Exam SC-300: Microsoft Identity and Access Administrator

The Microsoft Identity and Access Administrator designs, implements, and operates an organization's identity and access management systems by using Azure Active Directory (Azure AD). They manage 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.

The Identity and Access Administrator may be a single individual or a member of a larger team. This role collaborates with many other roles in the organization to drive strategic identity projects to modernize identity solutions, to implement hybrid identity solutions, and to implement identity governance.

Part of the requirements for: Microsoft Certified: Identity and Access Administrator Associate
Related exams: none
Important: See details
Go to Certification Dashboard

Table of Contents

SC-300 part 1: Implement an identity management solution

Unit 1: Implement initial configuration of Azure Active Directory

Introduction

https://docs.microsoft.com/en-us/learn/modules/implement-initial-configuration-of-azure-active-directory/1-introduction

Unit 2: Configure and manage Azure Active Directory roles

https://docs.microsoft.com/en-us/learn/modules/implement-initial-configuration-of-azure-active-directory/2-configure-manage-roles

Unit 3: Exercise manage users roles

https://docs.microsoft.com/en-us/learn/modules/implement-initial-configuration-of-azure-active-directory/3-exercise-manage-users-roles

Unit 4: Configure and manage custom domains

https://docs.microsoft.com/en-us/learn/modules/implement-initial-configuration-of-azure-active-directory/4-configure-manage-custom-domains

Unit 5: Configure and manage device registration

https://docs.microsoft.com/en-us/learn/modules/implement-initial-configuration-of-azure-active-directory/5-configure-manage-device-registration

- Azure AD registered devices
- Azure AD joined devices
- Hybrid Azure AD joined devices

Unit 6: Configure delegation by using administrative units

https://docs.microsoft.com/en-us/learn/modules/implement-initial-configuration-of-azure-active-directory/6-configure-delegation-administrative-units

- Plan your administrative units
- Delegate administration in Azure Active Directory
- Plan for Delegation
- Define roles
- Delegate app administration
- Delegate app ownership
- Develop a security plan
- Establish emergency accounts

- Secure your administrator roles

Unit 7: Configure tenant-wide setting

https://docs.microsoft.com/en-us/learn/modules/implement-initial-configuration-of-azure-active-directory/7-configure-tenant-wide-options

- Configure tenant-wide user settings
- Member and guest users
- Sign in with LinkedIn
- Manage security defaults
- Configure the external user options
- Configure tenant properties for the directory