1. **Key concepts to understand with Azure AD:** Identity, Account, Azure AD Account, Azure subscription, Azure tenant/directory
2. **What is Identity?:** An Object that can get authenticated. Can be a user with a username and password or other items like servers that require authentication through secret keys or certificates.
3. **What is Account?:** An identity that had data associated with it.
4. **What is an Azure AD Account?:** An identity created through Azure AD or another Microsoft cloud service, such as Microsoft 365, Sometimes called a work or school account.
5. **What is an Azure tenant/directory?:** A dedicated and trusted instance of Azure AD, it is automatically created when your organization signs up for a Microsoft cloud service subscription.
6. **What are the four editions of Azure Active Directory?:** Free, Microsoft 365 Apps, Premium P1 and Premium P2
7. **What features are in Azure Active Directory Free?:** Provides user and group management, on-premises directory synchronization, basic reports, and single sign-on across Azure, Microsoft 365, and many popular SaaS apps, limited to 500,000 directory objects
8. **What features are in Azure Active Directory Microsoft 365 Apps?:** This edition is include with O365, In addition to the free features, this edition provides identity and access management for Microsoft 365 apps including branding, MFA, group access management, and self service password reset for cloud users.
9. **What features are in Azure Active Directory Premium P1?:** In addition to the free features, P1 also lets your hybrid users access both on-premises and cloud resources. It also supports advanced administration, such as dynamic groups, self-service group management, Microsoft Identity Manager (an on-premises identity and access management suite) and cloud write-back capabilities, which allow self-service password reset for your on-premises users.
10. **What features are in Azure Active Directory Premium P2?:** In addition to the free and P1 features, P2 also offers Azure Active Directory identity protection to help provide risk-based conditional access to your apps and critical company data. Privileged Identity Management is included to help discover, restrict, and monitor administrators and their access to resources and to provide just-in-time access when needed.
11. **What is Azure AD Join?:** Its designed to provide access to organizational apps and resources and to simplify Windows deployments of work-owned devices. Single Sign On (SSO) Enterprise compliant roaming, Access to Microsoft store for business, Windows Hello, Restriction of Access, Seamless access to on-premises resources.

12. **How do you connect to Azure AD join?:** To get a device under the control of Azure AD, you have two options.
Registering a device to Azure AD enables you to manage a devices identity. Azure AD device registration provides the device with an identity that is used to authenticate the device when a user signs-in to Azure AD. You can use the identity to enable or disable a device.
Joining a device is an extension to registering a device. Joining provides the benefits of registering and changes the local state of a device. Changing the local state enables your users to sign in to a device using an organizational work or school account instead of a personal account.
13. **Configure Self-Service Password Reset:** From your Azure AD tenant, on the Azure portal under Azure Active Directory (Users) select Password Reset
You can set it to None, Selected, or All.
Selected allows specific groups who have self service password reset enabled.
Authentication methods
You can pick the number of methods required to reset a password. This can be a notification, a test, a code sent to user's mobile or office phones, or a set of security questions
14. **What are Azure Regions?:** Geographical areas that contain at leas one, but potentially multiple datacenters.
15. **What is an Azure Subscription?:** Its a logical unit of Azure services that is linked to an Azure account.
16. **How do you obtain a Subscription?:** Enterprise agreements, Resellers, Partners, Personal free account.
17. **How do you implement cost management?:** You use Azure Cost Management and Billing features to conduct billing administrative tasks and manage billing access to costs.
18. **What are management groups?:** If your organization has many subscriptions, you may need a way to efficiently manage access, policies, and compliance for those subscriptions. Azure management groups provide a level of scope above subscriptions.
19. **How do you add a management group?:** Using the portal, PowerShell, or azure CLI.
20. **What are the two identifiers of Management groups?:** The Management group ID - A Directory unique identifies that is used throughout the azure system to identify this group. Not editable after creation
The Display Name - the name that is displayed within the azure portal, a separate display name is an optional field when creating the group and can be changed at any time

21. **What is Azure Policy?:** A Service that you use to create, assign, and manage policies. These policies enforce different rules over your resources, so those resources stay compliant with your corporate standards and SLA. Can be applied a management group level.
22. **What are the steps to creating Azure Policies?:** Follow these steps, Browse Policy definitions, Create initiative Definitions, Scope the Initiative Definitions, View Policy evaluation Results.
23. **What do you do if there is not a built-in policy for what you need?:** When there isn't an applicable policy definition built-in you can load policies from GitHub, Policy definitions have a specific JSON format.
24. **Why should you create an Initiative Definition?:** Once you have determined what policy definitions you need you create it to group those policies and apply them to a scope
25. **How do you Scope your Initiative Definition?:** You can assign it to a subscription and then a resource group optionally
26. **How do you see how your policy application is doing?:** Use the Compliance blade to review non-compliant initiatives, policies, or resources. This occurs about once an hour
27. **What is a security principal?:** An object that represents something that is requesting access to resources
28. **What is a role definition?:** Collection of permissions that lists the operations that can be performed.
29. **What is a Scope?:** Boundary for the level of access that is requested
30. **What is an Assignment?:** Attaching a role definition to a security principal at a particular scope.
31. **What's a best practice for access control?:** Grant users the least privilege to get their work done.
32. **What is a role?:** A set of properties defined in a JSON file.
33. **What are Actions and NotActions?:** Properties that can be tailored to grant and deny the exact permissions you need.
34. **What is the AssignableScopes property?:** The area that the role my perform their actions, can be subscriptions, resource groups, or resources.
35. **How do you grant people access to certain roles?:** You assign a role to a user, group, service principal, or managed identity
36. **What are the built in roles in Azure RBAC?:** Owner, Contributor, and Reader
37. **What are Roles?:** Roles are are groups that users can be assigned to to grant various permissions
38. **What are Permissions?:** Actions allowed to be completed by that role.

39. **What are Member users?:** A native member of the Azure AD organization that have a set of default permissions. like edit their profile information
40. **What are Guest users?:** Restricted Azure AD organization permissions. They sign in with their account and are granted access to your network and access is determined from there.
41. **What happens when you delete a user?:** It stays in a suspended state for 30 days, can be restored in that window
42. **What is Federation trust?:** When you establish a trust with another organization or a collection of domains for shared access to a set of resources.
43. **What is Azure AD Connect?:** An offering to extend your on-prem active directory to the cloud. Allowing you to use your existing work identities to manage azure subscriptions