Study guide for Exam AZ-700: Designing and Implementing Microsoft Azure Networking Solutions

Purpose of this document

This study guide should help you understand what to expect on the exam and includes a summary of the topics the exam might cover and links to additional resources. The information and materials in this document should help you focus your studies as you prepare for the exam.

Useful links	Description
Review the skills measured as of May 2, 2023	This list represents the skills measured AFTER the date provided. Study this list if you plan to take the exam AFTER that date.
Review the skills measured prior to May 2, 2023	Study this list of skills if you take your exam PRIOR to the date provided.
Change log	You can go directly to the change log if you want to see the changes that will be made on the date provided.
How to earn the certification	Some certifications only require passing one exam, while others require passing multiple exams.
Certification renewal	Microsoft associate, expert, and specialty certifications expire annually. You can renew by passing a **free** online assessment on Microsoft Learn.
Your Microsoft Learn profile	Connecting your certification profile to Microsoft Learn allows you to schedule and renew exams and share and print certificates.
Exam scoring and score reports	A score of 700 or greater is required to pass.
Exam sandbox	You can explore the exam environment by visiting our exam sandbox.

Useful links	Description
Request accommodations	If you use assistive devices, require extra time, or need modification to any part of the exam experience, you can request an accommodation.
Take a practice test	Are you ready to take the exam or do you need to study a bit more?

Updates to the exam

Our exams are updated periodically to reflect skills that are required to perform a role. We have included two versions of the Skills Measured objectives depending on when you are taking the exam.

We always update the English language version of the exam first. Some exams are localized into other languages, and those are updated approximately eight weeks after the English version is updated. While Microsoft makes every effort to update localized versions as noted, there may be times when the localized versions of an exam are not updated on this schedule. Other available languages are listed in the **Schedule Exam** section of the **Exam Details** webpage. If the exam isn't available in your preferred language, you can request an additional 30 minutes to complete the exam.

Note

The bullets that follow each of the skills measured are intended to illustrate how we are assessing that skill. Related topics may be covered in the exam.

Note

Most questions cover features that are general availability (GA). The exam may contain questions on Preview features if those features are commonly used.

Skills measured as of May 2, 2023

Audience profile

Candidates for this exam should have subject matter expertise in planning, implementing, and managing Azure networking solutions, including core network infrastructure, hybrid connectivity, application delivery services, private access to Azure services, and network security.

Responsibilities for Azure network engineers include optimizing performance, resiliency, scale, and security of Azure networking solutions. These professionals deploy the solutions by using the Azure portal, the command line, and templates. They proactively monitor network environments to identify issues and minimize risk.

Azure network engineers work with solution architects, cloud administrators, security engineers, application developers, and DevOps engineers to deliver Azure solutions. They also assist Azure support engineers in resolving connectivity issues reported by customers.

Candidates for this exam should have experience creating and managing compute, storage, and networking resources in Azure. They should understand networking fundamentals, such as name resolution, network protocols, and network address management.

- Design and implement core networking infrastructure (20–25%)
- Design, implement, and manage connectivity services (20–25%)
- Design and implement application delivery services (20–25%)
- Design and implement private access to Azure services (15–20%)
- Secure network connectivity to Azure resources (15–20%)

Design and implement core networking infrastructure (20–25%)

Design and implement private IP addressing for Azure resources

- Plan and implement network segmentation and address spaces
- Create a virtual network (VNet)
- Plan and configure subnetting for services, including VNet gateways, private endpoints, firewalls, application gateways, VNet-integrated platform services, and Azure Bastion
- Plan and configure subnet delegation
- Create a prefix for public IP addresses
- Choose when to use a public IP address prefix
- Plan and implement a custom public IP address prefix (bring your own IP)
- Create a new public IP address
- Associate public IP addresses to resources

Design and implement name resolution

- Design name resolution inside a VNet
- Configure DNS settings for a VNet
- Design public DNS zones
- Design private DNS zones
- Configure a public or private DNS zone
- Link a private DNS zone to a VNet

Design and implement VNet connectivity and routing

- Design service chaining, including gateway transit
- Design virtual private network (VPN) connectivity between VNets
- Implement VNet peering
- Design and implement user-defined routes (UDRs)
- Associate a route table with a subnet
- Configure forced tunneling
- Diagnose and resolve routing issues
- Design and implement Azure Route Server

- Identify appropriate use cases for a Virtual Network NAT gateway
- Implement a NAT gateway

Monitor networks

- Configure monitoring, network diagnostics, and logs in Azure Network Watcher
- Monitor and repair network health by using Azure Network Watcher
- Activate and monitor distributed denial-of-service (DDoS) protection
- Activate and monitor Microsoft Defender for DNS

Design, implement, and manage connectivity services (20–25%)

Design, implement, and manage a site-to-site VPN connection

- Design a site-to-site VPN connection, including for high availability
- Select an appropriate VNet gateway SKU for site-to-site VPN requirements
- Implement a site-to-site VPN connection
- Identify when to use a policy-based VPN versus a route-based VPN connection
- Create and configure an IPsec/IKE policy
- Diagnose and resolve virtual network gateway connectivity issues
- Implement Azure Extended Network

Design, implement, and manage a point-to-site VPN connection

- Select an appropriate virtual network gateway SKU for point-to-site VPN requirements
- Select and configure a tunnel type
- Select an appropriate authentication method
- Configure RADIUS authentication
- Configure certificate-based authentication
- Configure authentication by using Azure Active Directory (Azure AD), part of Microsoft Entra
- Implement a VPN client configuration file
- Diagnose and resolve client-side and authentication issues
- Specify Azure requirements for Always On authentication
- Specify Azure requirements for Azure Network Adapter

Design, implement, and manage Azure ExpressRoute

- Select an ExpressRoute connectivity model
- Select an appropriate ExpressRoute SKU and tier
- Design and implement ExpressRoute to meet requirements, including cross-region connectivity, redundancy, and disaster recovery
- Design and implement ExpressRoute options, including Global Reach, FastPath, and ExpressRoute Direct
- Choose between private peering only, Microsoft peering only, or both
- Configure private peering

- Configure Microsoft peering
- Create and configure an ExpressRoute gateway
- Connect a virtual network to an ExpressRoute circuit
- Recommend a route advertisement configuration
- Configure encryption over ExpressRoute
- Implement Bidirectional Forwarding Detection
- Diagnose and resolve ExpressRoute connection issues

Design and implement an Azure Virtual WAN architecture

- Select a Virtual WAN SKU
- Design a Virtual WAN architecture, including selecting types and services
- Create a hub in Virtual WAN
- Choose an appropriate scale unit for each gateway type
- Deploy a gateway into a Virtual WAN hub
- Configure virtual hub routing
- Create a network virtual appliance (NVA) in a virtual hub
- Integrate a Virtual WAN hub with a third-party NVA

Design and implement application delivery services (20–25%)

Design and implement an Azure Load Balancer

- Map requirements to features and capabilities of Azure Load Balancer
- Identify appropriate use cases for Azure Load Balancer
- Choose an Azure Load Balancer SKU and tier
- Choose between public and internal
- Create and configure an Azure Load Balancer
- Implement a load balancing rule
- Create and configure inbound NAT rules
- Create and configure explicit outbound rules, including SNAT

Design and implement Azure Application Gateway

- Map requirements to features and capabilities of Azure Application Gateway
- Identify appropriate use cases for Azure Application Gateway
- Create a back-end pool
- Configure health probes
- Configure listeners
- Configure routing rules
- Configure HTTP settings
- Configure Transport Layer Security (TLS)
- Configure rewrite sets

Design and implement Azure Front Door

- Map requirements to features and capabilities of Azure Front Door
- Identify appropriate use cases for Azure Front Door
- Choose an appropriate tier
- Configure an Azure Front Door, including routing, origins, and endpoints
- Configure SSL termination and end-to-end SSL encryption
- Configure caching
- Configure traffic acceleration
- Implement rules, URL rewrite, and URL redirect
- Secure an origin by using Azure Private Link in Azure Front Door

Design and implement Azure Traffic Manager

- Identify appropriate use cases for Azure Traffic Manager
- Configure a routing method
- Configure endpoints

Design and implement private access to Azure services (15–20%)

Design and implement Azure Private Link service and Azure private endpoints

- Plan an Azure Private Link service
- Create a Private Link service
- Integrate a Private Link service with DNS
- Plan private endpoints
- Create private endpoints
- Configure access to Azure resources by using private endpoints
- Connect on-premises clients to a private endpoint
- Integrate a private endpoint with DNS

Design and implement service endpoints

- Choose when to use a service endpoint
- Create service endpoints
- Configure service endpoint policies
- Configure access to service endpoints

Secure network connectivity to Azure resources (15–20%)

Implement and manage network security groups

- Create a network security group (NSG)
- Associate an NSG to a resource
- Create an application security group (ASG)
- Associate an ASG to a network interface card (NIC)

- Create and configure NSG rules
- Interpret NSG flow logs
- Validate NSG flow rules
- Verify IP flow
- Configure an NSG for remote server administration, including Azure Bastion

Design and implement Azure Firewall and Azure Firewall Manager

- Map requirements to features and capabilities of Azure Firewall
- Select an appropriate Azure Firewall SKU
- Design an Azure Firewall deployment
- Create and implement an Azure Firewall deployment
- Configure Azure Firewall rules
- Create and implement Azure Firewall Manager policies
- Create a secure hub by deploying Azure Firewall inside an Azure Virtual WAN hub

Design and implement a Web Application Firewall (WAF) deployment

- Map requirements to features and capabilities of WAF
- Design a WAF deployment
- Configure detection or prevention mode
- Configure rule sets for WAF on Azure Front Door
- Configure rule sets for WAF on Application Gateway
- Implement a WAF policy
- Associate a WAF policy

Study resources

We recommend that you train and get hands-on experience before you take the exam. We offer self-study options and classroom training as well as links to documentation, community sites, and videos.

Study resources	Links to learning and documentation
Get trained	Choose from self-paced learning paths and modules or take an instructor-led course
Find documentation	Azure documentation Virtual Private Networking (VPN) Azure Active Directory (AD) RADIUS authentication with Azure Active Directory Azure ExpressRoute Overview

Study resources	Links to learning and documentation
	Create virtual network (VNet) DNS Zones and Records overview - Azure DNS Azure Virtual WAN Overview Azure Route Server documentation Load Balancer Azure Application Gateway documentation Azure Front Door and CDN Documentation Azure Traffic Manager Azure Virtual Network NAT Documentation Azure Firewall documentation Web Application Firewall documentation Azure Monitor documentation What is Azure Private Link? Manage Azure Private Endpoints
Ask a question	Microsoft Q&A | Microsoft Docs
Get community support	Azure Community Support
Follow Microsoft Learn	Microsoft Learn - Microsoft Tech Community
Find a video	Exam Readiness Zone Azure Fridays Browse other Microsoft Learn shows

Change log

Key to understanding the table: The topic groups (also known as functional groups) are in bold typeface followed by the objectives within each group. The table is a comparison between the two versions of the exam skills measured and the third column describes the extent of the changes.

Skill area prior to May 2, 2023	Skill area as of May 2, 2023	Changes
Audience profile		No change
Design and implement core networking infrastructure	**Design and implement core networking infrastructure**	No change
Design and implement private IP addressing for Azure resources	Design and implement private IP addressing for Azure resources	No change
Design and implement name resolution	Design and implement name resolution	Minor
Design and implement VNet connectivity and routing	Design and implement VNet connectivity and routing	No change
Monitor networks	Monitor networks	No change
Design, implement, and manage connectivity services	**Design, implement, and manage connectivity services**	No change
Design, implement, and manage a site-to-site VPN connection	Design, implement, and manage a site-to-site VPN connection	No change
Design, implement, and manage a point-to-site VPN connection	Design, implement, and manage a point-to-site VPN connection	No change
Design, implement, and manage Azure ExpressRoute	Design, implement, and manage Azure ExpressRoute	No change
Design and implement Azure Virtual WAN architecture	Design and implement Azure Virtual WAN architecture	Minor
Design and implement application delivery services	**Design and implement application delivery services**	No change
Design and implement an Azure Load Balancer	Design and implement an Azure Load Balancer	No change
Design and implement Azure Application Gateway	Design and implement Azure Application Gateway	No change
Design and implement Azure Front Door	Design and implement Azure Front Door	No change

Skill area prior to May 2, 2023	Skill area as of May 2, 2023	Changes
Design and implement Azure Traffic Manager	Design and implement Azure Traffic Manager	No change
Design and implement private access to Azure services	**Design and implement private access to Azure services**	No change
Design and implement Azure Private Link service and Azure private endpoints	Design and implement Azure Private Link service and Azure private endpoints	No change
Design and implement service endpoints	Design and implement service endpoints	No change
Secure network connectivity to Azure resources	**Secure network connectivity to Azure resources**	No change
Implement and manage network security groups (NSGs)	Implement and manage network security groups (NSGs)	No change
Design and implement Azure Firewall and Azure Firewall Manager	Design and implement Azure Firewall and Azure Firewall Manager	No change
Design and implement a Web Application Firewall (WAF) deployment	Design and implement a Web Application Firewall (WAF) deployment	No change

Skills measured prior to May 2, 2023

Audience profile

Candidates for this exam should have subject matter expertise in planning, implementing, and managing Azure networking solutions, including core network infrastructure, hybrid connectivity, application delivery services, private access to Azure services, and network security.

Responsibilities for Azure network engineers include optimizing performance, resiliency, scale, and security of Azure networking solutions. These professionals deploy the solutions by using the Azure portal, the command line, and templates. They proactively monitor network environments to identify issues and minimize risk.

Azure network engineers work with solution architects, cloud administrators, security engineers, application developers, and DevOps engineers to deliver Azure solutions. They also assist Azure support engineers in resolving connectivity issues reported by customers.

Candidates for this exam should have experience creating and managing compute, storage, and networking resources in Azure. They should understand networking fundamentals, such as name resolution, network protocols, and network address management.

- Design and implement core networking infrastructure (20–25%)
- Design, implement, and manage connectivity services (20–25%)

- Design and implement application delivery services (20–25%)
- Design and implement private access to Azure services (5–10%)
- Secure network connectivity to Azure resources (15–20%)

Design and implement core networking infrastructure (20–25%)

Design and implement private IP addressing for Azure resources

- Plan and implement network segmentation and address spaces
- Create a virtual network (VNet)
- Plan and configure subnetting for services, including VNet gateways, private endpoints, firewalls, application gateways, VNet-integrated platform services, and Azure Bastion
- Plan and configure subnet delegation
- Create a prefix for public IP addresses
- Choose when to use a public IP address prefix
- Plan and implement a custom public IP address prefix (bring your own IP)
- Create a new public IP address
- Associate public IP addresses to resources

Design and implement name resolution

- Design name resolution inside a VNet
- Configure DNS settings inside a VNet
- Design public DNS zones
- Design private DNS zones
- Configure a public or private DNS zone
- Link a private DNS zone to a VNet

Design and implement VNet connectivity and routing

- Design service chaining, including gateway transit
- Design virtual private network (VPN) connectivity between VNets
- Implement VNet peering
- Design and implement user-defined routes (UDRs)
- Associate a route table with a subnet
- Configure forced tunneling
- Diagnose and resolve routing issues
- Design and implement Azure Route Server
- Identify appropriate use cases for a Virtual Network NAT gateway
- Implement a NAT gateway

Monitor networks

- Configure monitoring, network diagnostics, and logs in Azure Network Watcher
- Monitor and repair network health by using Azure Network Watcher

- Activate and monitor distributed denial-of-service (DDoS) protection
- Activate and monitor Microsoft Defender for DNS

Design, implement, and manage connectivity services (20–25%)

Design, implement, and manage a site-to-site VPN connection

- Design a site-to-site VPN connection, including for high availability
- Select an appropriate VNet gateway SKU for site-to-site VPN requirements
- Implement a site-to-site VPN connection
- Identify when to use a policy-based VPN versus a route-based VPN connection
- Create and configure an IPsec/IKE policy
- Diagnose and resolve virtual network gateway connectivity issues
- Implement Azure Extended Network

Design, implement, and manage a point-to-site VPN connection

- Select an appropriate virtual network gateway SKU for point-to-site VPN requirements
- Select and configure a tunnel type
- Select an appropriate authentication method
- Configure RADIUS authentication
- Configure certificate-based authentication
- Configure authentication by using Azure Active Directory (Azure AD), part of Microsoft Entra
- Implement a VPN client configuration file
- Diagnose and resolve client-side and authentication issues
- Specify Azure requirements for Always On authentication
- Specify Azure requirements for Azure Network Adapter

Design, implement, and manage Azure ExpressRoute

- Select an ExpressRoute connectivity model
- Select an appropriate ExpressRoute SKU and tier
- Design and implement ExpressRoute to meet requirements, including cross-region connectivity, redundancy, and disaster recovery
- Design and implement ExpressRoute options, including Global Reach, FastPath, and ExpressRoute Direct
- Choose between private peering only, Microsoft peering only, or both
- Configure private peering
- Configure Microsoft peering
- Create and configure an ExpressRoute gateway
- Connect a virtual network to an ExpressRoute circuit
- Recommend a route advertisement configuration
- Configure encryption over ExpressRoute
- Implement Bidirectional Forwarding Detection

- Diagnose and resolve ExpressRoute connection issues

Design and implement an Azure Virtual WAN architecture

- Select a Virtual WAN SKU
- Design a Virtual WAN architecture, including selecting types and services
- Create a hub in Virtual WAN
- Choose an appropriate scale unit for each gateway type
- Deploy a gateway into a Virtual WAN hub
- Configure virtual hub routing
- Create a network virtual appliance (NVA) in a virtual hub
- Integrate a Virtual WAN hub with a third-party NVA

Design and implement application delivery services (20–25%)

Design and implement an Azure Load Balancer

- Map requirements to features and capabilities of Azure Load Balancer
- Identify appropriate use cases for Azure Load Balancer
- Choose an Azure Load Balancer SKU and tier
- Choose between public and internal
- Create and configure an Azure Load Balancer
- Implement a load balancing rule
- Create and configure inbound NAT rules
- Create and configure explicit outbound rules, including SNAT

Design and implement Azure Application Gateway

- Map requirements to features and capabilities of Azure Application Gateway
- Identify appropriate use cases for Azure Application Gateway
- Create a back-end pool
- Configure health probes
- Configure listeners
- Configure routing rules
- Configure HTTP settings
- Configure Transport Layer Security (TLS)
- Configure rewrite sets

Design and implement Azure Front Door

- Map requirements to features and capabilities of Azure Front Door
- Identify appropriate use cases for Azure Front Door
- Choose an appropriate tier
- Configure an Azure Front Door, including routing, origins, and endpoints
- Configure SSL termination and end-to-end SSL encryption

- Configure caching
- Configure traffic acceleration
- Implement rules, URL rewrite, and URL redirect
- Secure an origin by using Azure Private Link in Azure Front Door

Design and implement Azure Traffic Manager

- Identify appropriate use cases for Azure Traffic Manager
- Configure a routing method
- Configure endpoints

Design and implement private access to Azure services (5–10%)

Design and implement Azure Private Link service and Azure private endpoints

- Plan an Azure Private Link service
- Create a Private Link service
- Integrate a Private Link service with DNS
- Plan private endpoints
- Create private endpoints
- Configure access to Azure resources by using private endpoints
- Connect on-premises clients to a private endpoint
- Integrate a private endpoint with DNS

Design and implement service endpoints

- Choose when to use a service endpoint
- Create service endpoints
- Configure service endpoint policies
- Configure access to service endpoints

Secure network connectivity to Azure resources (15–20%)

Implement and manage network security groups

- Create a network security group (NSG)
- Associate an NSG to a resource
- Create an application security group (ASG)
- Associate an ASG to a network interface card (NIC)
- Create and configure NSG rules
- Interpret NSG flow logs
- Validate NSG flow rules
- Verify IP flow
- Configure an NSG for remote server administration, including Azure Bastion

Design and implement Azure Firewall and Azure Firewall Manager

- Map requirements to features and capabilities of Azure Firewall
- Select an appropriate Azure Firewall SKU
- Design an Azure Firewall deployment
- Create and implement an Azure Firewall deployment
- Configure Azure Firewall rules
- Create and implement Azure Firewall Manager policies
- Create a secure hub by deploying Azure Firewall inside an Azure Virtual WAN hub

Design and implement a Web Application Firewall (WAF) deployment

- Map requirements to features and capabilities of WAF
- Design a WAF deployment
- Configure detection or prevention mode
- Configure rule sets for WAF on Azure Front Door
- Configure rule sets for WAF on Application Gateway
- Implement a WAF policy
- Associate a WAF policy