


Course Name	AZ-500: Microsoft Certified: Azure Security Engineer Associate	
About the Course	This is a comprehensive training program to gain expertise in securing cloud environments and protecting digital assets. It validates skills in: implementing security controls, identifying and fixing vulnerabilities, managing identity and access, and protecting data	
Key Skills You Will Learn	Manage identity and access, Secure networking, Secure compute, storage, and databases, Manage security operations	
Course Pre-Requisite	You should have practical experience in administration of Microsoft Azure and hybrid environments, Basic understanding of security best practices and procedures, Strong familiarity with compute, network, and storage in Azure and Microsoft Entra ID.	
Target Audience	The target audience for the AZ-500 Microsoft Azure Security Technologies course is IT professionals who are looking to: Become Azure Security Engineers, Prepare for the Microsoft AZ-500 exam, Secure Azure environments, Understand Microsoft Azure Security Technologies, Protect an organization's data, Specialize in providing security for Azure-based digital platforms	
Job prospects with this role	Cloud Security administrator, security engineer, senior security analyst, and cybersecurity consultant	
Course Duration	~ 32 Hrs	
Course Customisation	Not applicable	
Certification	READYBELL AZ-500: Microsoft Certified: Azure Security Engineer Associate Certificate	
Mode of Training	Instructor-led 100% Online or 100% Classroom (Salt Lake, Kolkata - India) or hybrid mode (Online + Classroom) as suitable for the learner	
Course Fees	Please contact us	
Refund Policy	Get a 3-hours free trial during which you can cancel at no penalty. After that, we don't give refunds	
Job Assistance	Will assist candidate in securing a suitable job	
Contact	READYBELL SOFTWARE SERVICES PVT. LIMITED AH 12, SALT LAKE SECTOR 2, KOLKATA (INDIA) - 700 091 E-MAIL: contact@readybellssoftware.com PH: +91 - 9147708045/9674552097, +91 - 33-79642872	 Software Services Pvt. Ltd.

CURRICULUM		
Topic	Sub-Topic	Duration (Hrs)
AZ-500: Microsoft Certified: Azure Security Engineer Associate	AZ-500: Manage identity and access	32 Hrs
	Module 1: Manage identities in Microsoft Entra ID	
	Introduction	
	What is Microsoft Entra ID?	
	Secure Microsoft Entra users	
	Create a new user in Microsoft Entra ID	
	Secure Microsoft Entra groups	
	Recommend when to use external identities	
	Secure external identities	
	Implement Microsoft Entra Identity protection	
	Module 2: Manage authentication by using Microsoft Entra ID	
	Introduction	
	Microsoft Entra connect	
	Microsoft Entra Cloud Sync	
	Authentication options	
	Password hash synchronization with Microsoft Entra ID	
	Microsoft Entra pass-through authentication	
	Federation with Microsoft Entra ID	
	What is Microsoft Entra authentication?	
	Implement multifactor authentication (MFA)	
	Passwordless authentication options for Microsoft Entra ID	
	Implement passwordless authentication	
	Implement password protection	
	Microsoft Entra ID single sign-on	
	Implement single sign-on (SSO)	
	Integrate single sign-on (SSO) and identity providers	
	Introduction to Microsoft Entra Verified ID	
	Configure Microsoft Entra Verified ID	
	Recommend and enforce modern authentication protocols	
	Module 3: Manage authorization by using Microsoft Entra ID	
	Introduction	
	Azure management groups	
Configure Azure role permissions for management groups, subscriptions, resource groups, and resources		
Azure role-based access control		
Azure built-in roles		

Assign Azure role permissions for management groups, subscriptions, resource groups, and resources
Microsoft Entra built-in roles
Assign built-in roles in Microsoft Entra ID
Microsoft Entra role-based access control
Create and assign a custom role in Microsoft Entra ID
Microsoft Entra Permissions Management
Implement and manage Microsoft Entra Permissions Management
Zero Trust security
Microsoft Entra Privileged Identity Management
Configure Privileged Identity Management
Microsoft Entra ID Governance
Entitlement management
Access reviews
Identity lifecycle management
Lifecycle workflows
Delegation and roles in entitlement management
Configure role management and access reviews by using Microsoft Entra ID Governance
Implement Conditional Access policies
Module 4: Manage application access in Microsoft Entra ID
Introduction
Manage access to enterprise applications in Microsoft Entra ID, including OAuth permission grants
Manage app registrations in Microsoft Entra ID
Configure app registration permission scopes
Manage app registration permission consent
Manage and use service principals
Manage managed identities for Azure resources
Recommend when to use and configure a Microsoft Entra Application Proxy, including authentication
AZ-500: Secure networking
Module 5: Plan and implement security for virtual networks
Introduction
What is an Azure Virtual Network
Plan and implement Network Security Groups (NSGs) and Application Security Groups (ASGs)
Plan and implement User-Defined Routes (UDRs)
Plan and implement Virtual Network peering or gateway
Plan and implement Virtual Wide Area Network, including secured virtual hub

Secure VPN connectivity, including point-to-site and site-to-site	
Azure ExpressRoute	
Implement encryption over ExpressRoute	
Configure firewall settings on PaaS resources	
Monitor network security by using Network Watcher, including network security groups	
Module 6: Plan and implement security for private access to Azure resources	
Introduction	
Plan and implement virtual network Service Endpoints	
Plan and implement Private Endpoints	
Plan and implement Private Link services	
Plan and implement network integration for Azure App Service and Azure Functions	
Plan and implement network security configurations for an App Service Environment (ASE)	
Plan and implement network security configurations for an Azure SQL Managed Instance	
Module 7: Plan and implement security for public access to Azure resources	
Introduction	
Plan and implement Transport Layer Security (TLS) to applications, including Azure App Service and API Management	
Plan, implement, and manage an Azure Firewall, Azure Firewall Manager and firewall policies	
Plan and implement an Azure Application Gateway	
Plan and implement a Web Application Firewall (WAF)	
Plan and implement an Azure Front Door, including Content Delivery Network (CDN)	
Recommend when to use Azure DDoS Protection Standard	
AZ-500: Secure compute, storage, and databases	
Module 8: Plan and implement advanced security for compute	
Introduction	
Plan and implement remote access to public endpoints, Azure Bastion and just-in-time (JIT) virtual machine (VM) access	
What is Azure Kubernetes Service?	
Configure network isolation for Azure Kubernetes Service (AKS)	
Secure and monitor Azure Kubernetes Service	
Configure authentication for Azure Kubernetes Service	
Configure security for Azure Container Instances (ACIs)	
Configure security for Azure Container Apps (ACAs)	

Manage access to Azure Container Registry (ACR)
Configure disk encryption, Azure Disk Encryption (ADE), encryption as host, and confidential disk encryption
Recommend security configurations for Azure API Management
Module 9: Plan and implement security for storage
Introduction
Azure Storage
Configure access control for storage accounts
Manage life cycle for storage account access keys
Select and configure an appropriate method for access to Azure Files
Select and configure an appropriate method for access to Azure Blobs
Select and configure an appropriate method for access to Azure Tables
Select and configure an appropriate method for access to Azure Queues
Select and configure appropriate methods for protecting against data security threats, including soft delete, backups, versioning, and immutable storage
Configure Bring your own key (BYOK)
Enable double encryption at the Azure Storage infrastructure level
Module 10: Plan and implement security for Azure SQL Database and Azure SQL Managed Instance
Introduction
Azure SQL Database and SQL Managed Instance security
Enable database authentication by using Microsoft Entra ID
Enable and monitor database audit
Identify use cases for the Microsoft Purview governance portal
Implement data classification of sensitive information by using the Microsoft Purview governance portal
Plan and implement dynamic mask
Implement transparent data encryption
Recommend when to use Azure SQL Database Always Encrypted
AZ-500: Manage security operations
Module 11: Plan, implement, and manage governance for security
Introduction
Azure governance
Create, assign, and interpret security policies and initiatives in Azure Policy
Configure security settings by using Azure Blueprint
Deploy secure infrastructures by using a landing zone
Azure Key Vault
Azure Key Vault security
Azure Key Vault authentication
Create and configure an Azure Key Vault

	Recommend when to use a dedicated Hardware Security Module (HSM)	
	Configure access to Key Vault, including vault access policies and Azure Role Based Access Control	
	Manage certificates, secrets, and keys	
	Configure key rotation	
	Configure backup and recovery of certificates, secrets, and keys	
	Module 12: Manage security posture by using Microsoft Defender for Cloud	
	Introduction	
	Implement Microsoft Defender for Cloud	
	Identify and remediate security risks by using the Microsoft Defender for Cloud Secure Score and Inventory	
	Assess compliance against security frameworks and Microsoft Defender for Cloud	
	Add industry and regulatory standards to Microsoft Defender for Cloud	
	Add custom initiatives to Microsoft Defender for Cloud	
	Connect hybrid cloud and multicloud environments to Microsoft Defender for Cloud	
	Identify and monitor external assets by using Microsoft Defender External Attack Surface Management	
	Module 13: Configure and manage threat protection by using Microsoft Defender for Cloud	
	Introduction	
	Enable workload protection services in Microsoft Defender for Cloud	
	Configure Microsoft Defender for Servers	
	Configure Microsoft Defender for Azure SQL Database	
	Container security in Microsoft Defender for Containers	
	Managed Kubernetes threat factors	
	Defender for Containers architecture	
	Configure Microsoft Defender for Containers components	
	Vulnerability assessments for Azure	
	Defender for Storage	
	Malware scanning in Defender for Storage	
	Detect threats to sensitive data	
	Deploy Microsoft Defender for Storage	
	Enable configure Azure built-in policy	
	Microsoft Defender for Cloud DevOps Security	
	DevOps Security support and prerequisites	
	DevOps environment security posture	
	Connect your GitHub lab environment to Microsoft Defender for Cloud	
	Configure the Microsoft Security DevOps GitHub action	

	Manage and respond to security alerts in Microsoft Defender for Cloud	
	Configure workflow automation by using Microsoft Defender for Cloud	
	Evaluate vulnerability scans from Microsoft Defender for Server	
	Module 14: Configure and manage security monitoring and automation solutions	
	Introduction	
	Monitor security events by using Azure Monitor	
	Configure data connectors in Microsoft Sentinel	
	Create and customize analytics rules in Microsoft Sentinel	
	Evaluate alerts and incidents from Microsoft Sentinel	
	Configure automation in Microsoft Sentinel	
To register for this course please e-mail/call us		