SC-300 Microsoft Identity and Access Administrator, Part 3 of 4: Access Management for Apps

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: 01:57:36

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 3, Implement Access Management for Apps

Course outline:

Microsoft Cloud App Security
- Introduction
- Domain Overview
- Microsoft Cloud App Security - CASB Solution from
- MCAS Architecture
- Need to Migrate from ADFS
- Demo: Discover AD FS applications
- Design and Implement App Management Roles
- Restrict Who Can Create Applications
- Configure Saas Based Applications
- Implement and Monitor SSO Apps - Introduction
- Token Customizations
- Summary

What is Consent
- Introduction
- What is Consent
- User Consent Settings
- What is Application Proxy
- How Azure App proxy works
- Comparision of Various Protocols used by IDP_s
- Implement Application User Provisioning
- Manual Vs Automatic user Provisioning
- Summary

System for Common Identity Management
- Introduction
- System for Common Identity Management
- SCIM Demonstration
- SCIM Attribute Exchange
- Usage Insights and Audit Reports for Enterprise A
- Application Registrations
- The need to Integrate Applications with Azure AD
- Summary

What are Application Objects.
- Introduction
- What are Application Objects.
- What are Service Principals
- Relation between Application Objects and Services
- Roles and permissions required
- Tenants - Who can sign in to your new app
- Azure Application registrations
- Summary

Types of Permissions
- Introduction
- Types of Permissions - Delegated and Application
- Requesting individual user consent
- Manifest File Token and claims
- Demo: Integrate Applications with Azure AD
- Troubleshooting SAML - SAML Tracer
- Domain Wrapup
- Summary