AZ-104 Azure RBAC - Understanding Roles in Azure

Manage RBAC

- Describing RBAC
- Describing Azure Roles
- Describing Azure AD Roles
- Azure Roles vs Azure AD Roles
- RBAC Architecture

Describing RBAC

"Who can do what, where, who what and where"

Describing Azure Roles

- Owner: Full access to resources and delegates access to other users
- Reader: Provides the ability to view sources, cannot perform actions on resources
- contributor: Can create and manage resources
- User Access Administrator: Can delegate access to resources

Describing Azure Entra ID Roles

- Special set of roles for providing access to manage identity objects inside our azure tenant, to manage user application or devices not resources.
- Global Administrator: Provide access to manage AD Resources
- Billing Administrator: Perform billing tasks

- User Administrator: Can manage users and groups inside Azure Entra ID Tenant
- Helpdesk Administrator: perform password resets if SSPR is not enabled.

Microsoft Entra and Azure roles

Microsoft Entra roles and Azure roles are often confused when you first work with Azure. Microsoft Entra roles provide the mechanism for managing permissions to Microsoft Entra resources, like user accounts and passwords. Azure roles provide a wealth of capabilities for managing Azure resources like virtual machines (VMs) at a granular level.

Azure Roles	Microsoft Entra ID Roles
Manage access to Azure resources like VMs, storage, networks, and more	Manage access to Microsoft Entra resources like user accounts and passwords
Multiple scope levels (management group, subscription, resource group, resource)	Scope only at tenant level
Role information accessible through Azure portal, Azure CLI, Azure PowerShell, Azure Resource Manager templates, REST API	Role information accessible in Azure admin portal, Microsoft 365 admin center, Microsoft Graph, Microsoft Graph PowerShell

Azure Roles	Azure Entra ID Roles
Manage access to Azure resources	Manage access to Azure AD Resources at tenant
Scope can be at multiple levels	Scope is at tenant level
Support custom roles	Support custom roles
Main roles: • Owner • Contributor • Reader • User Access Administrator	Main roles: • Global Administrator • User Administrator • Billing Administrator

Azure Roles	Azure Entra ID Roles
Control access to azure resources, VMs, Virtual Networks	Control Access to Azure AD REsources, user objects, group devices, ad features
Referred to as Azure RBAC	Built in roles
Built in roles	Custom roles
custom roles	Scope at Azure AD Tenant level, provide access for user that exist inside of our Azure Entra ID tenants to perform administrative functions inside of the tenant itself
Scope at management groups subscription groups resource groups and resources using identities that exist inside our azure AD Tenant	

Revision #3
Created 19 February 2024 23:13:48 by Cesar Gzz
Updated 20 February 2024 01:07:22 by Cesar Gzz