Introduction

1 minute

Azure Administrators need to secure access to their Azure resources like virtual machines (VMs), websites, networks, and storage. They need mechanisms to help them manage who can access their resources, and what actions are allowed. Organizations that do business in the cloud recognize that securing their resources is a critical function of their infrastructure.

In this module, your business is investigating how to ensure their corporate data and assets are protected. They want secure protection that enables them to control access to their data and resources by specifying roles and access privileges for employees and business partners. You're responsible for researching how to use role-based access control (RBAC) to accomplish these tasks. You need to ensure the company assets are protected, and also support user access to the resources.

Learning objectives

In this module, you learn how to:

- Identify features and use cases for role-based access control.
- List and create role definitions.
- Create role assignments.
- Identify differences between Azure RBAC and Azure Active Directory (Azure AD) roles.
- Manage access to subscriptions with RBAC.
- Review built-in Azure RBAC roles.

Skills measured

The content in the module helps you prepare for Exam AZ-104: Microsoft Azure Administrator. The module concepts are covered in:

Manage identities and governance in Azure (15-20%)

- Manage role-based access control (RBAC)
  - Create a custom role.
  - Provide access to Azure resources by assigning roles at different scopes.
  - Interpret access assignments.

Prerequisites

None.

Next unit: Implement role-based access control

Continue

How are we doing? ☆ ☆ ☆ ☆ ☆