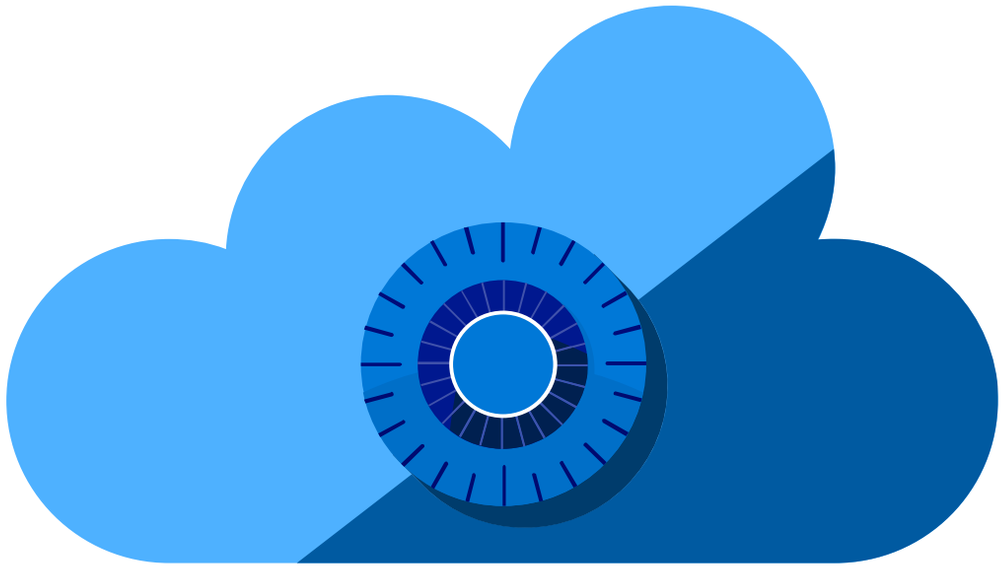
- Features
  - Application Authentication
    - Manage programmatically via Microsoft Graph or AAD Graph API
    - Process claims using SAML 2.0, OAuth 2.0, OpenID Connect
  - Customer/Partner Integration
    - AAD Business-to-Consumer (B2C)
      - Identity Broker-as-a-Service for Web and Mobile applications
      - Allows application authentication with social, enterprise, or local accounts
    - AAD Business-to-Business (B2B) Collaboration
      - Lets business partners BYOId
      - Creates guest account in AAD
      - Invite users via portal, API, bulk import
- Design Choices
  - Configure Identity Providers
  - Register Applications
  - Configure tokens
  - Configure SSO
  - Groups, Roles, Permissions
  - Manual/Programmatic/Bulk updates
  - Additional Features (e.g., MFA, etc.)

Session 7: Operations

Operations: Overview

Session Goals

- Understand monitoring and automation capabilities
- Learn how to identify resiliency objectives
- Recognize Azure services that can be used to monitor, respond, and recovery solutions



Automation and Configuration Management

- Features
  - Azure Automation Runbooks
    - Types: Graphical, Graphical PowerShell Workflow, PowerShell, PowerShell Workflow
    - Start runbook from portal, PS, API, webbooks, alerts, schedules
  - Azure Automation DSC
    - Use declarative statements to manage virtual machines
    - Compile configs in portal or PS
  - Other DSC tools
    - Chef, Puppet, Ansible, PS DSC
- Scenarios
  - Deployments
    - Deploy resources programmatically using ARM Templates and Automation runbooks
  - Updates
    - Update resources using automation runbooks.
    - Maintain configuration management using DSC tools
  - Incident Management
    - Associate diagnostic runbooks with alerts to create automated incident triage

Audit Logging and Monitoring

- Features
  - Activity logs
    - User actions in subscription
      - Examples: Add VNet, Delete VM
  - Diagnostic logs
    - Events performed by resource
      - Examples: OS event, security logs
  - Azure Diagnostics, Azure Monitor
    - Store logs in Azure Storage Account
    - Search, view logs in Portal
  - Log Analytics/Application Insights
    - Query and visualize logs
    - Create alerts and notifications
- Design Choices
  - Storage account for logs
  - Integration with Azure Services
    - Azure VMs via Azure Agent
    - Non-Azure VMs via MMS agent
    - Azure PaaS services
  - Retention requirements
  - Reporting requirements
  - Alerts and notifications
  - Delegation of access
  - SIEM integration
    - SCOM
    - Splunk
    - Others

Business Continuity Design

- Design Considerations
  - High Availability & Disaster Recovery
    - Alphabet soup: RTO, RPO, MTTR, and SLA
  - Planning for Failure
    - Design solutions to expect occasional failures and recover from them
    - Take advantage of platform resiliency features
      - Fault Domains (Availability Sets, Managed Disks)
      - Built-in geo-replication (Azure Storage, Azure SQL Database)
      - Load Balancing (Azure Traffic Manager, Load Balancer)
      - Site Recovery for VMs (A2A in Preview)
- Design Choices
  - High Availability
    - Uptime goals vs composite SLAs
      - Use Service-level HA Capabilities
  - Backup
    - Data Retention Policies
    - Operational data recovery
      - Use Azure Backup
  - Business Continuity (Failover)
    - RPO, RTO, MTTR for solution
      - Use Azure Site Recovery
        - On-premises to Azure
      - Use application-level replication

Session 8: Security

Security: Overview

Session Goals

- Understand where to find Microsoft resources related to security, compliance, privacy, and transparency
- Learn about how Azure Security can help reduce risk to your solutions
- Recognize how to take advantage of other built-in security features in Azure

Azure Trust Center

https://www.microsoft.com/en-us/trustcenter/cloudservices/azure

- Compliance
  - Access compliance information for specific Azure services
  - Review Audit controls and reports: SOC 1 Type 2, ISO 27001/27018, Pen Test
- Security
  - Access Microsoft Security Development Lifecyle (SDL) information
  - Review Microsoft Operational Security Assurance (OSA) framework
- Privacy
  - Review Privacy Standards, Online Service Terms, and Data Management processes
  - View Reports in Transparency Hub
    - Law Enforcement Requests, US National Security Orders

Azure Security

- Features
  - Prevent
    - Monitor security state of resources
    - Define security policies
    - Generate policy-driven security recommendations
  - Detect
    - Analyze security data, using global threat intelligence feeds, machine learning and behavioral analysis
  - Respond
    - Get insights into the source of the attack and impacted resources
    - Suggests ways to stop the current attack and help prevent future attacks
- Design Choices
  - Define roles and access
  - Set security polices
  - Implement Just in Time access
  - Implement security recommendations
  - Configure Security Alerts
  - Integrate with partner solutions
    - Endpoint protection
      - Trend Micro, Symantec, Microsoft
    - Web application firewall
      - Barracuda, F5, Imperva, Fortinet
    - Next-generation firewall
      - Check Point, Barracuda, Fortinet, and Cisco