<https://www.linkedin.com/pulse/exam-az-900-microsoft-azure-fundamentals-study-guide-jason-zandri/>

Identity – something that can be authenticated

Principal – an Identity acting with a certain role or claim.

Service Principal – An Identity used by a Service or an Application.

Roles can be granted at the individual service instance level, but they also flow down the Azure Resource Manager hierarchy.

Management Group-🡪Subscriptions🡪Resource group🡪Resource : Roles assigned to Subscriptions will get inherited by Resources.

**Symmetric encryption** uses the same key to encrypt and decrypt the data.

**Asymmetric encryption** uses a public key and private key pair. Either key can encrypt but a single key can't decrypt its own encrypted data. To decrypt, you need the paired key.

**Azure Disk Encryption** is a capability that helps you encrypt your Windows and Linux IaaS virtual machine disks.

**Transparent data encryption (TDE)** helps protect Azure SQL Database and Azure Data Warehouse against the threat of malicious activity. By default, TDE is enabled for all newly deployed Azure SQL Database instances.

1. **Service certificates** are used for cloud services
2. **Management certificates** are used for authenticating with the management API

**Azure Firewall** is a managed, cloud-based, network security service that protects your Azure Virtual Network resources. It is a fully stateful firewall as a service with built-in high availability and unrestricted cloud scalability. Azure Firewall provides inbound protection for non-HTTP/S protocols.

**Azure Application Gateway** is a load balancer that includes a Web Application Firewall (WAF) that provides protection from common, known vulnerabilities in websites. It is designed to protect HTTP traffic.

**Network virtual appliances (NVAs)** are ideal options for non-HTTP services or advanced configurations, and are similar to hardware firewall appliances.

**Network Security Groups** allow you to filter network traffic to and from Azure resources in an Azure virtual network.

To provide a dedicated, private connection between your network and Azure, you can use **Azure ExpressRoute.** ExpressRoute lets you extend your on-premises networks into the Microsoft cloud over a private connection facilitated by a connectivity provider.

**Microsoft Azure Information Protection** (sometimes referred to as AIP) is a cloud-based solution that helps organizations classify and optionally protect documents and emails by applying labels.

**Azure Advanced Threat Protection** (Azure ATP) is a cloud-based security solution that identifies, detects, and helps you investigate advanced threats, compromised identities, and malicious insider actions directed at your organization. It is a Managed Services solution.

* Azure ATP Portal
* Azure ATP Sensor (installed on domain controllers)
* Azure ATP Cloud Service

Azure resources can interact with resources in other access groups.

A resource group can contain resources from multiple Azure regions.

Resources in a Resource Group inherit permissions, not tags.

Azure Advisor **does not** provide recommendations on improving security of an Azure AD environment, **does not** provide recommendations on how to configure network settings on Azure VMs, **does** provide recommendations on how to reduce cost of running Azure VMs.

Windows 10, Ubuntu, MacOS Mojave – from all of these, you can use the 3 Management tools Azure CLI, Azure Portal, and Azure PowerShell.

Azure Log Analytics can be used to correlate events from multiple resources into a centralized repository.

You have an Azure environment. You need to create a new Azure virtual machine from an Android laptop.

Solution: You use PowerShell in Azure Cloud Shell.

Answer : Possible.

Solution : You use PowerApps portal.

Answer : Not possible , PowerApps is not part of Azure.

Solution : You use Azure Portal.

Answer : Possible.

If you have Azure resources deployed to every region, **does not** mean you can implement Availability Zones in every region.

When you need to delegate permissions to several Azure virtual machines simultaneously, you must deploy the Azure virtual machines to the same resource group.

Azure DevTest labs is used by **Developers** to self-manage VMs, and PaaS , without having to wait for approvals.

Command Prompt and PowerShell can be used to run CLI.

When Azure Active Directory (Azure AD) users connect to Azure AD from the Internet by using an anonymous IP address, **Azure AD Identity Protection** can ensure the users are prompted automatically to change their password

An application needs to connect to Azure AD to retrieve security tokens.

Security Center blade from Azure Portal can help evaluate if a Company’s Azure environment meets regulatory standards.

When you assign an Azure Policy to an existing RG - By default, this assignment will only take effect on newly created resources. Existing resources will not be affected.

Azure Advanced Threat Protection monitors threat by using sensors.

Azure AD Identity Protection enforces Azure MFA based on conditions.

Virtual Machines can be moved from an existing subscription to another subscription.

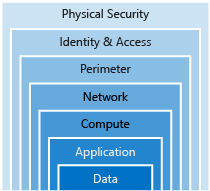
Each Azure subscription can contain multiple Account administrators.

Each Azure subscription can be managed by using a Microsoft Account only.

An Azure Resource Group cannot contain multiple Azure subscriptions.

Unused Public IP addresses can be removed to effect cost savings.

You can create an Azure support request from the Azure Portal.



DDoS and Firewall are at perimeter layer

Security Center – Incident Response Cycle :

Detect🡪Assess🡪Diagnose

To upgrade a subscription to the Standard tier, you must be assigned the role of Subscription Owner, Subscription Contributor, or Security Admin.

Network Virtual Appliances are the Virtual equivalent of Azure Firewalls as those also work for non-HTTP(s) for inbound

Azure Firewall – non HTTP(s)

Application gateway – HTTP(s)

DDOS Standard can protect against volumetric attacks, protocol attacks and resource (application) attacks

Azure Load Balancer distributes traffic within the same region to make your services more highly available and resilient. Traffic Manager works at the DNS level, and directs the client to a preferred endpoint. This endpoint can be to the region that's closest to your user.

Load Balancer and Traffic Manager both help make your services more resilient, but in slightly different ways. When Load Balancer detects an unresponsive VM, it directs traffic to other VMs in the pool. Traffic Manager monitors the health of your endpoints.When Traffic Manager finds an unresponsive endpoint, it directs traffic to the next closest endpoint that is responsive.

| **Service** | **Global/regional** | **Recommended traffic** |
| --- | --- | --- |
| Azure Front Door (Layer 7) | Global | HTTP(S) |
| Traffic Manager | Global | non-HTTP(S) |
| Application Gateway (Layer 7) | Regional | HTTP(S) |
| Azure Load Balancer (Layer 4) | Regional | non-HTTP(S) |

Availability Zones are primarily for VMs, managed disks, load balancers, and SQL databases. Azure services that support Availability Zones fall into two categories:

* **Zonal services** – you pin the resource to a specific zone (for example, virtual machines, managed disks, IP addresses)
* **Zone-redundant services** – platform replicates automatically across zones (for example, zone-redundant storage, SQL Database).

Azure PowerShell is a module that you can install for Windows PowerShell or PowerShell Core, which is a cross-platform version of PowerShell that runs on Windows, Linux, or macOS. Azure PowerShell enables you to connect to your Azure subscription and manage resources. Windows PowerShell and PowerShell Core provide services such as the shell window and command parsing. Azure PowerShell then adds the Azure-specific commands.

Azure CLI is a cross-platform command-line program that connects to Azure and executes administrative commands on Azure resources. Cross-platform means that it can be run on Windows, Linux, or macOS.

[Azure Cloud Shell](https://shell.azure.com/) is an interactive, authenticated, browser-accessible shell for managing Azure resources. It provides the flexibility of choosing the shell experience that best suits the way you work, either Bash or PowerShell.

|  |  |
| --- | --- |
| Code-first (imperative) | Designer-first (declarative) |

RBAC focuses on user actions at different scopes. You might be added to the contributor role for a resource group, allowing you to make changes to anything in that resource group. Azure Policy focuses on resource properties during deployment and for already-existing resources. Azure Policy controls properties such as the types or locations of resources. Unlike RBAC, Azure Policy is a **default-allow-and-explicit-deny system**.

Azure Management Groups are containers for managing access, policies, and compliance across multiple Azure subscriptions. Management groups allow you to order your Azure resources hierarchically into collections, which provide a further level of classification that is above the level of subscriptions. All subscriptions within a management group automatically inherit the conditions applied to the management group.

We can execute Powershell scripts on Linux only when Powershell Core and Azure CLI are installed

From the Azure portal, if you use Azure Cloud shell, you can run both Bash and Powershell-based scripts