**Manage identity and access (30-35%)**

**Manage Azure Active Directory (Azure AD) identities**

* Create and manage a managed identity for Azure resources
* [Managed identity best practice recommendations](https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/managed-identity-best-practice-recommendations?WT.mc_id=EM-MVP-4039827)
* [About managed identities for Azure resources](https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview?WT.mc_id=EM-MVP-4039827)
* Manage Azure AD groups
* [Create a dynamic group](https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-create-rule?WT.mc_id=EM-MVP-4039827)
* [PowerShell for Azure AD groups](https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-settings-v2-cmdlets?WT.mc_id=EM-MVP-4039827)
* Manage Azure AD users
* [Add or delete users using Azure Active Directory](https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/add-users-azure-active-directory?WT.mc_id=EM-MVP-4039827)
* Manage external identities by using Azure AD
* [Understand the B2B guest user](https://docs.microsoft.com/en-us/azure/active-directory/external-identities/user-properties)
* [How a B2B guest redeems an invitation](https://docs.microsoft.com/en-us/azure/active-directory/external-identities/redemption-experience)
* Manage administrative units
* [Administrative units](https://docs.microsoft.com/en-us/azure/active-directory/roles/administrative-units?WT.mc_id=ES-MVP-4039827)

**Manage secure access by using Azure AD**

* Configure Azure AD Privileged Identity Management (PIM)
* [Deploy Azure AD Privileged Identity Management (PIM)](https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-deployment-plan?WT.mc_id=EM-MVP-4039827)
* [Configure security alerts for Azure AD roles in Privileged Identity Management](https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-configure-security-alerts?WT.mc_id=EM-MVP-4039827)
* Implement Conditional Access policies, including multifactor authentication
* [Secure Azure Active Directory users with Multi-Factor Authentication](https://docs.microsoft.com/en-us/learn/modules/secure-aad-users-with-mfa/?WT.mc_id=EM-MVP-4039827)
* [Configure Azure Multi-Factor Authentication settings](https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings?WT.mc_id=EM-MVP-4039827)
* Implement Azure AD Identity Protection
* [What is Azure Active Directory Identity Protection?](https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection?WT.mc_id=EM-MVP-4039827)
* Implement passwordless authentication
* [Passwordless authentication options for Azure Active Directory](https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-passwordless?WT.mc_id=EM-MVP-4039827)
* Configure access reviews
* [Plan Access review deployment](https://docs.microsoft.com/en-us/azure/active-directory/governance/deploy-access-reviews?WT.mc_id=ES-MVP-4039827)
* [Create an access review of Azure AD roles in Privileged Identity Management](https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-start-security-review?WT.mc_id=EM-MVP-4039827)
* [Create an access review of an access package in Azure AD entitlement management](https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-access-reviews-create?WT.mc_id=ES-MVP-4039827)

**Manage application access**

* Integrate single sign-on (SSO) and identity providers for authentication
* [Build an app using Microsoft identities or social accounts](https://docs.microsoft.com/en-us/azure/active-directory/develop/v2-overview?WT.mc_id=EM-MVP-4039827)
* Create an app registration
* [QuickStart: Register an application with the Microsoft identity platform](https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app)
* Configure app registration permission scopes
* [Permissions and consent in the Microsoft identity platform endpoint](https://docs.microsoft.com/en-us/azure/active-directory/develop/v2-permissions-and-consent?WT.mc_id=EM-MVP-4039827)
* Manage app registration permission consent
* [Configure how end-users consent to applications](https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/configure-user-consent?WT.mc_id=EM-MVP-4039827)
* Manage API permissions to Azure subscriptions and resources
* [Get access on behalf of a user](https://docs.microsoft.com/en-us/graph/auth-v2-user?WT.mc_id=EM-MVP-4039827)
* [Authentication flows and application scenarios](https://docs.microsoft.com/en-us/azure/active-directory/develop/authentication-flows-app-scenarios?WT.mc_id=EM-MVP-4039827)
* Configure an authentication method for a service principal
* [Application and service principal objects in Azure Active Directory](https://docs.microsoft.com/en-us/azure/active-directory/develop/app-objects-and-service-principals?WT.mc_id=EM-MVP-4039827)

**Manage access control**

* Configure Azure role permissions for management groups, subscriptions, resource groups, and resources
* [Elevate access to manage all Azure subscriptions and management groups](https://docs.microsoft.com/en-us/azure/role-based-access-control/elevate-access-global-admin?WT.mc_id=AZ-MVP-4039827)
* [Add or change Azure subscription administrators](https://docs.microsoft.com/en-us/azure/cost-management-billing/manage/add-change-subscription-administrator?WT.mc_id=AZ-MVP-4039827)
* [What is Azure role-based access control (Azure RBAC)?](https://docs.microsoft.com/en-us/azure/role-based-access-control/overview)
* Interpret role and resource permissions
* [Quickstart: View the access a user has to Azure resources](https://docs.microsoft.com/en-us/azure/role-based-access-control/check-access?WT.mc_id=AZ-MVP-4039827)
* [List Azure role definitions](https://docs.microsoft.com/en-us/azure/role-based-access-control/role-definitions-list?WT.mc_id=AZ-MVP-4039827)
* [List Azure role assignments using the Azure portal](https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-list-portal?WT.mc_id=AZ-MVP-4039827)
* [Best practices for Azure RBAC](https://docs.microsoft.com/en-us/azure/role-based-access-control/best-practices)
* [Lock resources to prevent unexpected changes](https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources?WT.mc_id=AZ-MVP-4039827)
* Assign built-in Azure AD roles
* [Assign directory roles](https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-add-role-to-user?WT.mc_id=EM-MVP-4039827)
* [View roles assigned to a group](https://docs.microsoft.com/en-us/azure/active-directory/roles/groups-view-assignments?WT.mc_id=EM-MVP-4039827)
* Create and assign custom roles, including Azure roles and Azure AD roles
* [Create Custom Azure Roles](https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles?WT.mc_id=AZ-MVP-4039827)
* [Create custom Azure AD roles](https://docs.microsoft.com/en-us/azure/active-directory/roles/custom-create)

**Implement platform protection (15-20%)**

**Implement advanced network security**

* Secure the connectivity of hybrid networks
* [VPN Gateway design](https://docs.microsoft.com/en-us/azure/vpn-gateway/design?WT.mc_id=AZ-MVP-4039827)
* [ExpressRoute encryption](https://docs.microsoft.com/en-us/azure/expressroute/expressroute-about-encryption?WT.mc_id=AZ-MVP-4039827)
* [About Point-to-Site VPN](https://docs.microsoft.com/en-us/azure/vpn-gateway/point-to-site-about?WT.mc_id=AZ-MVP-4039827)
* [Create a Site-to-Site connection in the Azure portal](https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal?WT.mc_id=AZ-MVP-4039827)
* [Configure virtual network connectivity](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview?WT.mc_id=AZ-MVP-4039827)
* Secure the connectivity of virtual networks
* [Network security groups](https://docs.microsoft.com/en-us/azure/virtual-network/security-overview?WT.mc_id=AZ-MVP-4039827)
* [Create, change, or delete a network security group](https://docs.microsoft.com/en-us/azure/virtual-network/manage-network-security-group?WT.mc_id=AZ-MVP-4039827)
* [Tutorial: Filter network traffic with a network security group using the Azure portal](https://docs.microsoft.com/en-us/azure/virtual-network/tutorial-filter-network-traffic?WT.mc_id=AZ-MVP-4039827)
* [Bastion and VNet peering](https://docs.microsoft.com/en-us/azure/bastion/vnet-peering?WT.mc_id=AZ-MVP-4039827)
* [Quickstart: Connect to a virtual machine using a private IP address and Azure Bastion](https://docs.microsoft.com/en-us/azure/bastion/quickstart-host-portal?WT.mc_id=AZ-MVP-4039827)
* [Application security groups](https://docs.microsoft.com/en-us/azure/virtual-network/application-security-groups?WT.mc_id=AZ-MVP-4039827)
* Create and configure Azure Firewall
* [Tutorial: Deploy and configure Azure Firewall using the Azure portal](https://docs.microsoft.com/en-us/azure/firewall/tutorial-firewall-deploy-portal?WT.mc_id=AZ-MVP-4039827)
* [Tutorial: Deploy and configure Azure Firewall in a hybrid network using the Azure portal](https://docs.microsoft.com/en-us/azure/firewall/tutorial-hybrid-portal?WT.mc_id=AZ-MVP-4039827)
* Create and configure Azure Firewall Manager
* [Secure virtual hub – ARM template](https://docs.microsoft.com/en-us/azure/firewall-manager/quick-secure-virtual-hub?WT.mc_id=AZ-MVP-4039827)
* [General deployment process](https://docs.microsoft.com/en-us/azure/firewall-manager/deployment-overview?WT.mc_id=AZ-MVP-4039827)
* Create and configure Azure Application Gateway
* [Encrypt network traffic end to end with Azure Application Gateway](https://docs.microsoft.com/en-us/learn/modules/end-to-end-encryption-with-app-gateway/?WT.mc_id=AZ-MVP-4039827)
* Create and configure Azure Front Door
* [Quickstart: Create a Front Door for a highly available global web application](https://docs.microsoft.com/en-us/azure/frontdoor/quickstart-create-front-door?WT.mc_id=AZ-MVP-4039827)
* Create and configure Web Application Firewall (WAF)
* [Azure Web Application Firewall on Azure Application Gateway](https://docs.microsoft.com/en-us/azure/web-application-firewall/ag/ag-overview?WT.mc_id=AZ-MVP-4039827)
* Configure a resource firewall, including storage account, Azure SQL, Azure Key Vault, or Azure App Service
* [Security in Azure App Service](https://docs.microsoft.com/en-us/azure/app-service/overview-security?WT.mc_id=AZ-MVP-4039827)
* [Azure SQL Database and Azure Synapse IP firewall rules](https://docs.microsoft.com/en-us/azure/azure-sql/database/firewall-configure?WT.mc_id=AZ-MVP-4039827)
* [Configure Azure Storage firewalls and virtual networks](https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security?WT.mc_id=AZ-MVP-4039827)
* [Access Azure Key Vault behind a firewall](https://docs.microsoft.com/en-us/azure/key-vault/general/access-behind-firewall?WT.mc_id=AZ-MVP-4039827)
* Configure network isolation for Web Apps and Azure Functions
* [Security in Azure App Service](https://docs.microsoft.com/en-us/azure/app-service/overview-security?WT.mc_id=AZ-MVP-4039827)
* Implement Azure Service Endpoints
* [Virtual Network service endpoints](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoints-overview?WT.mc_id=AZ-MVP-4039827?WT.mc_id=AZ-MVP-4039827)
* [Tutorial: Restrict network access to PaaS resources with virtual network service endpoints using the Azure portal](https://docs.microsoft.com/en-us/azure/virtual-network/tutorial-restrict-network-access-to-resources?WT.mc_id=AZ-MVP-4039827?WT.mc_id=AZ-MVP-4039827)
* [Create, change, or delete service endpoint policy using the Azure portal](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoint-policies-portal?WT.mc_id=AZ-MVP-4039827)
* Implement Azure Private Endpoints, including integrating with other services
* [Quickstart: Create a Private Endpoint using Azure portal](https://github.com/gvnshtn/ExamGuides/blob/main)
* [Use private endpoints for Azure Storage](https://github.com/gvnshtn/ExamGuides/blob/main)
* Implement Azure Private Links
* [What is Azure Private Link?](https://docs.microsoft.com/en-us/azure/private-link/create-private-endpoint-portal?WT.mc_id=AZ-MVP-4039827)
* [Use portal to create private link for managing Azure resources](https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/create-private-link-access-portal?WT.mc_id=EM-MVP-4039827)
* Implement Azure DDoS Protection
* [Azure DDoS Protection Standard overview](https://docs.microsoft.com/en-us/azure/virtual-network/ddos-protection-overview?WT.mc_id=AZ-MVP-4039827)

**Configure advanced security for compute**

* Configure Azure Endpoint Protection for virtual machines (VMs)
* [Endpoint protection assessment and recommendations](https://docs.microsoft.com/en-us/azure/security-center/security-center-endpoint-protection?WT.mc_id=AZ-MVP-4039827)
* [Feature coverage for machines](https://docs.microsoft.com/en-us/azure/security-center/security-center-services?tabs=features-windows#supported-endpoint-protection-solutions-?WT.mc_id=AZ-MVP-4039827)
* [Security management in Azure](https://docs.microsoft.com/en-us/azure/security/fundamentals/management?WT.mc_id=AZ-MVP-4039827)
* [Microsoft Antimalware for Azure Cloud Services and Virtual Machines](https://docs.microsoft.com/en-us/azure/security/fundamentals/antimalware?WT.mc_id=AZ-MVP-4039827)
* Implement and manage security updates for VMs
* [Manage updates and patches for your Azure VMs](https://docs.microsoft.com/en-us/azure/automation/automation-tutorial-update-management?WT.mc_id=AZ-MVP-4039827)
* [Manage updates for multiple VMs](https://docs.microsoft.com/en-us/azure/automation/manage-update-multi?WT.mc_id=AZ-MVP-4039827)
* [Keep your virtual machines updated](https://docs.microsoft.com/en-us/learn/modules/keep-your-virtual-machines-updated/?WT.mc_id=AZ-MVP-4039827)
* Security best practices for IaaS workloads in Azure](<https://docs.microsoft.com/en-us/azure/security/fundamentals/iaas?WT.mc_id=AZ-MVP-4039827>)
* [Vulnerability assessments for your Azure Virtual Machines](https://docs.microsoft.com/en-us/azure/security-center/security-center-vulnerability-assessment-recommendations?WT.mc_id=AZ-MVP-4039827)
* [Integrated vulnerability scanner for virtual machines](https://docs.microsoft.com/en-us/azure/security-center/built-in-vulnerability-assessment?WT.mc_id=AZ-MVP-4039827)
* Configure security for container services
* [Container Security in Azure](https://azure.microsoft.com/mediahandler/files/resourcefiles/container-security-in-microsoft-azure/Open%20Container%20Security%20in%20Microsoft%20Azure.pdf?WT.mc_id=AZ-MVP-4039827)
* [How to use managed identities with Azure Container Instances](https://docs.microsoft.com/en-us/azure/container-instances/container-instances-managed-identity?WT.mc_id=AZ-MVP-4039827)
* [Security concepts for applications and clusters in Azure Kubernetes Service (AKS)](https://docs.microsoft.com/en-us/azure/aks/concepts-security?WT.mc_id=AZ-MVP-4039827)
* [Best practices for cluster isolation in Azure Kubernetes Service (AKS)](https://docs.microsoft.com/en-us/azure/aks/operator-best-practices-cluster-isolation?WT.mc_id=AZ-MVP-4039827)
* [Update containers in Azure Container Instances](https://docs.microsoft.com/en-us/azure/container-instances/container-instances-update?WT.mc_id=AZ-MVP-4039827)
* [Service principals with Azure Kubernetes Service (AKS)](https://docs.microsoft.com/en-us/azure/aks/kubernetes-service-principal?WT.mc_id=AZ-MVP-4039827)
* [Integrate Azure Active Directory with Azure Kubernetes Service](https://docs.microsoft.com/en-us/azure/aks/azure-ad-integration)
* [Use managed identities in Azure Kubernetes Service](https://docs.microsoft.com/en-us/azure/aks/use-managed-identity?WT.mc_id=AZ-MVP-4039827)
* Manage access to Azure Container Registry
* [Authenticate with an Azure container registry](https://docs.microsoft.com/en-us/azure/container-registry/container-registry-authentication?WT.mc_id=AZ-MVP-4039827)
* Configure security for serverless compute
* [Serverless Functions app security](https://docs.microsoft.com/en-us/azure/architecture/serverless-quest/functions-app-security?WT.mc_id=EM-MVP-4039827)
* Configure security for an Azure App Service
* [Authentication and authorization in Azure App Service and Azure Functions](https://docs.microsoft.com/en-us/azure/app-service/overview-authentication-authorization?WT.mc_id=AZ-MVP-4039827)
* [OS and runtime patching in Azure App Service](https://docs.microsoft.com/en-us/azure/app-service/overview-patch-os-runtime?WT.mc_id=AZ-MVP-4039827)
* Configure encryption at rest
* [Azure Disk Encryption for Windows VMs](https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-overview?WT.mc_id=AZ-MVP-4039827)
* [Azure Storage encryption for data at rest](https://docs.microsoft.com/en-us/azure/storage/common/storage-service-encryption?WT.mc_id=AZ-MVP-4039827)
* Configure encryption in transit
* [Add a TLS/SSL certificate in Azure App Service](https://docs.microsoft.com/en-us/azure/app-service/configure-ssl-certificate?WT.mc_id=AZ-MVP-4039827)
* [Secure a custom DNS name with a TLS/SSL binding in Azure App Service](https://docs.microsoft.com/en-us/azure/app-service/configure-ssl-bindings?WT.mc_id=AZ-MVP-4039827)

**Manage security operations (25-30%)**

**Configure centralized policy management**

* Configure a custom security policy
* [Tutorial: Create and manage policies to enforce compliance](https://docs.microsoft.com/en-us/azure/governance/policy/tutorials/create-and-manage?WT.mc_id=AZ-MVP-4039827)
* [Tutorial: Create a custom policy definition](https://docs.microsoft.com/en-us/azure/governance/policy/tutorials/create-custom-policy-definition?WT.mc_id=AZ-MVP-4039827)
* [Integrate Azure Key Vault with Azure Policy](https://docs.microsoft.com/en-us/azure/key-vault/general/azure-policy?toc=%2Fazure%2Fgovernance%2Fpolicy%2Ftoc.json&bc=%2Fazure%2Fgovernance%2Fpolicy%2Fbreadcrumb%2Ftoc.json?WT.mc_id=AZ-MVP-4039827)
* Create a policy initiative
* [Initiative Definition](https://docs.microsoft.com/en-us/azure/governance/policy/overview#initiative-definition?WT.mc_id=EM-MVP-4039827)
* Configure security settings and auditing by using Azure Policy
* [Working with security policies](https://docs.microsoft.com/en-us/azure/security-center/tutorial-security-policy?WT.mc_id=AZ-MVP-4039827)
* [Azure security policies monitored by Security Center](https://docs.microsoft.com/en-us/azure/security-center/security-center-policy-definitions?WT.mc_id=AZ-MVP-4039827)

**Configure and manage threat protection**

* Configure Azure Defender for Servers (not including Microsoft Defender for Endpoint)
* [Overview of Azure Defender for servers](https://docs.microsoft.com/en-us/azure/security-center/defender-for-servers-introduction?WT.mc_id=EM-MVP-4039827)
* [Secure your management ports with just-in-time access](https://docs.microsoft.com/en-us/azure/security-center/security-center-just-in-time?WT.mc_id=AZ-MVP-4039827)
* [File integrity monitoring](https://docs.microsoft.com/en-us/azure/security-center/security-center-file-integrity-monitoring?WT.mc_id=EM-MVP-4039827)
* [Use adaptive application controls to reduce your machines’ attack surfaces](https://docs.microsoft.com/en-us/azure/security-center/security-center-adaptive-application?WT.mc_id=EM-MVP-4039827)
* [Improve your network security posture with adaptive network hardening](https://docs.microsoft.com/en-us/azure/security-center/security-center-adaptive-network-hardening?WT.mc_id=EM-MVP-4039827)
* Evaluate vulnerability scans from Azure Defender
* [Vulnerability assessments for your Azure Virtual Machines](https://docs.microsoft.com/en-us/azure/security-center/security-center-vulnerability-assessment-recommendations?WT.mc_id=AZ-MVP-4039827)
* [Integrated vulnerability scanner for virtual machines](https://docs.microsoft.com/en-us/azure/security-center/built-in-vulnerability-assessment)
* Configure Azure Defender for SQL
* [Use Azure Defender for SQL](https://docs.microsoft.com/en-us/azure/security-center/defender-for-sql-usage?WT.mc_id=AZ-MVP-4039827)
* [Advanced Threat Protection for Azure SQL Database, SQL Managed Instance, and Azure Synapse Analytics](https://docs.microsoft.com/en-us/azure/azure-sql/database/threat-detection-overview?WT.mc_id=AZ-MVP-4039827)
* Use the Microsoft Threat Modeling Tool
* [Getting started with the Threat Modeling Tool](https://docs.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-getting-started?WT.mc_id=EM-MVP-4039827)

**Configure and manage security monitoring solutions**

* Create and customize alert rules by using Azure Monitor
* [Create, view, and manage log alerts using Azure Monitor](https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-log?WT.mc_id=AZ-MVP-4039827)
* [Create, view, and manage metric alerts using Azure Monitor](https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-metric?WT.mc_id=AZ-MVP-4039827)
* [Tutorial: Set up automated threat responses in Azure Sentinel](https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook?WT.mc_id=AZ-MVP-4039827)
* Configure diagnostic logging and log retention by using Azure Monitor
* [Create diagnostic setting to collect resource logs and metrics in Azure](https://docs.microsoft.com/en-us/azure/azure-monitor/platform/diagnostic-settings?WT.mc_id=AZ-MVP-4039827)
* [Overview of Azure platform logs](https://docs.microsoft.com/en-us/azure/azure-monitor/platform/platform-logs-overview?WT.mc_id=AZ-MVP-4039827)
* Monitor security logs by using Azure Monitor
* [Security alerts in Azure Security Center](https://docs.microsoft.com/en-us/azure/security-center/security-center-alerts-overview?WT.mc_id=AZ-MVP-4039827)
* [Manage and respond to security alerts in Azure Security Center](https://docs.microsoft.com/en-us/azure/security-center/security-center-managing-and-responding-alerts?WT.mc_id=AZ-MVP-4039827)
* [Tutorial: Get started with Log Analytics queries](https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/get-started-portal?WT.mc_id=AZ-MVP-4039827)
* [Get started with log queries in Azure Monitor](https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/get-started-queries?WT.mc_id=AZ-MVP-4039827)
* Create and customize alert rules in Azure Sentinel
* [Automatically create incidents from Microsoft security alerts](https://docs.microsoft.com/en-us/azure/sentinel/create-incidents-from-alerts?WT.mc_id=AZ-MVP-4039827)
* [Tutorial: Create custom analytic rules to detect suspicious threats](https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom?WT.mc_id=AZ-MVP-4039827)
* [Quickstart: Get started with Azure Sentinel](https://docs.microsoft.com/en-us/azure/sentinel/quickstart-get-visibility?WT.mc_id=AZ-MVP-4039827)
* Configure connectors in Azure Sentinel
* [Connect data sources](https://docs.microsoft.com/en-us/azure/sentinel/connect-data-sources?WT.mc_id=AZ-MVP-4039827)
* Evaluate alerts and incidents in Azure Sentinel
* [Tutorial: Visualize and monitor your data](https://docs.microsoft.com/en-us/azure/sentinel/tutorial-monitor-your-data?WT.mc_id=AZ-MVP-4039827)
* [Tutorial: Investigate incidents with Azure Sentinel](https://docs.microsoft.com/en-us/azure/sentinel/tutorial-investigate-cases?WT.mc_id=AZ-MVP-4039827)

**Secure data and applications (25–30%)**

**Configure security for storage**

* Configure access control for storage accounts
* [Authorizing access to data in Azure Storage](https://docs.microsoft.com/en-us/azure/storage/common/storage-auth-aad-app?WT.mc_id=AZ-MVP-4039827)
* [Security recommendations for Blob storage](https://docs.microsoft.com/en-us/azure/storage/blobs/security-recommendations?WT.mc_id=AZ-MVP-4039827)
* [Configure Azure Defender for Storage](https://docs.microsoft.com/en-us/azure/storage/common/azure-defender-storage-configure?WT.mc_id=AZ-MVP-4039827&tabs=azure-security-center)
* Configure storage account access keys
* [Manage storage account access keys](https://docs.microsoft.com/en-us/azure/storage/common/storage-account-keys-manage?tabs=azure-portal?WT.mc_id=AZ-MVP-4039827)
* [Use the Azure portal to access blob or queue data](https://docs.microsoft.com/en-us/azure/storage/common/storage-access-blobs-queues-portal?toc=/azure/storage/blobs/toc.json?WT.mc_id=AZ-MVP-4039827)
* Configure Azure AD authentication for Azure Storage and Azure Files
* [Authorize access to blobs and queues using Azure Active Directory](https://docs.microsoft.com/en-us/azure/storage/common/storage-auth-aad?WT.mc_id=AZ-MVP-4039827)
* [Acquire a token from Azure AD for authorizing requests from a client application](https://docs.microsoft.com/en-us/azure/storage/common/storage-auth-aad-app?WT.mc_id=AZ-MVP-4039827)
* [Overview – on-premises Active Directory Domain Services authentication over SMB for Azure file shares](https://docs.microsoft.com/en-us/azure/storage/files/storage-files-identity-auth-active-directory-enable?WT.mc_id=AZ-MVP-4039827)
* [Enable Azure Active Directory Domain Services authentication on Azure Files](https://docs.microsoft.com/en-us/azure/storage/files/storage-files-identity-auth-active-directory-domain-service-enable?WT.mc_id=AZ-MVP-4039827)
* Configure delegated access
* [Grant limited access to Azure Storage resources using shared access signatures](https://docs.microsoft.com/en-us/azure/storage/common/storage-sas-overview?WT.mc_id=AZ-MVP-4039827)

**Configure security for data**

* Enable database authentication by using Azure AD
* [Use Azure Active Directory authentication](https://docs.microsoft.com/en-us/azure/azure-sql/database/authentication-aad-overview?WT.mc_id=AZ-MVP-4039827)
* [Configure and manage Azure AD authentication with Azure SQL](https://docs.microsoft.com/en-us/azure/azure-sql/database/authentication-aad-configure?tabs=azure-powershell?WT.mc_id=AZ-MVP-4039827)
* Enable database auditing
* [Auditing for Azure SQL Database and Azure Synapse Analytics](https://docs.microsoft.com/en-us/azure/azure-sql/database/auditing-overview?WT.mc_id=AZ-MVP-4039827)
* Configure dynamic masking on SQL workloads
* [Dynamic data masking](https://docs.microsoft.com/en-us/azure/azure-sql/database/dynamic-data-masking-overview?WT.mc_id=AZ-MVP-4039827)
* Implement database encryption for Azure SQL Database
* [Tutorial: Secure a database in Azure SQL Database](https://docs.microsoft.com/en-us/azure/azure-sql/database/secure-database-tutorial?WT.mc_id=AZ-MVP-4039827)
* [Transparent Data Encryption](https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/transparent-data-encryption?view=sql-server-2017?WT.mc_id=AZ-MVP-4039827)
* [Always Encrypted](https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/always-encrypted-database-engine?view=sql-server-2017?WT.mc_id=AZ-MVP-4039827)
* [Overview of key management for Always Encrypted](https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/overview-of-key-management-for-always-encrypted?view=sql-server-2017?WT.mc_id=AZ-MVP-4039827)
* [Configure Always Encrypted by using Azure Key Vault](https://docs.microsoft.com/en-us/azure/azure-sql/database/always-encrypted-azure-key-vault-configure?tabs=azure-powershell?WT.mc_id=AZ-MVP-4039827)
* Implement network isolation for data solutions, including Azure Synapse Analytics and Azure Cosmos DB
* [Synapse workspace data exfiltration protection](https://docs.microsoft.com/en-us/azure/cosmos-db/how-to-configure-private-endpoints?WT.mc_id=AZ-MVP-4039827)
* [Synapse workspace Managed private endpoints](https://docs.microsoft.com/en-us/azure/synapse-analytics/security/synapse-workspace-managed-private-endpoints?WT.mc_id=AZ-MVP-4039827)
* [Cosmos DB Configure access from virtual networks](https://docs.microsoft.com/en-us/azure/cosmos-db/how-to-configure-vnet-service-endpoint?WT.mc_id=AZ-MVP-4039827)
* [Cosmos DB Configure access from private endpoints](https://docs.microsoft.com/en-us/azure/cosmos-db/how-to-configure-private-endpoints?WT.mc_id=AZ-MVP-4039827)

**Configure and manage Azure Key Vault**

* Create and configure Key Vault
* [Azure Key Vault security](https://docs.microsoft.com/en-us/azure/key-vault/general/overview-security?WT.mc_id=AZ-MVP-4039827)
* [Azure Defender for Key Vault](https://docs.microsoft.com/en-us/azure/security-center/defender-for-key-vault-introduction?WT.mc_id=AZ-MVP-4039827)
* Configure access to Key Vault
* [Secure access to a key vault](https://docs.microsoft.com/en-us/azure/key-vault/general/secure-your-key-vault?WT.mc_id=AZ-MVP-4039827)
* [Provide Key Vault authentication with a managed identity](https://docs.microsoft.com/en-us/azure/key-vault/general/managed-identity?WT.mc_id=AZ-MVP-4039827)
* [Azure Policy built-in policy definitions for Key Vault](https://docs.microsoft.com/en-us/azure/key-vault/policy-samples?WT.mc_id=AZ-MVP-4039827)
* Manage certificates, secrets, and keys
* [About Azure Key Vault secrets](https://docs.microsoft.com/en-us/azure/key-vault/secrets/about-secrets?WT.mc_id=AZ-MVP-4039827)
* [Tutorial: Import a certificate in Azure Key Vault](https://docs.microsoft.com/en-us/azure/key-vault/certificates/tutorial-import-certificate?WT.mc_id=AZ-MVP-4039827)
* [Configure customer-managed keys with Azure Key Vault by using the Azure portal](https://docs.microsoft.com/en-us/azure/storage/common/storage-encryption-keys-portal?WT.mc_id=AZ-MVP-4039827)
* Configure key rotation
* [About Azure Key Vault keys](https://docs.microsoft.com/en-us/azure/key-vault/keys/about-keys?WT.mc_id=AZ-MVP-4039827)
* [Set up Azure Key Vault with key rotation and auditing](https://docs.microsoft.com/en-us/azure/key-vault/secrets/key-rotation-log-monitoring?WT.mc_id=AZ-MVP-4039827)
* [Tutorial: Configure certificate autorotation in Key Vault](https://docs.microsoft.com/en-us/azure/key-vault/certificates/tutorial-rotate-certificates?WT.mc_id=AZ-MVP-4039827)
* [Automate the rotation of a secret for resources that use single-user/single-password authentication](https://docs.microsoft.com/en-us/azure/key-vault/secrets/tutorial-rotation?WT.mc_id=AZ-MVP-4039827)
* Configure backup and recovery of certificates, secrets, and keys
* [Azure Key Vault soft-delete overview](https://docs.microsoft.com/en-us/azure/key-vault/general/overview-soft-delete?WT.mc_id=AZ-MVP-4039827)
* [Azure Key Vault backup](https://docs.microsoft.com/en-us/azure/key-vault/general/backup?WT.mc_id=AZ-MVP-4039827&tabs=azure-cli)