Student Name: **Weight: 3%**

Student ID: **Marks: /10**

Lab 2: Azure Identities

Lab Objectives

In this lab you'll explore how to create Azure identities, use RBAC (role-based access control) and organize your identity and access structure. You will:

1. Create a new Azure Active Directory (Az AD) tenant.
2. Create Az AD users.
3. Create Az AD groups.
4. Add a device identity.
5. Assign a RBAC role.
6. View roles in JSON.
7. Create a custom role.
8. Create Az AD Management groups.
9. Create Administrative Units.

Lab Requirements

- Up-to-date web browser
- Azure account
- UserCreatTemplate.csv file
- Windows 10 or 11 virtual machine

Instructions

1. Working individually, follow the procedure below.
2. Take screenshots, as described in the *Marking Criteria* section.
3. Create a document that includes all screenshots appropriately titled and described, and then upload it to Brightspace, as indicated by your instructor.

Marking Criteria

Screenshots	Marks
New Azure AD Tenant	/1
PowerShell screen with successful creation of a user	/2
Windows 10/11 device added	/2
User with Backup operator role on subscription	/2
Custom role definition	/2
Management group created with Az CLI	/1
Total	**/10**

Note: This icon indicates when a screenshot is required.

Source: Flatiron.com, Freepik, Image: screenshot_983871

Procedure

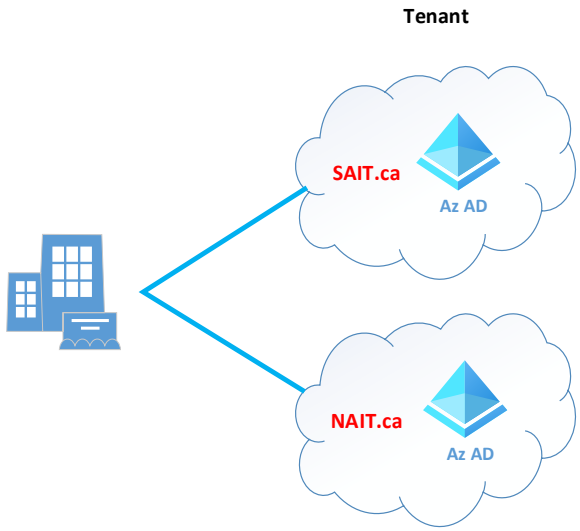
Part 1: Create a New Azure Active Directory (Az AD) Tenant

When you create your first subscription, a Tenant/Directory is created for your organization, usually associated with a single domain name. The Tenant is made up of a single instance of Azure AD.

- ☐ Log in to the Azure portal and select the **Azure Active Directory** tool.
- ☐ Notice your globally unique domain name, tenant ID, license and other information about your tenant.

  Note: Your domain name ends with OnMicrosoft.com.

  You might use a second tenant if you bought or created a second company with a different domain name. For example, if SAIT and NAIT were owned by one organization it might have a SAIT and a NAIT tenant.



- ☐ Select **Manage Tenants** from the top menu.
- ☐ Select **Create** from the top menu.

  One or more selections appear, depending on your license:

  - Azure AD – Used with your tenant to authenticate identities in your organization.
  - Azure AD (B2B) – Business-to-Business: used to authenticate your partners and suppliers.

Note: See External Identities in Azure Active Directory (https://learn.microsoft.com/en-us/azure/active-directory/external-identities/external-identities-overview) for more information.

- Azure AD (B2C) – Business-to-Customer/Consumer: used to authenticate your customers to your applications.

  Note: See https://learn.microsoft.com/en-us/azure/active-directory-b2c/overview (https://learn.microsoft.com/en-us/azure/active-directory-b2c/overview) for more information.

☐ Select **Azure AD** and click **Next**.

☐ Enter an organization, a fake domain name and select **Canada** as the location.

Note: The domain name must be globally unique.

☐ Review and create the new tenant.

☐ Return to the **Manage Tenants** page.

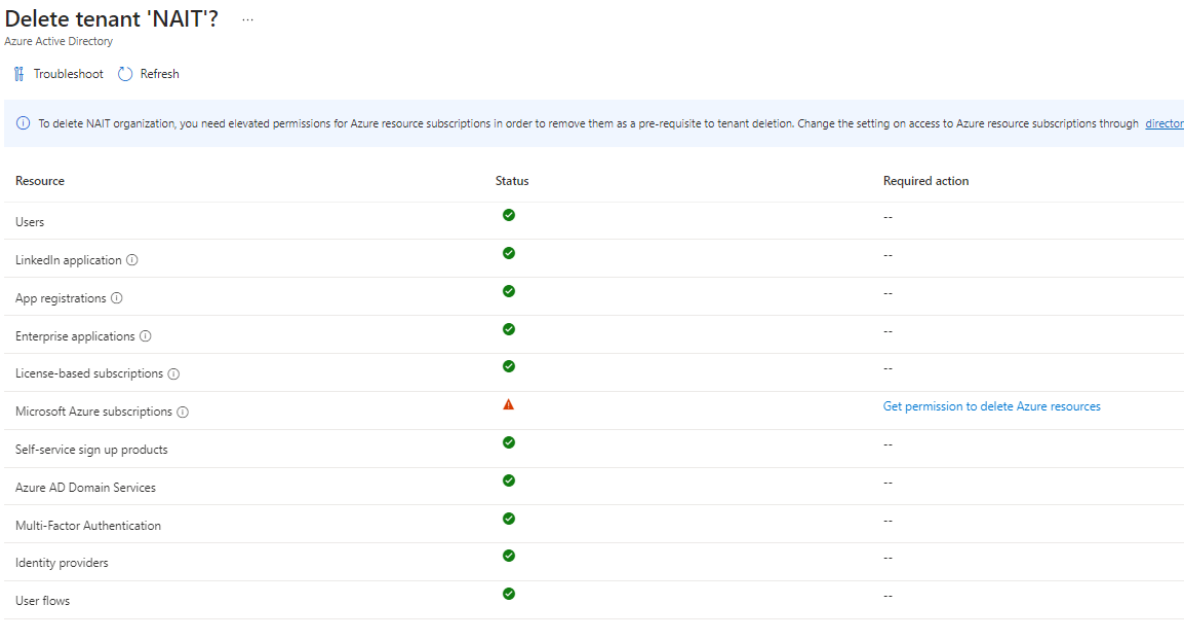
You should see that you now have two tenants with unique IDs.

☐ Select the checkbox beside your new tenant and select **Delete** from the top menu.

☐ If prompted, type the required letters to prove you are not a robot.

A page opens that evaluates your permissions to delete a tenant. By default, no one (not even the administrator) can delete tenants, but the administrator is authorized to grant that permission.

☐ To give yourself that permission, in the **Required action** column, select **Get permission to delete Azure resources**.



The *Azure AD properties* screen appears.

☐ Under Access management for Azure resources, select **Yes** and then **Save**.

☐ Return to the **Manage Tenants** page and delete the tenant.

Note: Be careful not to delete your original tenant.

☐ In the upper-right of the screen, click your account, select **Switch Directory** and select your original tenant.

Part 2: Create Azure AD Users

The most common type of identity in Azure is a user, but a user can be added in several ways:

- Cloud User – You have an Azure account and you log in to the Azure portal.
- Dir-Synch User – Your company has a Windows domain with an Active Directory server (not Az AD) and your company's users are synchronized with Az AD so they can log in to Azure.
- Guest User – A user added from a third party, such as Xbox or Google.

In this section, you will create a cloud user.

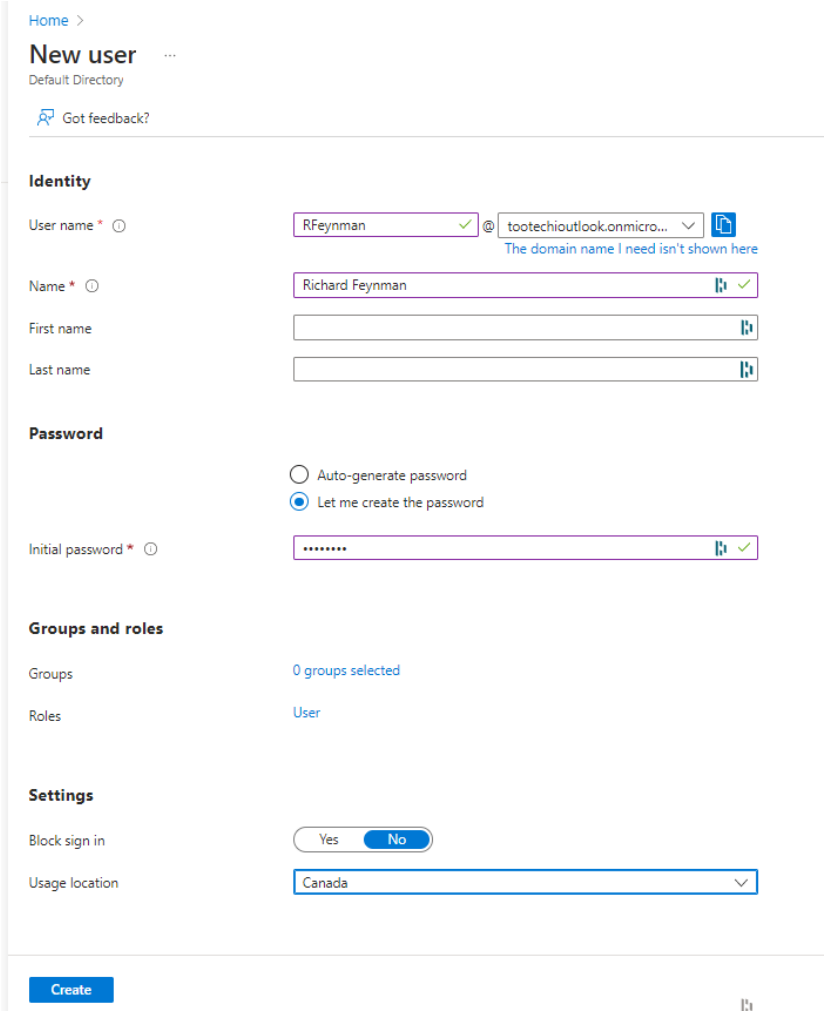
☐ Navigate to the **Azure Active Directory** window and select **Users**.

☐ Select **New User**.

You can either create a new user or invite an external (guest) user.

- ☐ Select **Create New User**.
- ☐ Fill in the information shown below, and then click **Create**.

  Note: To learn more about a particular field, click the ⓘ information icon. We will cover groups and roles later.



- ☐ Repeat the steps above to create a few more users.
- ☐ Return to the **Active Directory Users** page and click one of your users to see a summary of that user's identity information.
- ☐ Select **Edit Properties** from the top menu and examine the types of information you can create for each user.

If you need to create many users at the same time, you can use a .csv file to do a bulk upload. The **UserCreateTemplate.csv** file contains a list of three example users you can upload. The column titles tell you which columns are required and the rest are optional.

- ☐ Change the domain name under the *User name [userPrincipalName] Required* column to your domain.
- ☐ Add a few more users.
- ☐ Save the file, being sure to keep it in .csv format.
- ☐ Return to the **Active Directory Users** window and select **Bulk Operations, Bulk Create** from the top menu.
- ☐ Upload the .csv file and click **Submit**.
- ☐ When the *Success* message appears, refresh your browser to see the new users.

A useful feature that is set separately from the user account is the SSPR (Self Service Password Reset).

Note: You need a premium license to use this feature but you can see a demonstration in the learning module Allow users to reset their password (https://learn.microsoft.com/en-us/training/modules/allow-users-reset-their-password/).

- ☐ Return to the **Users** page and click **Password Reset**.
- ☐ To create users with PowerShell, type the following command to connect to AzAD:

```
Connect-AzureAD
```

- ☐ Create a password profile using the following two commands. Replace the text in red with your information.

```
$PasswordProfile = New-Object -TypeName
Microsoft.Open.AzureAD.Model.PasswordProfile

$PasswordProfile.Password = "T3stP@ssw0rd"
```

- ☐ Create the user.

```
New-AzureADUser -DisplayName "Usersname" -PasswordProfile
$PasswordProfile -UserPrincipalName "Usersname
@YourDomain.onmicrosoft.com" -AccountEnabled $true -MailNickName
"Usersname"
```

- ☐ Create 10 users.

Part 3: Create Azure AD Groups

Not all users require the same permissions and it would be time consuming to set each user's permissions individually. Azure AD uses groups so you can set permissions for a number of users at the same time.

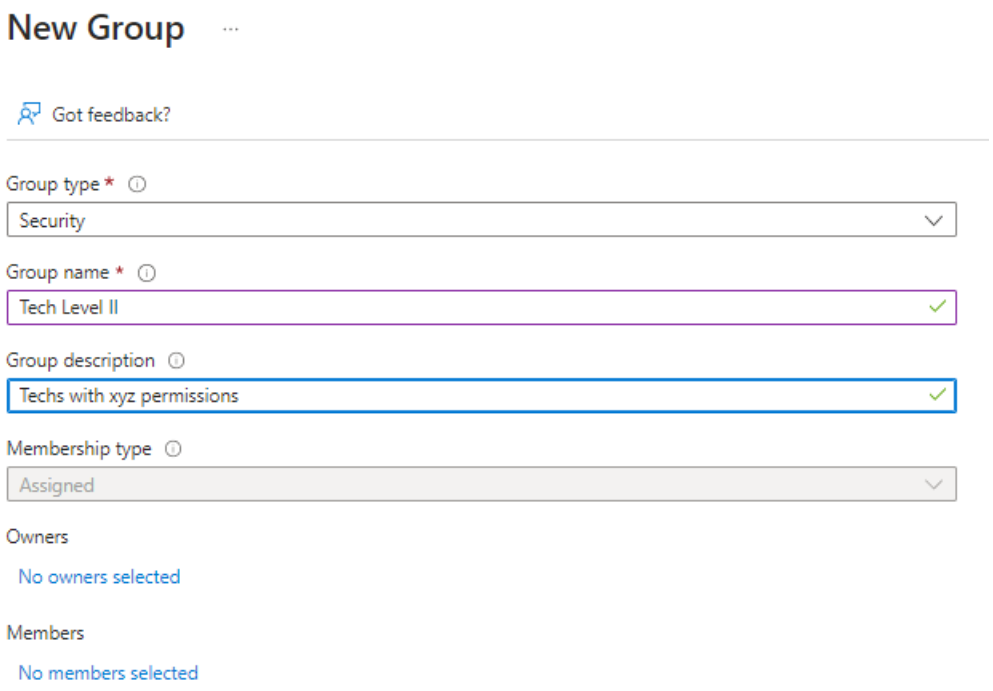
☐ Go to the **Azure Active Directory** page and select **Groups**.

☐ Select **New Group** from the top menu.

In the *Group Type* drop-down menu there are two choices:

- Security – Used to set Azure resource permissions.
- Microsoft 365 – Used to access Microsoft 365 resources like Outlook and Stream.

☐ Select **Security** and fill in the rest of the information as indicated below:



There are two types of membership:

- Assigned – The user is assigned to the group by an administrator.
- Dynamic – The user is assigned to the group dynamically by one of the user properties. For example, if you enter a department name for a user, all users in that department are placed in this group. This requires a premium license.

Note: For more information, see: [Dynamic membership rules for groups in Azure Active Directory](https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-dynamic-membership) (https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-dynamic-membership).

☐ Assign users to the group by clicking the blue **No members selected** link.

A long list of service names as well as user names may appear, because services can belong to groups too.

☐ Assign a couple of your users to the group and create the group.

Part 4: Add a Device Identity

☐ Navigate to the **Azure Active Directory** window and select **Devices**.

The Overview page shows a summary of your devices and their compliance.

☐ Select **Device settings** and then select the users or groups that may register their devices and whether multi-factor authentication (MFA) will be used.

Note: You should always use MFA for better security.

If you want your users to be able to sign in from multiple devices, like their workstation, phone or tablet, each device must have its own identity in Azure. There are three ways to connect a device and give it an Azure device identity:

- Azure AD registration – For users' BYOD, such as a phone or a tablet.
- Azure AD join – For Windows 10, Windows 11, Windows Server 2019 and later devices that belong to your on-prem AD domain.
- Hybrid Azure AD join – For older operating systems like Windows 7 or Windows Server 2008 that belong to your on-prem AD domain.

☐ Follow the tutorial: Azure AD join a new Windows device during the out of box experience (https://learn.microsoft.com/en-us/azure/active-directory/devices/azuread-joined-devices-frx) to join a Windows 11 virtual machine to your active directory.

Part 5: Assign an RBAC (Role-Based Access Control) Role

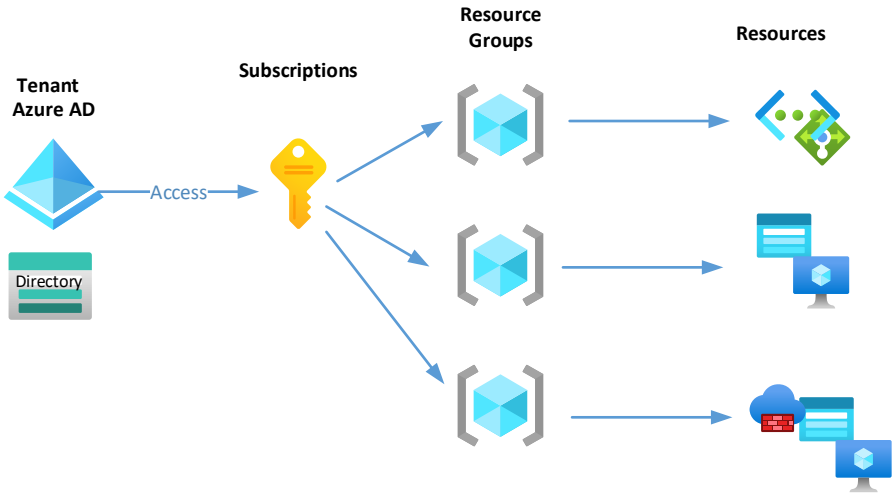
Earlier in the course, you created Azure policies to help you configure your resources to meet your business rules or SLAs (service level agreements). Some policies may restrict resources for business or compliance reasons, such as not allowing resources to be created in a certain region because of data laws. However, most detailed resource restrictions are done using Azure RBAC.

☐ Read: Compare and contrast Azure RBAC vs Azure policies (https://learn.microsoft.com/en-us/training/modules/enterprise-governance/7-azure-rbac-vs-azure-policies).

RBAC is designed to manage the resource permissions/authorization of users or groups of users. A role is a set of those permissions/authorizations that can be applied to the following:

- Management Groups
- Subscriptions
- Resource Groups
- Individual Resources

RBAC permissions are inherited, meaning that permissions applied to a resource group will also apply to the individual resources within that group. Permissions applied at the subscription level are inherited by the resource groups in that subscription and then to the individual resources within those groups.



© 2023, Microsoft Azure. Used with permission from Microsoft.

To be able to assign roles, a user must have the appropriate permissions.

- Microsoft.Authorization/roleAssignments/write
- Microsoft.Authorization/roleAssignments/delete

Roles that have this permission are:

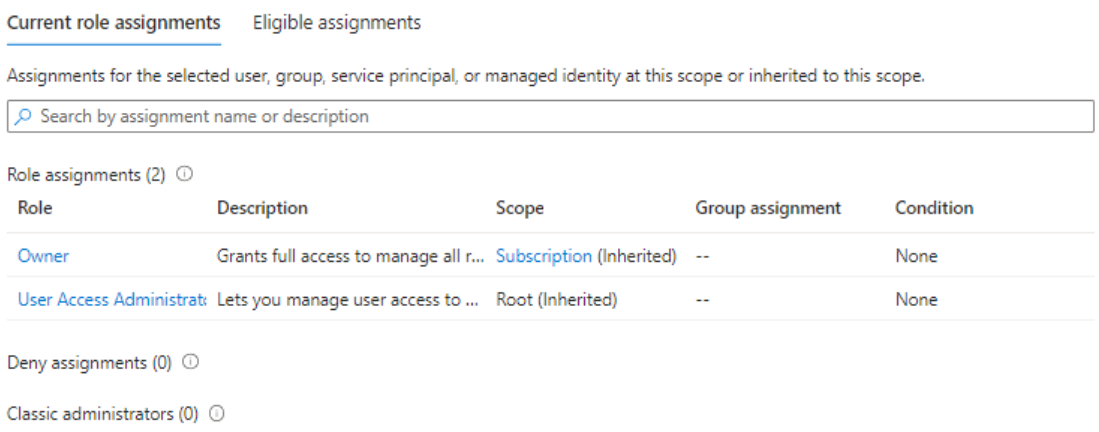
- User Access Administrator
- Owner

There are built-in roles or you can create custom roles. To create a custom role:

☐ Go to the **Resource Groups** window and select one of your resource groups.

☐ Select **Access Control (IAM)** and click **View My Access** to see the permissions granted to you as a user.

If you are owner of the subscription, you have full access to manage all resources on the subscription and to manage user access (create and assign roles).



☐ From the Access control (IAM) page, select Add Role Assignment.

You will see a list of all the built-in roles that could be applied to this resource group. Note the first three roles and their permissions. Most resources have these basic roles.

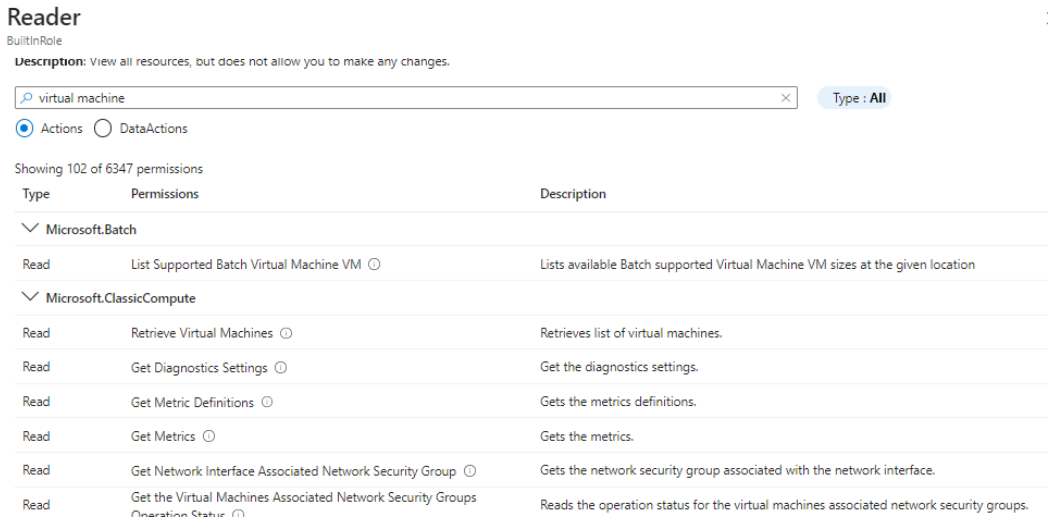
- Owner
- Contributor
- Reader

☐ Select the **Reader** role, and then in the *Details* column, click **View**.

This role allows you to view all resources, but it does not allow you to make any changes. It consists of several hundred individual permissions.

☐ Type **Virtual Machine** in the search bar.

You see all the permissions of this role that apply to virtual machines.



- ☐ Close the **View** page.

  You should now be on the **Add Role Assignment** page with the **Reader** role selected.

- ☐ Select **Members** to see any users or groups that have this role on this resource group.

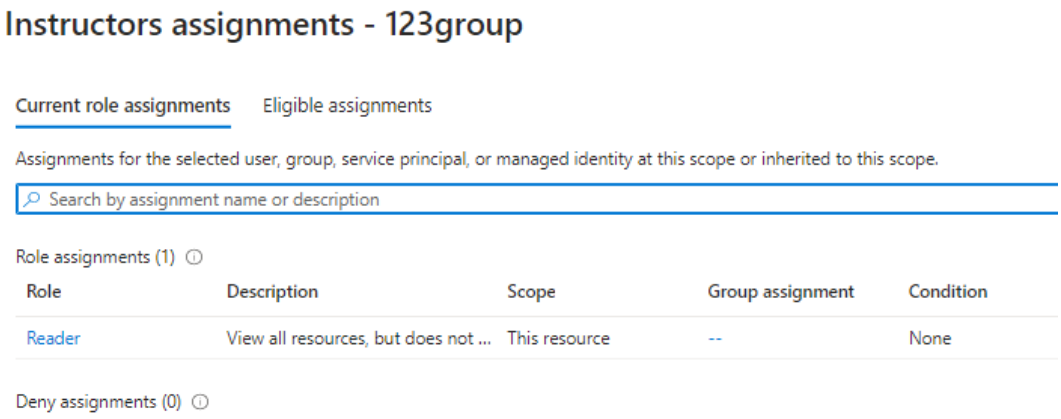
- ☐ Select **Add Member**, add one of your user groups to the role, and then click **Review + Assign**.

  You have now applied that role, to that group, on that resource group. This means that any user that is part of the group won't be able to do anything other than the specific permissions defined by that role.

- ☐ Return to the **Access Control (IAM)** page and select **Check Access**.

- ☐ Type your group name in the search bar and check the access of that group.

  In the example below, the group of users called *Instructors* are assigned to the resource group named *123group* with Reader permissions.



- ☐ Using the same procedure on your subscription, add one of your users as the Backup Operator for the subscription.

Part 6: View Roles in JSON

- ☐ Go to the **Subscription** page and click your subscription.

- ☐ From the **Access Control (IAM)** window, select **Roles**.

- ☐ Find and view the Storage Account Distributor role.

- ☐ Select **JSON** from the menu, and then review the permissions as they are written in JSON.

Part 7: Create a Custom RBAC Role

A role consists of:

- A security principle – A user, group or application (the identity that has the permissions).
- Role definition – A collection of permissions/authorizations.

A role is also applied to a scope, which is the set of resources that the access applies to.

☐ Read the article: Understand Azure role definitions (https://learn.microsoft.com/en-us/azure/role-based-access-control/role-definitions).

☐ From the **Access control (IAM)** page of your subscription, locate the *Create a Custom role* box and click **Add**.

☐ Click Permissions.

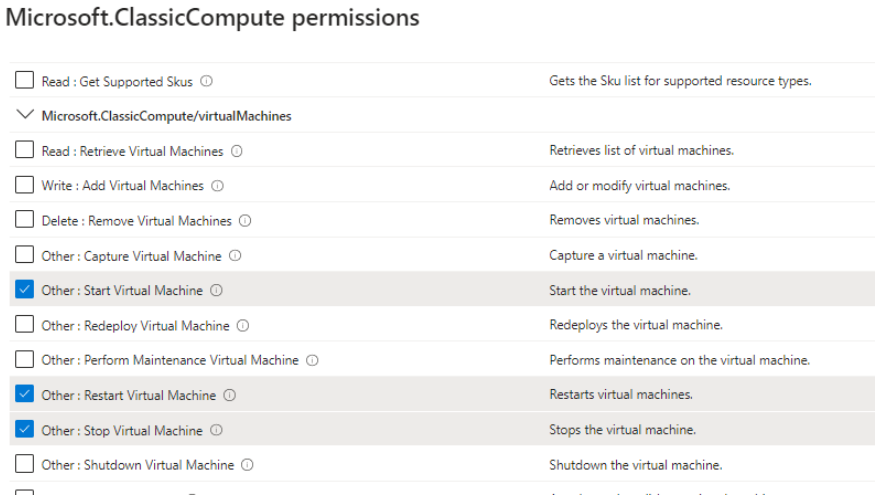
☐ Read the definitions of Control Plane, Data Plane and Wildcards on the right side of the screen. Note that you can add or exclude a permission.

☐ Click **Basics** from the top menu. Note that you can clone a built-in role and customize it, create a role from scratch, or create a role using JSON.

☐ Select **Create From Scratch**, name the role **VMAdmin** and click **Next**.

☐ Click Add Permissions and click the Microsoft Classic Compute box.

☐ Select the permissions shown below and click **Add**.



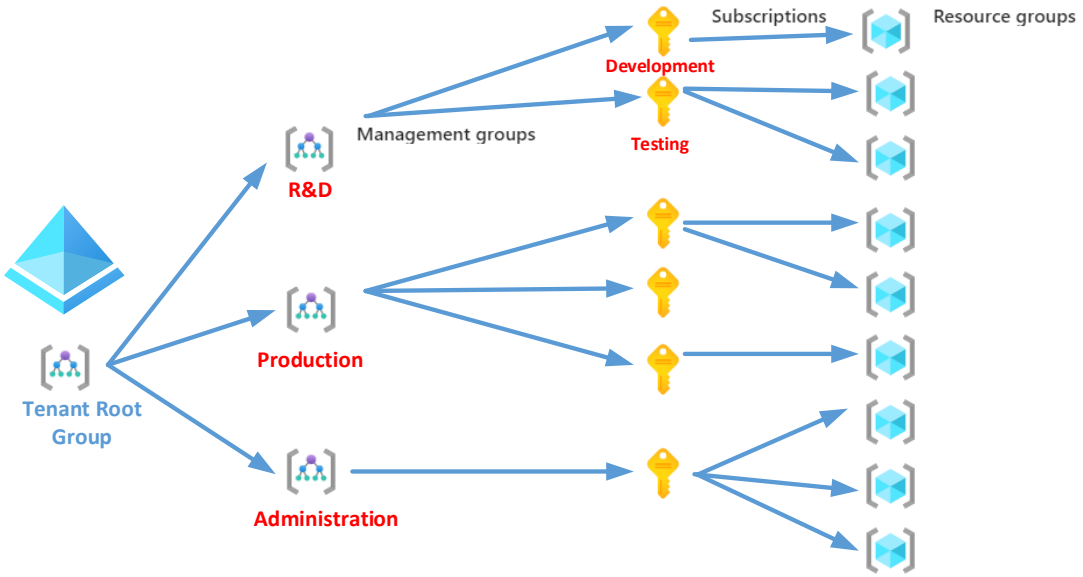
☐ On the top menu, click **Exclude Permissions** and select the **Remove Virtual Machine** permission as an exclusion.

☐ Click **Next**.

- ☐ The *Assignable Scopes* window appears, where you can select which scopes the role can be applied to. You could limit it to resource groups or even virtual machines.
- ☐ Click **Review + Create**, review your settings and create your role.
- ☐ Using the same procedure, create a custom role called **StoreAdmin** that allows the identity to do the following:
    - Read storage account locks
    - Read: Get File Share on Microsoft.Storage/storageAccounts/fileServices/shares
    - Read: List File Services on Microsoft.Storage/storageAccounts/fileServices
    - Read: List of blob containers
    - Not delete a storage account

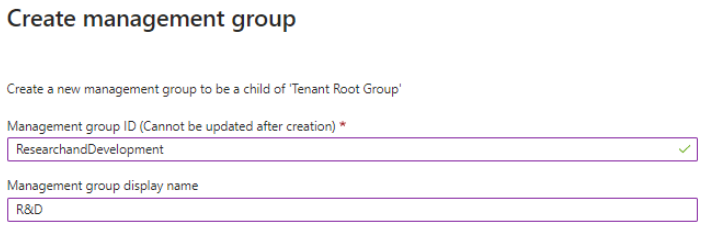
Part 8: Create Azure AD Management Groups

If your company has many subscriptions, you can use management groups to create an additional level of organization. In the example below, an electronic manufacturing company has three departments (R&D, Production and Administration). In the R&D department, they have created two subscriptions for separate billing and access policies.



When you create your Azure account, you get a single instance of Azure Active Directory, which contains a single management group called the *Tenant Root Group*. All other management groups are created under this group.

- ☐ Read the article: [What are Azure Management Groups?](https://learn.microsoft.com/en-us/azure/governance/management-groups/overview) (https://learn.microsoft.com/en-us/azure/governance/management-groups/overview).
- ☐ Navigate to **Management Groups** and click **Create** on the top menu.
- ☐ Create the following Management group, and then click **Submit**.



- ☐ After a few moments (or a screen refresh) you will see your *Root Tenant Group*, your subscription and your new group.

  Note: The new group is indented to show that it is located under the *Root Tenant Group*.
- ☐ Click your R&D group and review the options.
- ☐ Use the Azure CLI command to create a new management group called **Production**.

  Note: For more information, see [Create a management group with the Azure CLI](https://learn.microsoft.com/en-us/azure/governance/management-groups/create-management-group-azure-cli) (https://learn.microsoft.com/en-us/azure/governance/management-groups/create-management-group-azure-cli).

Part 9: Create Azure Administrative Units

Your Azure AD stores its identity information in a directory (similar to a database), and you create users and groups in that directory. The Az AD is the directory service; the system that allows you to manage identities.

Administrative units are an extra layer of organization for your company's administrative permissions and roles within Az AD. Administrative units are often confused with management groups but they do not perform the same function.

- Administrative units cannot be nested
- Administrative units can contain users, groups and devices (identities)
- A user can belong to multiple administrative groups

- You assign administrative roles to administrative groups, not resource permissions

The following is a list of built-in administrative roles.

Administrative roles

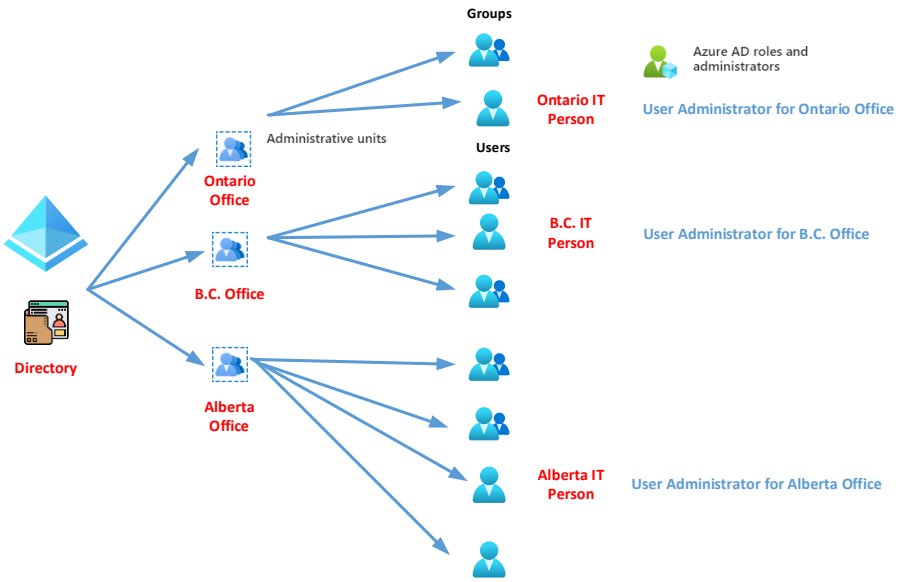
Administrative roles can be used to grant access to Azure AD and other Microsoft services. Learn more

Role	Description	Type
Authentication Administrator	Can access to view, set and reset authentication method information for any non-admin user.	Built-in
Cloud Device Administrator	Limited access to manage devices in Azure AD.	Built-in
Groups Administrator	Members of this role can create/manage groups, create/manage groups settings like naming and e...	Built-in
Helpdesk Administrator	Can reset passwords for non-administrators and Helpdesk Administrators.	Built-in
License Administrator	Can manage product licenses on users and groups.	Built-in
Password Administrator	Can reset passwords for non-administrators and Password Administrators.	Built-in
Printer Administrator	Can manage all aspects of printers and printer connectors.	Built-in
SharePoint Administrator	Can manage all aspects of the SharePoint service.	Built-in
Teams Administrator	Can manage the Microsoft Teams service.	Built-in
Teams Devices Administrator	Can perform management related tasks on Teams certified devices.	Built-in
User Administrator	Can manage all aspects of users and groups, including resetting passwords for limited admins.	Built-in

If your company has three offices (Alberta, B.C. and Ontario), you may have an IT person who performs functions like creating user or group accounts, managing printers or resetting passwords. If you give the *User Administrator* role to a member of the IT team, that person would have complete user control over all users in all of the offices, which does not meet security best practices.

To prevent this problem:

- Create an Administrative Unit for each of your offices.
- Add all the users and groups for each office to the appropriate administrative unit.
- Give the IT person for each office the User Administrator role.



- ☐ Go to the **Az AD** page and select **Administrative units**.
- ☐ Select **Add** from the top menu.
- ☐ Type **Alberta Office** as the name of the *Administrative group*, and then click **Next**.
- ☐ On the *Assign Roles* page, select **User Administrator** and add one of your users as the administrator.
- ☐ Review and create the administrative unit.

  Note: If you don't have a premium licence, creating the administrative unit will succeed but it won't add the *User/User Administrator* role.

- ☐ Return to the **Administrative Units** page and select the **Alberta Office** unit.
- ☐ Add several of your users to the unit.
- ☐ Using the same procedure, create administrative units for the B.C. and Ontario offices.
- ☐ Examine the administrative roles.

Additional Resource

What is Azure Active Directory? (https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis)