summary Governing Azure Resources

- Azure Policy is a tool to enforce bueineess rules and assess complaince with those standards.
- A polify definition defines the rules that must be followed and what effects will be applied if the rules are not followed
- policy definitions can be bundled into policy initiatives
- policy definitions can be saved at either the mgmt group or subscription level.
- policies must be assigned to eval the compliacne of resources (scope)
- policies can be assigned to a maangement, subscription, resource group or individual resources
- assigned policies with the `DeployIfNotExists` or `Modify` effect can be remeidated through Remediation Tasks
- the `Resource Policy Contributor` role is a least prived role that can create and assign policies

summary Deploying secure infrastructure

- Azure Blueprints are a package of artifacts including RGs, policy assignments, role assignments, and ARM templates
- Azure Blueprints support versioning to update existing infra deployed by Blueprints.
- Blueprints are the only method of creating Azure RBAC deny assignments using locked deployments.
- Azure Landing Zones are the foundation for deployments to Azure and accelerate depoyment of a best-practice deployment architecture.

summary Managing Cloud Security Posture

- to use the regulatory compliacne or attack path analysis featurs of MSFT defender for Cloud, you will need a Defender Plan enabled
- the MCSB provides a set of best practices and recommendations to help improbe the security of your workloads across Azure, AWS, GCP and on prem
- MSFT Secure Score provides a perncetage that indicates how compliant you are with the recommendations of the MCSB
- Security initaitives are powered by Azure Policy and used to measure compliance against the benchmarks.

summary Customizing security policies

- custom security initiatives allow you to measure and report on compliance for your specific requirements
- your customr security initatives must be both defined and assigned to a subscription or mgmt group
- `resource policy contributor` role is the least-rpived azure role that can create and assign customer security initiatives

summary securing multi-cloud environments

- CSPM provides compliance reporting for multi cloud envs (inc. AWS and GCP)
    - to setup the CSPM connector:
        - AWS: need `Administrator` perms
        - GCP: need `Owner` privs

- EASM: allows you to inventory and build a complete picture of your external attack surface with dependencies and vulnerabilities

summary Enabling Cloud Workload Protection (CWP)

- defender for services plan 2: provides adaptive app controls, qualys vuln scanning and FIM
- a Log Analytics workspace is required for Defender for Servers and Defender for SQL on VMs
- Defender for OSS RDBMS is enabled at the resource level only
- Defender for Cosmos DB only supports the NoSQL API

summary Responding to Security Governance Issues

- CSPM generates recommendations
  - in response to recommenddations you can use enforce or deny actions to prevent reoccurence
- CWP generate security alerts
- for both recommendations and alerts, use workflow automation to prevent reoccurence
- workflow automation is powered by azure logic apps

summary Introducing Monitoring on Azure

- log Analytics workspaces storeage data for Defender for Cloud, Sentinel and Azure monitor
- The resource-context Log Analytics workspace access mode provides access to logs based on resource access
- Log Analytics worksapces can storage data from 31 days upt o 730 days
- Individual tables in a workspace can store data up to 7 years.
- For immurtable logs, export data to a storage account

summary configuring monitoring on Azure

- `Log Analytics Contributor` role can deploy a Log Analytics Workspace and config monitoring for all Azure resources
- Collecting tenant, activity and resource logs requires diagnostics settings to be configured
- Collecting logs from an Azure VM or server outside of Azure requires the deployment of an Agent and the config of data collection rules

summary Introducing Microsoft Sentinel

- Sentinel is enabled on Log Analytics Workspace
- Data connectors are used to collect data into a Log Analytics workspace for Sentinel to analyze
- Analytics rules are used to detect and correlate threats into incidents
- Playbooks, powered by Azure Log Apps, are used to automate workflows in response to incidents
- `Logic Apps Contributor` role or a more prived role is required to create and edit playbooks.

summary Collecting SEcurity Events

- service-to-service connector can be used to collect data from M365, Azure and AWS
- built-in connectors can be used for syslog and SEF logs
- some appliances will require the deployment of a linux based log forwarder
- Azure Functions can be used to ingest logs from APIs

- KQL is sometimes used to transform data before ingesting into the Log Analytics Workspace.

summary Responding to Security Threats

- USe Azure Monitor alert rules to directly trigger notifications or automations based on an alert using actions groups
- Analytics rules in SEntinel help yuou find and be alerted to security threats
- automation rules in Sentinel can be used to automate the response to a security alert or incident, including running a playbook
- To use automation that involves playbooks, Sentinel must be granted privs to run playbooks

summary Deploying secret storage using Azure Key Vault

- key vault can be used to store encryption keys, text based secrets, and certs.
- key vault can also manage storage account keys
- There are two key services:
  - Key Vault and Managed HSM
- Managed HSM is required:
  - to support symmetric keys
  - for FIPS 140-2 Level 3 compliance
- Key Vault has two service tiers: standard and premium
- Premium tier is required to support software and HSM-protected keys

summary Managing access to Azure Key Vault

- Private endpoint: provides access to Key Vault without traversing the internet.
- Enable a firewall: to block public access
- Entra RBAC Control: you must grant access to both Control Plane and Data Plane.
- Remember:
  - access must be permitted at network and authorization layers
  - `key vault reader` and `key vault contributor` roles cannot access secrets

summary Managing Azure Key Vault Secrets

- secrets are versioned.
- only the enabled status of a secret affects the ability to retrive the secret
- Event Grid can be used to automatically rotate secrets
- can use a key rotation plicy to automatically rotate cryptographic keys

summary Protecting Key Vault Secrets

- use soft-delete and purge protection to protect against secret deletion
- once purge protection is enabled, it cannot be disabled
- key vault rotation is configurable anywhere between 7-90 days
- to recover a vault, subscription-level perms are required
- when a **vault** is recovered, linked resources are not recovered (IAM grants, etc)
- secrest must be restored to the same subscription and geography
- to recover a secret, data plane access is required

Summary securing access to VMs

- access to mgmt ports should be restricted
- can be used to conenct to VMs using RDP and SSH
- To deploy Bastion, a dedicated subnet named AzureBastionSubnet with at least a /26 addr space is required
- Use the Standard Bastion SKU for features like ip connectivity, sharable links and additional scalability
- you can perform a one-way upgrade of the SKU

summary Providing temporary access to VMs (via Just-in-Time VM access)

- JIT VM Access requires: Defender for SErvers Plan 2, an NSG, and/or Azure Firewall
    - Azure firewall must b eusing classic firewall rules
- Default mgmt ports are prtoected and you can customize the ports

summary securing Azure API Management service

- use the priciple of least priv when creating and assigning subscription keys
- transform inbound and outbound requests with sec policies
- ensure traffic is secure to,from,between your API gateway and backend service
- VNet integration and private endpoints are **NOT** supported in the consumption tier of API management

summary securing Azure Container registry

- use Entra ID sec principals to access ACR
- user managed identities for app/script access whenever possible
- avoid using the built-in admin account and disable it
- use built-in roles to authorize access
    - push images: `acrpush`
    - pull images: `acrpull`

summary securing Azure Container instances

- secure your container images throughout the lifecycle and control access to your container registry
- protect secrets with Azure Key Vault or where possible, use managed identities
- secure network traffic and integrate your workload with your VNets where applicable
- monitor your app code, and audit mgmt actions against your registry and workloads

summary securing Azure Container Apps

- Azure Container Apps that share an Azure Container Apps Environment share access to networking and logging
- Diagnostic Settings can be configed to collect system level and app logs
- Each app deployed to an environment shares ingress rules and managed identities
- Secrets can be stored per app or referenced from Key Vault

summary securing Azure Kubernetes Service (AKS)

- API Server: network layer, auth/auth

- Secure images in registry: shift-left methodology, access control
- Securing persistent and other storage: access control, encryption at rest
- Secrets management: access control, rotation of secrets
- secure traffic between pods: to allow microservice communication (between pods)
- secure user communication: provide general endpoint to pod ingress traffic encryption
- logging and monitoring: yarp.

summary monitoring AKS

- to use Container Insights, you will require a Log Analytics Workspace
- Config Diagnostic Settings to collect control plane logs
- To colelct Prometheus metrics from your AKS cluster, you will need an Azure Monitor Workspace
- To visualize Prometheus metrics, you can use Azure Managed Grafana

summary Managing authentication for AKS

- best practice dictates use Entra IDs to authenticate access to managed your AKS clusters and disable local k8s accounts
- use k8s RBAC to provide least priv access to manage the AKS cluster internals
- authorization must be provided at the control plan layer to retrive data plane API layer creds
- AKS **RBAC** roles only grant API access when you integrate Azure RBAC with AKS for Kubernetes

summary Securing AKS networking

- Azure CNI network plugin provides the best performance
- kubenet is recommended for dev/test env
- `Ingress` rules using ingress controllers are recommended for distributing prod https traffic
- Calico is recommended for network policy
- Network Policy can't be changed after cluster has been created

summary Securing VM data

- ADE uses BitLocker on Windows and DM-Crypt on Linux to protect VM disks
- To use ADE, key vault and the VM must reside in the same Azure region and subscription
- VM must have at least 2GB of RAM and be a supported SKU
- Confidential Disk Encryption provides additional protecting using the VM's TPM

summary Securing access to Storage Account

- whenever possible, use Entra and Azure RBAC to authenticate and authorize access to your storage accounts
- SAS can be used to delegate granular access to storage account data
- Stored Access Policies can be used to proviate greater control over service Shared Access Signatures
- User-delgation SAS can be used with blob storage to avoid the limitations of storage account key rotation

summary Secure access to Azure Blob Storage

- `Storage Blob Data Reader/Contributor/Owner` roles provide authorization to access blob data using Azure RBAC (respecting management hierarchy)
- storage account keys grant full access to an individual storage account
- SAS grant granular access to the storage account, a container, or individual blobs
- public access must be enabled on the storage account, and the individual contains where public access is permitted

summary Securing access to Azure Files

- you can access Azure Files using the REST API and SAS for granular auth
- Avoid usign Storage Account Keys to access Azure Files
- identity-based access is recommended when using the SMB protocol
- Identity-based access requires synced identities
- Share-level perms are configured using Azure RBAC
- file/directory level perms are configured usign Windows ACLs
- both share-level and file/directory level are required to authorize access

summary Securing Access to Azure Tables and Queues

- use Entra ID and Azure RBAC whenever possible
- prefer Service SAS over Account SAS to provide granular access to indificual tables or queues
- user-delegation SAS is not supported for tables and queues
- Consider setting a SAS expiration policy for your storage account and monitor for violations

summary protecting storage account data

- keep multiple indepenent copies of your storage account data
- user versioning and soft delete to protect data in place
- combine soft delete, versioning and the change feed with point-in-time restore
- storage account version immutability must be enabled on creation and cannot be disabled
- storage accounts enabled with version immutability cannot be combined with legal hold

summary configing advanced storage account security

- storage accoutn encryption is supported on Azure storage Accounts
- Bring your own keys using either customer managed or customer provided encryption keys
- customer managed keys requires an Azure Key Vault and a managed identity
- Enable infra encryption upon creation of a storage account to double-encrypt your data.

summary configuring database authentication

- Entra ID auth is recommended
- use Windows auth with Azure SQL Managed Instance for backwards compatiblity
- Create database-contained users with the command `CREATE USER name FROM EXTERNAL PROVIDER`
- provide grants with `ALTER ROLE database_role ADD MEMBER user_identity`

summary Auditing database access

- microsoft recommends server-level auditing

- auditing configed at the server level will apply auditing to all current and future databases
- dup logs will be created if auditing is configed at both server and database level
- use Managed Identities to avoid the need to manage the rotation of storage account keys

summary governing databases

- use Purview to identify and protect sensitive and business critical data
- use the Data Map to register data sources, setup scans, and create classificaitons
- use the Data Catalog to browse search and discovery your data
- use Insights to understand how assets are distributed across your estate

summary protecting sensitive information

- use SQL SERver Data Masking to limit sensitive data exposure
- Admins are automatically excluded from data masking rules and additional users can be excluded.
- Masking functions, applied to column with data masking rules that determine how data is masked
- to confgiure granular masking you have to use TSQL

summary configuring database encryption

- dynamic data maskign only masks the data from users
- transparent database encryption (TDE) encrypts data at rest, but still allows users managing the database to see data.
- Always Encrypted data can only be decrypted by client apps with access to the encryption key

summary understanding hybrid networks

- vnet is a set of azure resources connected to a dedicated private IP addr spoace
- VNets reside in an azure subscription within an azure region
- Azure supports both public resources, which ahve a public endpoint and private resources connected to a virtual network
- resources are connected to virtual networks using networking interfaces, and communicate using their private IP address.
- hybrid networks include Azure VNets, on prem networks, roaming users, and other clouds.

summary connecting azure VNets

- VNet peering enables private connectivity between resources in separate VNets
- VNets can be peered across subscriptiosn and regions
- VNET peering is non-trasitive, use a device capable of routing to forward traffic
- the addr space of peered networks cannot over lap
- you can resize the addr space peered VNets

summary controlling network traffic flow

- azure provides default system routes to route traffic within VNets and conencted networks
- you can override default system routes with custom routes
- custom routes include user-defined and BGP routes
    - user-defined routes override default routes

    - BGP routes are exhcange between routers
- routes with the longest prefix take precedence

summary connecting medium-sized networks and remotes users part 1

- use VPN Gateway to create S2S and VNet-to-VNet connections over the itnernet
- use zone-redundant, active-active connections for best availabiluty and performance
- VPN Gateway requires a dedicated subnet named `GatewaySubnet` with at least /29 CIDR block
- the Local Network Gateway resource specifies the remote connection ip addr or DNS name and remote IP range
- the Connection resource specifies how the how the VPN Gateway and remote device will connect, includign authentication, encryption and routing settings.
- Peering and route table settings may need to be updated to support VPN Gateways

summary Connecting medium sized network and remote users part 2

- remote users can connect to Azure VNets with P2S connections
- protocols include: OpenVPN, SSTP, IKEv2
- firewall traversal: OpenVPN, SSTP
- Auth options: cert based, Entra ID, RADIUS
    - Entra ID: supports conditional access
    - RADIUS: supports AD DS
- S2S and P2S can coexist on route-based VPN gateways (not policy based)
- likely, re-download client if you change auth or network topology for Windows clients

summary connecting large distributed networks part 1

- ExpressRoute provides physical private connections
- Can use ExpressRoute with a service provider or Expressroute Direct
- Use IPsec via a VPN gateway over Expressroute for end-to-end encryption
- use MACSec for point-to-point encryption

summary connecting large distributed networks part 2

- Easily manage large distributed networks using Azure VWAN
- VWAN provides a fully managed hub and spoke network architecture
- VWAN supports mutihub and manages routing between hubs
- Virtual hubs are decured by NVAs or Azure Firewall
- security policies and routing settings configed using Azure Firewall Manager are required to secure traffic usign a secured virtual hub

summary protecting against DOS attacks

- DDos Infrastructure Protection is built-in and provides automatic basic protection for all Public IP addrs
- DDoS IP Protection can be enabled per ip addr.
- DDoS IP Protection doesn't include rapid response, cost protection an WAF discounts
- DDos Network Protection protects up to 100 public IP addresses in all subscriptsiona nd regions within a signle tenant and provides the additional features that IP Protection does not

summary Protecting network boundaries: part 1

- Azure Firewall is deployed to a dedicated subnet named `AzureFirewallSubnet`
- Firewall Manager policies can be used to managed Azure Firewall in both VNet and Virtual WAN deployments
- DNAT rules are processed first, then network rules, then application rules in `priority` order
- force tunneling can be used to route all internet-bound traffic through another security appliance

summary protecting network boundaties: part 2

- a service firewall can be configed to secure public access to Azure PaaS services
- public IP addr and CIDR addr ranges can be permitted to access the public endpoint, with public access is disabled
- service firewalls are a network-layer security feature
- securign access to a specific VNet subnet requires Service Endpoints to be enabled on the subnet

summary Providing regional availability

- performance layer 7 load balance within an Azure region
- supports both public and private frontend ip addr
- supports header and path-based routing for web apps
- supports end-to-end encryption or TLS/SSL termination
- can integrate with WAF for protection again advanecd web-based threats

summary providing global availability

- Front Door performsn layer 7 traffic distributon and LB for internet-facing globally distributed apps and APIs
- Premium Tier is required for MSFT-managed WAF rule sets, bot protection and private bakcend connectivity using PRivate Link
- Front Door can improve the pefroamcne of web apps usign caching and compression
- Front Door supprots URL path-based routign, end-to-end encryption or TLS/SSL termination
- Front Door protects against common web security threast usign WAF

summary introduction to WAF

- WAF protects web apps against common and emerging threats
- WAF can be used with App Gatway, Front Door, and CSN in preview
- WAF tier of App Gateway is required to use WAF with App Gateway
- Premium tier of Front Door is required to use MSFt-managed rules with Front Door

summary securing application traffic

- enable TLS to secure app traffic
- azure service offer MSFT provided cert or you can bring your own certs
- Entra Application Proxy can be used to provide secure access to private web apps withotu the need to open ports and expose the application to the internet

summary Accessing Platform Services Privately Part 1

- Service Endpoints...
    - enable secure, private access to PaaS resources
    - enabled per subnet, per Azure service instance
    - are supported on many Azure services includign storage accounts, Azure SQL database, Key Vault and more
- use Service Endpoint Policies to protect allow traffic to only specific Azure resoruces and prevent data exfil
- Azure Firewall can be used with Service Endpoints to centrally control and log traffic to service endpoints

summary accessing platform services privately: part 2

- private endpoints provide private connectivity to indivdual PaaS resoruces
- all connected networks can access the private endpoints
- Private endpoints require DNS resource recrods
- integrate Private Endpoints with Azure Private DNS Zones for easy DNS management

summary Enabling Virtual Network Access for Applications

- Azure SQL Managed Instance is VNet integrated by default
- for App Service Plan, use VNet integration to provide outbound network connectivity from App Service to all VNet connected resources
- Isolated App Service Environments proviate native VNet integration for both inbound and outbound connectivity
- VNet integration requires a dedicated subnet that is delegated to Azure App Service
- VNet integration is posible across regions using Gateway-required VNet integration
- which reuqires a P2S VPN gateway

summary Filtering Network traffic

- NSGs are used to control network traffic
- NSGs can be assocaited with a subnet or NIC
- a NIC or subnet can have a maximum of 1 NSG
- NSGs must be in the same region as the resources they are associated with
- As traffic flows to and from a NIC, all associate NSGs are evaled
- security rules are stateful
- Security rules are process in priority from 100 to 4096, first match

summary simplifying network traffic filtering

- Augmented Security rules use Service Tags and ASGs instead of CIDR block ranges
- a Service Tag is a group of IP prefixes that represent a service or network segment
- ASGs allow you to group VMs and apply security rules using the group
- All NICs assigned to an ASG must exist in the same VNet

summary Monitoring and tshooting network traffic

- NEtwork Watcher provides a range of tools to monitor, diag, and analyze your network traffic
- Flow logs can be configed to capture ip flow info for an NSG or a VNet

- flow logs require a Standard General Purpose v2 Storage Account int he same region and tenant
- Version 2 NSG flow logs include additioanl throughput info

summary Differentiating authentication and authorization

- authentication is the process of verifying an identity
- authorization is the process of granting, denying, and determining the level of access to a resource
- OIDC and SAML are industry standard authentication protocols
- OAuth is an industry standard authorization protocol

summary understanding identity providers

- AAD tenant is the security and mgmt boundary for your enterprise
- AAD Premium P1 is required to use Azure AD Application Proxy, dynamic groups, password writeback, Conditional Access and Password Protection
- AAD Premium P1 is required to use Identity Protection, access review, JiT access mgmt

summary understanding security principals

- user principals represent people that need to access resoruces secured by AAD
- service principals represent apps and services that require acces sto resources secured by AAD
- groups can be used to manage security princiapls at scale
- AAD and AD DS groups can exist in your tenant

summary managing users

- to add users, you must have at least `User Administrator` role
- to update or delete prived role holders, you must have at least the `Privileged Authentication Adminsitrator` role.
- User should be managed where they are created
- Remember the structure of Powershell and azcli commands

summary Understanding Groups

- security groups are used to manage access to resources that are secured by AAD
- users, service principals, and other security groups can all be members of security groups
- M365 groups are used for collaboration in M365
- only users can be members of M365 groups
- dynamic groups can be either a dynamic user or dynamic device group. You can't mix membership
- service principals cannot be members of dynamic groups
- delete M365 groups are retained for 30 days
- security groups are not retained

summary Managing Service Principals

- an app registration is a global identity for your app
- a service principal is used to authon and author your app int he home tenant
- service principals are identities that are assigned to an app or background process
- service principals can be applications running anywhere (azure, on prem, other cloud)

- cert based auth is recommended when using self-managed service principals

summary managing identities for azure resources

- system-assigned managed identities are associate with a singel azure resource and share their lifecycle with the resource
- user-assigned managed identities have a many-to-many relationship with azure resources
- the lifecycle of user-assigned managed identities isindependent of the resources they are associated with
- the `Managed Identity Contributor` and `Managed Identity Operator` roles ahave required privs to create and assign user-assigne managed identities

summary managing external identities

- self-service sign up can't be used with Microsoft Apps
- to provide access to Microsoft resoruces like Azure and AAD, youc an invite Azure B2B guests into your azure AD tenant
- Azure AD B2C can be used to create a separate tenant for users to provide them with acecss to company-developed apps

summary enhancing authentication

- security defaults provide a baseline level of protection for all AAD users
- when you enable security defaults, users will have 14 days after their first login to enable MFA
- Azure AD Premium P1 provides conditional access based on scenarios or events at login
- Azure AD Premium P2 provides conditional access based on risks at login

summary implementing conditional access

- policy templates enable quick and efficient creation of common policies
- Always enable policies in report-only mdoe and test before enabling the policy
- Named locations can be used to define locations where policies might relax or deny access

summary protecting identities

- user risk is the probability that an identity is compromised
- sign-in risk is the probability that a sign in is compromised
- To configure Identity PRotection, you will need `Conditional Access Administrator` or `Security Administrator` role and an Azure AD Premium P2 license
- custom banned password lists require an Azure AD Premium P1 license
- Each AD DS domain controller requires two agents for complete protection

summary deploying SSO

- Azure AD Connect Cloud Sync with Password Hash Sync is the recommended hybrid identity solution
- Password writeback enables SSPR for AD DS
- AD DS password writeback requires Azure AD Premium P1 lciense
- Azure AD Connectcloud sync uses provisioning agents deploy to AD DS member servers to sync identities to AAD

summary going passwordless

- passwordless authentication is easier to use and more secure than authentication that involes passwords
- user Windows Hello for Business where users use a dedicated Windows device every day
- use Microsoft Authenticator where users use a non-Windows device
- use FIDO2-compliant security keys where use of phones is restricted, such as a helpdesk or call center, for customer-facing roles, or for highly prived identities

summary decentralizing identities

- an AAD tenant can be configed to both issue and verify decentralized identities
- AAD and an Azure Key Vault are the minimum required Azure resources to support verfieid identities
- to config Verified ID using the priciple of least priv, you need the following roles:
  - `Authentication Policy Administrator` and `Application Administrator`
  - `Contributor` access to the RG where the key vault will be located

summary introducing authorization

- a Global Administrator must elevate access to manage the root management group
- AAD roles can be scoped to the tenant, an application registration, or an administrative unit.
- Azure RBAC roles can be scoped to a management group, subscription, resource group, or individual resource
- An Azure AD Premium P1 license is needed for each administrative unit administrator
- Administrative units cannot be nested

summary using built-in roles

- Azure AD roles:
  - Azure AD role-assignable groups require at least an Azure AD Premium P1 license
  - to assign AAD roles you need at least the `Privileged Role Administrator` role
- Azure Roles:
  - Azure roles can be assigned at either the control plane or the data plane
  - to assign Azure roles, you need at least the `User Access Administrator` role

summary Customizing Roles

- MSGraph is the API driven service that's used to interact with Entra ID via powershell
- an Zure AD Premium P1 license is required for every user with a custom Azure AD role assignment
- Azure RBAC custom roles can include both control plane and data plane actions
- `NotActions` in Azure RBAC roles are exclusions to the actions, not deny permissions
- Assignable scopes are used to define the scope to which an Azure RBAC role can be assigned

summary enabling Just-in-Time authorization

- PIM can provide just-in-time and time-bound access to Azure AD roles, Azure roles, and Groups
- PIM can also require approvals, justification, and MFA prior to activation
- Assigned roles are available until they expire and can be used without activation
- eligible roles must be activated and, once activated, they are available until they expire

- PIM requires Azure AD Premium P2 licenses

summary continuously evaluating authorization

- access reviews allow you to manage group memberships, access appl, and role assignments either on demand or periodically
- access reviews for Azure AD roles and Azure roles require an Azure AD Premium P2 license
- access reviews cannot be used with AD DS groups and groups with dynamic membership

summary authorizing applications

- two types of app permissions
    - applications permissions: allow an application to access Azure AD secured resources directly
    - delegate persmissions: allow an app to access resoruces on behalf of a user
- two types of consent:
    - user consent: user consents the app to access data they have access to
    - admin consent: the administrator consents on the behalf of the users