**Lesson 4 Demo 3**

**RBAC (Role-Based Access Control) and Policy**

**Objective**: To configure delegation of provisioning and management of Azure resources by using built-in Role-Based Access Control (RBAC) roles and built-in Azure policies

**Tools required**: Azure account with administrator access

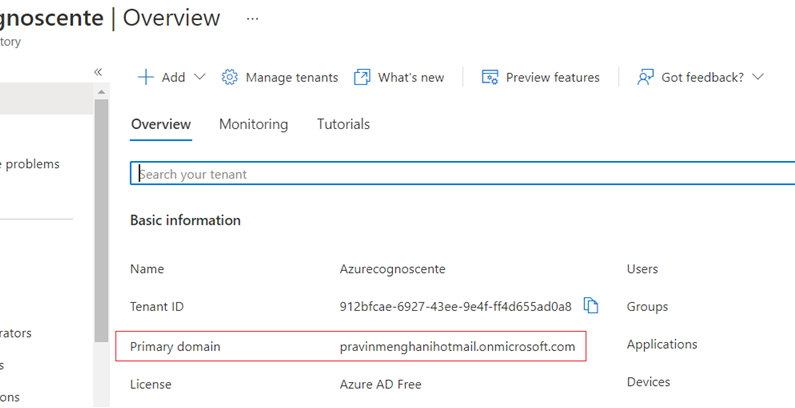
**Prerequisites**: None

**Steps to be performed:**

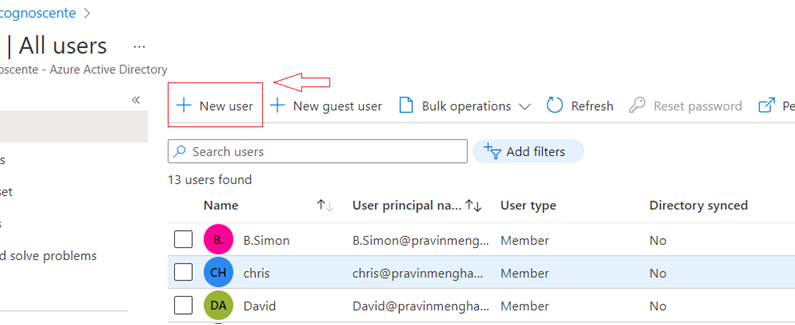
1. Create Azure Active Directory (AD) users and groups
2. Create Azure resource groups
3. Delegate management of an Azure resource group via a built-in RBAC role
4. Assign a built-in Azure policy to an Azure resource group

**Step 1: Create Azure AD users and groups**

* 1. Browse the Azure portal at [**http://portal.azure.com**](http://portal.azure.com/) and sign in using a Microsoft account
  2. In the Azure portal, navigate to the **Azure Active Directory** blade
  3. From the **Azure Active Directory** blade, navigate to the **overview** blade and identify the primary DNS (Domain Name System) domain name associated with the Azure AD tenant. (Note its value - you will need it later in this task)



* 1. From the Azure AD **Overview** blade, navigate to the **Users - All users'** blade



* 1. From the **Users - All users** blade, create a new user with the following settings:

Username: **aaduser305011@*<DNS-domain-name>*** where ***<DNS-domain-name>*** represents the primary DNS domain name you identified earlier in this task.

Name: **aaduser305011**

First name: Not set

Last name: Not set

Password: Auto-generate password

Password: Select the checkbox **Show Password** and note the string appearing in the **Password** text box (You will need it later in this lab)

Groups: **0 groups selected**

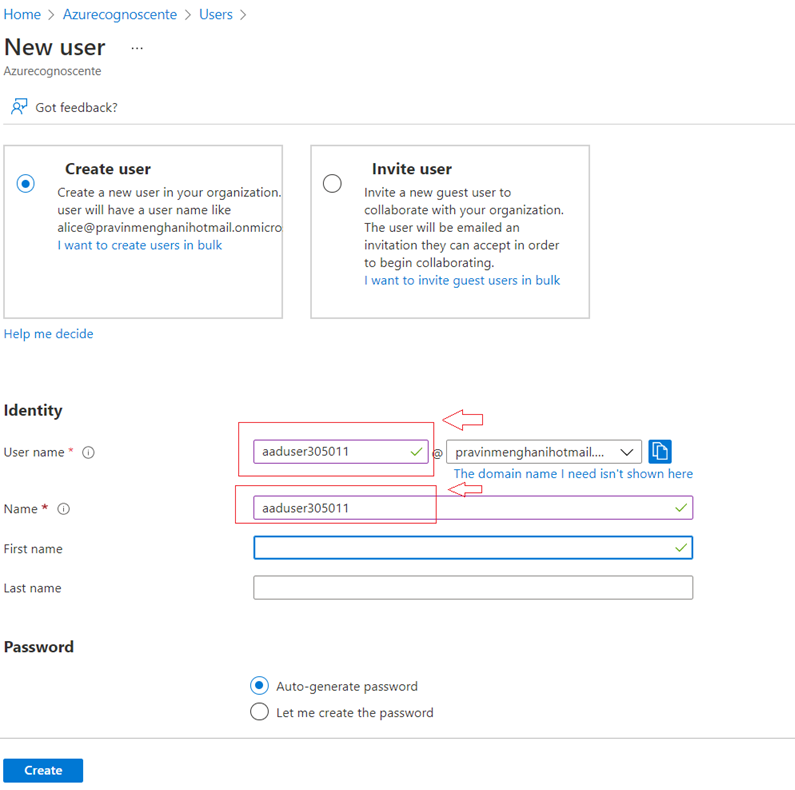
Roles: **User**

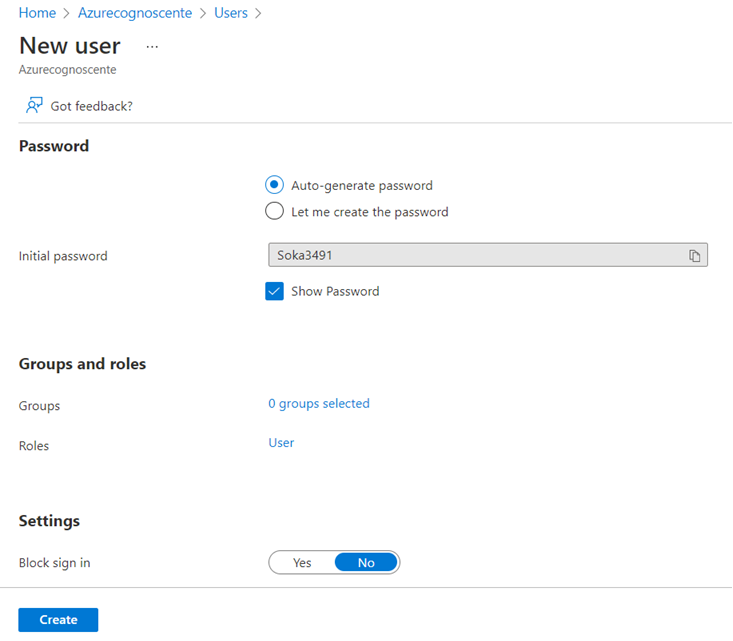
Block sign in: **No**

Usage location: **United States**

Job title: Not set

Department: Not set





* 1. From the **Users - All users** blade, navigate to the **Groups - All groups** blade
  2. From the **Groups - All groups** blade, create a new group with the following settings:

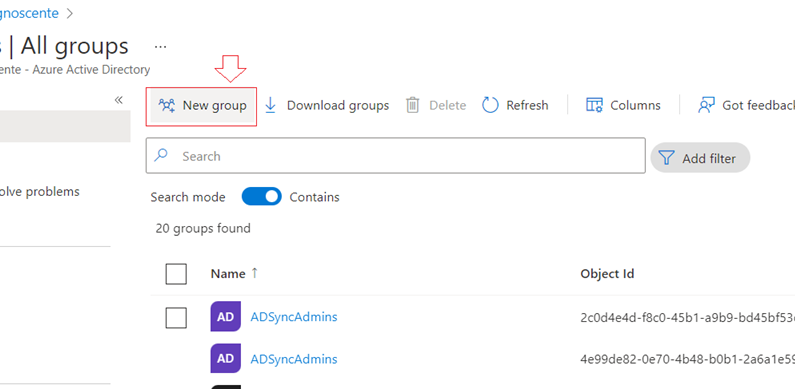
Group type: **Security**

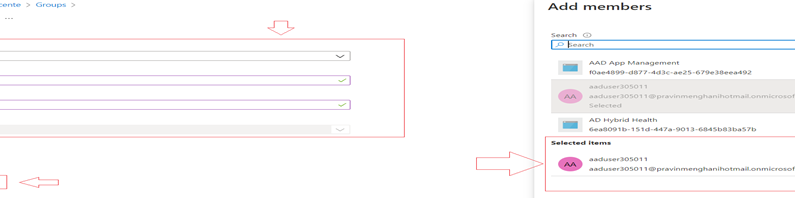
Group name: **az3051 Contributors**

Group description: **az3051 Contributors**

Membership type: **Assigned**

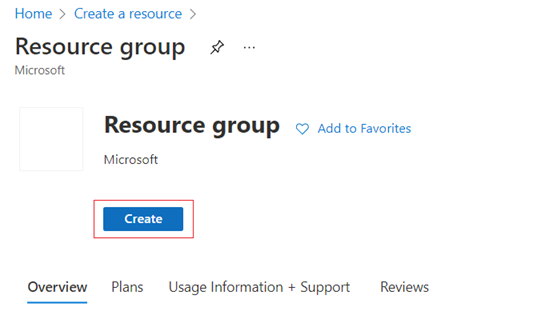
Members: **aaduser305011**





**Step 2: Create Azure resource groups**

* 1. In the Azure portal, navigate to the **Resource groups** blade



* 1. From the **Resource groups** blade, create the first resource group with the following settings:

Resource group name: **az3050101-RG**

Subscription: The name of the subscription you are using in this lab

Resource group location: The name of the Azure region which is closest to the lab location and where you can provision Azure VMs (virtual machines)

* 1. From the **Resource groups** blade, create the second resource group with the following settings:

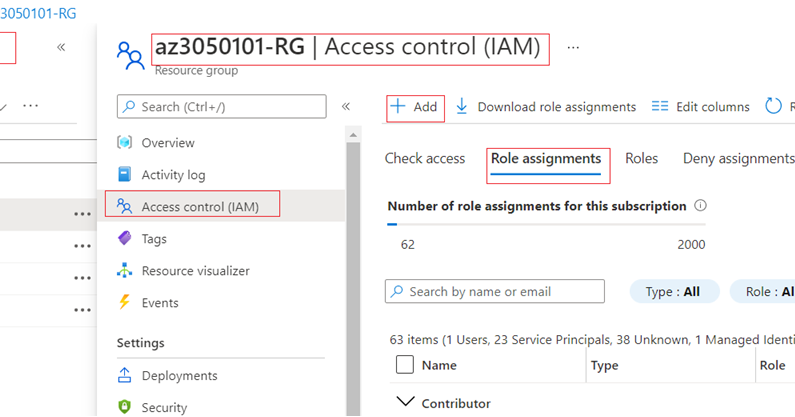
Resource group name: **az3050102-RG**

Subscription: The name of the subscription you selected in the previous step

Resource group location: The name of the Azure region you selected in the previous step

**Step 3: Delegate management of an Azure resource group via a built-in RBAC role**

* 1. In the Azure portal, from the **Resource groups** blade, navigate to the **az3050101-RG** blade
  2. From the **az3050101-RG** blade, display its **Access control (IAM)** blade
  3. From the **az3050101-RG - Access control (IAM)** blade, display the **Role assignments** blade

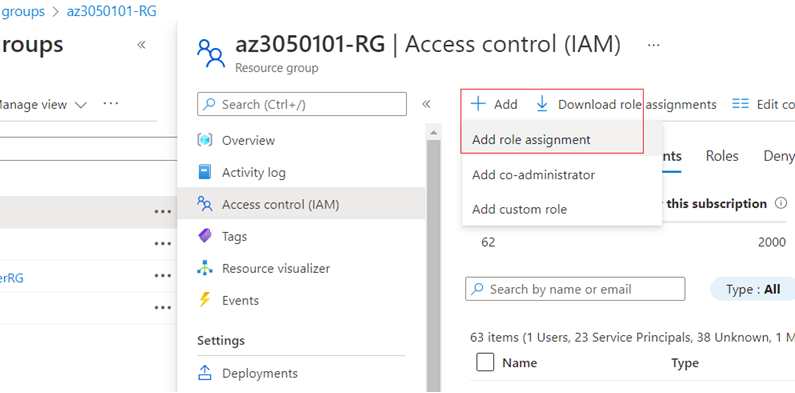


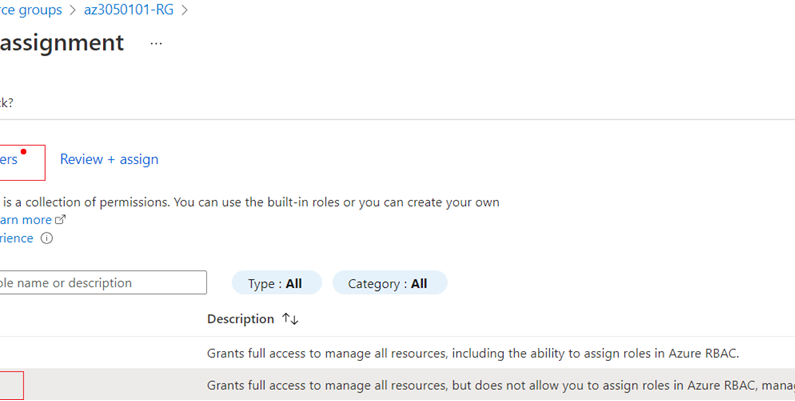
* 1. From the **Role assignments** blade, create the following **role assignment**:

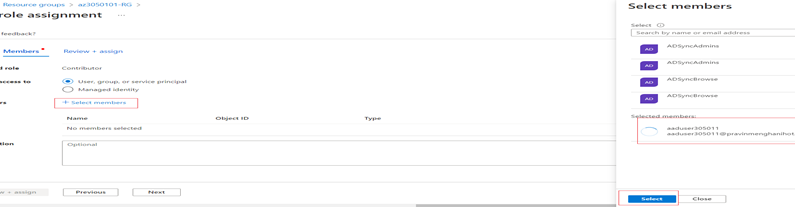
Role: **Contributor**

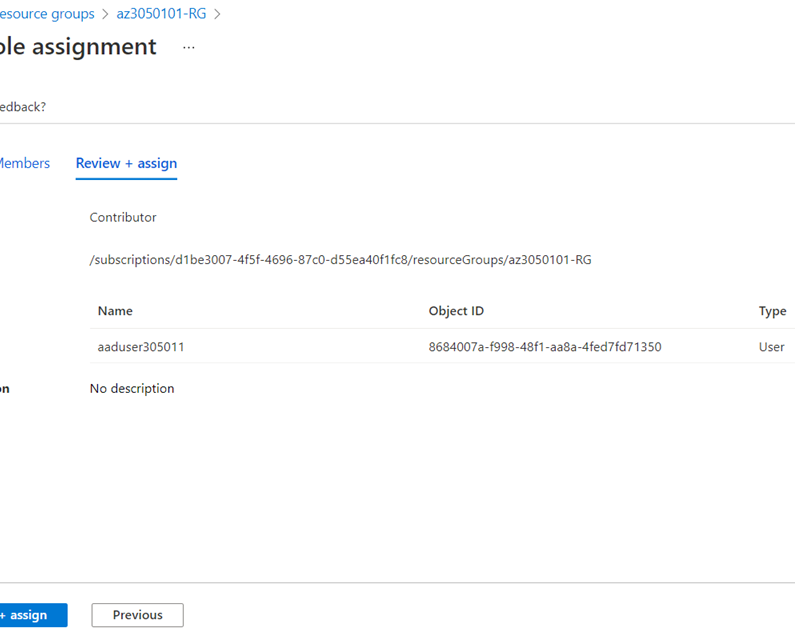
Assign access: **Azure AD user, group, or service principal**

Select: **az3051 Contributors**



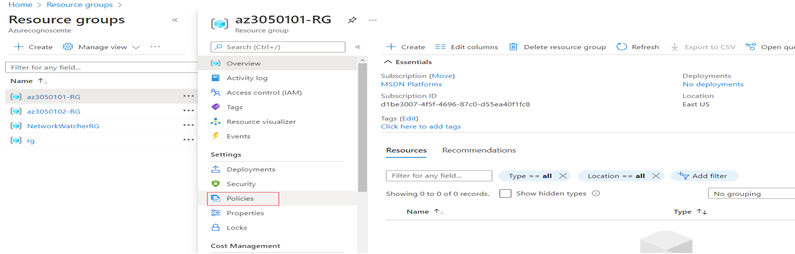




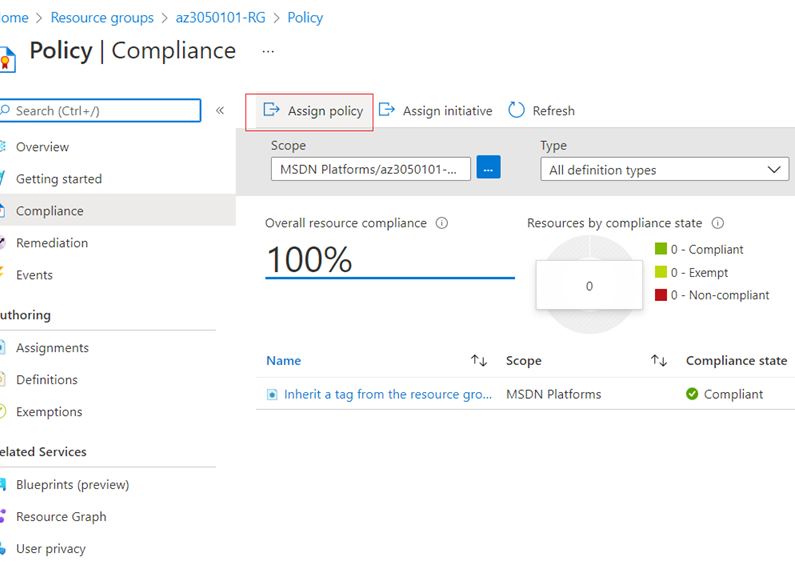


**Step 4: Assign a built-in Azure policy to an Azure resource group**

* 1. From the **az3050101-RG** blade, display its **Policies** blade



* 1. From the **Policy - Compliance** blade, display the **Assign policy** blade



* 1. Assign the policy with the following settings under the basics tab:

Scope: ***<name of the subscription you are using in this lab>*/az3050101-RG**

Exclusions: Leave the entry blank

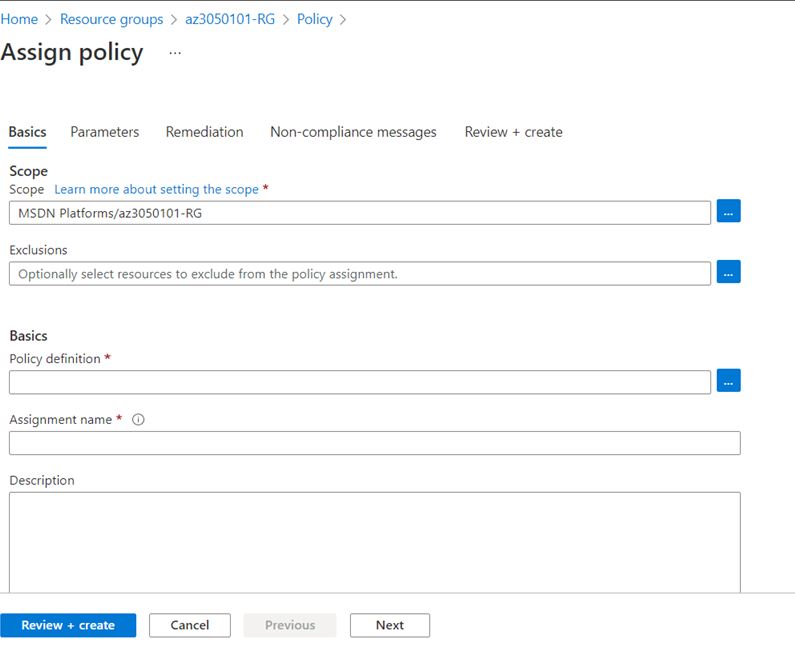
Policy definition: **Allowed virtual machine SKUs**

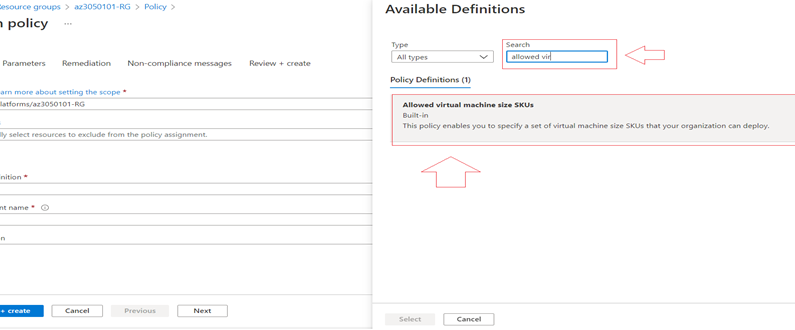
Assignment name: **Allowed virtual machine SKUs**

Description: **Allowed selected virtual machine SKUs (Standard\_DS1\_v2)**

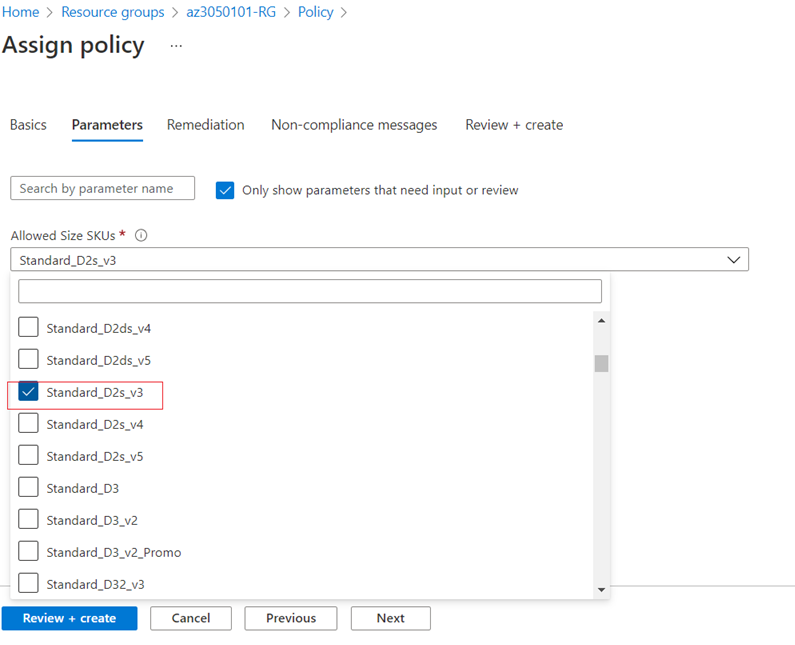
Policy enforcement: **Enabled**

Assigned by: Leave the entry set to its default value





Parameter's tab > Allowed SKUs: **Standard\_D2s\_v3**



Remediation tab > Create a Managed Identity: leave the entry blank

**Result**: After you complete this exercise, you have created an Azure AD user and an Azure AD group, two Azure resource groups, delegated management of the first Azure resource group via the built-in Azure VM (Virtual Machine), contributor RBAC role, and assigned the same built-in Azure policy restricting SKUs that can be used for Azure VMs to the same resource group.