Microsoft

Microsoft Identity and Access Administrator

Exam Ref SC-300

Razi Rais
Ilya Lushnikov
Jeevan Bisht
Padma Chilakapati
Vinayak Shenoy

Microsoft

Exam Ref SC-300 Microsoft Identity and Access Administrator

Razi Rais
Ilya Lushnikov
Jeevan Bisht
Padma Chilakapati
Vinayak Shenoy

Exam Ref SC-300 Microsoft Identity and Access Administrator

Table of Contents

Cover

Title Page

Copyright Page

Contents

Introduction

Organization of this book

Preparing for the exam

Microsoft certifications

Quick access to online references

Errata, updates, & book support

Stay in touch

Chapter 1 Implement identities in Azure AD

- Skill 1.1: Configure and manage an Azure AD tenant
  - Configure and manage Azure AD roles
  - Configure delegation by using administrative units
  - Analyze Azure AD role permissions
  - Configure and manage custom domains
  - Configure tenant-wide settings
- Skill 1.2: Create, configure, and manage Azure AD identities
  - Create, configure, and manage users
  - Create, configure, and manage groups

Table of Contents

Configure and manage device joins and registrations, including writeback

Assign, modify, and report on licenses

Skill 1.3: Implement and manage external identities

Manage external collaboration settings in Azure AD

Invite external users, individually or in bulk (collectively)

Manage external user accounts in Azure AD

Configure identity providers, including SAML and WS-Fed

Skill 1.4: Implement and manage hybrid identity

Implement and manage Azure Active Directory Connect

Implement and manage Azure AD Connect cloud sync

Implement and manage Password Hash Synchronization (PHS)

Implement and manage Pass-Through Authentication (PTA)

Implement and manage Seamless Single Sign-On (Seamless SSO)

Implement and manage Federation, excluding manual ADFS deployment

Implement and manage Azure AD Connect Health

Troubleshoot synchronization errors

Chapter summary

Thought experiment

Thought experiment answers

Chapter 2 Implement an authentication and access management solution

Skill 2.1: Plan, implement, and manage Azure Multifactor Authentication (MFA) and self-service password reset

Plan Azure MFA deployment, excluding MFA Server

Configure and deploy self-service password reset

Implement and manage Azure MFA settings

Manage MFA settings for users

Extend Azure AD MFA to third-party and on-premises devices

Monitor Azure AD MFA activity

Table of Contents

Skill 2.2: Plan, implement, and manage Azure AD user authentication

Plan for authentication

Implement and manage authentication methods

Implement and manage Windows Hello for Business

Implement and manage password protection and smart lockout

Implement certificate-based authentication in Azure AD

Configure Azure AD user authentication for Windows and Linux virtual machines on Azure

Skill 2.3: Plan, implement, and manage Azure AD conditional access

Plan conditional access policies

Implement conditional access policy assignments

Implement conditional access policy controls

Test and troubleshoot conditional access policies

Implement session management

Implement device-enforcement restrictions

Implement continuous access evaluation

Create a conditional access policy from a template

Skill 2.4: Manage Azure AD Identity Protection

Implement and manage a user risk policy

Implement and manage sign-in risk policy

Implement and manage MFA registration policy

Monitor, investigate, and remediate elevated risky users

Implement security for workload identities

Skill 2.5: Implement access management for Azure resources

Assign Azure roles

Configure custom Azure roles

Create and configure managed identities

Use managed identities to access Azure resources

Analyze Azure role permissions

Table of Contents

Configure Azure Key Vault RBAC and policies

Chapter summary

Thought experiment

Thought experiment answers

Chapter 3 Implement Access Management for Apps

Skill 3.1: Plan, implement, and monitor the integration of Enterprise apps for SSO

Discover apps by using Microsoft Defender for Cloud Apps or an ADFS application activity report

Design and implement app management roles

Understand and plan various built-in roles for application management

Configure pre-integrated gallery SaaS apps for SSO and implement access management

Integrate custom SaaS apps for SSO

Implement Application User Provisioning

Integrate on-premises apps by using the Azure AD Application Proxy

Monitor and audit access/sign-ons to an Azure AD integrated Enterprise application

Implement and configure consent settings

Skill 3.2: Implement app registrations

Plan your line-of-business application registration strategy

Implement application registrations

Configure application permissions and implement application authorization

Skill 3.3: Manage and monitor application access by using Microsoft Defender for Cloud Apps

Implement application-enforced restrictions

Configure connectors to apps

Deploy Conditional Access App Control for apps using Azure Active Directory

Create access and session policies in Microsoft Defender for Cloud Apps

Implement and manage policies for OAuth apps

Table of Contents

Chapter summary

Thought experiment

Thought experiment answers

Chapter 4 Plan and implement an Identity Governance strategy

Skill 4.1: Plan and implement entitlement management

Plan entitlements

Create and configure catalogs

Create and configure access packages

Manage access requests

Implement and manage Terms of Use

Manage the lifecycle of external users in Azure AD Identity Governance settings

Configure and manage connected organizations

Review per-user entitlement by using Azure AD entitlement management

Configure separation of duties checks for an access package

Skill 4.2: Plan, implement, and manage access reviews

Plan for access reviews

Create and configure access reviews for groups and apps

Create and configure access reviews for access packages

Create and configure access reviews for Azure AD and Azure resource roles

Create and configure access review programs

Monitor access review activity

Manage licenses for access reviews

Respond to access review activity, including automated and manual responses

Skill 4.3: Plan and implement privileged access

Plan and manage Azure roles in Privileged Identity Management (PIM), including settings and assignments

Plan and manage Azure resources in PIM, including settings and assignments

Plan and configure privileged access groups

Table of Contents

Analyze PIM audit history and reports

Create and manage break-glass accounts

Skill 4.4: Monitor Azure AD

Design a strategy for monitoring Azure AD

Review and analyze sign-in, audit, and provisioning logs by using the Azure AD admin center

Configure diagnostic settings, including Log Analytics, storage accounts, and Event Hub

Export sign-in and audit logs to a third-party SIEM

Monitor Azure AD by using Log Analytics, including KQL queries

Analyze Azure AD by using workbooks and reporting in the Azure Active Directory admin center

Configure notifications

Monitor and improve the security posture by using the Identity Secure Score

Chapter summary

Thought experiment

Thought experiment answers

Index