# Microsoft Azure Security Technologies

SECOND EDITION

# Exam Ref AZ-500

Yuri Diogenes
Orin Thomas

Microsoft

# Exam Ref AZ-500 Microsoft Azure Security Technologies

## Second Edition

Yuri Diogenes
Orin Thomas

| Role | Description |
|---|---|
| Conditional Access Administrator | Administrative rights over Azure AD conditional access configuration. |
| Customer Lockbox access approver | Manages Customer Lockbox requests. Can also enable and disable the Customer Lockbox feature. |
| Device Administrators | Users assigned this role will become local administrators on all computers running Windows 10 that are joined to Azure AD. |
| Directory Readers | Role for applications that do not support the consent framework. Should not be assigned to users. |
| Directory Synchronization Accounts | Assigned to the Azure AD Connect service and not used for user accounts. |
| Directory Writers | A legacy role assigned to applications that do not support the consent framework. Should only be assigned to applications, not user accounts. |
| Dynamics 365 Administrator / CRM Administrator | Administrative access to Dynamics 365 Online. |
| Exchange Administrator | Administrative access to Exchange Online. |
| Global Administrator / Company Administrator | Administrative access to all Azure AD features. This includes administrative access to services that use Azure AD Identities, including Microsoft 365 security center, Microsoft 365 compliance center, Exchange Online, SharePoint Online, and Skype for Business Online. The account used to sign up for the tenancy becomes the global administrator. Global administrators can reset the passwords of any user, including other global administrators. |
| Guest Inviter | Can manage Azure AD B2B guest user invitations. |
| Information Protection Administrator | Can manage all aspects of Azure Information Protection, including configuring labels, managing protection templates, and activating protection. |
| Intune Administrator | Has full administrative rights to Microsoft Intune. |
| License Administrator | Can manage license assignments on users and groups. Cannot purchase or manage subscriptions. |
| Message Center Reader | Can monitor notification and Microsoft advisories in the Microsoft 365 Message Center. |
| Password Administrator / Helpdesk Administrator | Can perform the following tasks for all users except those who have administrative roles:<br>■ Change passwords<br>■ Invalidate refresh tokens<br>■ Manage service requests<br>■ Monitor service health |
| Power BI Administrator | Has administrator permissions over Power BI. |

| Role | Description |
|---|---|
| Privileged Role Administrator | Can manage all aspects of Azure AD Privileged Identity Management. Can manage role assignments in Azure AD. |
| Reports Reader | Can view reporting data in the Microsoft 365 reports dashboard. |
| Security Administrator | Has administrator-level access to manage security features in the Microsoft 365 security center, Azure AD Identity Protection, Azure Information Protection, and Microsoft 365 Security and Compliance Center. |
| Security Reader | Has read-only access to security Microsoft 365–related security features. |
| Service Support Administrator | Can open and view support requests with Microsoft for Microsoft 365–related services. |
| SharePoint Administrator | Has global administrator permissions for SharePoint Online workloads. |
| Skype for Business / Lync Administrator | Has global administrator permissions for Skype for Business workloads. |
| Teams Administrator | Can administer all elements of Microsoft Teams. |
| Teams Communications Administrator | Can manage Microsoft Teams workloads related to voice and telephony, including telephone number assignment and voice and meeting policies. |
| Teams Communications Support Engineer | Can troubleshoot communication issues within Teams and Skype for Business. Can view details of call records for all participants in a conversation. |
| Teams Communications Support Specialist | Can troubleshoot communication issues within Teams and Skype for Business. Can only view user details in the call for a specific user. |
| User Account Administrator | Can create and manage user accounts. Can create and manage groups. Can manage user views and support tickets and can monitor service health. |

***MORE INFO*** **AZURE AD ADMINISTRATOR ROLES**

**You can learn more about Azure AD Administrator roles at *https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-assign-admin-roles*.**

To assign a user to a specific role within Azure AD, perform the following steps:

1. In the Azure AD admin center, select **Roles And Administrators**.
2. Select the role to which you want to add a user. This will open the role's properties page.
3. On the **Role Properties** page, click **Add Member**. Figure 1-92 shows adding the user Adele Vance to the Security Administrator role.

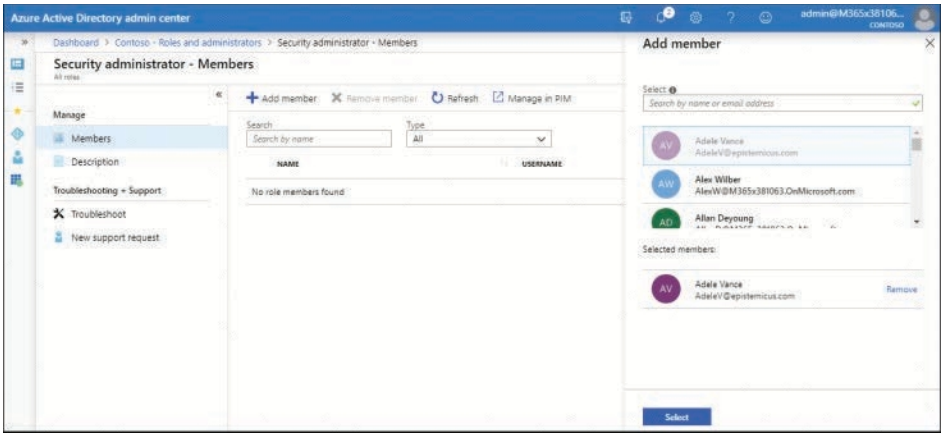


**FIGURE 1-92** Members of the Security Administrators role

You can use the following Azure PowerShell cmdlets to manage role memberships:

- **Add-AzureADDirectoryRoleMember** Adds a user to an Azure AD Directory role
- **Remove-AzureADDirectoryRoleMember** Removes a user from an Azure AD Directory role

***MORE INFO*** **VIEW AND ASSIGN AZURE AD ADMINISTRATOR ROLES**

**You can learn more about viewing and assigning administrator roles at *https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-manage-roles-portal*.**

## Create and assign custom roles, including Azure roles and Azure AD roles

If one of the many existing RBAC roles doesn't meet your organization's requirements, you can create a custom RBAC role. For example, there are three RBAC roles related to virtual machines: Virtual Machine Administrator Login, Virtual Machine Contributor, and Virtual Machine Users Login. If you want to allow a user to restart a VM (but not log in to the VM or delete the VM), you could create a custom RBAC role that allows that specific permission. As with existing Azure RBAC roles, you can assign custom roles to users, groups, service principals, and managed identities at the management group, subscription, resource group, and individual resource levels.

You can create a custom role through the Azure portal, Azure PowerShell, Azure CLI, or Azure REST API, or you can create an ARM Template. In general, creating a custom role involves following these basic steps:

1. Determine which method you will use to create the custom role. Determine what permissions the role requires. You can learn what operations are available to define your permission by viewing the Azure Resource Manager resource provider operations. For management operations, these will be `Actions` or `NotActions`. For data operations, these will be `DataActions` or `NotDataActions`.
2. Create the role. You can do this by cloning an existing role and then making modifications or by creating a new role from scratch. The most straightforward method of doing this is through the Azure portal.
3. Test the custom role. Make sure that you test the role thoroughly to determine that it only allows what you want it to allow and doesn't have some unexpected permissions, such as allowing Wally the VM operator to type something in Cloud Shell that locks out every other user in the Azure AD tenancy.

When creating a custom RBAC role, remember to only add the fewest necessary privileges to the role. When you create a custom role, it will appear in the Azure portal with an orange—rather than blue—resource icon. Custom RBAC roles are available between subscriptions that are associated with the same Azure AD tenancy. Each Azure AD tenancy supports up to 5,000 custom roles.

To clone and then modify a role in the Azure portal, perform the following steps:

1. In the Azure portal, open the **Access Control (IAM)** blade at the subscription level or resource group level where you want the custom role to be assignable.
2. Select the **Roles** tab to see the list of all available built-in and custom roles.
3. Select the role that you want to clone and modify. Figure 1-93 shows the **Virtual Machine Contributor** role being selected for cloning.

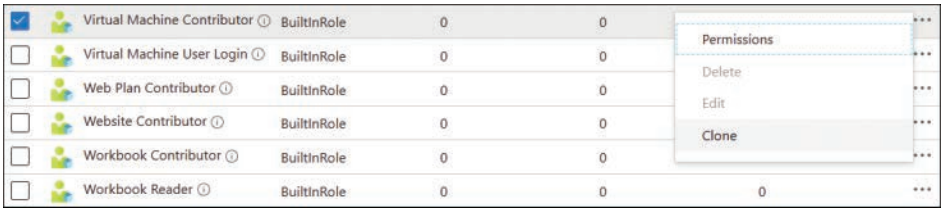


**FIGURE 1-93** Select a role to clone

4. On the **Basics** tab of the **Create A Custom Role** page shown in Figure 1-94, provide a **Custom Role Name**.

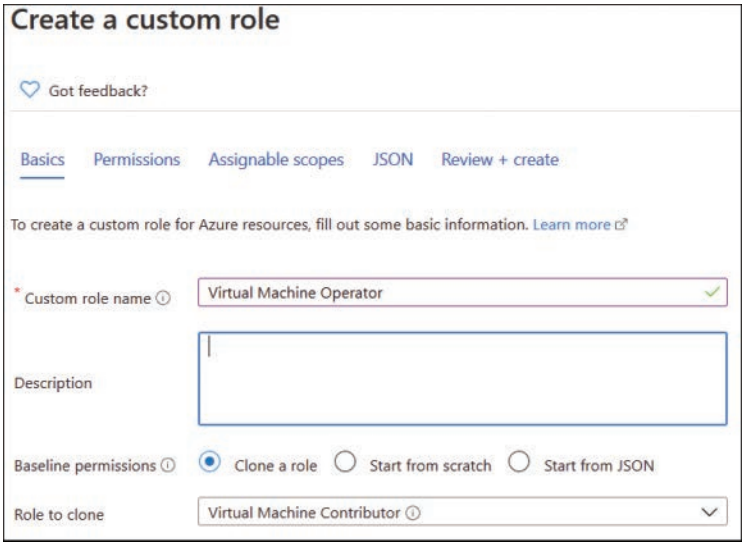


**FIGURE 1-94** Create A Custom Role wizard with the Basics tab selected

5. On the **Permissions** tab shown in Figure 1-95, you can delete existing permissions or add new permissions.

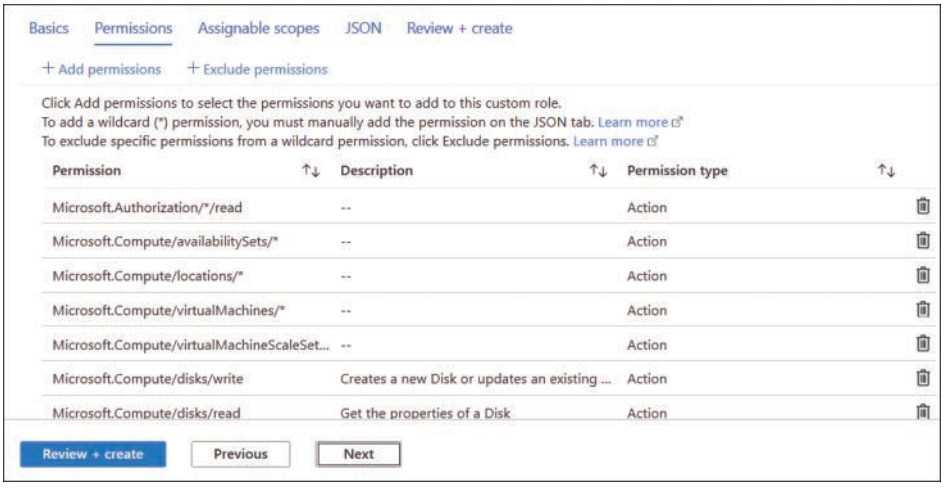


**FIGURE 1-95** Create A Custom Role wizard with the Permissions tab selected

6. On the **Assignable Scopes** tab, you can specify where the role can be assigned. You can select subscriptions associated with the Azure AD tenancy, as well as resource groups that are contained within those subscriptions.
7. On the **JSON** tab, you can view the custom role formatted in JSON. This tab gives you the opportunity to edit the role in JSON. If you want to add a wildcard permission, you do so on this tab because this is not possible at other points during the creation of a custom role.

8. Once you have reviewed the JSON code, click **Review And Create** to create the custom role.

***MORE INFO*** **AZURE CUSTOM ROLES**

**You can learn more about Azure custom roles at *https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles*.**

***EXAM TIP***

**Remember to always apply the principal of least privilege when attempting to determine which role to assign to a user who needs access to a resource.**

# Thought experiment

In this thought experiment, demonstrate your skills and knowledge of the topics covered in this chapter. You can find answers to this thought experiment in the next section.

## Identity and access at Tailwind Traders

You are one of the Azure administrators for Tailwind Traders, an online general store that specializes in a variety of products used around the home. As a part of your duties for Tailwind Traders, you have registered a new application with your Azure AD instance. Even though the application is registered, you want to limit what actions the application can perform against resources in the Tailwind Traders Azure Subscription by applying a custom RBAC role. Tailwind Traders has been using PIM for some time as a method of improving security to resources within subscriptions owned by the organization. Because the access was configured some time ago, you are aware that several users who were configured as eligible for PIM roles have changed job roles. To improve security, you want to remove PIM eligibility if it is no longer required. Another goal of Tailwind Traders is to allow some users of the new application to access the application from outside the workplace. However, from a security perspective, anyone accessing the application from outside the Tailwind Traders internal network should take extra steps to verify their identity. With this information in mind, answer the following questions:

- How can you assign the custom RBAC role to the new application?
- How can you determine which staff to remove from eligibility for PIM roles?
- How can you ensure that all users perform MFA if they are accessing the new application from a location outside the Tailwind Traders office?