

- **Concepts and Terminology**
 - Azure Monitor
 - Key Capabilities
 - Monitor and visualize metrics
 - Query and analyze logs
 - Setup alerts and actions
 - General
 - Contains log, metrics, and traces
 - Collects from Application, Guest OS, Resource, Subscription, and Tenant
 - Monitoring solutions may require both Log Analytics Workspace and Automation account if using Runbooks
 - Metrics
 - General
 - Most metrics retained for 93 days for most metrics
 - Log-based metrics inherit retention of the Log Analytics workspace
 - Application Insight logs are retained for 90 days
 - Aggregate on min, max, count, sum and adjust time span
 - Two metrics can be monitored in a single rule
 - Log data can be converted to metrics
 - Components
 - Platform Metrics - Collected from Azure resources at one minute frequency
 - Guest OS Metrics - Agent-based metrics retrieved from VM using Windows Diagnostic Extension or InfluxData Telegraf Agent
 - Application Metrics - Created by application insights
 - Custom Metrics - defined with application via Application Insights or via API
 - Logs
 - General
 - Log data is stored in a Log Analytics Workspace
 - Application Insights stores application log data in a separate workspace for each application
 - Cross-resource queries can be used to query across workspaces
 - Application Monitoring
 - Application Insights monitors availability, performance, and usage of web apps running in Azure or on-premises
 - Azure Monitor for Containers monitors container workloads running in Azure Kubernetes Service
 - Azure Monitor for VM
 - Alerting
 - General
 - Alerts that used to be managed by Log Analytics and Application Insights are now called Classic Metrics
 - Alerts have a state of new, acknowledged, or closed
 - Alerts have a monitoring state of fired or resolved
 - Smart Groups are groups of alerts analyzed by ML to reduce noise and aggregate

- Service Health Alerts
 - Configured in Service Health blade
 - Components
 - Class of service interruption (service issues, planned maintenance, health advisory)
 - Affected subscriptions
 - Azure Service
 - Region
 - Action Group
 - Alert Rules
 - General
 - Enabled or disabled
 - Components
 - Target resource
 - Signal - metric, activity log, application insights, log
 - Criteria
 - Name
 - Description
 - Severity (0-4)
 - Action
 - Sources
 - Metrics values
 - Log search queries
 - Activity log events
 - Health of underlying azure platform
 - Website availability
 - Action Groups
 - General
 - Used by Azure Monitor and Service Health Alerts to notify alert has occurred
 - Can be used by multiple alerts
 - Limit of 2000 per sub
 - Limits of 1 SMS / Voice every 5 minutes and <100 emails per hour
 - Create in Azure Monitor -> Alerts ->
 - Actions
 - Email/SMS/Push/Voice
 - Logic App
 - Azure Function
 - Webhooks
 - ITSM
 - Automation Runbook
- Diagnostic Logging
 - General
 - Tenant and resource logs
 - Send to Azure Monitor Logs, Event Hubs, Azure Storage
 - Retention for logs in storage accounts can be 0 (forever) - 365 days

- Enable on each resource or centrally through Azure Monitor (for everything but Activity Monitor and Azure AD Sign In/Audit)
 - Multiple diagnostic settings are supported per resource allowing for variation in where and what is sent
 - Requires no agent and captures data from Hypervisor
 - Storage Accounts and Event Hubs can be in different subscriptions
- Diagnostic Setting
 - Turn on or off
 - Max of 5 per resource
 - Send to Azure Storage Account, Event Hub, or Log Analytics Workspace
 - Set retention for archiving to Storage Account for 0-365 days
- Metric Alerts for Dynamic Threshold
 - General
 - ML learns metrics history and identifies behavior (baseline)
 - Allows for three sensitivities, high, medium, low
 - Alerts can be trigger on greater/lower than maximum threshold, greater than threshold, or lower than threshold
 - Thresholds can be ignored until a certain date (testing period) or adjust alerting through deviations
 - Enable/Disable
 - Create when setting up a new alert rule for a metric and move the threshold from static to Dynamic
- Log Analytics
 - General
 - Configure which OS event logs and metrics are logged to the workspace in Advanced Settings -> Data
 - Union joins other tables and workspaces
 - Key Tables
 - Event -> Windows Event Logs
 - Heartbeat -> Agent communication
 - <LOGNAME>_CL -> Text file on Win/Lin
 - Alert
 - Perf
 - W3CIISLogs -> IIS Logs
 - Key Queries
 - Event | union Syslog | where EventLevelName == "Error" or SeverityLevel == "Error"
 - Heartbeat | summarize count() by Computer, bin(TimeGenerated, 5min)
- Azure Advisor
 - General
 - Recommended for cost effectiveness, performance, HA, security
 - Provides recommendations for VM, availability sets, application gateway, App Services, SQL Services, Azure Cache for Redis
 - Recommendations are rated high, medium, and low
 - Can be dismissed, postponed, or can follow links to remediate
 - Subs and RGs can be excluded in the Configuration Section

- Underutilized CPU can be adjusted from 5%
- Cost Recommendations
 - Resize or shutdown VM are evaluated for 14 days and are underutilized if <5% CPU and <2% network
 - Unprovisioned ExpressRoute
 - Delete/Reconfigure idle virtual network gateways (idle for > 90 days)
 - RIs
 - Unassociated Public IP
- Cost Analysis and Budgets
 - Subscription Blade -> Cost Management -> Cost Analysis/Budgets
 - Filter to costs by resource
 - Monitor progress towards a budget
- Azure Activity Log
 - General
 - Platform activities for write operations only
 - Filters can be saved and re-used on dashboard
 - Download as CSV, export to Event Hub/Storage Account
 - Send to Log Analytics Workspace (subscription-level setting)
 - 90 days of retention
 - Azure Activity Logs Solution
 - Monitoring solution for Azure Monitor
 - Used to retain logs for longer than 90 days by adjusting retention of Logs Analytics Workspace up to 730 days
 - Add through **More** option in Insights section of Azure Monitor or through choosing **Logs** option in Activity Logs
 - Cross Tenant
 - Deliver across tenants by using the pattern of Source account Activity Log -> Source account Event Hub -> Destination Account Logic App -> Destination Account Log Analytics
 - Useful for CSP
- Azure Storage Accounts
 - General
 - Page blob max size is 8TB
 - Block blob max size is 4.75TB
 - Containers have an access policy of Private, Blob (anonymous read access for blocks only), Container (anonymous read access for containers + blobs)
 - Store accounts end with core.windows.net
 - Standard or Premium
 - Premium Storage Accounts
 - Page blobs only
 - Backed by SSD
 - LRS replication only
 - Types
 - GPv1 -> Legacy, no support for tiering
 - Blob -> Old don't use, less features, no tiering
 - GPv2 -> everything can go here
 - Block Blob Storage -> blob only w/ premium performance
 - FileStorage -> premium performance for files

- Tiers
 - Hot
 - Cold -> ideal for data remaining cool for 30+ days
 - Archive -> Set at blob level only
- Replication
 - LRS - 3 times single data center
 - ZRS - GPv2 only, 3AZ
 - GRS - 2nd region
 - RA-GRS - 2nd region and read
- Shared Access Signatures
 - Account SAS (blob, file, table, queue) and Service SAS
 - Uses hash-based message encryption
 - Limit to set of IPs and a secure protocol
- Stored Access Policies
 - Supported only for Service SAS
 - SAS associated with policy inherit start/expiry time and permissions and revocation
 - Can be created with GUI using Storage Explorer
- Custom Domains
 - Can be used to access blob data in storage account
 - One per storage account
 - Direct (create each CNAME) or indirect (no downtime and uses ASVERIFY subdomain)
- Special Features
 - Require secure transfer
 - Allows access from all networks or a single Vnet
 - Soft delete for blobs
 - Hierarchical namespace for DataLakes V2
- PowerShell CLI Commands
 - New-AzStorageAccount -ResourceGroupName -Name -Location -SkuName (Standard_LRS, etc) -kind (StorageV2, etc)
 - Az storage create --name --resource-group --location --sku --kind
- **Azure Storage Explorer**
 - GUI-based tool to navigate Azure storage
 - Connect to storage account via Azure AD, connection string + SAS URI, or storage account name and key
- **AzCopy**
 - AzCopy /Source:<source> [/SourceKey:<key>] /Dest:<dest> [/Destkey:<key>]
 - /pattern, /Source/DestSAS:, /S (recursive), /L (list only), /SyncCopy (copy locally first)
- **Azure Import/Export Service**
 - General
 - Move large amounts of data to and from Azure
 - Manage jobs in Azure Portal and create jobs in using WAImportExport tool
 - Use HDD or SSD drives
 - Encrypt with BitLocker
 - WAImportExport

- v1 for Blob and v2 for File
 - PrepImport /j:<journal_name> /sk:<storage account key> /srcdir:<on_prem> /dstidir:<container>
- Azure Backup
 - General
 - Replicate using LRS or GRS
 - No charge for data transfer
 - 9,999 recover points for protected VM
 - MARS, DPM, MABS
 - Daily, weekly, monthly, yearly schedule and retention
 - Backup Sources
 - On-prem (MARS, DPM, MABS)
 - Files and Folders
 - Hyper V
 - VMWare
 - SQL
 - SharePoint
 - Exchange
 - System State
 - Bare Metal
 - Azure Stack (MABS)
 - Files and Folders
 - SQL Server
 - SharePoint
 - System State
 - Azure
 - VM
 - SQL Server in VM
 - Azure FileShare
 - Other recovery options
 - Snapshot Recovery
 - Blob snapshot of VM page blob
 - Copy to another region
 - Create new VM from snapshot
- Virtual Machine
 - General
 - ACU - 100 for A1
 - Ultra SSD, Premium SSD, Standard SSD, Standard HDD
 - WinRMHTTPS 5986, WinRMHTTP 5985
 - Data Disk has max capacity of 32TB
 - OS Disk has max capacity of 2TB
 - Temporary disk persists after successful reboot and uses /dev/sdb and E:
 - Support OS
 - Windows 2003+ supported but earlier than 2008 R2 must provide own images
 - Server roles of DHCP, HyperV, RMS, WDS not supported
 - BitLocker not supported for OS disk
 - Types

- A - Basic (no support for autoscaling or load balancers) and Standard
 - B - burstable
 - D - General purpose
 - Dc - confidentiality and integrity
 - E - in memory hyperthreading (SAP HANA)
 - F - CPU opt
 - G - memory and storage (big data)
 - H - HPC
 - Ls - Storage
 - M -> Large memory
 - N - GPU
- VM Specialization
 - S - Premium Storage available
 - M - large memory optimized
 - R - RDMA
- Accelerated Networking
 - Bypass host and virtual switch and go directly to physical NIC
 - Supported only on some VM series
 - Enable on existing VM if it is Azure Gallery image and all VMs in VMSS must be stopped and deallocated
 - VMs with AdvNet can only be resized if the VM type being moved to supports it
- Setup WinRM
 - Create Key Vault
 - Create Self-signed Cert
 - Upload cert to Key Vault
 - Get URL for cert
- VM Storage
 - Standard HDD -> 32TB, 500MB/s, 2,000 IOPS
 - Standard SSD -> 32TB, 750MB/s, 6,000 IOPS
 - Premium SSD -> 32TB, 900MB/s, 20,000 IOPS
 - Ultra SSD -> 65TB, 2,000MB/s, 160,000 IOPS
- Unmanaged Disk vs Managed Disk
 - Unmanaged you manage underlying storage account and the limit of 20,000 IOPS per storage account
 - Unmanaged allows you to do LRS, ZRS, GRS, and RA-GRS replication
 - Managed Disks only support LRS replication
 - Managed Disks are integrated with VMSS to ensure FD and UD
 - Unmanaged Disks handle RBAC on Storage Account while Managed Disks handle RBAC directly on the Managed Disk
- Managed Disk Snapshot
 - Read-only copy of managed disk at a point of time
 - Can be used to create new disks
- Managed Disk Image
 - Create an image of all managed disks associated with VM when it is generalized and deallocated
- Disk Caching
 - Method for improving performance of VM

- Utilize RAM and SSD from underlying host
 - Available for both standard and premium
 - Read-only / Read-Write
 - OS disk is by default Read-Write
- Modify Disk Caching
 - \$vm = Get-AzVM -Name
 - Set-AzDataDisk -VM \$vm -Name "data disk name" -Caching ReadWrite | Update-AzVm
- Availability Sets
 - Group 2+ machines to protect against failure
 - Max of 3 FD and 20 UD
 - Managed disks are automatically managed by availability set
- Virtual Machine Scale Sets
 - Max of 1,000 for gallery image and 600 for own image
 - Low priority saves costs but can be evicted
 - Load balance w/ load balancer or Application Gateway
 - Set a min and max of VMs
 - Scale out on metrics or a time schedule
 - Metrics can be infrastructure or application metrics
- PowerShell / CLI
 - Get-AzRemoteDesktopFile - ResourceGroupName -Name -Launch
- Public Ips
 - Basic SKU can be dynamic or static and are open by default
 - Standard SKU is only static, supports AZ, and are closed by default
 - Load Balancer SKU and Public IP SKU must match
- Virtual Network
 - General
 - New-AzVirtualNetwork -ResourceGroupName -Name -Location - AddressPrefix
 - Add-AzVirtualNetworkSubnetConfig -Name -AddressPrefix -VirtualNetwork <Vnet_object>
 - <vnet_object> | Set-AzVirtualNetwork
 - Azure reserves first three IPs and last IPs
 - Apply DNS to NIC or VNET
 - Network Security Group
 - Rules evaluated by priority 100-4096 with lowest being evaluated first
 - Service Tags of VirtualNetwork, AzureLB, Internet
 - 100 NSGs per Sub (raise to 400)
 - 200 NSGs rules per NSG (raise to 500)
 - Vnets per Sub 50 (raise to 500)
 - PIP dynamic 60 PIP reserved 20
 - Vnet Peering
 - Forwarded Traffic - allow VNA in another Vnet to forward traffic to this Vnet over the peering
 - Gateway Transit / Remote Gateway
 - Create using az network peering create
 - Add-AzVirtualNetworkPeering
 - Vnet-to-Vnet

- Connection between two Vnets in same or different subscriptions that is encrypted with IPSec
 - Uses Virtual Network Gateway and Vnet-to-Vnet connection
 - Requires Route-Based VPN
- P2S VPN
 - Supports SSTP, IKEv2, SSL/TLS
 - Authenticate with certificate or RADIUS
 - Basic SKU only support SSTP while VpnGw1+ supports IKEv2
 - Clients download a config file
- VPN Gateways
 - Basic SKU
 - Route-based VPN doesn't support RADIUS or IKEv2 for P2S and supports 10 tunnels
 - Policy-based VPN supports 1 tunnel and no P2S
 - VpnGw1-3
 - Supports route-based only
 - Up to 30 tunnels, P2S, BGP, active-active, custom IPSec/IKE and ExpressRoute coexistence
- ExpressRoute
 - Standard is geopolitical region only and premium is global
 - 50Mbps to 10Gbps
 - Unlimited inbound traffic but outbound can be unlimited or metered
 - Microsoft Peering and Private Peering
 - /30 required for BGP peering for each path
 - ASN for Azure is 12076
- Network Watcher
 - General
 - Requires Network Watcher Agent be installed on Linux/Windows (VM)
 - Enabled on region by region basis and enabled in Network Watcher -> Overview blade
 - Functions
 - Topology
 - Connection Monitor - Continuously monitor connections from VM to URI, IP, FQDN
 - IP Flow Verify - Determine why packet allowed or denied and relevant NSG
 - Effective Security Rules - see effective NSG cumulative, subnet, NIC
 - VPN Troubleshooter
 - Packet capture and log to storage account or to VM file system
 - View Azure quotas and limits
 - View and enable NSG flow logs
 - Enable/Disable Diagnostic Logging for networking components
 - Enable and view Traffic Analytics
- Network Performance Monitor
 - Log Analytics Solution
 - Monitor performance across cloud and on-premises
 - Monitor network connectivity using HTTP, HTTPS, TCP, ICMP
 - Monitor ExpressRoute
- Azure Load Balancer

- General
 - Layer 4 (TCP/UDP)
 - Supports IPv4/IPv6
 - Internal or external
 - Uses 5 tuple hash to distribute (source IP/port, dest IP/port, protocol)
 - Supports session affinity (sticky sessions) using 2-tuple or 3-tuple
 - Basic VMs cannot be used as targets
- Health Probes
 - Basic supports TCP/HTTP and Standard support TCP/HTTP/HTTPS
 - Select port, path (HTTP/HTTPS), internal, unhealthy threshold
- Rule
 - Port and backend port
 - Backend pool
 - Health probe
 - Session persistence (two-tuple, three tuple)
 - Idle timeout (minutes)
 - Floating IP (SQL AlwaysOn)
- Basic vs Standard
 - More capacity in standard
 - Standard supports HTTPS in addition to HTTP and TCP
 - Standard supports AZ
 - Standard supports outbound Rules / TCP Reset
 - Standard has SLA of 99.99 w/ 2 health VM
- Inbound NAT Rule
 - Front-end IP
 - Service
 - Protocol
 - Port
 - Associations
 - Port mapping (def/custom)
- Azure Application Gateway
 - General
 - Layer 7
 - Cookie-based session affinity
 - SSL offload
 - End to end SSL
 - Comes in standard, standardv2, WAF, WAFv2
 - V2 supports AZ
 - URL-based content filtering
 - Requires its own subnet already exists
 - Connection draining
 - Components
 - Front-end IP -> single public/private IP or both
 - Listener -> port, protocol, host, IP, which further sends based on request routing rule (1 to 1)
 - Request routing rule -> basic or path based
 - Backend pool -> NIC, VMSS, Public IP, Private IP, FQDN, multi-tenant backend

- Azure Traffic Manager
 - DNS-level
 - Supports VM, Cloud Services, Azure Web Apps, External Endpoints
 - Internet-facing applications only
 - HTTP/HTTPS GET-only
- Azure AD
 - Send Sign-In and Audit logs to Log Analytics
 - Configure on Azure AD blade
 - Diagnostic Setting
 - Send to Log Analytics
 - Enterprise State Roaming
 - Requires AAD Premium
 - Synchronize user and app settings to Azure AD and encrypted with Azure RMS
 - Data retained for 90-180 days
 - Enable in Azure AD -> Devices -> Enterprise State Roaming
- Azure AD Self-Service Password Portal
 - General
 - Enforce one or two authentication methods
 - Option to require user registration and set re-confirmation from 0-730 days
 - Notify users if password reset and all admins if any admin reset
 - Write-back on-prem requires P1 or above
 - Customize help desk link
 - Authentication Methods
 - Mobile phone
 - Office phone
 - Email
 - Security questions
 - Mobile app code
 - Mobile app notification
 - Pricing Details
 - Free < 500,000 objects
 - Basic -> SSPR, AAD Proxy
 - P1 -> Advanced reports, write-back, MFA
 - P2 -> Identity protection, PIM
- Azure AD PIM
 - PIM Roles
 - PIM Administrator -> manage role assignments in Azure AD and all aspects of PIM
 - Security Administrator -> read info and report and manage AD and O365
 - General
 - Enable PIM must be global admin and becomes PIM Administrator
 - PIM and Azure RBAC
 - Subscription must be enrolled in RBAC
 - Role assignment settings are eligible and active
 - RBAC Settings
 - Allow role to be permanent (eligible or active)

- Set time for how long eligible or active
 - Require MFA
 - Require justification
 - Require approval
- Role Based Access Control
 - General
 - Max of 2000 role assignments per subscription
 - Allow only, must use deny assignments to explicitly deny something
 - Three authZ models: classic subscription administration roles, Azure RBAC roles, Azure AD Admin roles
 - Owner, contributor, reader, user access administrator
 - Azure AD Global Admin can take control of subs by settings "Global Admin can manage Azure subs and Management Groups" and become User Access Admin for all subs in tenant
 - Role Assignments
 - Security principal -> user, group, service principal, managed identity
 - Role definition (role) -> actions, notactions, dataactions, notdataactions
 - Scope -> management group, subscription, resource group, resource
 - RBAC - Classic Subscription Administrative Roles
 - Account used to sign-up for Azure is Account Administrator/Service Administrator
 - Account Administrator (1), Service Administrator (1), Co-administrator (200)
 - Account Administrator -> billing owner, manage sub lifecycle
 - Service Administrator
 - Co-Administrator -> all but change Service Admin and associate sub w/ different directory
- Azure Instance Metadata Service (IMDS)
 - REST endpoint accessible to IaaS VM
 - <http://169.254.169.254/metadata/<API>?api-version=<VERSION>>
 - Instance/computer,network
 - Attest -> signature validation metadata
 - Scheduledevents -> upcoming maintenance
 - Identity -> used to obtain access tokens for managed identities
- Azure Policies
 - Default allow and explicit deny
 - Assigned at management group, subscription, and resource group
 - Inherited unless excluded
 - Audit, deny, or deploy
- Azure Resource Locks
 - CanNotDelete and ReadOnly
 - Scope of sub, rg, resource
- Azure Apps
 - Service Plans
 - Free - 10 apps, 1 GB disk
 - Shared - 100 apps, 1GB disk, LB, custom domains
 - Basic - 10GB disk, 3 instances, functions

- Standard - 50GB, 10 instances, deployment slots, VNET integration, autoscale
 - Premium - 250GB, 20 instances, clone app
 - Isolated - 1TB disk, 100 instances
 - Linux -> docker, ruby/.NET Core/Node.js/PHP
 - All plans but Linux -> .NET, .NET Core, Java, Node.js, PHP, Python
- Azure Service Environment (ASE)
 - Container for up to 100 single instance App Services in a subscription
 - Goes directly into customer Vnet subnet
 - External or internal
 - High scale, isolation and secure network access, high memory
 - Integrate with WAF
 - Dedicated environment for Windows/Linux Web Apps, Docker, mobile apps, functions
- Azure Service Plan Metrics - All Plans
 - CPU %
 - Memory %
 - Data In/Data Out
 - Disk queue length
 - HTTP Queue Length
- Azure Service Plan Metrics - Free/Shared
 - CPU (short), CPU (Day)
 - Memory
 - Bandwidth (per day)
 - Storage
- Azure Service Plan Quote Overage - Free/Shared
 - CPU short/day - 403
 - Memory - restart
 - Bandwidth - 403
 - Filesystem - write fail
- Azure Web App Diagnostics
 - Application -> Error, Warning, Information, Verbose (Application/)
 - Web Server -> Web Server Logging (http/RawLogs), Dedicated Error Message (DetailedError/), Failed Request Tracing (W3SVC#####), Deployment (/Git)
 - Obtain via FTP or CLI (az webapp log download)
- Azure Web App Application Insights Alerts
 - Metrics
 - Web Tests
 - Proactive Diagnostics
- Azure App Services - Application Setting
 - Configure version of .NET and PHP
 - Turn Java or Python on (off by def)
 - Change to 64-bit platform (basic+)
 - Turn on web socket
 - Enable apps to always run (basic+)
 - Auto-swap and move deployment into slot to prod automatically
 - Custom domains associated w/ web apps

- Cookie affinity (on by def)
- Azure App Services - Connection String
 - Configure db per deployment slot or global
 - Variable instead of file
 - SQLCONNSTR_, MYSQLCONNSTR_, SQLAZURECONNSTR_, CUSTOMCONNSTR_
- Azure App Services - Handler Mapping
 - External script processes
 - Extension, handler path, argument
- Azure App Services - Virtual Application
 - Subdirectories of app that do something specific
 - Virtual directory, physical path, application
- Azure App Services - Deployment Slots (Not Swapped)
 - Publishing endpoints
 - Custom domains
 - SSL Cert and binding
 - Scale setting
 - Webjob scheduling
 - Swap with preview or swap
- WebJob
 - Run program or script in same context as Web App
 - Continuous (start immediately, runs on all instances, remote debug)
 - Triggered (manual/scheduled, single instance, no remote debug)
 - CMD, Bash, PowerShell, Python, PHP, Node.js, Java
- Azure Functions App
 - Name is unique and ends with .azurewebsite.net
 - Consumption or App Service Plan
 - Requires storage account w/ Blob, Queue, and Tables
 - Pay for execution time and number of executions
 - Linux supports .NET, JavaScript, Python, and Docker
 - Windows supports .NET, JavaScript, Java, PowerShell
- Event Hub
 - General
 - Stream data to analytics
 - Throughput units are preallocated or set to a maximum
 - End with .servicebus.windows.net
 - Basic SKU - 1 consumer group, 100 connections
 - Standard SKU - 20 consumer group, 1000 connections, AZ, georecovery
 - Namespace -> Event Hub -> Consumer Group
 - Namespace
 - Shared access policy
 - Geo-recovery (paired region)
 - Firewall (allow Vnet, IP)
 - Create event hub
 - Entity
 - Shared access policy
 - Enable/disable hub
 - Partition count

- Message retention (7 days by def)
- Event Grid
 - General
 - Similar to CloudWatch Events and Lambda
 - Event Sources -> Event Grid -> Event Handlers
 - React to state changes
 - Publisher/Subscriber model
 - Limit is 64KB per event
 - Handlers
 - Azure Automation
 - Azure Functions
 - Event Hub
 - Hybrid Connections
 - Logic App
 - Microsoft Flow
 - Queue Storage
 - Webhook
 - Sources
 - Azure Subscription / Resource Group (Management)
 - Container Registry
 - Custom Topics
 - Event Hub
 - IoT Hub
 - Media Services
 - Service Bus
 - Storage Blob
 - Azure Maps
- Azure Service Bus
 - General
 - Basic -> shared capacity, 256KB message size, queues, variable pricing
 - Standard -> same as basic but topics, message operations
 - Premium -> standard and dedicated capacity, 1024KB message size, georecovery
 - Queue
 - Max size 1GB - 5GB
 - Message TTL (def 14 days)
 - Lock duration (def 60 sec)
 - Duplicate detection
 - Dead letter queue
 - Sessions (FIFO)
 - High throughput (partitioning)
 - Topic
 - Max size 1GB - 5GB
 - Message TTL
 - Duplicate detection

- Partitioning
 - Subs can be filtered to certain operations in a topic
- Azure Relay Service
 - Allows messages to be received by a public endpoint and relayed to on-premises applications
 - Application installed on-premises and established outgoing session to listen for messages
 - Applications on-premises are WCF and Hybrid Connections (Web Sockets)
- Azure SQL Database
 - General
 - Single database, elastic pool, and managed instance
 - Pricing model vCPU and DTU
 - Server container object handles scope of firewall and failover
 - Firewall can whitelist Ips, restrict Vnets, and allow Azure Services
 - Automated backups
 - Automatic and manual failover
 - Backup and Redundancy
 - Point-in-time backups done every 5-10ms for transaction logs and 12 hours for differential backups
 - Long-term-retention backups are available for all plans except for Basic with retention for up to 10 years
 - Automated backups are saved for 7 days and up to 35 days (except basic which is 7 only)
 - Georeplication allows for read-only in another region
 - Automatic failover is enabled at the server node
 - vCore Pricing Model
 - Gen4 - 24vCore, 168GB RAM, Gen5 - 80vCore, 408GB RAM
 - General Purpose -> 7,000 IOPS, 5-10ms latency, 1 replicate and no read scale
 - Business Critical -> 200,000 IOPS, 1-2ms latency, 3 replicas, 1 read scale and zone redundant
 - DTU Pricing Model
 - Performance promise
 - Basic - 5 DTU, 2GB, 7 day retention, no long-term retention
 - Standard - 300 DTU, 250GB, 35 day retention, LTR
 - Premium - 4000 DTU, 1TB, 35 day retention, LTR
 - Size for DTU by using larger of two calculations
 - Number of databases X average DTU per database
 - Number of currently peaking database X peak DTU
- Cosmos DB
 - General
 - Globally distributed and add/remove regions w/o downtime
 - Multimaster
 - Automatic and manual failover
 - Account is logical object and is container for DBs and ends with documents.azure.com
 - Logical setup - Account -> Container -> Contents

- Container RU max of 100,000 RU and increment 100 RU which each RU is 1KB
 - API is determined at account level
 - Consistency Level
 - Strong
 - Bounded Staleness - you choose for # week or time
 - Session
 - Consistent Prefix - reads never see out of order writes
 - Eventual consistency
 - API
 - Core (SQL)
 - Cassandra
 - Gremlin
 - Azure Table
 - Partitioning
 - Single partition limited to 10GB
 - Partitions limited to 400 requests/s (RU)
 - For unique key choose property you filter on
- Azure Recovery Vault
 - Logical container for backup
 - 500 vaults per sub
 - Replicates LRS or GRS
- Azure Migrate
 - Assess on-premises VM for Azure Migrate (VMWare only)
 - Provides size recommendations, monthly costs estimates, and visualize dependencies
 - Only create in East US and Central West US
 - OVA installed on VMWare Server
 - Comfort factor can be adjust by 1.3x
- Azure Site Recover (ASR)
 - Scenarios
 - Region to region
 - VMWare/Hyper V/physical servers/Azure Stack to Azure
 - VMWare/Hyper V/SCVMM/Physical servers to second data center
 - Replication Policy
 - Recovery point retention is default of 24 hours (oldest 72 hours) for crash consistent and 60 minutes for app consistent
 - Associate with a configuration server
 - Azure Requirements
 - Recovery Services Vault
 - V1 Storage Account in same region as Vault
 - Existing Vnet
- **Commands and CLI**
 - Enable Diagnostic Logging
 - PS - Set-AzDiagnosticSetting
 - CLI - az monitor diagnostic-setting
 - ARM - providers/diagnosticSettings (subresource of a resource)
 - RBAC

- PS - Get-AzRoleDefinitions, Get-AzRoleAssignments
 - CLI - az role definition list
- Resource Locks
 - PS - New-AzResourceLock
 - CLI - az lock create --name --lock-type
- Change Azure AD Connector Password
 - Add-ADSyncAADServiceAccount
- Deploy ARM Template
 - New-AzResourceGroupDeployment -ResourceGroupName -TemplateFile - TemplateParameterFile
- Configure Web App for Docker
 - Az webapp container set --name <app-name> --resource-group --docker-custom-image-name <registry>.azurecr.io.<container> --docker-register-server-url <http://<registry>.azurecr.io>
- Configure ACR and Push Docker Image
 - Az acr create --name <registry_name> --resource-group
 - Docker login <registry>.azurecr.io
 - Docker tag <container> <registry>.azurecr.io/<container>:vXXX
 - Docker push <registry>.azurecr.io/<container>:vXXXX
- Create Managed Disk Snapshot
 - \$vm = Get-AzVM -ResourceGroup -Name
 - \$config = New-AzSnapshotConfig -SourceURI \$vm.StorageProfile.OsDisk.ManagedDisk.Id -location <LOC> -CreateOption Copy
 - New-AzSnapshot -snapshot \$config -SnapshotName <NAME> - ResourceGroupName
- Encrypt Disk
 - Set-AzVMDiskEncryptionExtension -ResourceGroupName -Name - DiskEncryptionKeyVaultURI -DiskEncryptionKeyVaultId
 - Disable-AzDiskEncryption
 - Az vm encryption enable/disable
- Modify Disk Caching
 - \$vm = Get-AzVM -Name
 - Set-AzVMDisk -VM \$vm -Name <data_disk_name> -Caching ReadWrite | Update-AzVM
- Create Image of VM
 - Sysprep image
 - Stop and de-allocate
 - Set to Generalize -> Set-AzVM -Generalized
 - Get VM object -> \$vm = Get-AzVM
 - Create image config
 - \$config = New-AzImageConfig -Location -SourceVirtualMachineld \$vm.id
 - Create image
 - New-AzImage -Image \$config
- Create VM from VHD
 - Add-AzVhd -ResourceGroupName -Destination -LocalFilePath
 - New-AzDiskConfig -AccountType Standard_LRS -Location -CreateOption Import - SourceURI
 - New-AzDisk -DiskName -Disk <disk_config> -ResourceGroupName

- `Set-AzOSDisk -VM <vm_config> -ManagedDisk <os_disk>.id -StorageAccountType Standard_LRS -CreateOption Attach -Windows`