Security, Compliance, Privacy, & Trust

Chapter	Chapter 4
Domain Coverage	**Domain 4a** - Describe Azure Security Features, **Domain 4b** - Describe Azure Network Security, **Domain 5a** - Describe Core Azure Identity Services **Domain 5b** - Describe Azure Governance Features **Domain 5c** - Describe Privacy & Compliance Resources
Page	75

Summary

Azure Security Center

- Monitoring service that provides a framework for advanced threat protection for workloads in the cloud and on-premise.
- Automatic assessment of your environment for security risks and providing security-based monitoring, alerts, and recommendations.

Key Vault

- Provides a centralized, cloud-based service for creating, storing, and managing keys.

Azure Information Protection (AIP)

- Enables you to classify and protect documents and emails by applying labels to them.
- Enables you to optionally protect documents with encryption, identity, & authorization.

Advanced Threat Protection (ATP)

- Ability to detect and deal with the following threats:
    - Reconnaissance attacks
    - Compromised credentials
    - Lateral account movement
    - Domain dominance

Trust Center

- A website that provides information on how Microsoft implements and supports compliance, security, privacy, and transparency.

Service Trust Portal

- Public site through which Microsoft publishes audit reports and other compliance-relates information for it's cloud services.

- Also offers information on how Azure can help you meet standards and regulation requirements.

Compliance Manager

- Enables you to build a compliance framework where you can create and assign compliance related tasks to individuals in your organization and track progress towards completion.

Azure Government

- Separate instance of Azure that caters to the US government and it's strict regulatory requirements.

Azure China

- Hosted and managed by 21Vianet to meet strict Chinese regulatory requirements.

Exam Essentials

Describe securing network connectivity in Azure

- **Azure Firewall**
  - broad-based firewall coverage for networks and resources in Azure.
  - Use when you need to filter traffic based on IP address, port, and/or protocol.
- **Web Application Firewall (WAF)**
  - Works in concert with Application Gateway, Front Door, & CDN and is specific to web application scenarios. For other scenarios use Azure Firewall or Network Security Groups.
- **Network Security Groups (NSGs)**
  - https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview

    - Deployed at the subnet or VM level to provide traffic filtering at those levels.
    - Filter based on protocol, source address, source port, destination address, and destination port.
    - Will often be used with Application Security Groups (ASGs)
- **Application Security Groups (ASGs)**
    - https://docs.microsoft.com/en-us/azure/virtual-network/application-security-groups
    - Application security groups enable you to configure network security as a natural extension of an application's structure, allowing you to group virtual machines and define network security policies based on those groups. You can reuse your security policy at scale without manual maintenance of explicit IP addresses. The platform handles the complexity of explicit IP addresses and multiple rule sets, allowing you to focus on your business logic.
    - Enable you to group servers based on applications running on them and manage security for them as a group.
    - An ASG is an object reference within an NSG, making it easy to apply rules to the VMs contained within an ASG.
- **User-defined routes (UDRs)**
    - Enable you to create custom routes to direct traffic through non-default routes.
- **Azure DDoS Protection**
    - Protection against DDoS attacks
    - **DDoS Basic**
        - Offers traffic monitoring and automatic attack mitigation.
    - **DDoS Standard**
        - Adds an SLA, mitigation policies, metrics & alerts, & reporting.

Describe Core Azure Identify Services

- **Azure AD**
  - https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-how-subscriptions-associated-directory
  - Provides identity management for Azure, enabling users to log into cloud services such as Office 365.
  - Setting up a tenant
    - https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-create-new-tenant
    - A **tenant** represents an organization.
  - Associate or add an Azure subscription to your Azure Active Directory tenant
    - https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-how-subscriptions-associated-directory
- **Azure AD Free**
  - Provides management of users and groups, synchronization with on-premises AD, basic reporting, and self-service password change for Azure AD accounts, along with SSO for Azure, Microsoft 365, Dynamics 365.
- **Azure AD Premium**
  - Offers additional services such as the ability to authenticate to on-premises resources, self-serve password reset for on-premise users, dynamic groups, and more.

Describe Security Tools & Features in Azure

- **Azure Security Center**
  - provides monitoring, alerts, and recommendations for security risks for Windows & Linux systems.

    - Integrates with Microsoft Defender for risk assessment and detection.
    - Automatically discovers and assesses resources when you deploy them.
    - **Just-in-Time Access**
        - https://docs.microsoft.com/en-us/azure/security-center/security-center-just-in-time?tabs=jit-config-asc%2Cjit-request-asc
- **Azure Key Vault**
    - Provides a secure repository for certificates, keys, and other secrets, along with the capability for applications to call Key Vault to access secrets.
    - You can create and manage secrets with Key Vault.
- **Azure Information Protection (AIP)**
    - Uses rights management and labels to classify and optionally protect documents and emails with encryption, identity, and authorization.
- **Advanced Threat Protection (ATP) - Microsoft Defender for Identity**
    - https://docs.microsoft.com/en-us/defender-for-identity/what-is
    - Leverages on-premises Active Directory to detect and identify threats directed at your organization.
    - Protects against reconnaissance attacks, compromised credentials, lateral movement, & domain dominance attacks.
- **Azure Management Groups**
    - https://docs.microsoft.com/en-us/azure/governance/management-groups/overview
    - https://docs.microsoft.com/en-us/azure/governance/management-groups/create-management-group-portal
    - If your organization has many subscriptions, you may need a way to efficiently manage access, policies, and compliance for those subscriptions. Azure management groups provide a level of scope above subscriptions. You organize subscriptions into containers called

    "management groups" and apply your governance conditions to the management groups.

  - Management groups are containers that help you manage access, policy, and compliance across multiple subscriptions.

- **Azure Activity Log**
  - The Activity log is a platform log in Azure that provides insight into subscription-level events. This includes such information as when a resource is modified or when a virtual machine is started. You can view the Activity log in the Azure portal or retrieve entries with PowerShell and CLI. For additional functionality, you should create a diagnostic setting to send the Activity log to Azure Monitor Logs, to Azure Event Hubs to forward outside of Azure, or to Azure Storage for archiving.
  - https://docs.microsoft.com/en-us/azure/azure-monitor/essentials/activity-log
- **Azure Policy**
  - Azure Policy helps to enforce organizational standards and to assess compliance at-scale. Through its compliance dashboard, it provides an aggregated view to evaluate the overall state of the environment, with the ability to drill down to the per-resource, per-policy granularity.
  - https://docs.microsoft.com/en-us/azure/governance/policy/overview
  - What is a security initiative?
    - https://docs.microsoft.com/en-us/azure/security-center/security-policy-concept
    - An Azure initiative is a collection of Azure policy definitions, or rules, that are grouped together towards a specific goal or purpose. Azure initiatives simplify management of your policies by grouping a set of policies together, logically, as a single item.
- **Azure Identity Protection**
  - https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection

Describe Azure Governance Methadologies

- Azure offers several features to help you design and enforce a governance model.
- Azure AD responsible for AUTHENTICATION
- RBAC responsible for AUTHORIZATION.
- **Role-Based Access Control (RBAC)**

  https://docs.microsoft.com/en-us/azure/role-based-access-control/overview

  - The primary authorization mechanism in Azure enables you to define who has access to Azure resources and what they can do with them.
  - You apply RBAC by creating a **security principle ,** assigning a **role definition**, and defining a **scope** to which the role assignment applies.
  - **Predefined Roles**
    - Owner
    - Contributer
    - Reader
    - User Access Administrator
  - Permissions are additive
  - Classic subscription administrator roles, Azure roles, and Azure AD roles
    - https://docs.microsoft.com/en-us/azure/role-based-access-control/rbac-and-directory-admin-roles
- **Resource Locks**
  - Enable you to control what actions can be performed on resources
  - The most restrictive lock applies.
  - **ReadOnly**
    - Applies a read only lock that enables authorized administrators the ability to read a resource but not delete or modify it.
  - **CanNotDelete**

        - Enables authorized users to read and modify a resource but not delete it.

- **Azure Blueprints**
    - Enables you to define a repeatable group of Azure resources and associated role assignments and policies, then quickly and easily deploy those resources where needed.
    - A blueprint is in draft until published and must be assigned to a resource group to apply it to those resources.
    - Deleting a blueprint does not delete those resources but it does remove resource locks, deleting the blueprint assignment object, & deleting the system-assigned management identity if one was used.

Describe Monitoring & Reporting Options in Azure

- Azure Monitor is a group of services and features that work in concert to provide a robust reporting, analysis, & alerting capability in Azure.
- Azure Monitor collects monitoring telemetry from a variety of on-premises and Azure sources. Management tools, such as those in Azure Security Center and Azure Automation, also push log data to Azure Monitor.
- https://azure.microsoft.com/en-us/services/monitor/#:~:text=Azure Monitor collects monitoring telemetry,optimized for cost and performance.
- **Application Insights**
    - Enables developers to send telemetry data from your custom applications to Azure, where data is consumed for monitoring & reporting.
- **Azure Status Portal**
    - Provides a view of the global health state for Azure services by geography and region.
- **Azure Service Health**
    - https://docs.microsoft.com/en-us/azure/service-health/service-health-overview

  - Provides information on the health of Azure globally and your resources deployed in Azure
  - Service Health tracks four types of health events that may impact your resources:
    1. **Service issues** - Problems in the Azure services that affect you right now.
    2. **Planned maintenance** - Upcoming maintenance that can affect the availability of your services in the future.
    3. **Health advisories** - Changes in Azure services that require your attention. Examples include deprecation of Azure features or upgrade requirements (e.g upgrade to a supported PHP framework).
    4. **Security advisories** - Security-related notifications or violations that may affect the availability of your Azure services.
- **Resource Health**
  - Is a component of Service Health and shows information about resources you host in Azure.

Describe Privacy, Compliance, & Data Protection Standards in Azure

- Azure provides many features to enable organizations to meet standards, both regulatory and non-regulatory.
- **Nonregulatory Standards**
  - ISO
  - IEC
  - NIST
- **Regulatory Standards**
  - HIPAA
  - GDPR
- **Microsoft Privacy Statement**

    - Describes the personal data that Microsoft processes, as well as how and why they process it.
    - Using some Microsoft services requires providing some personal data.
    - Microsoft can and does share personal data with its vendors, affiliates, and subsidiaries.
- **Trust Center**
    - Is a website containing information about security, privacy, compliance, transparency, and related products and services.
    - Does not provide risk assessment or provide a means for you to configure or apply compliance settings and policies.
- **Service Trust Portal**
    - A public site you can use to access audit and compliance reports for Azure.
    - You can access information to help you understand how to meet standards and regulations.
    - Also hosts Compliance Manager
- **Compliance Manager**
    - Enables you to view information that Microsoft provides third-party auditors to demonstrate compliance.
    - You can can use to build a compliance framework and assign and track compliance tasks in your organization.
    - Uses a workflow-based risk assessment to develop your organization's compliance score.
- **Azure Government**
    - An isolated instance of Azure supporting US federal agencies, state, local governments, and solution providers that serve the US government.
    - Managed by screened US personnel.
- **Azure China**

- Isolated instance of Azure supporting organizations that need to host Azure resources in China.
- Hosted and supported by 21Vianet under a license from Microsoft.
- Data connections between Azure China and other sites inside China require ExpressRoute
    - Connection through a telecom provider licensed by the Chinese Ministry of Industry & Information technology
- Connections between Azure China and other sites inside China require a site-to-site VPN.
    - Connection through a telecom provider licensed by the Chinese Ministry of Industry & Information technology.