

# **Cybersecurity Azure Security Engineer Associate Exam**



**Tech Foundation Group Meeting**

---

**Presenter: Razi Rais**

<https://www.linkedin.com/in/razirais>

# Tech Foundation | User Group

---



## Tech Foundation

📍 New York, NY

👤 785 members · Public group ?

👤 Organized by Razi

<https://www.meetup.com/techfoundation>

Share: [f](#) [t](#) [in](#)

About

Events

Members

Photos

Discussions

More

Join this group

...

# Who Am I?

---

- ✓ 16 Years in Software Industry
  - ✓ Author, Speaker, Trainer, Software Engineer, Architect, Technical Program Manager
- ✓ Currently work at Microsoft
- ✓ MCT: Microsoft Certified Trainer
- ✓ LinkedIn: <https://www.linkedin.com/in/razirais>
- ✓ Web: <https://razibinrais.com>
- ✓ Git: <https://github.com/razi-raais>

# Agenda

---

- ✓ Overview of AZ-500 Exam Objectives
- ✓ Career Path
- ✓ Exam Preparation
- ✓ Training Resources
- ✓ Q&A
- ✓ *NOTE: Session content will be shared after the event.*

# About AZ-500 Exam

---

- Microsoft Certification Program Blog:
  - <https://techcommunity.microsoft.com/t5/microsoft-learn-blog/bg-p/MicrosoftLearnBlog>
- Exam Details: <https://docs.microsoft.com/en-us/learn/certifications/exams/az-500>
- IT Pro/Ops
- Technical Exam
- More Breadth than Depth

<https://docs.microsoft.com/en-us/learn/certifications/exams/az-500>

# AZ-500 Exam Objectives

---

- Manage identity and access (30-35%)
- Implement platform protection (15-20%)
- Manage security operations (25-30%)
- Secure data and applications (20-25%)

NOTE: Exam objectives were updated by Microsoft on July 29, 2020 by :

<https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE3VC70>

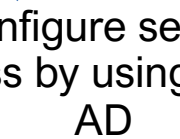
Manage identity and access (30-35%)

# Manage identity and access


---



Manage Azure Active  
Directory identities



Configure secure  
access by using Azure  
AD



Manage application  
access



Manage access control



# Manage Azure Active Directory identities

---

- Configure security for service principals | <https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal>
- Manage Azure AD directory groups | <https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-groups-create-azure-portal>
- Manage Azure AD users | <https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/add-users-azure-active-directory>
- Configure password writeback | <https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-sspr-writeback>
- Configure authentication methods including password hash and Pass Through Authentication (PTA), OAuth, and passwordless (not ADFS) | <https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn>
- Transfer Azure subscriptions between Azure AD tenants | <https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-how-subscriptions-associated-directory>

# Configure secure access by using Azure AD

---

- Monitor privileged access for Azure AD Privileged Identity Management (PIM) | <https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/azure-ad-pim-approval-workflow>
- Configure Access Reviews | <https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-start-security-review> , <https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-resource-roles-start-access-review>
- Activate and configure PIM | <https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-security-wizard>
- Implement Conditional Access policies including Multi-Factor Authentication (MFA) | <https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-policies> , <https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-azure-management>
- Configure Azure AD identity protection| <https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-policies>

# Manage application access

---

- Create App Registration | <https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app>
- Configure App Registration permission scopes | <https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-configure-app-expose-web-apis>
- Manage App Registration permission consent | <https://docs.microsoft.com/en-us/azure/active-directory/develop/v2-permissions-and-consent>
- Manage API access to Azure subscriptions and resources | <https://docs.microsoft.com/en-us/azure/api-management/api-management-subscriptions>

# Manage access control

---

- Configure subscription and resource permissions | <https://docs.microsoft.com/en-us/azure/cost-management-billing/manage/create-subscription>
- Configure resource group permissions | <https://docs.microsoft.com/en-us/azure/role-based-access-control/overview>
- Configure custom RBAC roles | <https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/roles-create-custom>
- Identify the appropriate role | <https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-assign-admin-roles>
- Apply principle of least privilege | <https://docs.microsoft.com/en-us/azure/azure-australia/role-privileged> , <https://docs.microsoft.com/en-us/azure/security/fundamentals/identity-management-best-practices>
- Interpret permissions
- Check access | <https://docs.microsoft.com/en-us/azure/role-based-access-control/check-access>

Implement platform protection (15-20%)

# Manage identity and access

---

Implement advanced network security



Configure advanced security for compute



# Manage access control

---

- Secure the connectivity of virtual networks (VPN authentication, Express Route encryption) | <https://docs.microsoft.com/en-us/azure/virtual-wan/virtual-wan-about>
- Configure Network Security Groups (NSGs) and Application Security Groups (ASGs) | <https://docs.microsoft.com/en-us/azure/virtual-network/security-overview> , <https://docs.microsoft.com/en-us/azure/virtual-network/application-security-groups>
- Create and configure Azure Firewall | <https://docs.microsoft.com/en-us/azure/firewall/tutorial-firewall-deploy-portal> , <https://docs.microsoft.com/en-us/azure/firewall/deploy-ps> , <https://docs.microsoft.com/en-us/azure/firewall/tutorial-hybrid-portal>
- Configure Azure Front Door service as an Application Gateway | <https://docs.microsoft.com/en-us/azure/frontdoor/front-door-faq>, <https://docs.microsoft.com/en-us/azure/frontdoor/front-door-lb-with-azure-app-delivery-suite>

# Manage access control (Cont.)

---

- Configure a Web Application Firewall (WAF) on Azure Application Gateway | <https://docs.microsoft.com/en-us/azure/web-application-firewall/ag/ag-overview>
- Configure Azure Bastion | <https://docs.microsoft.com/en-us/azure/bastion/bastion-create-host-portal>
- Configure a firewall on a storage account, Azure SQL, KeyVault, or App Service | <https://docs.microsoft.com/en-us/azure/key-vault/general/network-security>
- Implement DDoS | <https://docs.microsoft.com/en-us/azure/virtual-network/ddos-protection-overview>



# Configure advanced security for compute

---

- Configure endpoint protection | <https://docs.microsoft.com/en-us/azure/security-center/security-center-endpoint-protection>
- Configure and monitor system updates for VMs <https://docs.microsoft.com/en-us/azure/automation/automation-tutorial-update-management>
- Configure authentication for Azure Container Registry | <https://docs.microsoft.com/en-us/azure/container-registry/container-registry-authentication>
- Configure security for different types of containers | <https://docs.microsoft.com/en-us/azure/security-center/container-security>
- Implement vulnerability management | <https://docs.microsoft.com/en-us/azure/security/benchmarks/security-control-vulnerability-management>
- Configure isolation for AKS: <https://docs.microsoft.com/en-us/azure/aks/operator-best-practices-cluster-isolation>

# Configure advanced security for compute (Cont.)

---

- Configure security for container registry | <https://docs.microsoft.com/en-us/azure/security-center/azure-container-registry-integration> , <https://docs.microsoft.com/en-us/azure/container-registry/security-baseline>
- Implement Azure Disk Encryption: <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-overview>, <https://docs.microsoft.com/en-us/azure/virtual-machines/linux/disk-encryption-overview>
- Configure authentication and security for Azure App Service | <https://docs.microsoft.com/en-us/azure/app-service/overview-authentication-authorization>
- Configure SSL/TLS certs | <https://docs.microsoft.com/en-us/azure/app-service/configure-ssl-certificate>
- Configure authentication
- Configure automatic updates | <https://docs.microsoft.com/en-us/azure/automation/automation-tutorial-update-management>

Manage security operations (25-30%)

# Manage security operations

---



Monitor security  
by using Azure  
Monitor

Monitor security  
by using Azure  
Security Center

Monitor security  
by using Azure  
Sentinel

Configure security  
policies

# Monitor security by using Azure Monitor

---

- Create and customize alerts | <https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-log>
- Monitor security logs by using Azure Monitor | <https://docs.microsoft.com/en-us/azure/security/fundamentals/log-audit>
- Configure diagnostic logging and log retention| <https://docs.microsoft.com/en-us/azure/azure-monitor/platform/platform-logs-overview>

# Monitor security by using Azure Security Center

---

- Evaluate vulnerability scans from Azure Security Center | <https://docs.microsoft.com/en-us/azure/security-center/built-in-vulnerability-assessment>
- Configure Just in Time VM access by using Azure Security Center | <https://docs.microsoft.com/en-us/azure/security-center/security-center-just-in-time?tabs=jit-config-asc%2Cjit-request-asc>
- Configure centralized policy management by using Azure Security Center | <https://docs.microsoft.com/en-us/azure/security-center/tutorial-security-policy>, <https://docs.microsoft.com/en-us/azure/security-center/security-center-policy-definitions>
- Configure compliance policies and evaluate for compliance by using Azure Security Center | <https://docs.microsoft.com/en-us/azure/security-center/security-center-compliance-dashboard>, <https://docs.microsoft.com/en-us/azure/security-center/custom-security-policies>

# Monitor security by using Azure Sentinel

---

- Create and customize alerts | <https://docs.microsoft.com/en-us/azure/sentinel/create-incidents-from-alerts>
- Configure data sources to Azure Sentinel | <https://docs.microsoft.com/en-us/azure/sentinel/connect-data-sources>
- Evaluate results from Azure Sentinel | <https://docs.microsoft.com/en-us/azure/sentinel/quickstart-get-visibility>
- Configure a playbook for a security event by using Azure Sentinel | <https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook>

# Configure security policies

---

- Configure security settings by using Azure Policy | <https://docs.microsoft.com/en-us/azure/governance/policy/overview> , <https://docs.microsoft.com/en-us/azure/governance/policy/tutorials/create-and-manage>, <https://docs.microsoft.com/en-us/azure/security-center/configure-security-policy-azure-policy>
- Configure security settings by using Azure Blueprint | <https://docs.microsoft.com/en-us/azure/governance/blueprints/overview>, <https://docs.microsoft.com/en-us/azure/governance/blueprints/create-blueprint-portal>



Secure data and applications (20-25%)

# Manage security operations

---

Configure security for storage



Configure security for databases



Configure Security for Key Vault



# Configure access control for storage accounts

---

- Configure access control for storage accounts | <https://docs.microsoft.com/en-us/azure/storage/common/storage-auth>
- Configure key management for storage accounts | <https://docs.microsoft.com/en-us/azure/storage/common/storage-account-keys-manage?tabs=azure-portal>
- Configure Azure AD authentication for Azure Storage | <https://docs.microsoft.com/en-us/azure/storage/common/storage-auth-aad>
- Configure Azure AD Domain Services authentication for Azure Files | <https://docs.microsoft.com/en-us/azure/storage/files/storage-files-identity-auth-active-directory-domain-service-enable>

# Monitor security by using Azure Monitor

---

- Create and manage Shared Access Signatures (SAS) | <https://docs.microsoft.com/en-us/azure/storage/common/storage-sas-overview>
- Create a shared access policy for a blob or blob container | <https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-service-sas-create-dotnet>
- Configure Storage Service Encryption | <https://docs.microsoft.com/en-us/azure/storage/common/storage-service-encryption>

# Configure security for databases

---

- Enable database authentication | <https://docs.microsoft.com/en-us/azure/azure-sql/database/authentication-aad-overview>, <https://docs.microsoft.com/en-us/azure/azure-sql/database/security-overview>, <https://docs.microsoft.com/en-us/azure/azure-sql/database/logins-create-manage>
- Enable database auditing | <https://docs.microsoft.com/en-us/azure/azure-sql/database/auditing-overview>
- Configure Azure SQL Database Advanced Threat Protection | <https://docs.microsoft.com/en-us/azure/azure-sql/database/threat-detection-configure>
- Implement database encryption | <https://docs.microsoft.com/en-us/azure/security/fundamentals/encryption-atrest#azure-sql-database>, <https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/transparent-data-encryption?redirectedfrom=MSDN&view=sql-server-ver15>
- Implement Azure SQL Database Always Encrypted | <https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/always-encrypted-database-engine?view=sql-server-ver15>

# Configure and manage Key Vault

---

- Configure and manage Key Vault | <https://docs.microsoft.com/en-us/azure/key-vault/general/overview-security>
- Manage access to Key Vault | <https://docs.microsoft.com/en-us/azure/key-vault/general/secure-your-key-vault>
- Manage permissions to secrets, certificates, and keys | <https://docs.microsoft.com/en-us/azure/key-vault/general/secure-your-key-vault>
- Configure RBAC usage in Azure Key Vault | <https://docs.microsoft.com/en-us/azure/key-vault/general/overview-security>
- Manage certificates | <https://docs.microsoft.com/en-us/azure/key-vault/certificates/certificate-scenarios>

# Configure and manage Key Vault (Cont)

---

- Manage secrets | <https://docs.microsoft.com/en-us/azure/key-vault/secrets/about-secrets>
- Configure key rotation | <https://docs.microsoft.com/en-us/azure/key-vault/secrets/tutorial-rotation>
- Backup and restore of Key Vault items | <https://docs.microsoft.com/en-us/powershell/module/azurerm.keyvault/backup-azurekeyvaultkey?view=azurerm-6.13.0> | <https://docs.microsoft.com/en-us/powershell/module/azurerm.keyvault/restore-azurekeyvaultkey?view=azurerm-6.13.0>

# Resources

---

- GitHub: <https://github.com/MicrosoftLearning/AZ500-AzureSecurityTechnologies> (Free)
- On-Demand Trainings:
  - <https://docs.microsoft.com/en-us/learn/certifications/exams/az-500?tab=tab-learning-paths> (Free)
  - <https://skillmeup.com/course/bypath/az-500-microsoft-azure-security-technologies> (Paid)
  - <https://learning.oreilly.com/videos/microsoft-az-500-certification/1018947655> (Paid)
  - <https://www.pluralsight.com/paths/microsoft-azure-security-engineer-az-500> (Paid)
- Live Training:
  - <https://docs.microsoft.com/en-us/learn/certifications/courses/az-500t00> (Paid)
- Private Training:
  - [contact@razibinrais.com](mailto:contact@razibinrais.com)





Thank You

---