Microsoft Azure Fundamentals
Training Bootcamp

Module Completion & Exam Hints

Microsoft Azure Fundamentals
Training Bootcamp

Azure Cloud Shared Responsibility Model

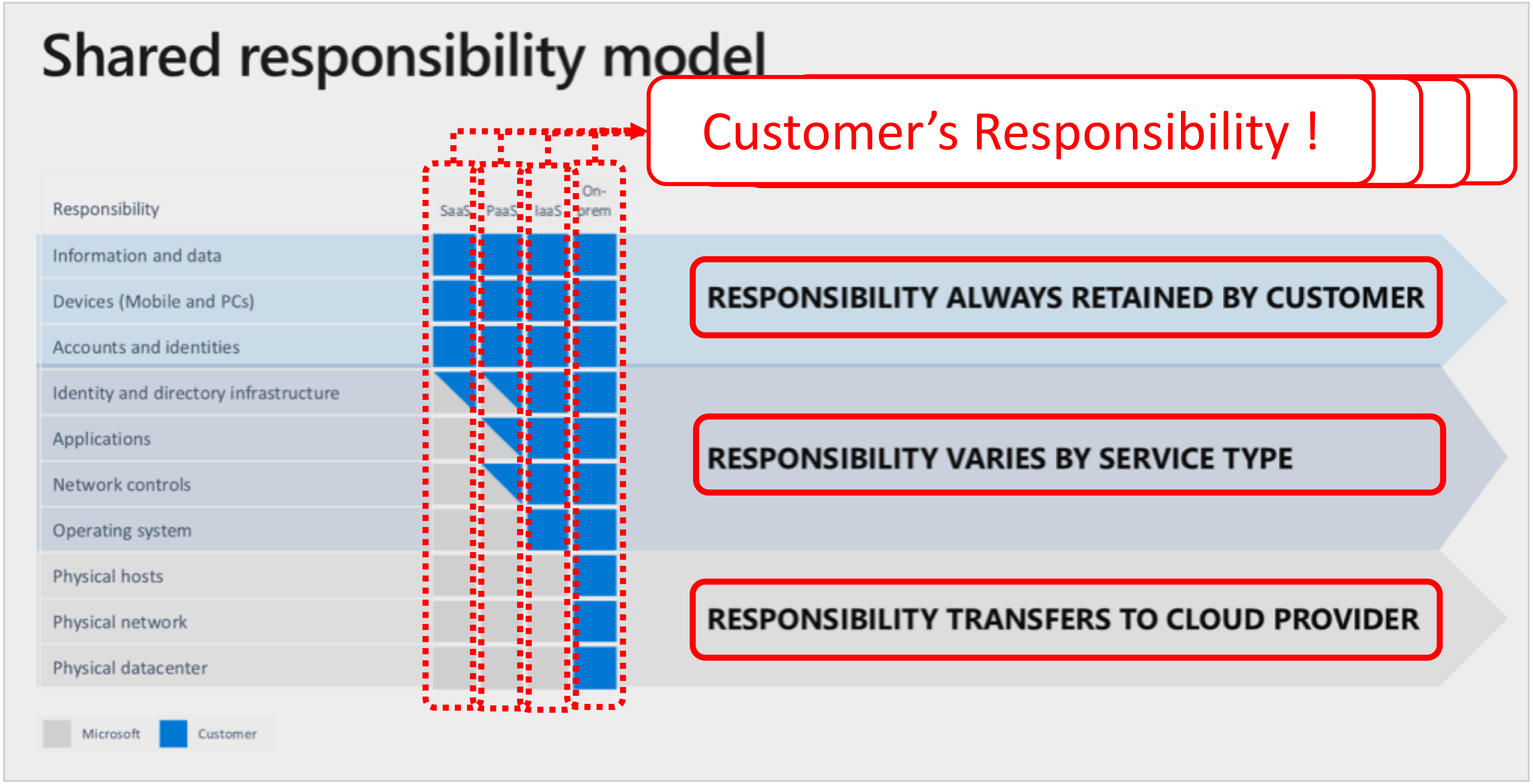
Azure Cloud Shared Responsibility Model

- When you hear cloud shared responsibility model, you must think SECURITY; it's about responsibilities and how you manage SECURITY in your cloud/hybrid environment

- In general, responsibility is shared between the cloud provider and the client and the responsibility level depends on type of apps and cloud deployment model

- https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility
- 2 minutes read

Security – A Shared Responsibility



Shared responsibility model

Customer's Responsibility !

Responsibility	SaaS	PaaS	IaaS	On-prem
Information and data	🟦	🟦	🟦	🟦
Devices (Mobile and PCs)	🟦	🟦	🟦	🟦
Accounts and identities	🟦	🟦	🟦	🟦
Identity and directory infrastructure	◩	◩	🟦	🟦
Applications	⬜	◩	🟦	🟦
Network controls	⬜	◩	🟦	🟦
Operating system	⬜	⬜	🟦	🟦
Physical hosts	⬜	⬜	⬜	🟦
Physical network	⬜	⬜	⬜	🟦
Physical datacenter	⬜	⬜	⬜	🟦

⬜ Microsoft 🟦 Customer

RESPONSIBILITY ALWAYS RETAINED BY CUSTOMER

RESPONSIBILITY VARIES BY SERVICE TYPE

RESPONSIBILITY TRANSFERS TO CLOUD PROVIDER

https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

Azure Security Center

Azure Security Center Overview

- Azure Security Center is a monitoring service that provides threat protection across all of your services both in Azure and on-premises infrastructures

- Azure Security Center capabilities:
  - Strengthen security posture, Protect against threats and Get your environment secure faster

- Free and Standard tiers available
  - Free - assessments and recommendations
  - Standard – advanced monitoring and threat detection

Security Center

Microsoft Azure Fundamentals
Training Bootcamp

Azure Active Directory

Authentication vs Authorization

- ❑ The two major topics around identity and access control are authentication and authorization

- ❑ Authentication – establishes if the user (or service) is who it says it is; identity is challenged and checked through username and password or authentication keys, certs.

- ❑ Authorization – once the user or service is authenticated, authorization establishes what level of access should be provided; read-only, editor, full admin; what resources and what permissions!

Azure Active Directory (AD) Overview

- Azure Active Directory (Azure AD) is Microsoft’s cloud-based identity service, that can also integrate with your traditional on-premises infrastructure

- Common Azure AD capabilities:
  - Authentication
  - Single-Sign-On (SSO)
  - User management
  - Conditional access to your apps
  - Privileged Identity Management (PIM)

Azure AD

Azure Privileged Identity Management (PIM)

- Azure AD PIM is a service that enables you to manage, control and monitor access to resources in your org.

- PIM provides time-based and approval-based role activation on resources that you care about

- Examples:
  - Assign time-bound access to resources
  - Role activation upon approval
  - Enforce MFA to activate any role
  - Get notifications when privileged roles are activated

Azure PIM

Microsoft Azure Fundamentals
Training Bootcamp

Azure Multi-factor Authentication (MFA)

Azure MFA Overview

- ❑ Azure Multi-factor authentication (MFA) provides additional security for your identities by requiring two or more of the following authentication methods:
  - ❑ Something you know – e.g. password
  - ❑ Something you have – e.g. App on smartphone
  - ❑ Something you are – Biometrics; fingerprint or face scan
- ❑ Azure MFA increases security of your identities, by requesting an additional authentication factor

Microsoft Azure Fundamentals
Training Bootcamp

Azure RBAC – Role Based Access Control

Azure RBAC Overview

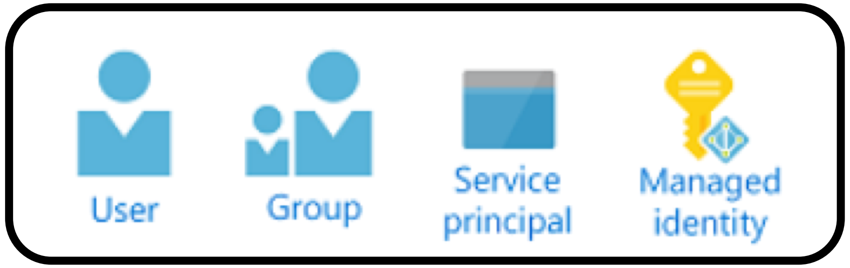
- ❑ RBAC is an authorization system built on Azure Resource Manager that you can use to provide granular access to Azure resources

- ❑ With RBAC, you can control access to resources using role assignments - it's how permissions are enforced

- ❑ A role assignment consists of three elements:
  - ❑ Security principal
  - ❑ Role definition
  - ❑ Scope

Azure RBAC – Security Principal

- A security principal is an object that is requesting access to Azure resources - user, group, service principal or managed identity
- User - individual who has a profile in Azure AD
- Group – a set of users in Azure AD



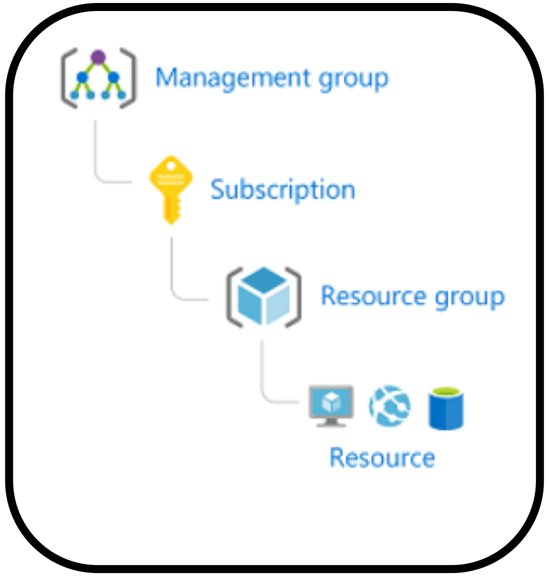
- Service Principal – security identity of an app or service
- Managed Identity – identity in Azure AD, Azure managed

Azure RBAC – Role Definition

- A role definition, or simply just role, is a collection of permissions (e.g. read, write and delete)
- Azure includes custom roles and built-in roles :
  - Owner – Full admin permissions
  - Contributor - create and manage any Azure resources, but can’t grant access to others
  - Reader - can view existing Azure resources
- Other built-in roles are available, targeting specific Azure resources; e.g. Virtual Machine Contributor

Azure RBAC – Scope

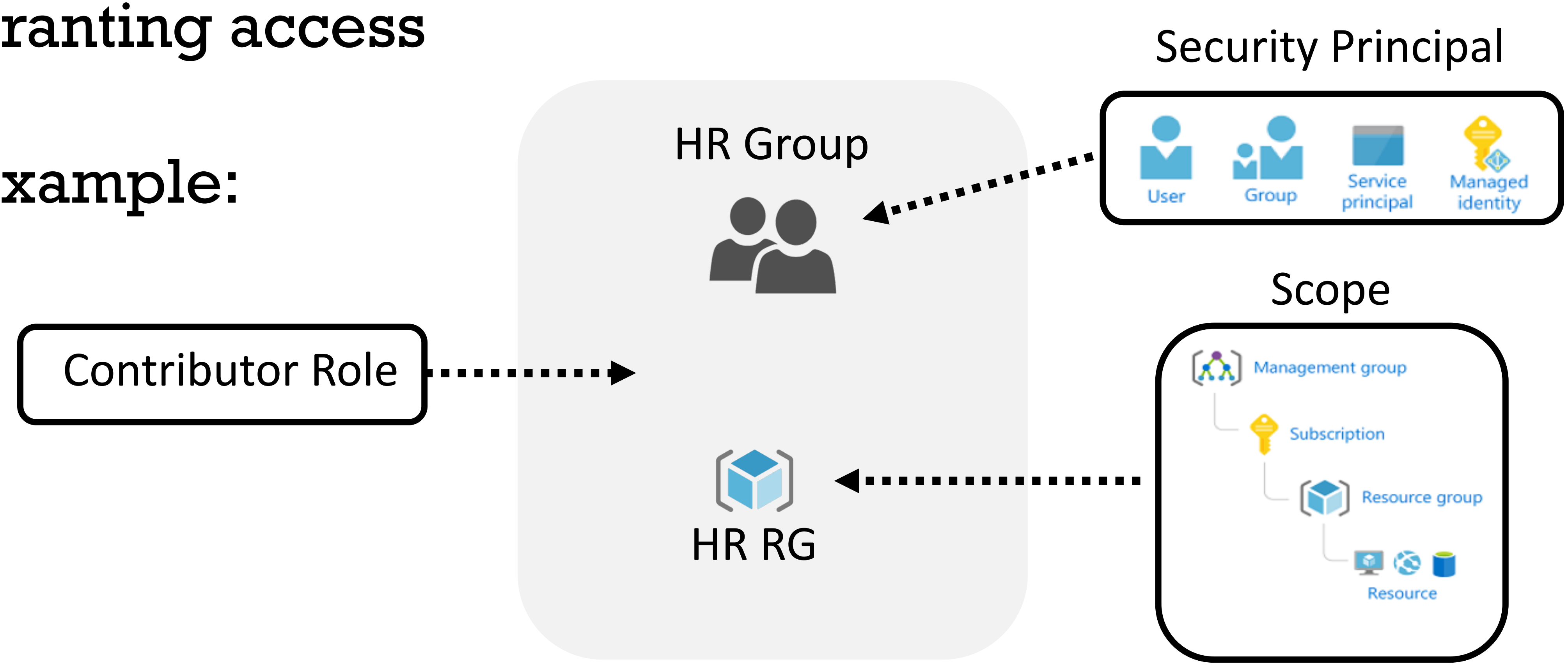
- ❑ Scope is the set of resources that the access applies to
- ❑ When you assign a role, you can further limit the actions allowed by defining a scope (e.g. VM Contributor for a specific Resource Group)
- ❑ You can specify scope at multiple levels; structured in a parent-child relationship
- ❑ When you grant access at a parent scope, permissions are inherited to the child scopes



Azure RBAC – Role Assignment

- ❑ A role assignment is the process of attaching a role definition to a security principal, at a particular scope, for the purpose of granting access

- ❑ Example:



Security Principal

HR Group

Contributor Role

HR RG

Scope

Microsoft Azure Fundamentals Training Bootcamp

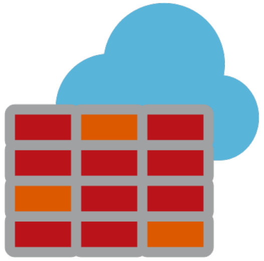
Azure Security Services. Firewall and DDoS Protection

Azure Firewall

❑ Azure Firewall is a managed, cloud-based network security service that protects your Azure Virtual Network resources

❑ You can use an Azure Firewall to grant access to resources in a VNET, based on the originating/source IP address

❑ Only clients from these granted IP addresses will be allowed to the internal resource



Azure Firewall

❑ Access is permitted/denied through firewall rules, that you create and specify ranges of IP addresses

What is DoS and DDoS ?

- ❑ Denial of Service (DoS) is a type of attack that aims to overwhelm a network resource by sending huge number of requests, so that the resource becomes slow/unresponsive

- ❑ A Distributed Denial of Service (DDoS) attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers

- ❑ Azure DDoS protection provides defense against DDoS attacks

Azure DDoS Service Tiers

- Basic
  - Enabled by default
  - Always-on traffic monitoring and real-time mitigation of common network-level attacks
  - Free, implies no cost

- Standard
  - Advanced mitigation capabilities over Basic tier
  - Price is based on usage, on a monthly basis

Microsoft Azure Fundamentals Training Bootcamp

Encryption Fundamentals and Azure Key Vault

Encryption Overview

- Encryption is the process of encoding a message or information in such a way that only authorized parties can access it

- Two types of encryption are available: symmetric and asymmetric

- Data must be encrypted, at rest and in transit
  - At rest – data stored, not traveling or moving
  - In transit – data traveling (unsecure medium)

Encryption in Azure

- Azure Storage Service Encryption
  - Protect data at rest
  - Data is automatically encrypted before storing it to Azure Storage and decrypted before retrieval

- Azure Transparent Data Encryption (TDE)
  - Real-time encryption and decryption for databases - Azure SQL Database and Azure Data Warehouse
  - Enabled by default

- Azure Key Vault – encrypt the actual keys

Key Vault

Azure Key Vault

- With Azure Key Vault we can ensure that the keys themselves are secure and store them in a centralized cloud service (AKV)

- Common use cases for Azure Key Vault:
  - Secrets Management – store passwords, certs.
  - Key Management – create and control encryption keys
  - Certificate Management – provision, manage and deploy private or public certificates

Key Vault

Microsoft Azure Fundamentals
Training Bootcamp

Azure Advanced Threat Protection (ATP). Azure Information Protection (AIP)

Advanced Threat Protection (ATP)

- ❑ Azure Advanced Threat Protection (ATP) is a cloud-based security solution that you can use to detect known malicious attacks, security issues and risks against your network

- ❑ Azure ATP includes several components: ATP portal, ATP sensor and ATP cloud service

- ❑ Sensors are installed on your domain controllers and send data to ATP portal; using ATP Portal, you can monitor, manage and investigate threats in your network environment

Azure Information Protection (AIP)

- ❑ Labels are applied to Data, depending on what information is contained

- ❑ For example, the Admin can define rules that detect sensitive data (such as credit card no.) and labels are applied automatically and accordingly

- ❑ After the content is classified (and optionally protected), you can then track and control how it is used and enforce restrictions (e.g. DLP – Data Loss Prevention)

Azure Security - Quiz

Microsoft Azure Fundamentals
Training Bootcamp

Thank you