SC-300 Microsoft Identity and Access Administrator, Part 4 of 4: Identity Governance Strategy

page 1

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: 01:57:10

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 4, Plan and Implement an Identity Governance Strategy.

Course outline:

Planning and Implementing Entitlement Management
- Introduction
- Domain Overview
- Planning and Implementing Entitlement Management
- What is Entitlement Mangement
- Capabilities of Entitelment Management
- Entitlement Management - Terminology
- What Resources can i Manage with Access Packages
- How do I Control Who Gets Access
- When Should I Use Access Packages
- Plan Implement and Manage Access Reviews
- Plan for Access Reviews
- Summary

What is Azure AD Identity Governance
- Introduction
- What is Azure AD Identity Governance
- Demo: Access Reviews
- Planning the scope
- Components of an access review
- Planning Communications
- Demo: Access Reviews Continued
- Managing Licenses for Access Reviews
- Plan and Implement Privileged Access
- Azure Active Directory Privileged Identity Manage
- Summary

Stakeholders
- Introduction
- PIM - Stakeholders
- Principle of Least priviledge 94928
- Decide the roles that should be protected by PIM
- Decide What to protect with PIM
- Demo: Assign Azure AD roles in Privileged Identit
- Configuring Pim for Azure AD roles
- Discovering Resource to Mange
- Audit History Lab
- Create and manage Emergency Access Accounts
- Creating and Managing Emergency Accounts
- Summary

Exclusions
- Introduction
- Exclusions
- Validating Emergency Accounts
- Overview
- Analyze Signin and Troubleshoot access issues- Co
- Access and Licenses
- Demo: Sign In Report
- Sign-in Data
- Audit log - users and Groups
- Exporting logs ot Third party security solutions
- Integration Recommendations
- Analyze Azure AD Workbooks and Reporting
- Domain Wrapup
- Summary