SC-300 Microsoft Identity and Access Administrator, Part 2 of 4: Authentication and Access Solution

Meet the expert: Anand Rao is a senior technical instructor and cloud consultant. He has worked with large enterprises for about 15 years and has a wide range of
technologies in his portfolio.Anand Rao has delivered instructor led trainings in several states in India as well as several countries like USA, Bahrain, Kenya and UAE. He has worked as a Microsoft Certified Trainer globally for Corporate Major Clients.

Prerequisites: A Candidate for the SC-300 exam manages tasks such as providing secure authentication and authorization access to enterprise applications. The administrator provides seamless experiences and self-service management capabilities for all users. Adaptive access and governance are core elements to the role. This role is also responsible for troubleshooting, monitoring, and reporting for the identity and access environment.

Basic Knowledge of Azure, Information Security and Exposure to Active Directory usage is very helpful.

Runtime: 03:20:16

Course description: The SC-300 Exam is split into 4 Domains:
Implement an identity management solution (25-30%)
Implement an authentication and access management solution (25-30%)
Implement access management for apps (10-15%)
Plan and implement an identity governance strategy (25-30%)

This course covers all the material for Domain 2, Implement an Authentication and Access Management Solution

Course outline:

Plan and Implement Azure Multifactor Authenticati
- Introduction
- Domain Overview
- Plan and Implement Azure Multifactor Authenticati
- Mitigation Measures in Azure AD
- What is Azure AD MFA
- How Multi-Factor Authentication works
- Planning the MFA
- Enforcing MFA with Conditional Access
- Deciding Supported Authentication Methods
- Azure AD Authentication Methods
- Summary

Monitoring and Usage
- Introduction
- Monitoring and Usage
- Manage User Authentication
- PasswordLess Authentication
- Security Usability availabilty of Authentication
- Demo: Configuring Fido Key for a User
- Windows Hello for Business
- Windows Hello for Business works-key points
- Azure AD Password Protection
- Demo: Azure AD Password protection
- Multiple Forests and RODC
- Plan Implement and Manage Conditional Access
- Summary

Security Defaults
- Introduction
- Security Defaults
- Enforce Policies
- Blocking legacy authentication
- Conditional Access Policies - Planning
- Conditional Access Policies - Benefits
- Conditional Access policies - components
- Conditional Access Policies - Best Practices
- Condition Access Policies - Most Common Policies
- Conditional Access Policies - Build and Test Poli
- Sign in Risk and User Risk - Conditional Access P
- Conditional Access Policy - Blocking Locations -
- Summary

Troubleshooting using Sign-in Logs
- Introduction
- Troubleshooting Using Sign-in Logs
- Device Compliance
- Demo: Conditional Access Policy
- User Exclusions
- Demo: Conditional Access Policy O365 Block MFA re
- Test and Troubleshoot Conditional Access Policies
- Implement Application Controls and Application
- Scenario 1 Microsoft 365 apps Require an Approved
- Scenario 2 Exchange Online and SharePoint Online
- Summary

App Protection Policies Overview
- Introduction
- App Protection Policies Overview
- How Can you Protect App Data
- Manage Azure AD Identity Protection - Introduction
- Manage Azure AD Identity Protection
- Risk detection and remediation
- Permissions required
- License requirements
- Sign in and User Risk Policy
- Choosing Acceptable Risk Levels
- Demo: Navigating through the Reports
- Remediate Risks and Unblock Users
- User Risk remediation Options
- Summary

Unblocking Users
- Introduction
- Unblocking Users
- Demo: Enable Azure AD MFA - EnterpriseWide
- Deploy SSPR - Setup
- Demo: Security Defaults
- Demo: Control User Sign in Frequency
- Smart Lockout Values
- Configuring User and Sign in risk policy
- Configure Azure AD MFA registration Policy
- Domain Wrapup
- Summary