**Study Guide**

**Exam AZ-900: Microsoft Azure Fundamentals**

Skills measured

• Describe cloud concepts (25–30%)

• Describe Azure architecture and services (35–40%)

• Describe Azure management and governance (30–35%)

**Describe cloud concepts (25–30%)**

**Describe cloud computing**

* Define cloud computing
  + Cloud computing is the delivery of computing services over the internet. Computing services include common IT infrastructure such as virtual machines, storage, databases, and networking. Cloud services also expand the traditional IT offerings to include things like Internet of Things (IoT), machine learning (ML), and artificial intelligence (AI).
  + Because cloud computing uses the internet to deliver these services, it doesn’t have to be constrained by physical infrastructure the same way that a traditional datacenter is. That means if you need to increase your IT infrastructure rapidly, you don’t have to wait to build a new datacenter—you can use the cloud to rapidly expand your IT footprint.
* Describe the shared responsibility model
  + With the shared responsibility model, these responsibilities get shared between the cloud provider and the consumer. Physical security, power, cooling, and network connectivity are the responsibility of the cloud provider.
  + You’ll always be responsible for:
* The information and data stored in the cloud
* Devices that are allowed to connect to your cloud (cell phones, computers, and so on)
* The accounts and identities of the people, services, and devices within your organization
  + The cloud provider is always responsible for:
* The physical datacenter
* The physical network
* The physical hosts
  + Your service model will determine responsibility for things like:
* Operating systems
* Network controls
* Applications
* Identity and infrastructure
* Define cloud models, including public, private, and hybrid
* identify appropriate use cases for each cloud model
* Describe the consumption-based model
* Compare cloud pricing models

**Describe the benefits of using cloud services**

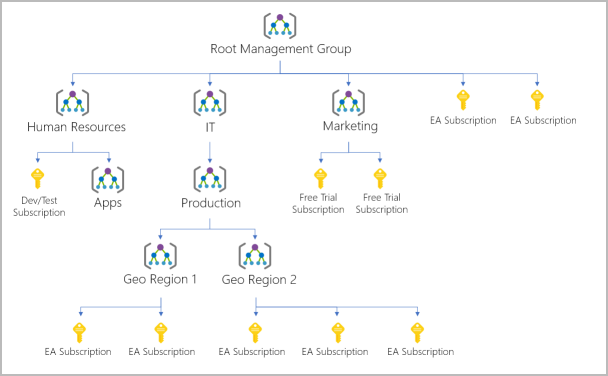
* Describe the benefits of high availability and scalability in the cloud
  + Azure is a highly available cloud environment with uptime guarantees depending on the service. These guarantees are part of the service-level agreements (SLAs).
  + Another major benefit of cloud computing is the scalability of cloud resources. Scalability refers to the ability to adjust resources to meet demand. If you suddenly experience peak traffic and your systems are overwhelmed, the ability to scale means you can add more resources to better handle the increased demand.
  + The other benefit of scalability is that you aren't overpaying for services. Because the cloud is a consumption-based model, you only pay for what you use. If demand drops off, you can reduce your resources and thereby reduce your costs.
* Describe the benefits of reliability and predictability in the cloud
  + Predictability can be focused on performance predictability or cost predictability
  + Performance predictability focuses on predicting the resources needed to deliver a positive experience for your customers. Autoscaling, load balancing, and high availability are just some of the cloud concepts that support performance predictability. If you suddenly need more resources, autoscaling can deploy additional resources to meet the demand, and then scale back when the demand drops. Or if the traffic is heavily focused on one area, load balancing will help redirect some of the overload to less stressed areas.
  + Cost predictability is focused on predicting or forecasting the cost of the cloud spend. With the cloud, you can track your resource use in real time, monitor resources to ensure that you’re using them in the most efficient way, and apply data analytics to find patterns and trends that help better plan resource deployments. By operating in the cloud and using cloud analytics and information, you can predict future costs and adjust your resources as needed. You can even use tools like the Total Cost of Ownership.
* Describe the benefits of security and governance in the cloud
  + Whether you’re deploying infrastructure as a service or software as a service, cloud features support governance and compliance. Things like set templates help ensure that all your deployed resources meet corporate standards and government regulatory requirements. Plus, you can update all your deployed resources to new standards as standards change. Cloud-based auditing helps flag any resource that’s out of compliance with your corporate standards and provides mitigation strategies. Depending on your operating model, software patches and updates may also automatically be applied, which helps with both governance and security.
  + On the security side, you can find a cloud solution that matches your security needs. If you want maximum control of security, infrastructure as a service provides you with physical resources but lets you manage the operating systems and installed software, including patches and maintenance. If you want patches and maintenance taken care of automatically, platform as a service or software as a service deployments may be the best cloud strategies for you.
  + And because the cloud is intended as an over-the-internet delivery of IT resources, cloud providers are typically well suited to handle things like distributed denial of service (DDoS) attacks, making your network more robust and secure.
* Describe the benefits of manageability in the cloud
  + There are two types of manageability for cloud computing that you’ll learn about in this series, and both are excellent benefits.
  + Management of the cloud speaks to managing your cloud resources. In the cloud, you can:
* Automatically scale resource deployment based on need.
* Deploy resources based on a preconfigured template, removing the need for manual configuration.
* Monitor the health of resources and automatically replace failing resources.
* Receive automatic alerts based on configured metrics, so you’re aware of performance in real time.
  + Management in the cloud speaks to how you’re able to manage your cloud environment and resources. You can manage these:
* Through a web portal.
* Using a command line interface.
* Using APIs.
* Using PowerShell.

**Describe cloud service types**

* Describe infrastructure as a service (IaaS)
  + Infrastructure as a service (IaaS) is the most flexible category of cloud services, as it provides you the maximum amount of control for your cloud resources. In an IaaS model, the cloud provider is responsible for maintaining the hardware, network connectivity (to the internet), and physical security. You’re responsible for everything else: operating system installation, configuration, and maintenance; network configuration; database and storage configuration; and so on. With IaaS, you’re essentially renting the hardware in a cloud datacenter, but what you do with that hardware is up to you.
  + IaaS places the largest share of responsibility with you. The cloud provider is responsible for maintaining the physical infrastructure and its access to the internet. You’re responsible for installation and configuration, patching and updates, and security.
  + Some common scenarios where IaaS might make sense include:
* Lift-and-shift migration: You’re standing up cloud resources similar to your on-prem datacenter, and then simply moving the things running on-prem to running on the IaaS infrastructure.
* Testing and development: You have established configurations for development and test environments that you need to rapidly replicate. You can stand up or shut down the different environments rapidly with an IaaS structure, while maintaining complete control.
* Describe platform as a service (PaaS)
  + Platform as a service (PaaS) is a middle ground between renting space in a datacenter (infrastructure as a service) and paying for a complete and deployed solution (software as a service). In a PaaS environment, the cloud provider maintains the physical infrastructure, physical security, and connection to the internet. They also maintain the operating systems, middleware, development tools, and business intelligence services that make up a cloud solution. In a PaaS scenario, you don't have to worry about the licensing or patching for operating systems and databases.
  + PaaS splits the responsibility between you and the cloud provider. The cloud provider is responsible for maintaining the physical infrastructure and its access to the internet, just like in IaaS. In the PaaS model, the cloud provider will also maintain the operating systems, databases, and development tools. Think of PaaS like using a domain joined machine: IT maintains the device with regular updates, patches, and refreshes.
  + Some common scenarios where PaaS might make sense include:
* Development framework: PaaS provides a framework that developers can build upon to develop or customize cloud-based applications. Similar to the way you create an Excel macro, PaaS lets developers create applications using built-in software components. Cloud features such as scalability, high-availability, and multi-tenant capability are included, reducing the amount of coding that developers must do.
* Analytics or business intelligence: Tools provided as a service with PaaS allow organizations to analyze and mine their data, finding insights and patterns and predicting outcomes to improve forecasting, product design decisions, investment returns, and other business decisions.
* Describe software as a service (SaaS)
  + Software as a service (SaaS) is the most complete cloud service model from a product perspective. With SaaS, you’re essentially renting or using a fully developed application. Email, financial software, messaging applications, and connectivity software are all common examples of a SaaS implementation.
  + While the SaaS model may be the least flexible, it’s also the easiest to get up and running. It requires the least amount of technical knowledge or expertise to fully employ.
  + The shared responsibility model applies to all the cloud service types. SaaS is the model that places the most responsibility with the cloud provider and the least responsibility with the user. In a SaaS environment you’re responsible for the data that you put into the system, the devices that you allow to connect to the system, and the users that have access. Nearly everything else falls to the cloud provider. The cloud provider is responsible for physical security of the datacenters, power, network connectivity, and application development and patching.
  + Some common scenarios for SaaS are:
* Email and messaging.
* Business productivity applications.
* Finance and expense tracking.
* Identify appropriate use cases for each cloud service (IaaS, PaaS, SaaS)

**Describe Azure architecture and services (35–40%)**

**Describe the core architectural components of Azure**

* Describe Azure regions, region pairs, and sovereign regions
  + With a decentralized design, the cloud enables you to have resources deployed in regions around the world. With this global scale, even if one region has a catastrophic event other regions are still up and running. You can design your applications to automatically take advantage of this increased reliability. In some cases, your cloud environment itself will automatically shift to a different region for you, with no action needed on your part.
* Describe availability zones
  + Availability zones are physically separate datacenters within an Azure region. Each availability zone is made up of one or more datacenters equipped with independent power, cooling, and networking. An availability zone is set up to be an isolation boundary. If one zone goes down, the other continues working. Availability zones are connected through high-speed, private fiber-optic networks.
* Describe Azure datacenters
  + The physical infrastructure for Azure starts with datacenters. Conceptually, the datacenters are the same as large corporate datacenters. They’re facilities with resources arranged in racks, with dedicated power, cooling, and networking infrastructure.
  + As a global cloud provider, Azure has datacenters around the world. However, these individual datacenters aren’t directly accessible. Datacenters are grouped into Azure Regions or Azure Availability Zones that are designed to help you achieve resiliency and reliability for your business-critical workloads.
* Describe Azure resources and resource groups
  + A resource is the basic building block of Azure. Anything you create, provision, deploy, etc. is a resource. Virtual Machines (VMs), virtual networks, databases, cognitive services, etc. are all considered resources within Azure.
  + Resource groups are simply groupings of resources. When you create a resource, you’re required to place it into a resource group. While a resource group can contain many resources, a single resource can only be in one resource group at a time. Some resources may be moved between resource groups, but when you move a resource to a new group, it will no longer be associated with the former group. Additionally, resource groups can't be nested, meaning you can’t put resource group B inside of resource group A.
  + Resource groups provide a convenient way to group resources together. When you apply an action to a resource group, that action will apply to all the resources within the resource group. If you delete a resource group, all the resources will be deleted. If you grant or deny access to a resource group, you’ve granted or denied access to all the resources within the resource group.
* Describe subscriptions
  + In Azure, subscriptions are a unit of management, billing, and scale. Similar to how resource groups are a way to logically organize resources, subscriptions allow you to logically organize your resource groups and facilitate billing.
* Describe management groups
  + If you have many subscriptions, you might need a way to efficiently manage access, policies, and compliance for those subscriptions. Azure management groups provide a level of scope above subscriptions. You organize subscriptions into containers called management groups and apply governance conditions to the management groups. All subscriptions within a management group automatically inherit the conditions applied to the management group, the same way that resource groups inherit settings from subscriptions and resources inherit from resource groups. Management groups give you enterprise-grade management at a large scale, no matter what type of subscriptions you might have. Management groups can be nested.
* Describe the hierarchy of resource groups, subscriptions, and management groups
  + 

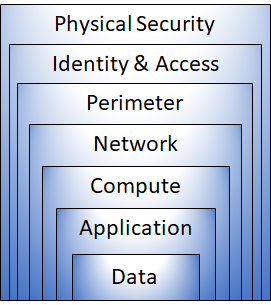
**Describe Azure compute and networking services**

* Compare compute types, including container instances, virtual machines (VMs), and functions
  + Azure Container Instances offer the fastest and simplest way to run a container in Azure; without having to manage any virtual machines or adopt any additional services. Azure Container Instances are a platform as a service (PaaS) offering. Azure Container Instances allow you to upload your containers and then the service will run the containers for you.
  + With Azure Virtual Machines (VMs), you can create and use VMs in the cloud. VMs provide infrastructure as a service (IaaS) in the form of a virtualized server and can be used in many ways. Just like a physical computer, you can customize all of the software running on your VM. VMs are an ideal choice when you need:
* Total control over the operating system (OS).
* The ability to run custom software.
* To use custom hosting configurations.
  + An Azure VM gives you the flexibility of virtualization without having to buy and maintain the physical hardware that runs the VM. However, as an IaaS offering, you still need to configure, update, and maintain the software that runs on the VM.
  + Azure Functions is an event-driven, serverless compute option that doesn’t require maintaining virtual machines or containers. If you build an app using VMs or containers, those resources have to be “running” in order for your app to function. With Azure Functions, an event wakes the function, alleviating the need to keep resources provisioned when there are no events.
  + Using Azure Functions is ideal when you're only concerned about the code running your service and not about the underlying platform or infrastructure. Functions are commonly used when you need to perform work in response to an event (often via a REST request), timer, or message from another Azure service, and when that work can be completed quickly, within seconds or less.
  + Functions scale automatically based on demand, so they may be a good choice when demand is variable.
  + Azure Functions runs your code when it's triggered and automatically deallocates resources when the function is finished. In this model, you're only charged for the CPU time used while your function runs.
  + Functions can be either stateless or stateful. When they're stateless (the default), they behave as if they're restarted every time they respond to an event. When they're stateful (called Durable Functions), a context is passed through the function to track prior activity.
  + Functions are a key component of serverless computing. They're also a general compute platform for running any type of code. If the needs of the developer's app change, you can deploy the project in an environment that isn't serverless. This flexibility allows you to manage scaling, run on virtual networks, and even completely isolate the functions.
* Describe VM options, including Azure Virtual Machines, Azure Virtual Machine Scale Sets, availability sets, and Azure Virtual Desktop
* Describe resources required for virtual machines
* Describe application hosting options, including the Web Apps feature of Azure App Service, containers, and virtual machines
* Describe virtual networking, including the purpose of Azure Virtual Networks, Azure virtual subnets, peering, Azure DNS, Azure VPN Gateway, and Azure ExpressRoute
* Define public and private endpoints

**Describe Azure storage services**

* Compare Azure storage services
  + A storage account provides a unique namespace for your Azure Storage data that's accessible from anywhere in the world over HTTP or HTTPS. Data in this account is secure, highly available, durable, and massively scalable.
  + When you create your storage account, you’ll start by picking the storage account type. The type of account determines the storage services and redundancy options and has an impact on the use cases.
* Describe storage tiers
* Describe redundancy options
  + Locally redundant storage (LRS)
  + Geo-redundant storage (GRS)
  + Read-access geo-redundant storage (RA-GRS)
  + Zone-redundant storage (ZRS)
  + Geo-zone-redundant storage (GZRS)
  + Read-access geo-zone-redundant storage (RA-GZRS)
* Describe storage account options and storage types
* Identify options for moving files, including AzCopy, Azure Storage Explorer, and Azure File Sync
  + AzCopy is a command-line utility that you can use to copy blobs or files to or from your storage account. With AzCopy, you can upload files, download files, copy files between storage accounts, and even synchronize files. AzCopy can even be configured to work with other cloud providers to help move files back and forth between clouds.
  + Azure Storage Explorer is a standalone app that provides a graphical interface to manage files and blobs in your Azure Storage Account. It works on Windows, macOS, and Linux operating systems and uses AzCopy on the backend to perform all of the file and blob management tasks. With Storage Explorer, you can upload to Azure, download from Azure, or move between storage accounts.
  + Azure File Sync is a tool that lets you centralize your file shares in Azure Files and keep the flexibility, performance, and compatibility of a Windows file server. It’s almost like turning your Windows file server into a miniature content delivery network. Once you install Azure File Sync on your local Windows server, it will automatically stay bi-directionally synced with your files in Azure.
* Describe migration options, including Azure Migrate and Azure Data Box
  + Azure Migrate is a service that helps you migrate from an on-premises environment to the cloud. Azure Migrate functions as a hub to help you manage the assessment and migration of your on-premises datacenter to Azure. It provides the following:
* **Unified migration platform**: A single portal to start, run, and track your migration to Azure.
* **Range of tools**: A range of tools for assessment and migration. Azure Migrate tools include Azure Migrate: Discovery and assessment and Azure Migrate: Server Migration. Azure Migrate also integrates with other Azure services and tools, and with independent software vendor (ISV) offerings.
* **Assessment and migration**: In the Azure Migrate hub, you can assess and migrate your on-premises infrastructure to Azure.
  + Azure Data Box is a physical migration service that helps transfer large amounts of data in a quick, inexpensive, and reliable way. The secure data transfer is accelerated by shipping you a proprietary Data Box storage device that has a maximum usable storage capacity of 80 terabytes. The Data Box is transported to and from your datacenter via a regional carrier. A rugged case protects and secures the Data Box from damage during transit.
  + You can order the Data Box device via the Azure portal to import or export data from Azure. Once the device is received, you can quickly set it up using the local web UI and connect it to your network. Once you’re finished transferring the data (either into or out of Azure), simply return the Data Box. If you’re transferring data into Azure, the data is automatically uploaded once Microsoft receives the Data Box back. The entire process is tracked end-to-end by the Data Box service in the Azure portal.

**Describe Azure identity, access, and security**

* Describe directory services in Azure, including Microsoft Azure Active Directory (Azure AD), part of Microsoft Entra and Azure Active Directory Domain Services (Azure AD DS)
  + Azure Active Directory (Azure AD) is a directory service that enables you to sign in and access both Microsoft cloud applications and cloud applications that you develop. Azure AD can also help you maintain your on-premises Active Directory deployment.
  + For on-premises environments, Active Directory running on Windows Server provides an identity and access management service that's managed by your organization. Azure AD is Microsoft's cloud-based identity and access management service. With Azure AD, you control the identity accounts, but Microsoft ensures that the service is available globally. If you've worked with Active Directory, Azure AD will be familiar to you.
  + When you secure identities on-premises with Active Directory, Microsoft doesn't monitor sign-in attempts. When you connect Active Directory with Azure AD, Microsoft can help protect you by detecting suspicious sign-in attempts at no extra cost. For example, Azure AD can detect sign-in attempts from unexpected locations or unknown devices.
  + Azure Active Directory Domain Services (Azure AD DS) is a service that provides managed domain services such as domain join, group policy, lightweight directory access protocol (LDAP), and Kerberos/NTLM authentication. Just like Azure AD lets you use directory services without having to maintain the infrastructure supporting it, with Azure AD DS, you get the benefit of domain services without the need to deploy, manage, and patch domain controllers (DCs) in the cloud.
  + An Azure AD DS managed domain lets you run legacy applications in the cloud that can't use modern authentication methods, or where you don't want directory lookups to always go back to an on-premises AD DS environment. You can lift and shift those legacy applications from your on-premises environment into a managed domain, without needing to manage the AD DS environment in the cloud.
  + Azure AD DS integrates with your existing Azure AD tenant. This integration lets users sign into services and applications connected to the managed domain using their existing credentials. You can also use existing groups and user accounts to secure access to resources. These features provide a smoother lift-and-shift of on-premises resources to Azure.
* Describe authentication methods in Azure, including single sign-on (SSO), multifactor authentication, and passwordless
  + **Single sign-on**: Single sign-on (SSO) enables you to remember only one username and one password to access multiple applications. A single identity is tied to a user, which simplifies the security model. As users change roles or leave an organization, access modifications are tied to that identity, which greatly reduces the effort needed to change or disable accounts.
  + Multifactor authentication is the process of prompting a user for an extra form (or factor) of identification during the sign-in process. MFA helps protect against a password compromise in situations where the password was compromised but the second factor wasn't.
  + Think about how you sign into websites, email, or online services. After entering your username and password, have you ever needed to enter a code that was sent to your phone? If so, you've used multifactor authentication to sign in.
  + Multifactor authentication provides additional security for your identities by requiring two or more elements to fully authenticate. These elements fall into three categories:
    - Something the user knows – this might be a challenge question.
    - Something the user has – this might be a code that's sent to the user's mobile phone.
    - Something the user is – this is typically some sort of biometric property, such as a fingerprint or face scan.
  + Multifactor authentication increases identity security by limiting the impact of credential exposure (for example, stolen usernames and passwords). With multifactor authentication enabled, an attacker who has a user's password would also need to have possession of their phone or their fingerprint to fully authenticate.
  + Features like MFA are a great way to secure your organization, but users often get frustrated with the additional security layer on top of having to remember their passwords. People are more likely to comply when it's easy and convenient to do so. Passwordless authentication methods are more convenient because the password is removed and replaced with something you have, plus something you are, or something you know.
  + Passwordless authentication needs to be set up on a device before it can work. For example, your computer is something you have. Once it’s been registered or enrolled, Azure now knows that it’s associated with you. Now that the computer is known, once you provide something you know or are (such as a PIN or fingerprint), you can be authenticated without using a password.
* Describe external identities and guest access in Azure
  + An external identity is a person, device, service, etc. that is outside your organization. Azure AD External Identities refers to all the ways you can securely interact with users outside of your organization. If you want to collaborate with partners, distributors, suppliers, or vendors, you can share your resources and define how your internal users can access external organizations. If you're a developer creating consumer-facing apps, you can manage your customers' identity experiences.
  + External identities may sound similar to single sign-on. With External Identities, external users can "bring their own identities." Whether they have a corporate or government-issued digital identity, or an unmanaged social identity like Google or Facebook, they can use their own credentials to sign in. The external user’s identity provider manages their identity, and you manage access to your apps with Azure AD or Azure AD B2C to keep your resources protected.
  + You also can easily ensure that guest users have appropriate access. You can ask the guests themselves or a decision maker to participate in an access review and recertify (or attest) to the guests' access. The reviewers can give their input on each user's need for continued access, based on suggestions from Azure AD. When an access review is finished, you can then make changes and remove access for guests who no longer need it.
* Describe Conditional Access in Microsoft Azure Active Directory (Azure AD), part of Microsoft Entra
  + Conditional Access is a tool that Azure Active Directory uses to allow (or deny) access to resources based on identity signals. These signals include who the user is, where the user is, and what device the user is requesting access from.
  + Conditional Access helps IT administrators:
    - Empower users to be productive wherever and whenever.
    - Protect the organization's assets.
  + Conditional Access also provides a more granular multifactor authentication experience for users. For example, a user might not be challenged for second authentication factor if they're at a known location. However, they might be challenged for a second authentication factor if their sign-in signals are unusual or they're at an unexpected location.
* Describe Azure role-based access control (RBAC)
  + managing that level of permissions for an entire team would become tedious. Instead of defining the detailed access requirements for each individual, and then updating access requirements when new resources are created or new people join the team, Azure enables you to control access through Azure role-based access control (Azure RBAC).
  + Azure provides built-in roles that describe common access rules for cloud resources. You can also define your own roles. Each role has an associated set of access permissions that relate to that role. When you assign individuals or groups to one or more roles, they receive all the associated access permissions.
  + So, if you hire a new engineer and add them to the Azure RBAC group for engineers, they automatically get the same access as the other engineers in the same Azure RBAC group. Similarly, if you add additional resources and point Azure RBAC at them, everyone in that Azure RBAC group will now have those permissions on the new resources as well as the existing resources.
* Describe the concept of Zero Trust
  + Zero Trust is a security model that assumes the worst case scenario and protects resources with that expectation. Zero Trust assumes breach at the outset, and then verifies each request as though it originated from an uncontrolled network.
* Describe the purpose of the defense in depth model
  + The objective of defense-in-depth is to protect information and prevent it from being stolen by those who aren't authorized to access it.
  + A defense-in-depth strategy uses a series of mechanisms to slow the advance of an attack that aims at acquiring unauthorized access to data.
  + You can visualize defense-in-depth as a set of layers, with the data to be secured at the center and all the other layers functioning to protect that central data layer.
  + 
* Describe the purpose of Microsoft Defender for Cloud
  + Defender for Cloud is a monitoring tool for security posture management and threat protection. It monitors your cloud, on-premises, hybrid, and multi-cloud environments to provide guidance and notifications aimed at strengthening your security posture.
  + Defender for Cloud provides the tools needed to harden your resources, track your security posture, protect against cyber attacks, and streamline security management. Deployment of Defender for Cloud is easy, it’s already natively integrated to Azure.

**Describe Azure management and governance (30–35%)**

**Describe cost management in Azure**

• Describe factors that can affect costs in Azure

• Compare the Pricing calculator and the Total Cost of Ownership (TCO) calculator

• Describe the Azure Cost Management and Billing tool

• Describe the purpose of tags

**Describe features and tools in Azure for governance and compliance**

• Describe the purpose of Azure Blueprints

• Describe the purpose of Azure Policy

• Describe the purpose of resource locks

• Describe the purpose of the Service Trust Portal

**Describe features and tools for managing and deploying Azure resources**

• Describe the Azure portal

• Describe Azure Cloud Shell, including Azure CLI and Azure PowerShell

• Describe the purpose of Azure Arc

• Describe Azure Resource Manager and Azure Resource Manager templates (ARM templates)

**Describe monitoring tools in Azure**

• Describe the purpose of Azure Advisor

• Describe Azure Service Health

• Describe Azure Monitor, including Log Analytics, Azure Monitor alerts, and Application Insights

<https://learn.microsoft.com/en-us/azure/azure-glossary-cloud-terminology>