MANAGING ROLE-BASED ACCESS CONTROL

Companion Guide for **AZ-104 Exam Prep: Microsoft Azure Administrator**

Contents

Introduction

This companion guide for the "Managing Role-Based Access Control" section of AZ-104 Exam Prep: Microsoft Azure Administrator is intended to provide some background context and use cases for topics covered in this section. Combining this information with the demos and hands-on labs should ensure you have a full grasp of the topics in this section of the course.

RBAC Overview

Azure Role-Based Access Control (Azure RBAC) is used to manage which users have access to what Azure resources, what they can do with those resources, and what areas they have access to.

As an authorization system that's built on Azure Resource Manager, Azure RBAC offers fine-grained access management of Azure resources.

Azure RBAC can be used to do things like:

- Allow certain users to manage VMs only, while allowing others to manage only vNets
- Allow your DBA group to manage only SQL databases in your subscription
- Allow a specific admin to manage all resources in a specific resource group

How Azure RBAC works

Access to resources is controlled using RBAC role assignments. Each role assignment consists of a security principal, a role definition, and a scope.

Security Principal

The security principal is an object that represents a user, group, service principal, or managed identity that is requesting access to Azure resources. An RBAC role can be assigned to any of these security principals.

Role Definition

The role definition is really just a collection of permissions. Generally referred to as just a "role", a role definition specifies what operations can be performed. These operations are typically read, write, and delete.

While Azure offers several built-in roles that you can use, you can create custom roles if those built-in roles don't meet your needs.

Scope

The Scope is the set of resources that the access applies to. This means that, when you assign a role, you can further limit the actions that are allowed by defining a scope.

Scopes can be defined at four levels in Azure: the management group, the subscription, the resource group, or the resource itself. Scopes are structured in a parent-child relationship. You can assign roles at any of these levels of scope.

Role Assignments

As mentioned previously, role assignments are used to grant access to resources. When you assign a role, you attach a role definition to a user, a group, a service principal, or a managed identity at a particular scope, for the purpose of granting access. Access is granted by creating a role assignment, and access is revoked by removing a role assignment.

Role assignments can be created via the Azure portal, Azure CLI, Azure PowerShell, Azure SDKs, or REST APIs.

Multiple Role Assignments

In a real-world environment, it's likely there will be instances where there are multiple overlapping role assignments in play. Because Azure RBAC is an additive model, the effective permissions in such a scenario would be the sum of your role assignments. For example, if a user is granted the Contributor role at the subscription scope and the Reader role on a resource group, the effective permissions for the user on the resource group would be the Contributor role.

Deny Assignments

Although Azure RBAC used to be an allow-only model with no deny assignments, it does now support limited deny assignments. Like a role assignment, a deny assignment attaches a set of deny actions to a user, group, service principal, or managed identity at a particular scope for the purpose of denying access.

While a role assignment defines a set of actions that are allowed, a deny assignment defines a set of actions that are not allowed. It's essentially the opposite of a role assignment. Deny assignments take precedence over role assignments.