SC-300 Microsoft Identity and Access Administrator, Part 1 of 4: Identity Access Management 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: 03:40:53

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 1, Implement an Identity Management Solution.

Course outline:

Active Directory
- Introduction
- Domain Overview
- Active Directory
- What is Azure Active Directory
- Who Uses Azure AD
- Azure AD Role
- Azure Roles vs. Azure AD Roles
- Capabilities of Global Admin
- Azure AD Roles
- Azure AD
- Summary

Custom Domains
- Introduction
- Custom Domains
- Deleting Custom Domains
- Bring your devices
- Azure AD Registered Devices
- Azure AD Join
- Demo: Azure AD domain Join
- Azure AD - Hybrid Joined
- Azure AD - Administrative Units
- Demo: Administrative Units
- Summary

Planning and delegation
- Introduction
- Planning and Delegation Administrative Units
- Plan for Delegation
- Security Defaults
- Create Configure and Manage Identities
- Azure AD Users
- Azure AD Groups
- Managing Licenses
- License Requirements
- Licensing Features
- Summary

Implement and Manage External Identities
- Introduction
- Implement and Manage External Identities
- Azure AD B2B Collaboration
- Demo: Azure AD B2B
- Azure AD External Collaboration Settings
- Dynamic Groups
- Demo: Dynamic Groups
- External Identities
- Demo: Azure AD B2B - Google Auth
- Summary

Implement and Manage Hybrid Identity
- Introduction
- Implement and Manage Hybrid Identity
- Plan - Design and and Implement Azure AD Connect
- Need for AD connect and Implement Azure AD Conne
- Selecting the Right Authentication Method
- Azure AD Password Hash Synchronization (PHS)
- Azure AD Passthrough Authentication (PHS)
- Federated authentication
- Architecture Diagrams
- Summary

Azure AD Design Considerations
- Introduction
- Azure AD Design Considerations
- Azure AD connect Components
- PHS - How Does it work
- Azure AD Connect LAB
- Troubleshooting Sync Errors
- InvalidSoftMatch
- Data Mismatch Errors - ObjectTypeMismatch
- Duplicate Attributes - AttributeValueMustBeUnique
- Data validation Failures - IdentityDataValidation
- Summary

Federated Domain Change Error
- Introduction
- FederatedDomainChangeError
- LargeObjects error
- Azure AD connect Health Installation
- Azure AD Connect health
- Self Remediation and Orphaned Objects
- Demo: Assigning Roles to User accounts
- Demo: Tenant Properties
- Demo: Assigning Licenses to groups
- Demo: Restoring Deleted Users
- Demo: external collaboration settings
- Domain Wrapup
- Summary