Azure Security Capstone Project

In this project, I will demonstrate how to apply multiple layers of security to protect a confidential design image for a fictional company called BuyforSure by utilizing the capabilities of Microsoft Azure. To this end, five main tasks need to be performed:

1. Creating users and groups and implementing mandatory multifactor authentication.

2. Creating a resource group and a new Storage account and providing access to users via a SAS token.

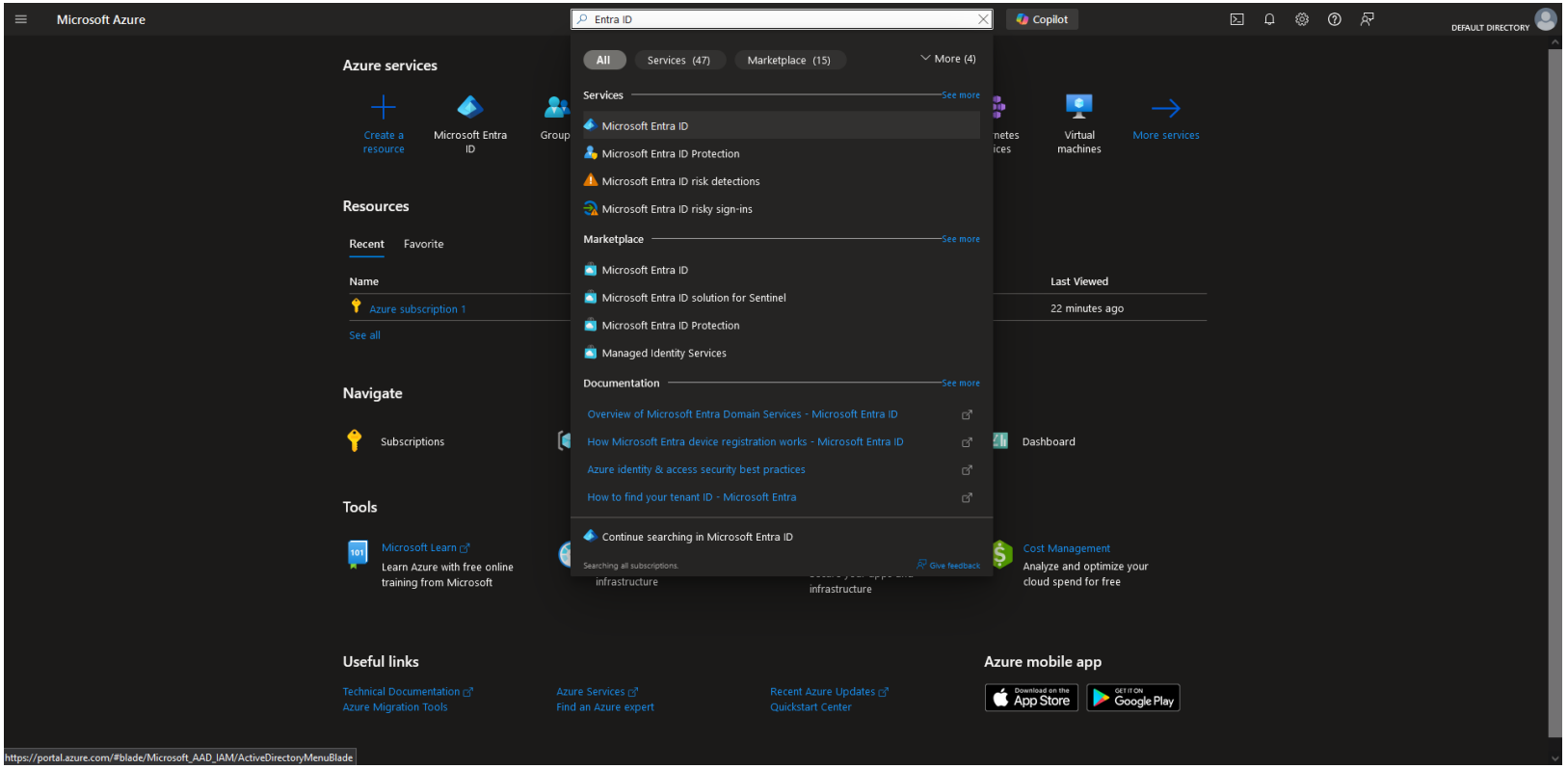
3. Enabling encryption on a Storage account.

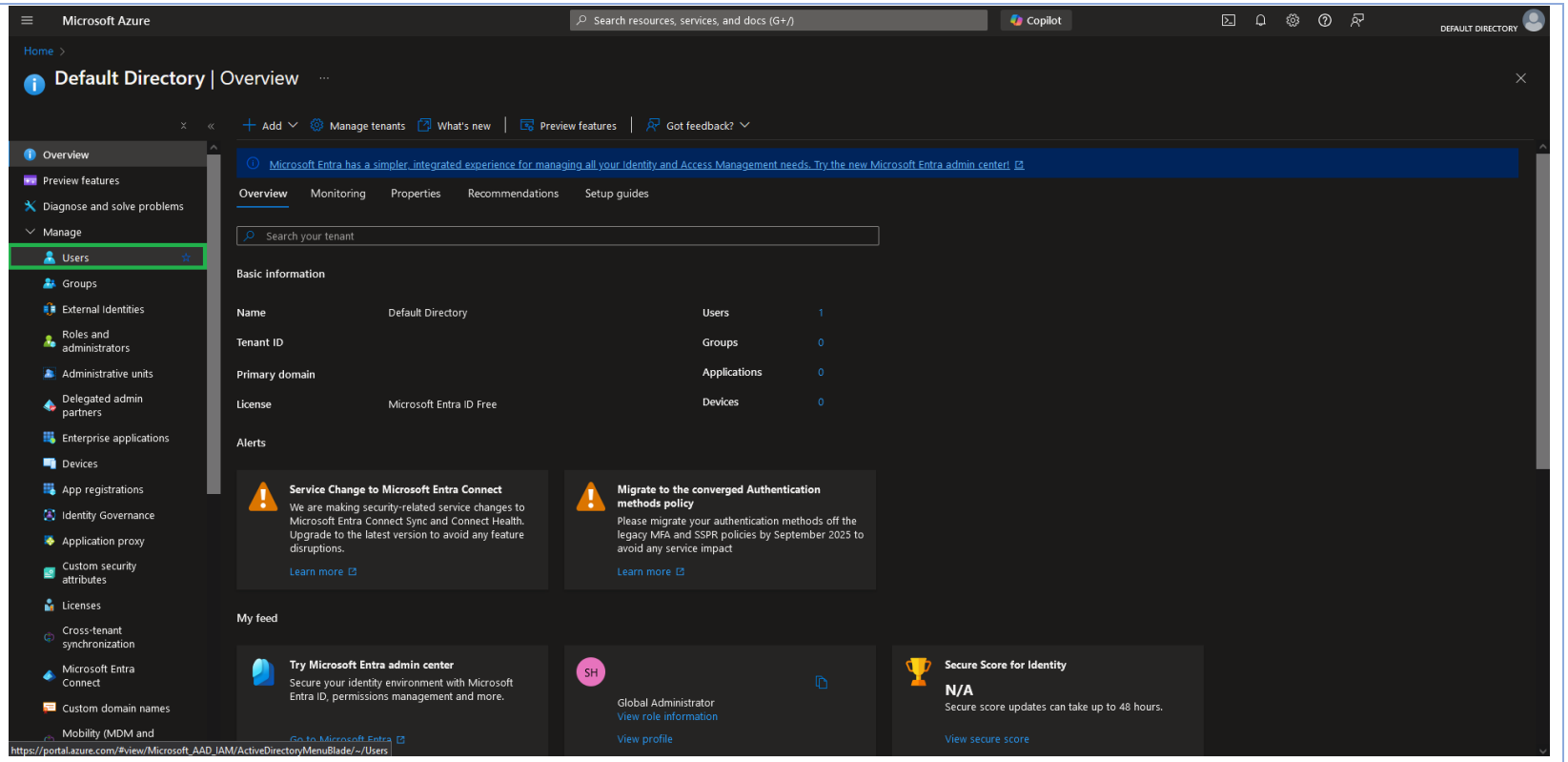
4. Creating a virtual machine and adding a network security group rule to allow inbound traffic on port 3389 for the virtual machine.

5. Implementing Azure security using Defender for Storage and configure diagnostics settings to send data to the Log Analytics workspace.

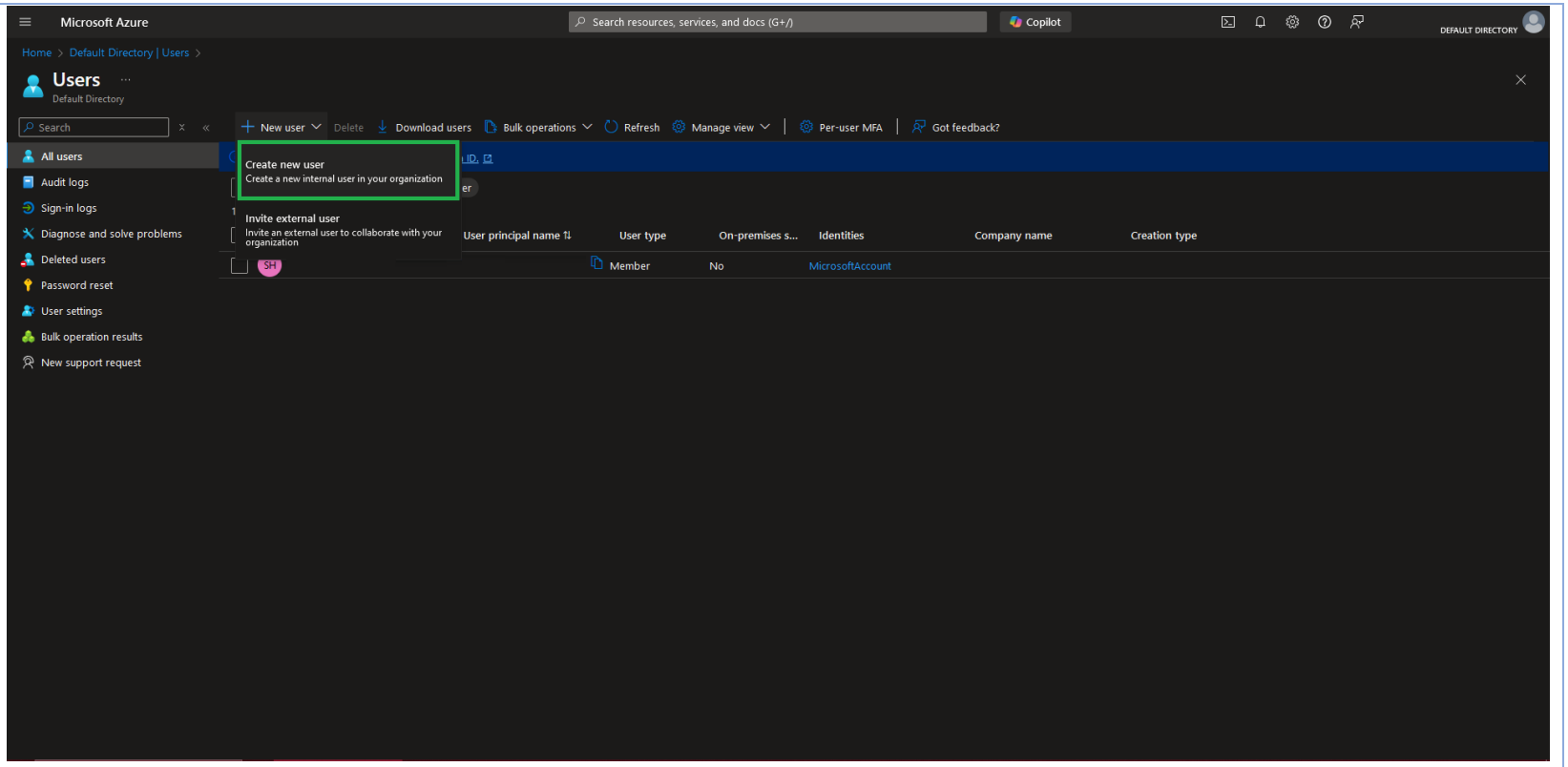
I will thoroughly go through all the required steps for successful deployment. This project was completed on the Azure platform as it was during October 2024. Changes to the Azure UI might have taken place since then but its core functionalities should remain the same.

Task 1: Create a group with three users, assign the Virtual Machine Administrator Login role, and implement multifactor authentication for the users.

Activity	Key evidence
Activity 1: Creating three users in Azure Active Directory (Azure AD).	1. After signing in to the Azure Portal, we type in "Microsoft Entra ID" (*formerly, Azure Active Directory*) into the search box.  2. On the **Default Directory** page, select **Users** under the *Manage* blade.

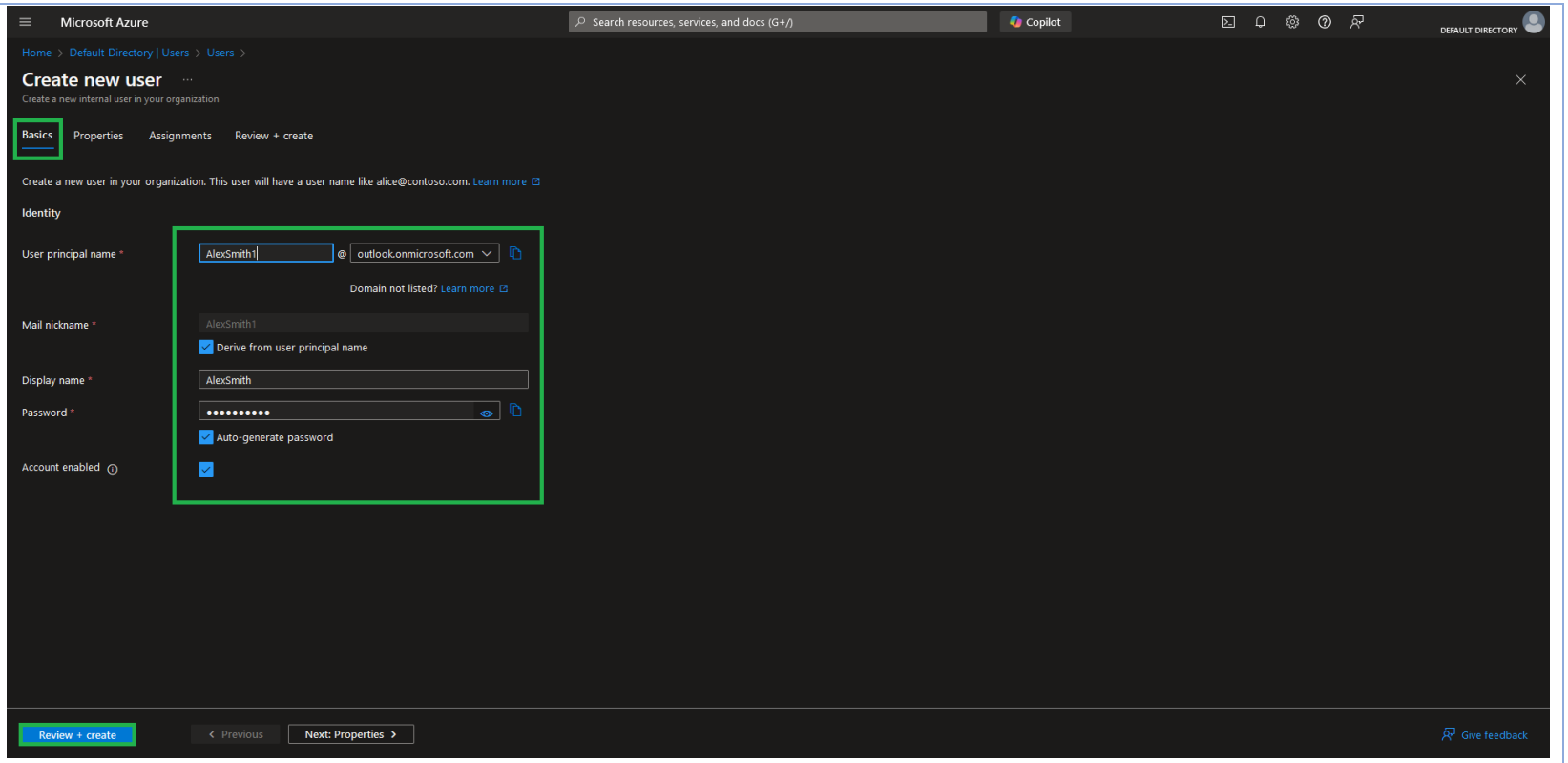


3. Select **Create New User** from the *New User* dropdown menu.



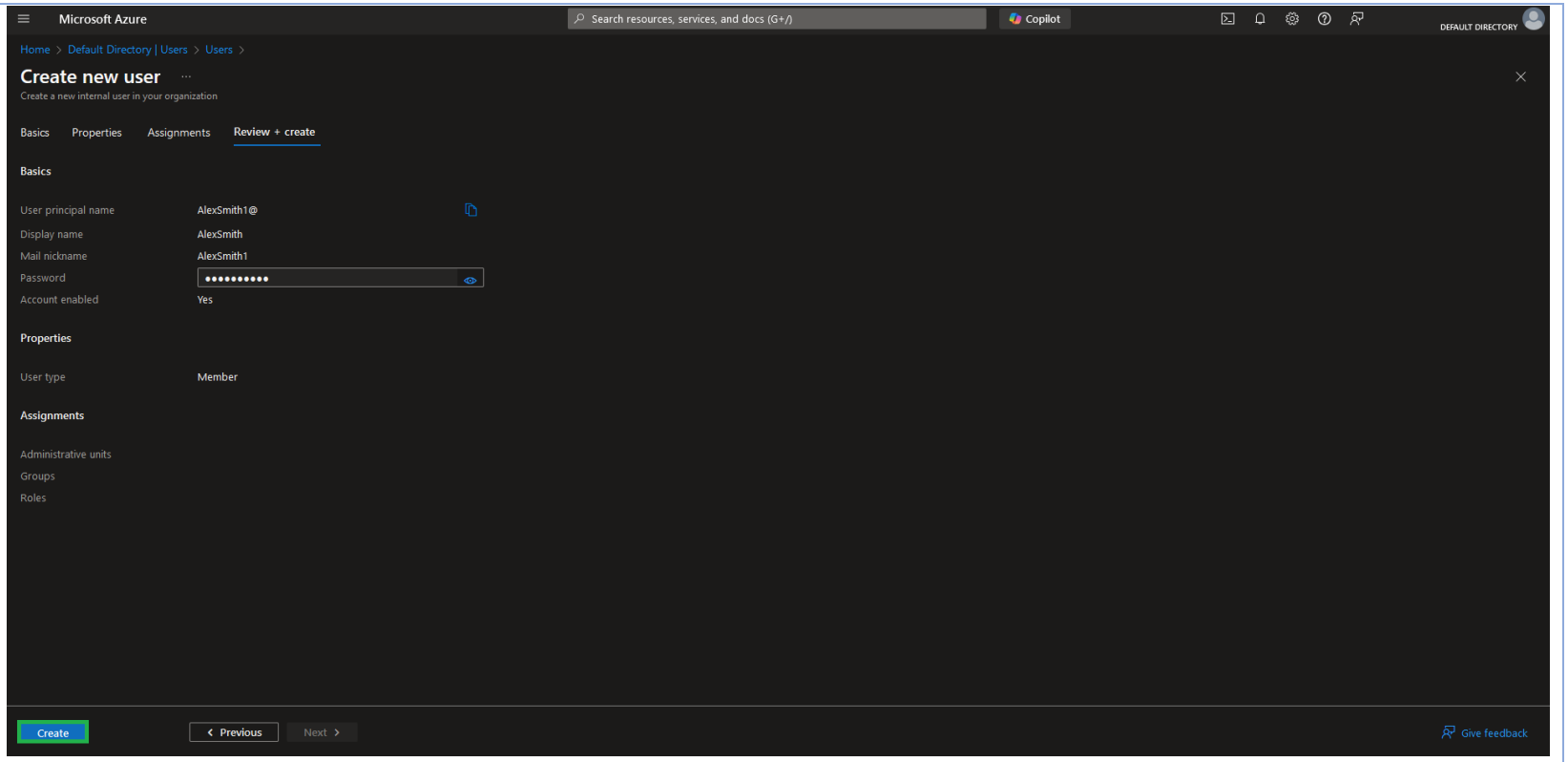
4. We now create a User with the following details on the *Basics* tab, and click on **Review + create**:

Field	Value
User principal name	Enter the username, **AlexSmith1**, and select a domain from the dropdown list beside the **@** symbol.
Mail nickname	Tick the **Derive from user principal name** checkbox.
Display name	Enter the user's name, **AlexSmith**.
Password	Tick the **Auto-generate password** checkbox.
Account enabled	Tick the **Account enabled** checkbox.

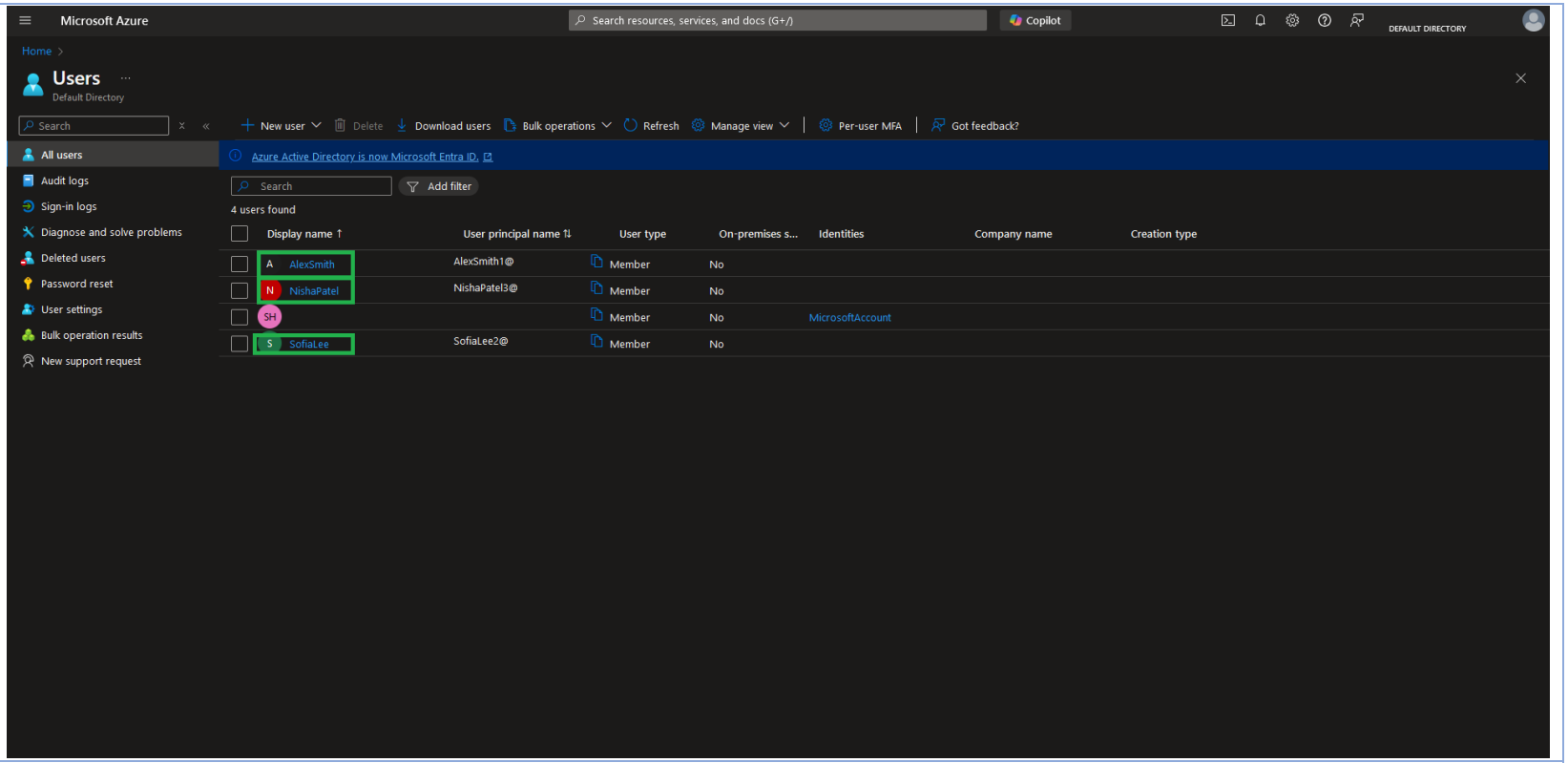


Note: For this project there is no need to add *Properties* or user-level *Assignments*.

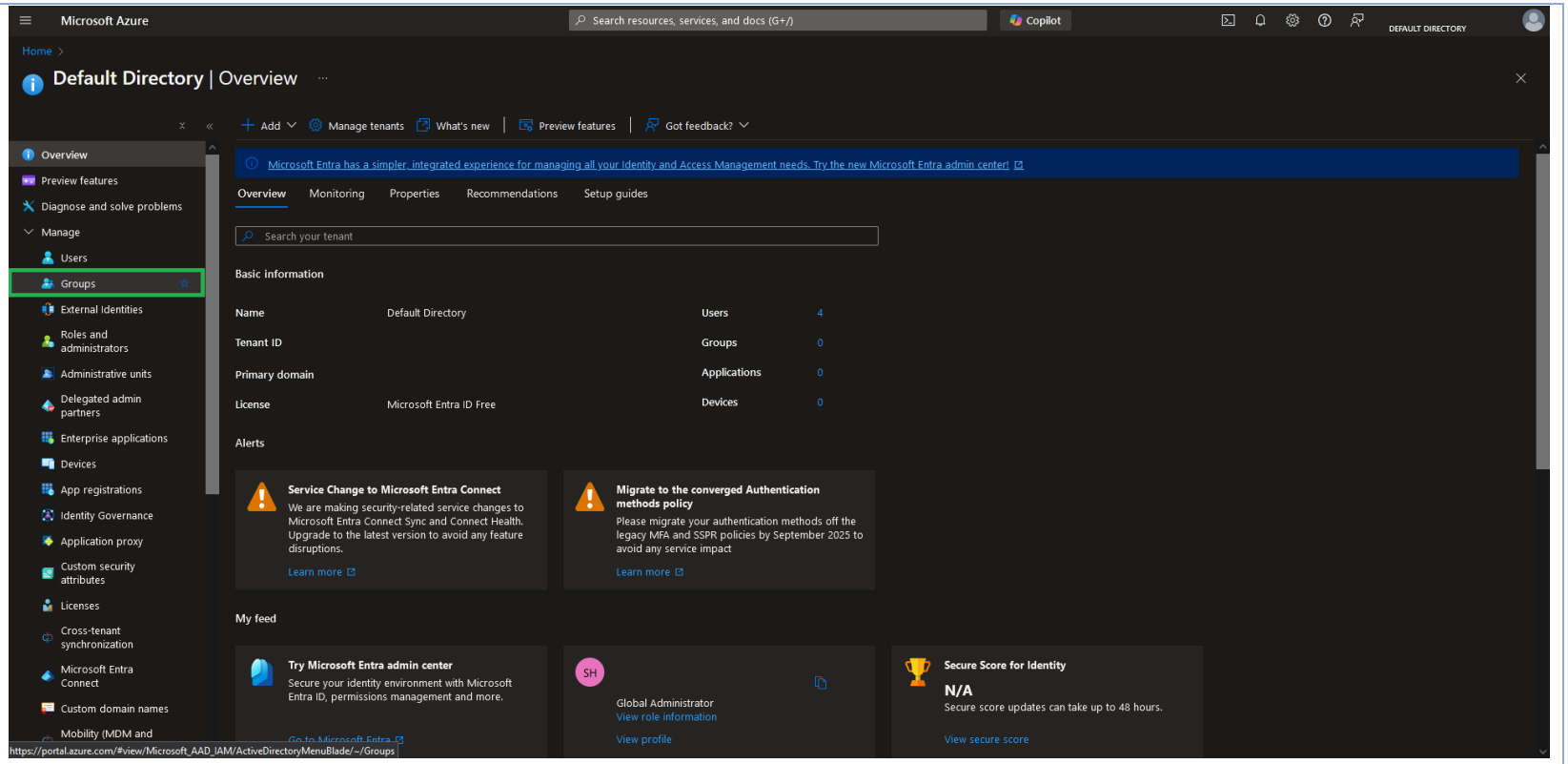
5. We check if all information is correct, and click **Create**



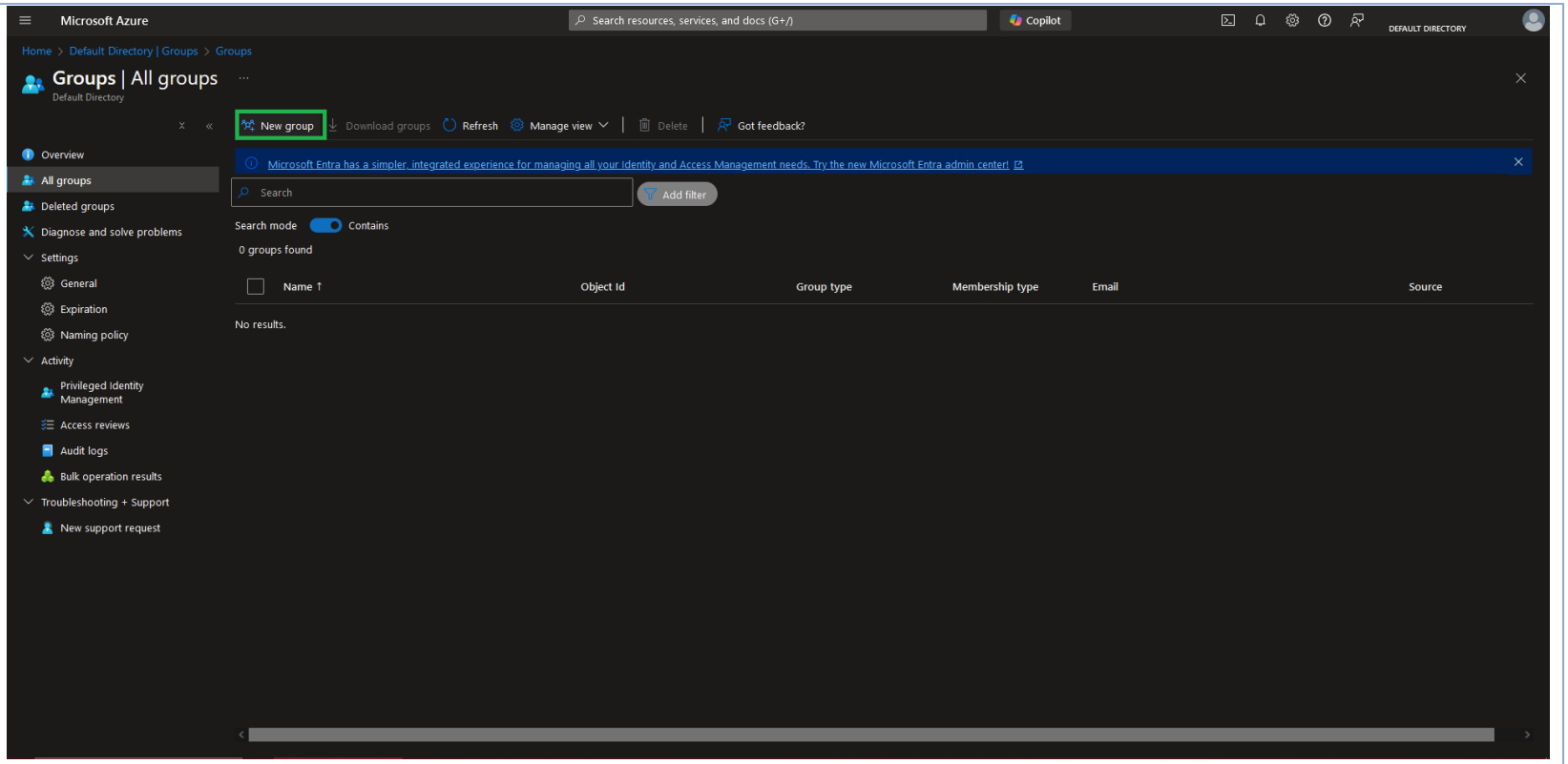
6. The process is then repeated for users **SofiaLee** and **NishaPatel**.
7. After all users are created, we go back to the **Users** page to check all three appear.



Activity 2: Create a group for the three users and assign the Virtual Machine Administrator Login role to this group.	1. We go back to the **Default Directory** page, and select **Groups** under the *Manage* blade.



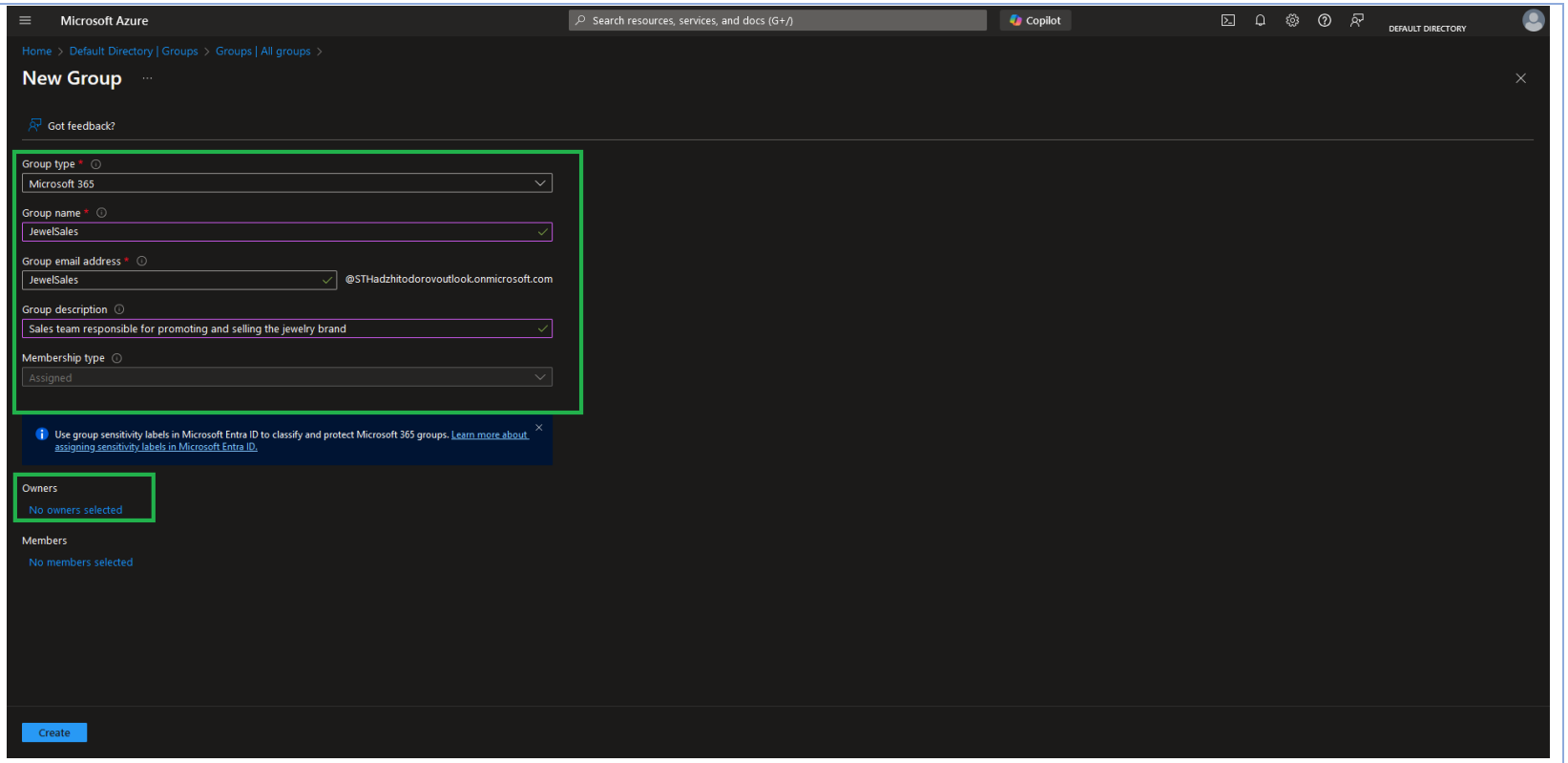
2. On the **Groups** page, we click on **New Group**



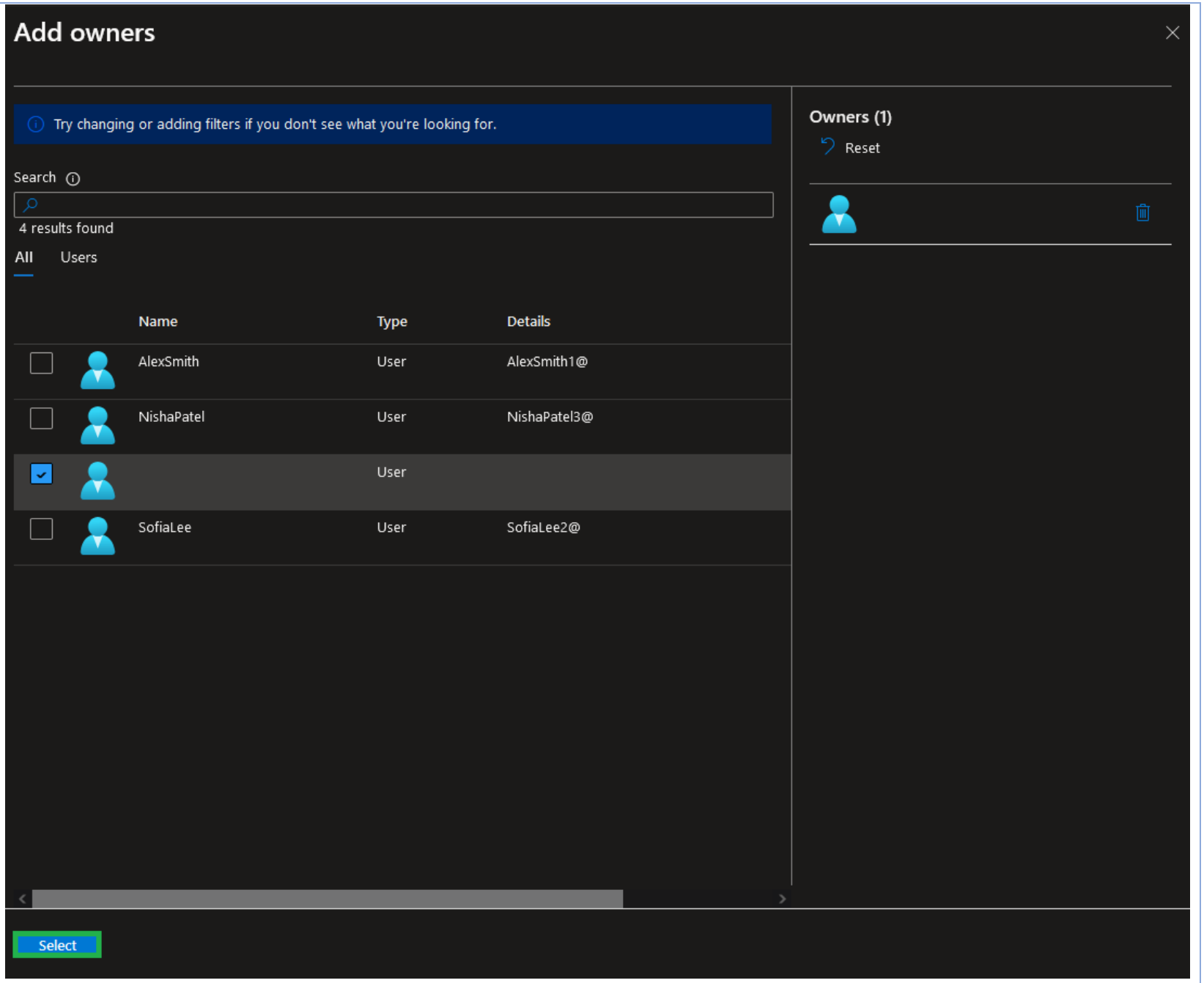
3. We then create a group with the following configuration:

Field	**Value**
Group type	**Microsoft 365**.
Group name	**JewelSales**.
Group email address	The group email address will be automatically populated from the group name.
Group description	A short description such as '**Sales team responsible for promoting and selling the jewelry brand.**'

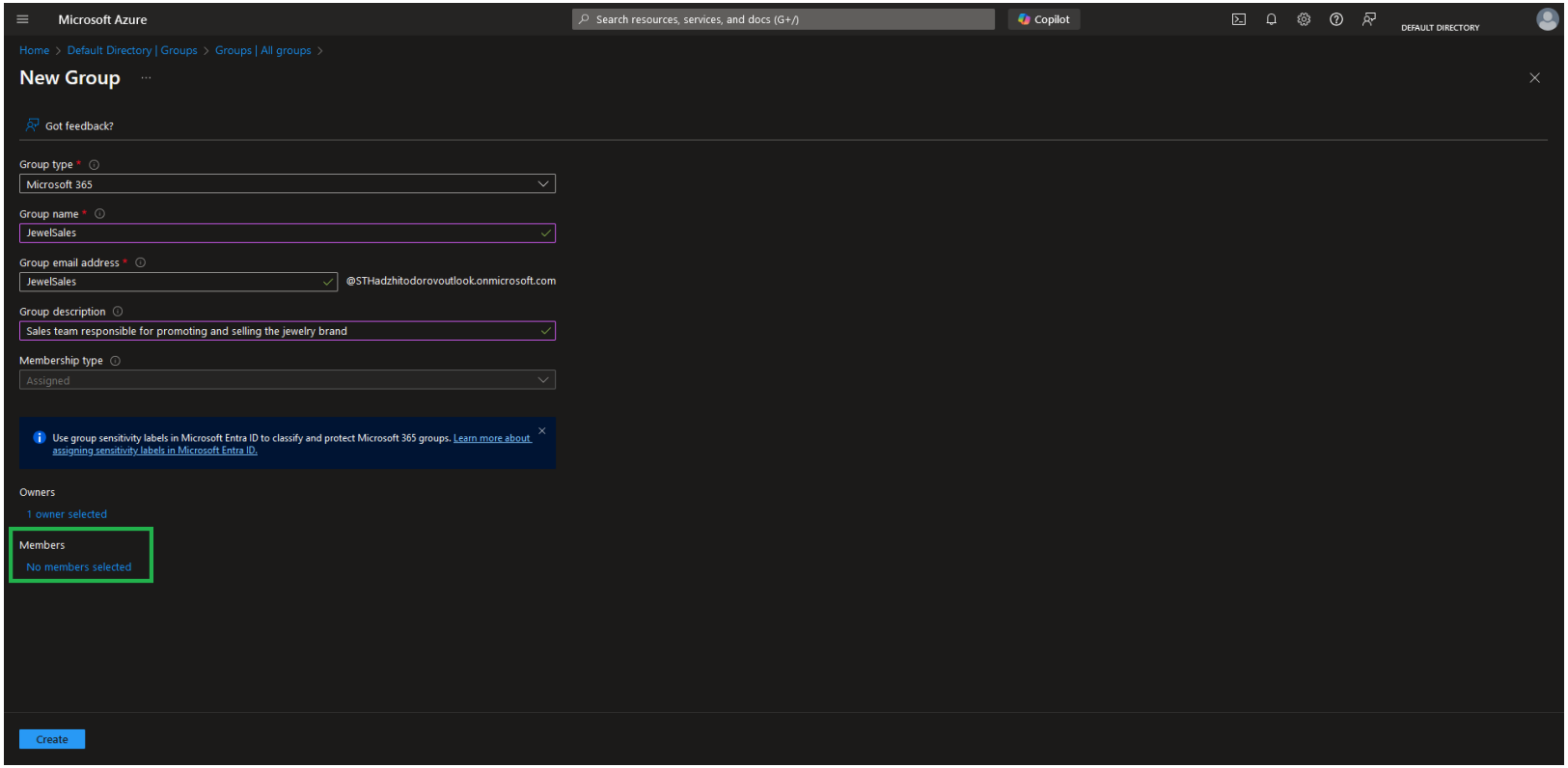
4. Under **Owners**, we click on **No owners selected**.



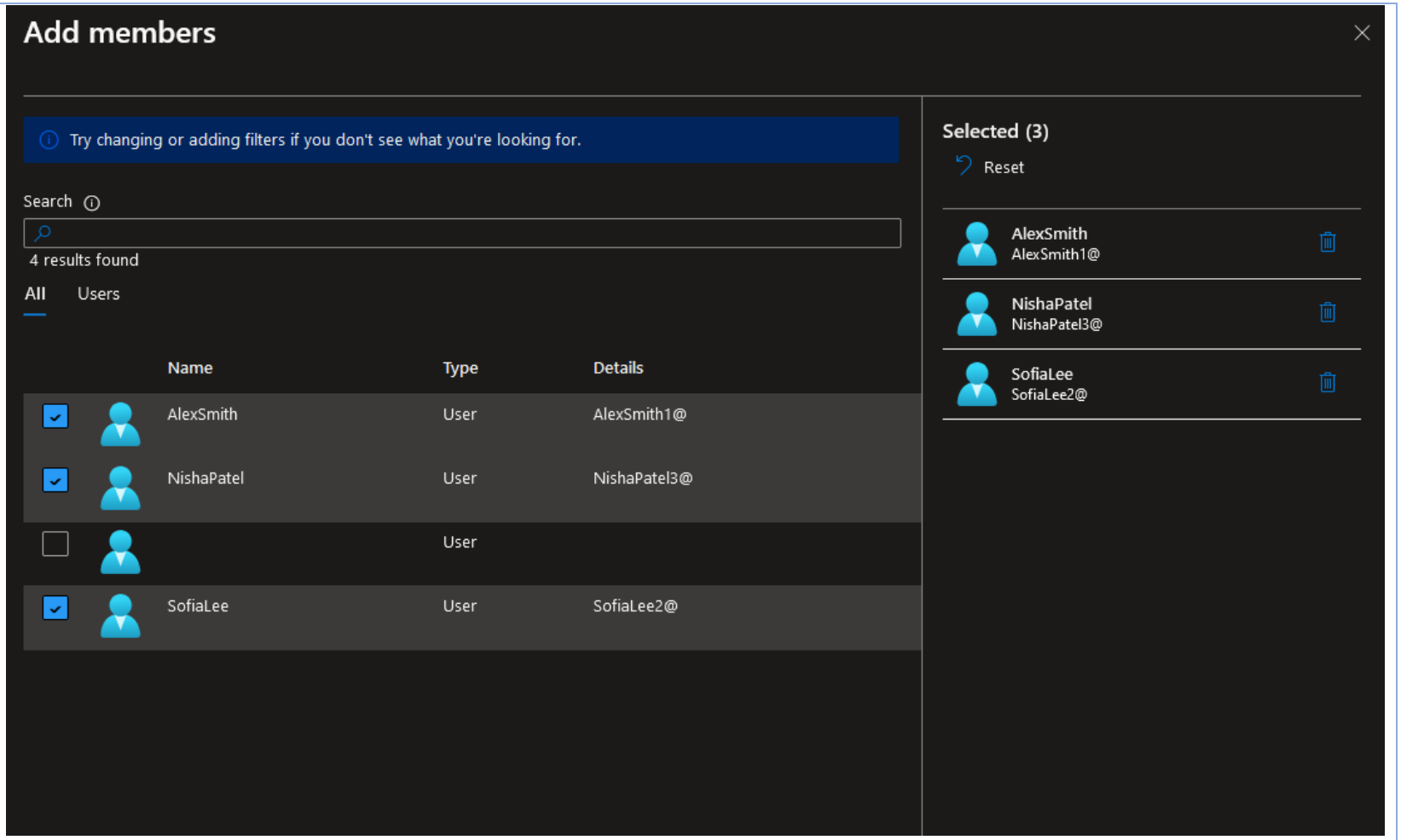
5. On the **Add owners** wizard, we select ourselves as the owner, and confirm by clicking on **Select**.


Add owners
Try changing or adding filters if you don't see what you're looking for.
Search
4 results found
All
Users
Name
Type
Details
AlexSmith
User
AlexSmith1@
NishaPatel
User
NishaPatel3@
User
SofiaLee
User
SofiaLee2@
Owners (1)
Reset
Select

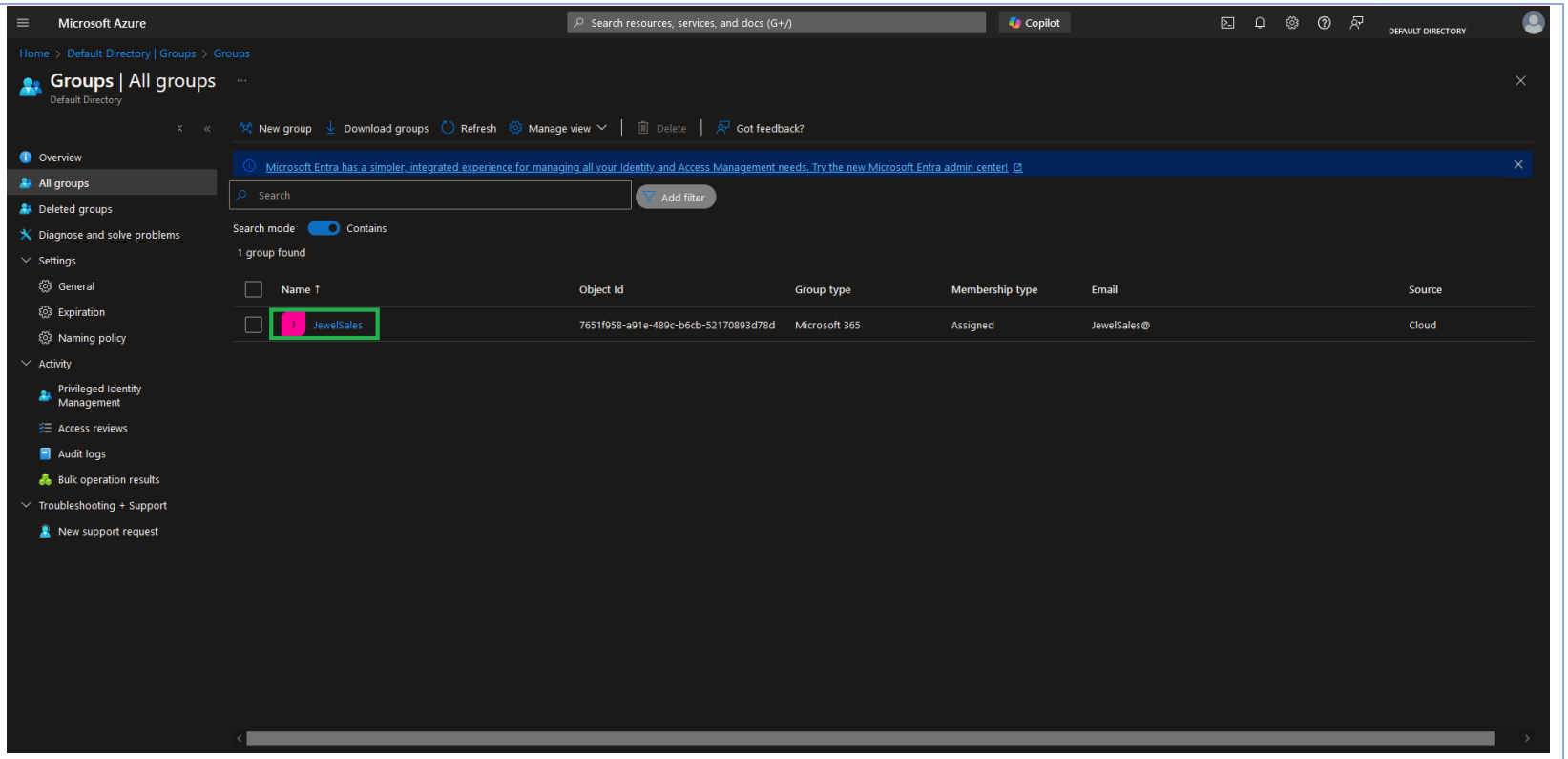
6. We then click on **No members selected** in the **Members** section



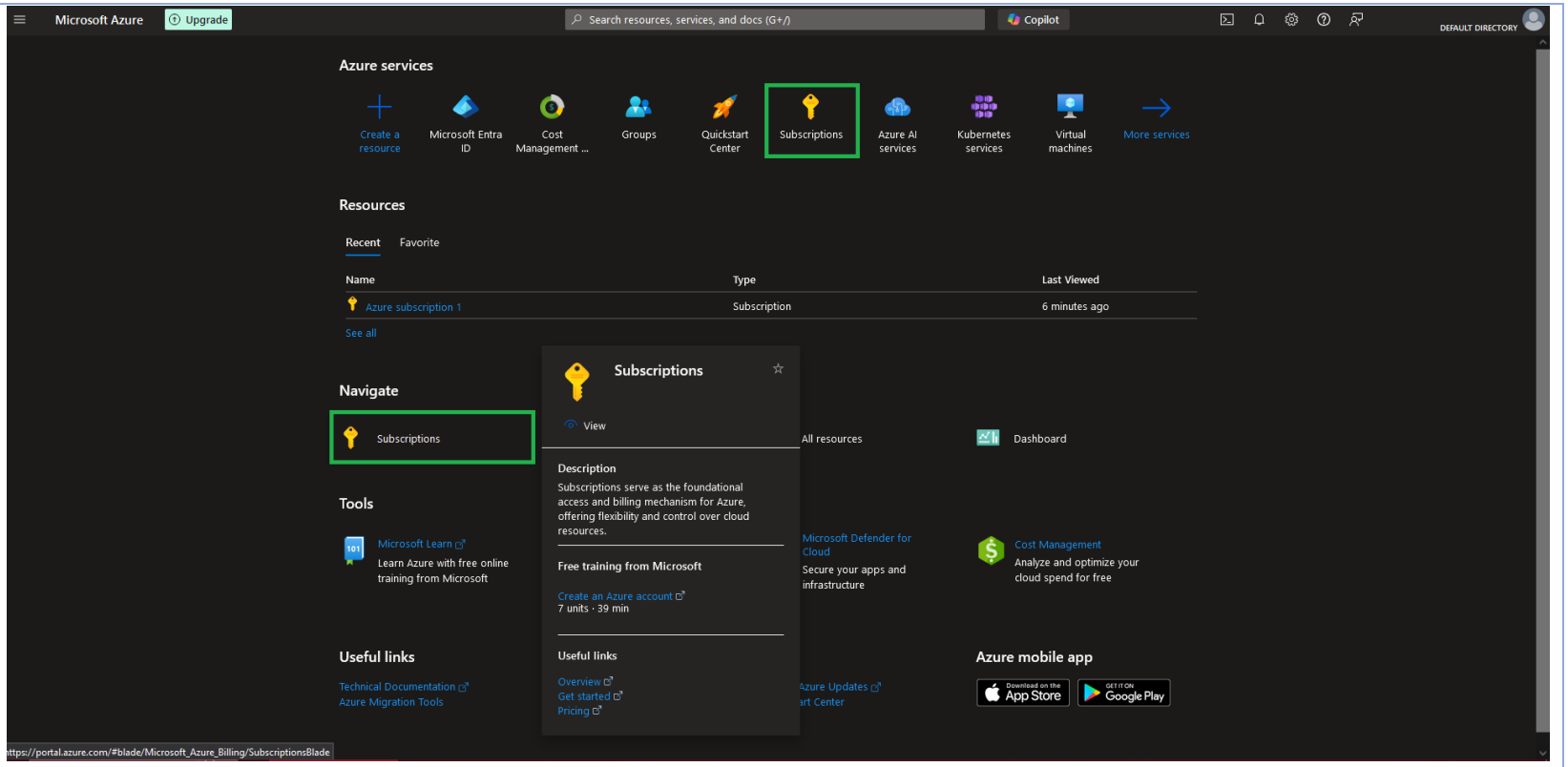
7. In the **Add members** wizard, we then select the three users we just created, and click on **Select**.



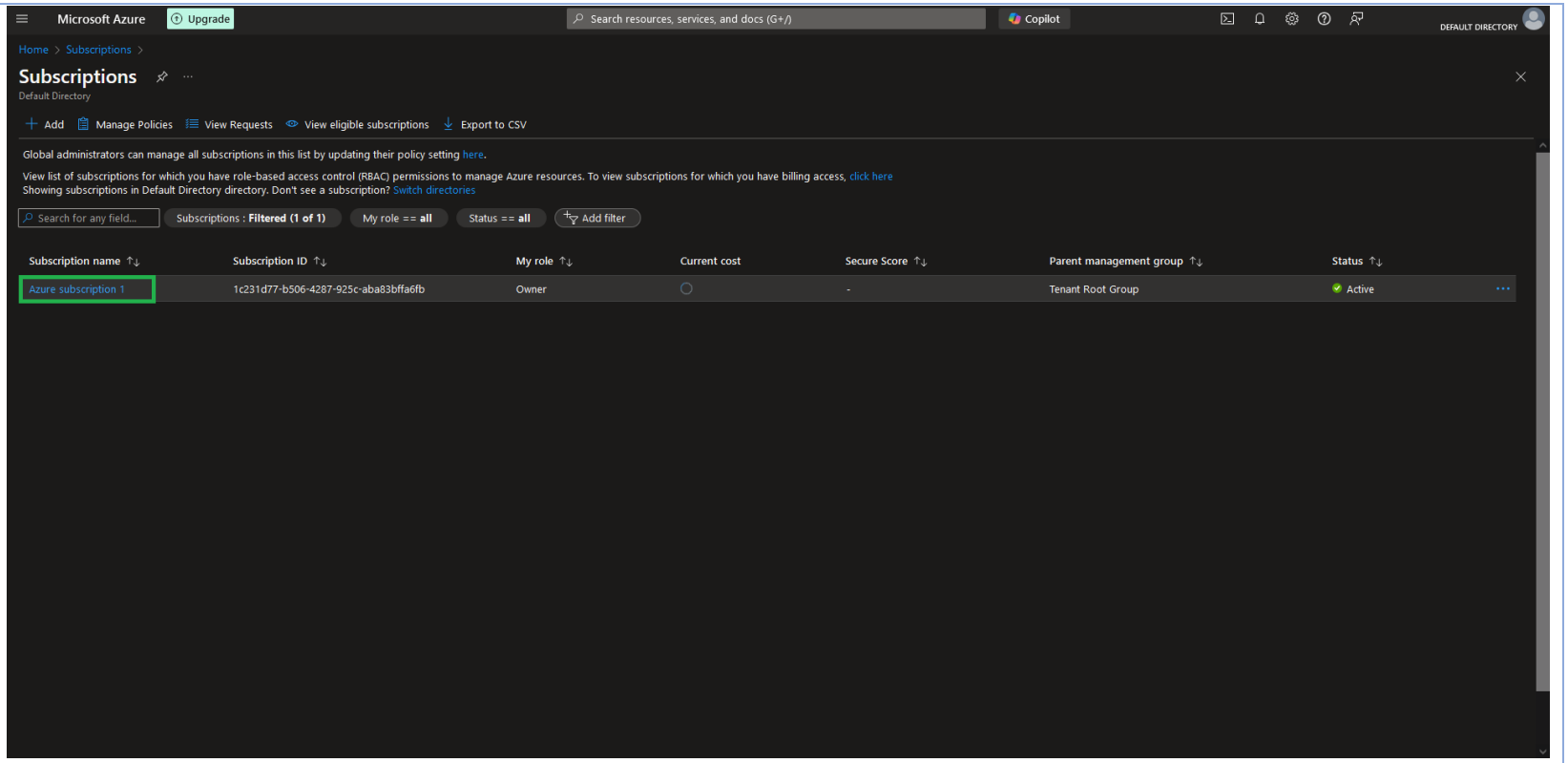
8. We then select **Create** on the **New Group** page, and go back to the **All groups** page to check if everything is in order.



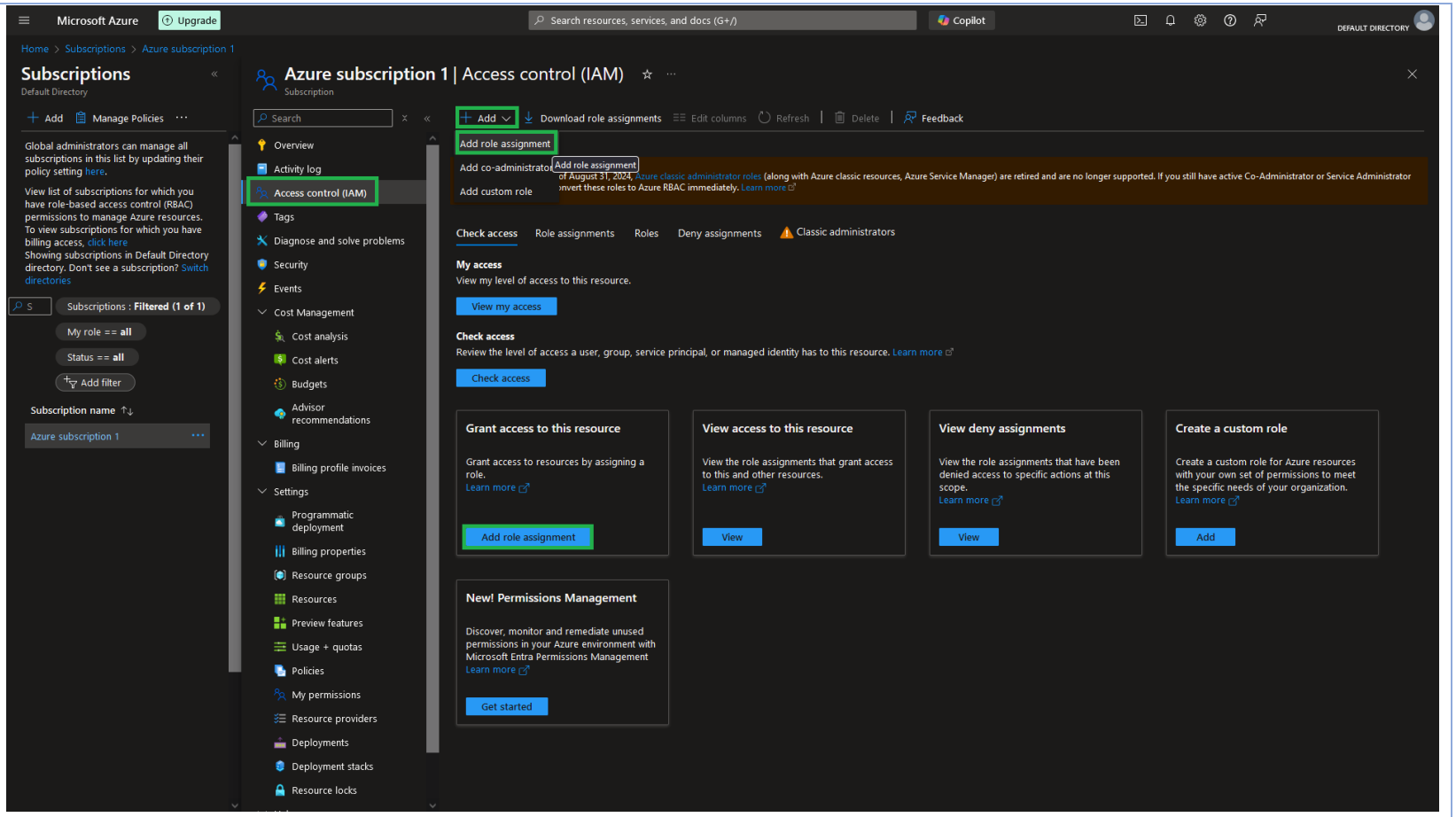
9. After this, we navigate back to the home page, and select **Subscriptions**



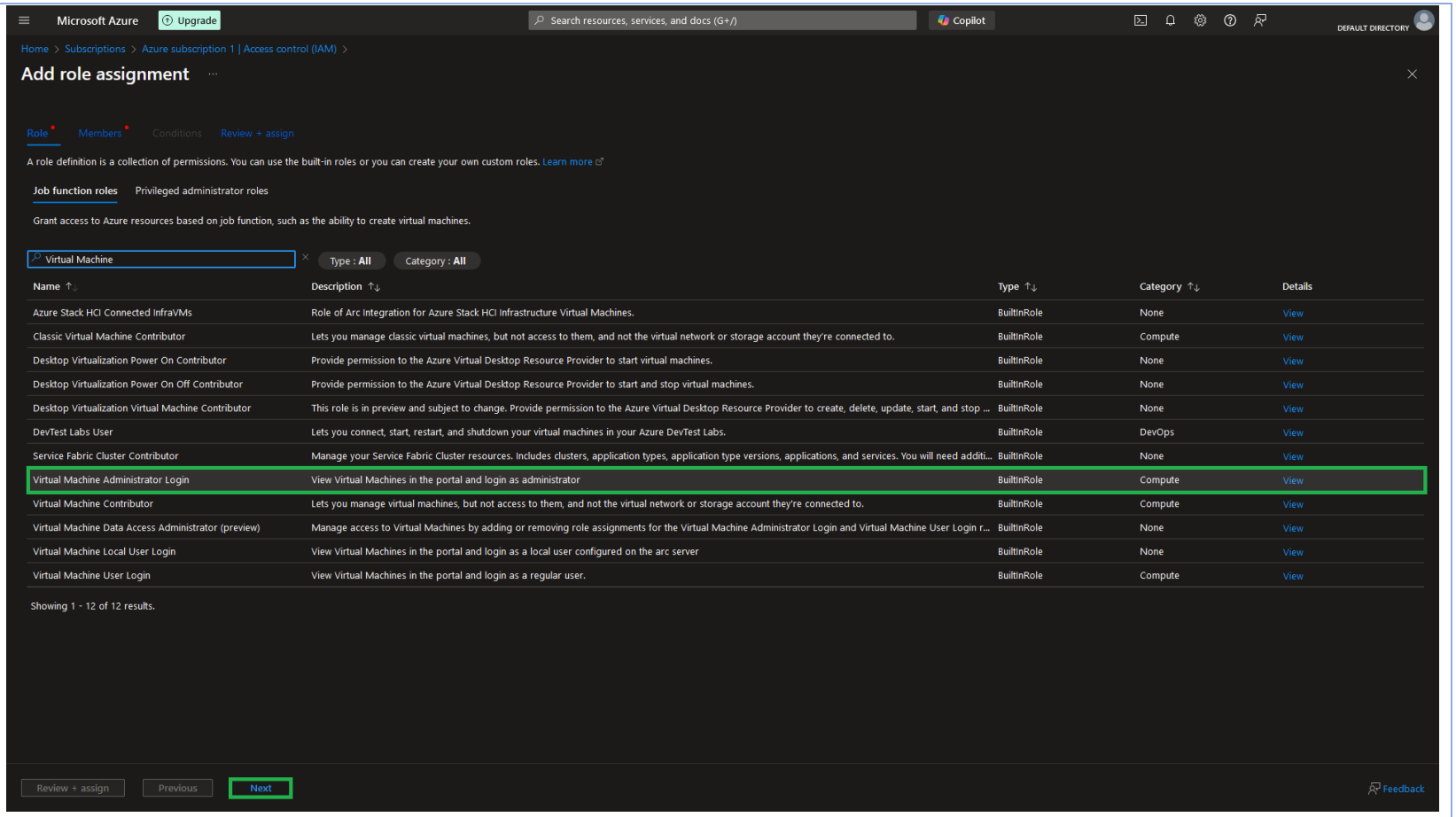
10. On the **Subscriptions** page, we click on our current subscription.



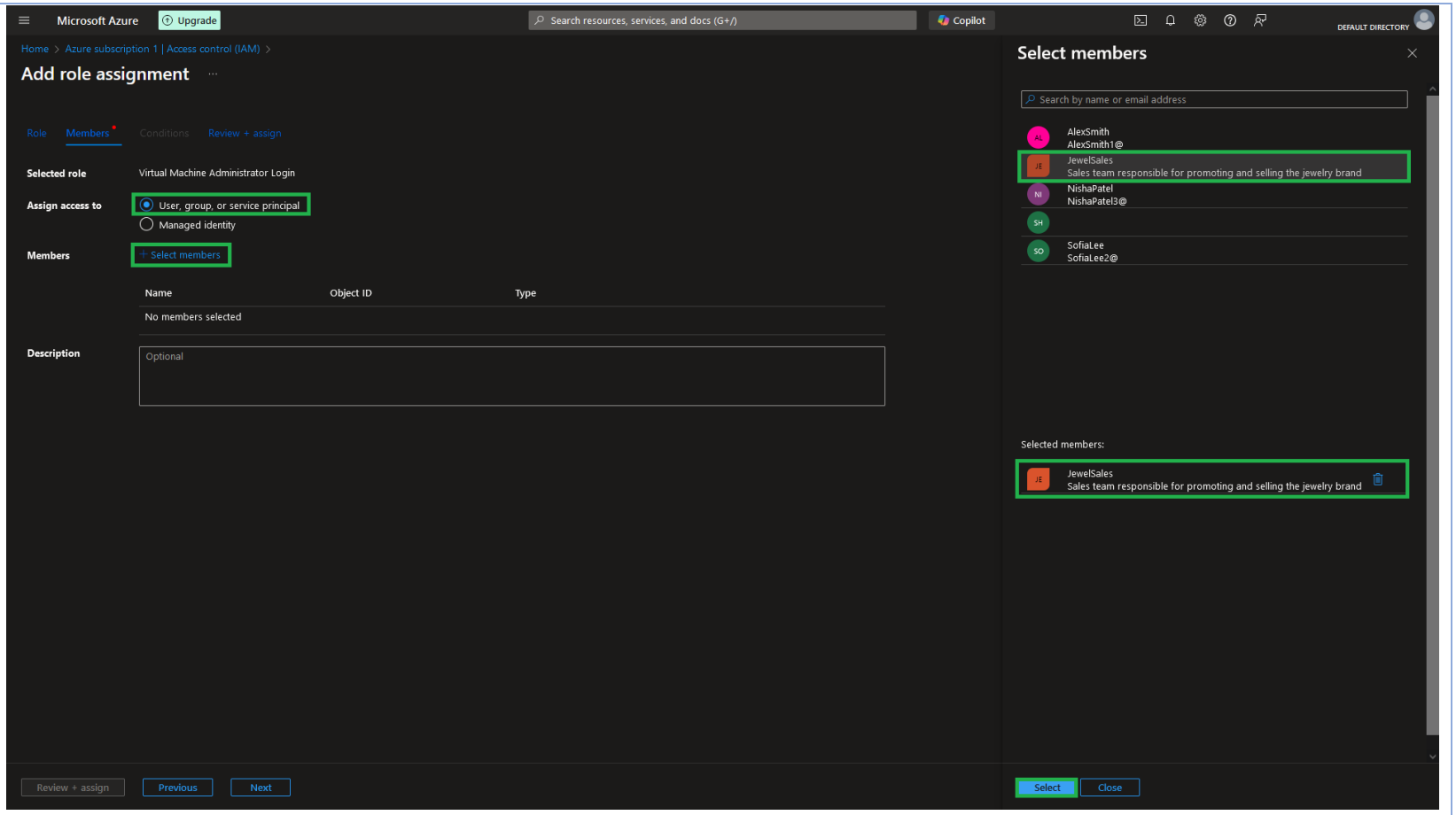
11. From the menu on the left, we click on **Access control (IAM)**, and select **Add role assignment** from the **Access control (IAM)** page.



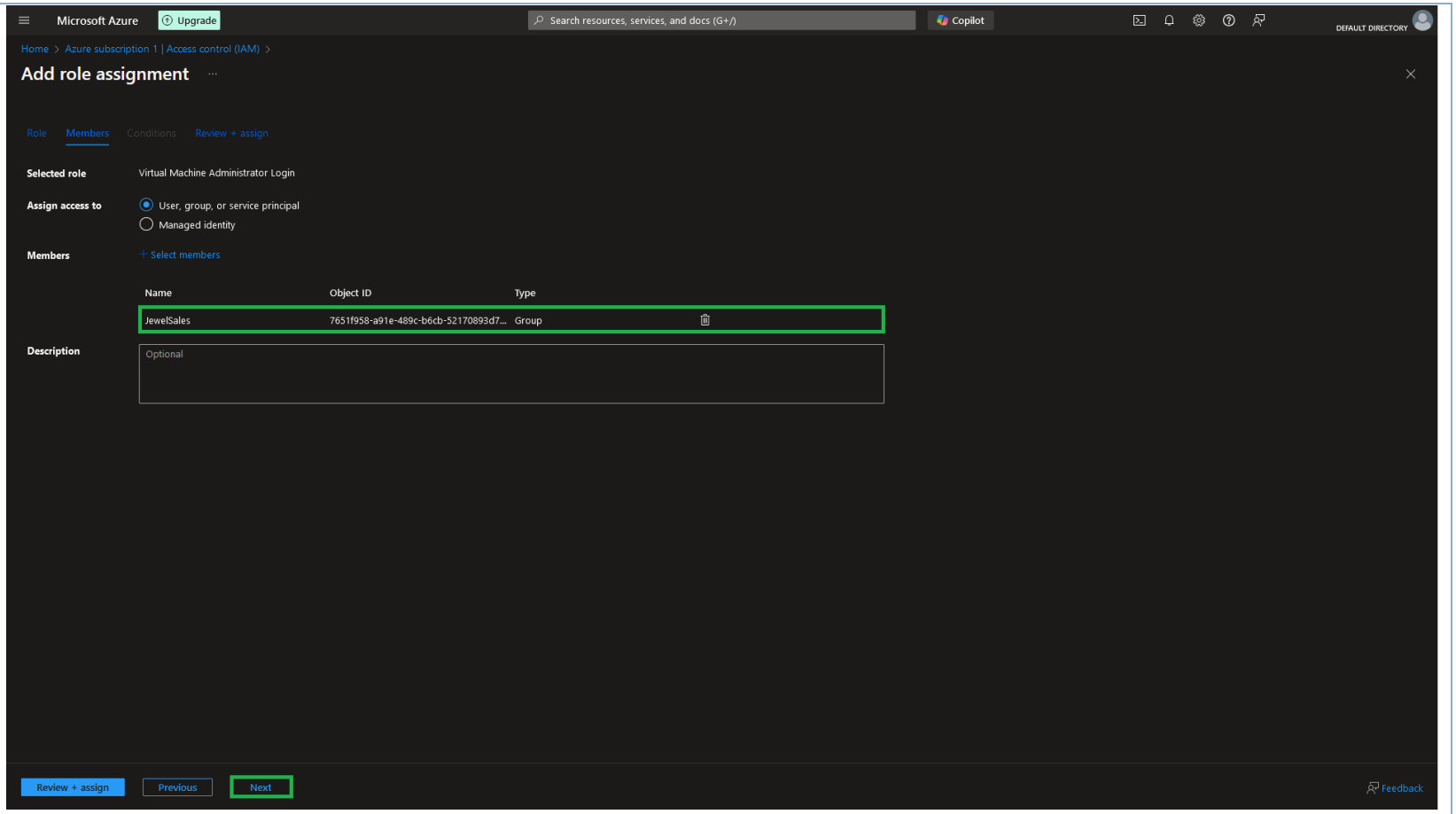
12. On the **Add role assignment** page, we either scroll down or use the search box to find the **Virtual Machine Administrator Login** role, and click on **Next**.



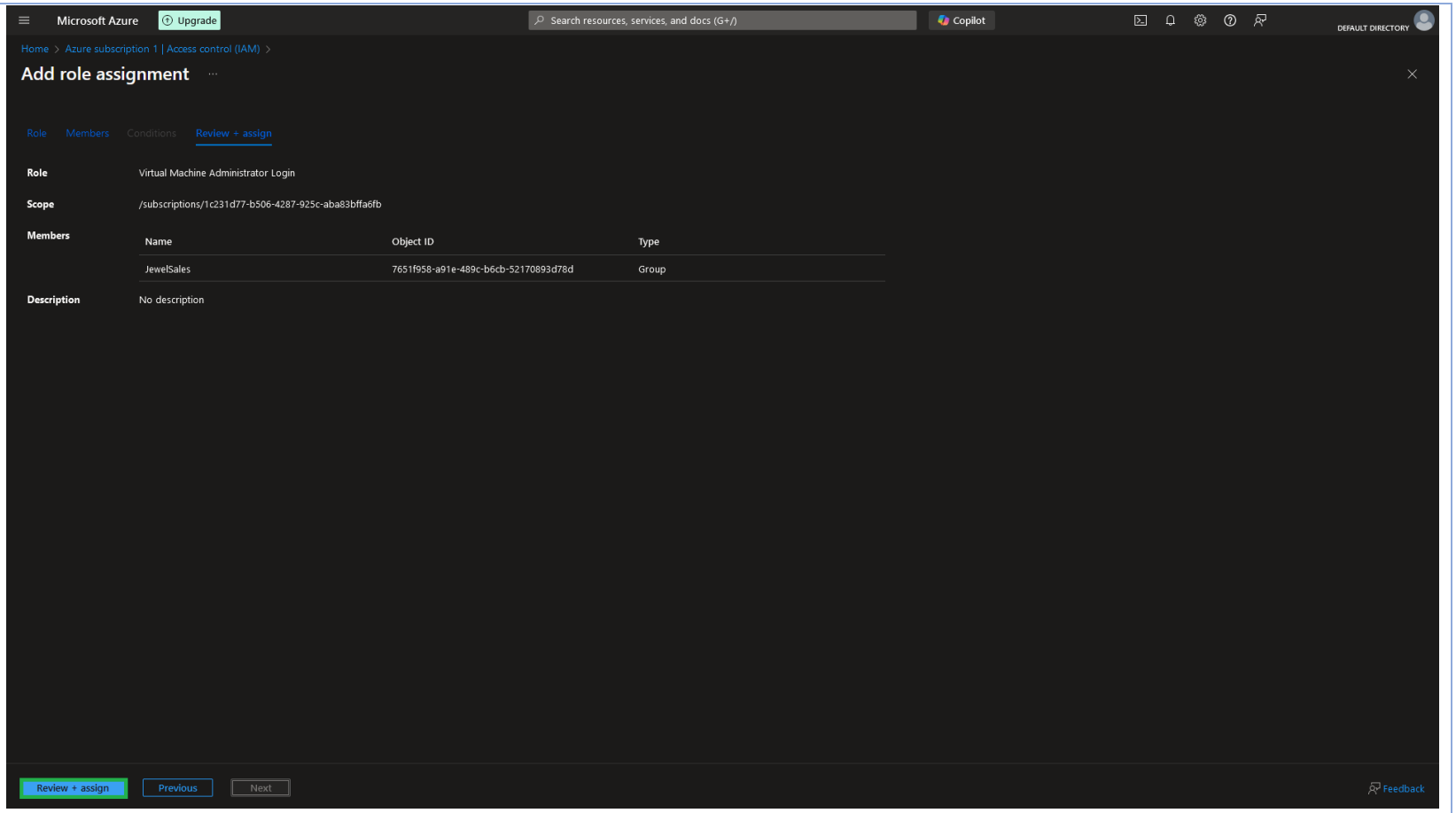
13. Then, on the **Add role assignment**, we select the **User, group, or service principal** radio button in the **Assign access to** section
14. After that, in the Members section, we click on **Select members**, choose the **JewelSales** group we created earlier, and confirm our decision with the **Select** button.



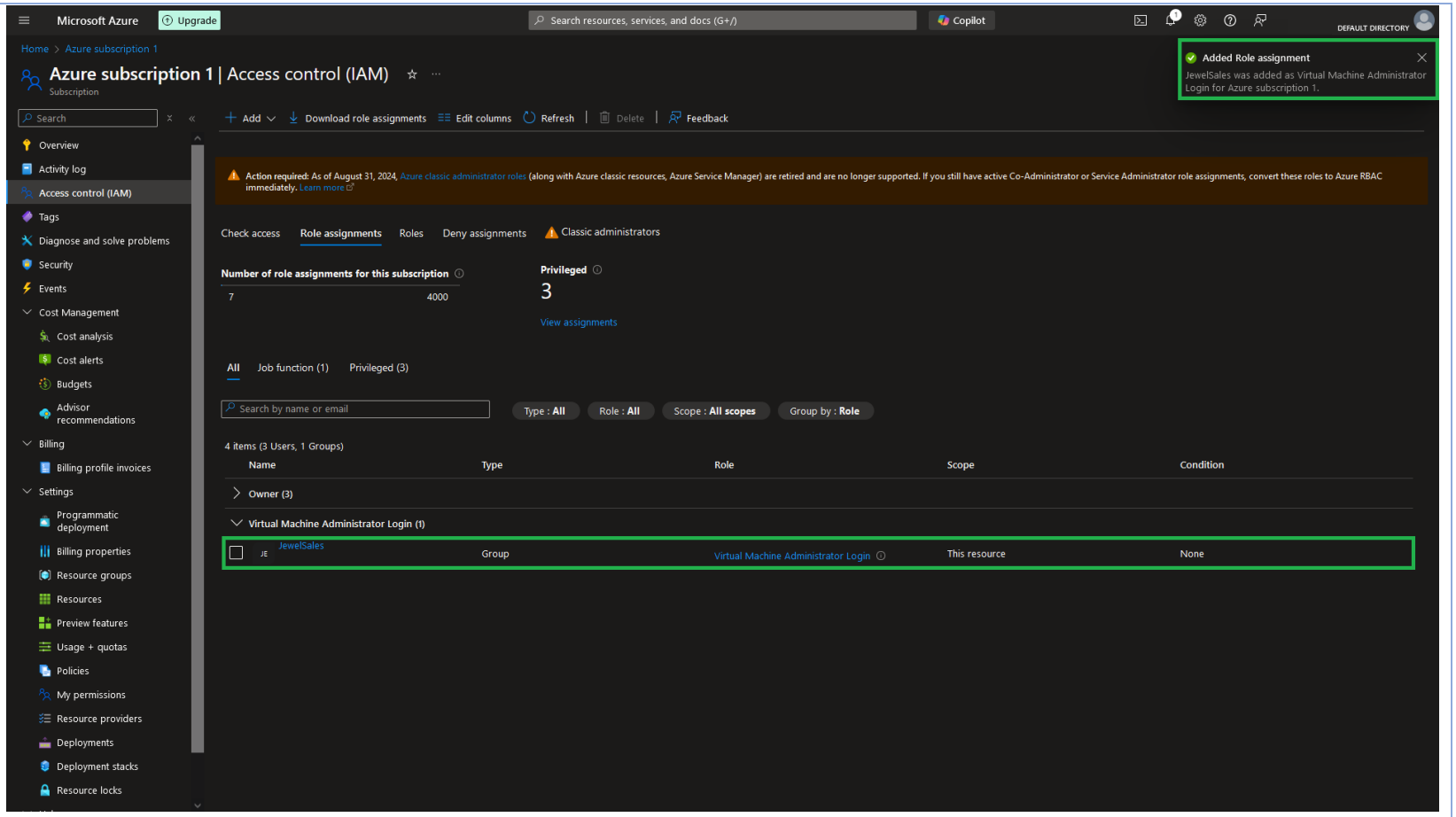
15. Now that the group has been successfully added, we click on **Next**.

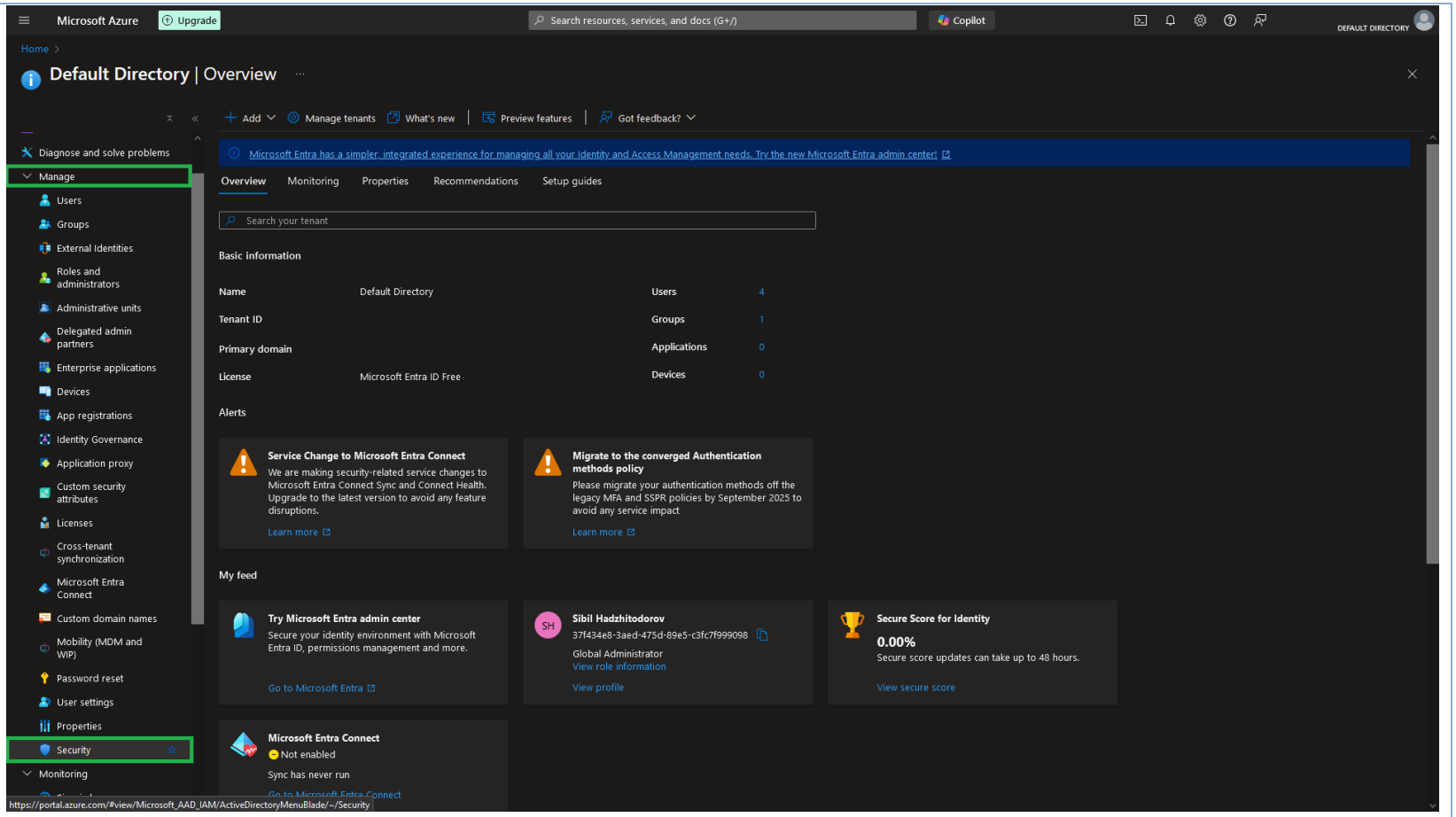


16. On the next page we click on the **Review + assign** button to complete the role assignment.

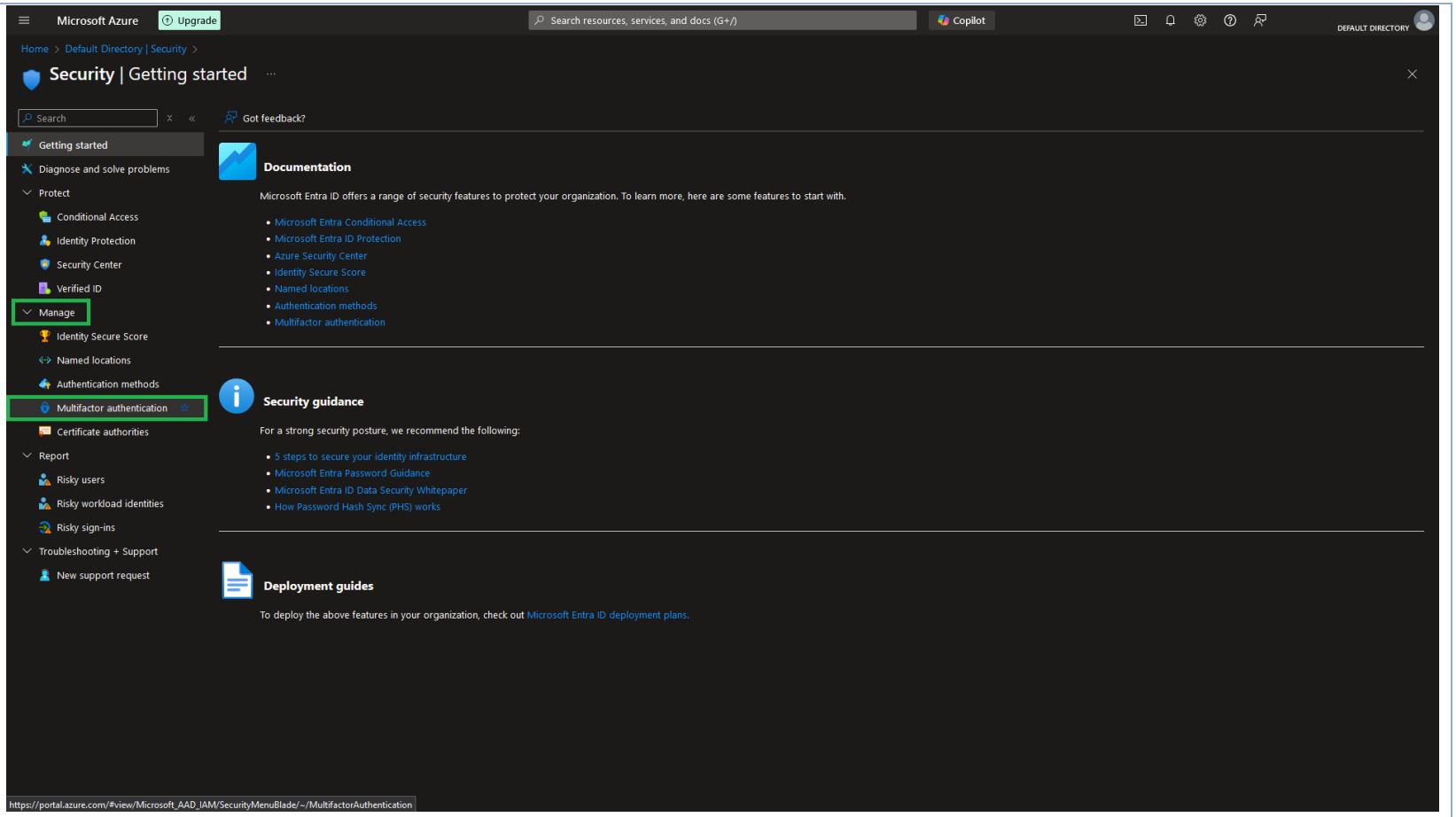


17. A notification should now appear that the role has been successfully assigned.

	
Activity 3: Implement mandatory multifactor authentication for all three users.	1. We go back to the **Default Directory** page once again, and select **Security** at the bottom of the *Manage* blade.

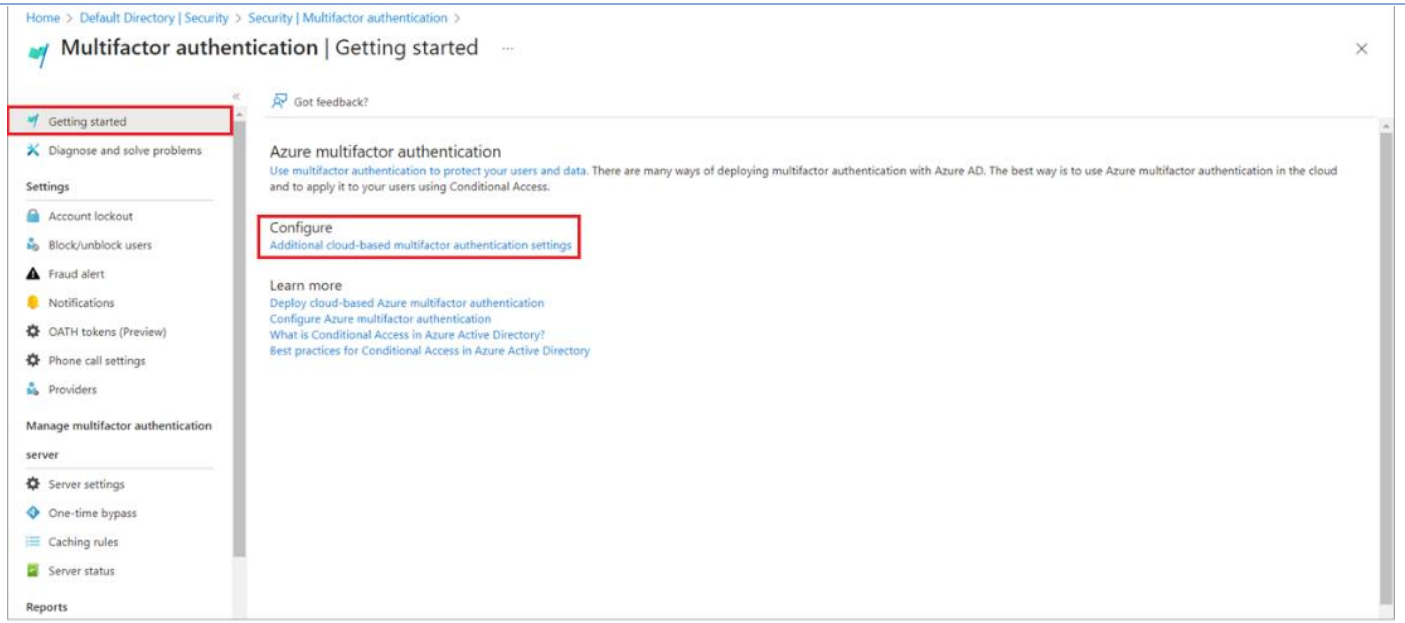


2. Once on the **Security** page, we click on **Multifactor authentication** under the *Manage* blade.

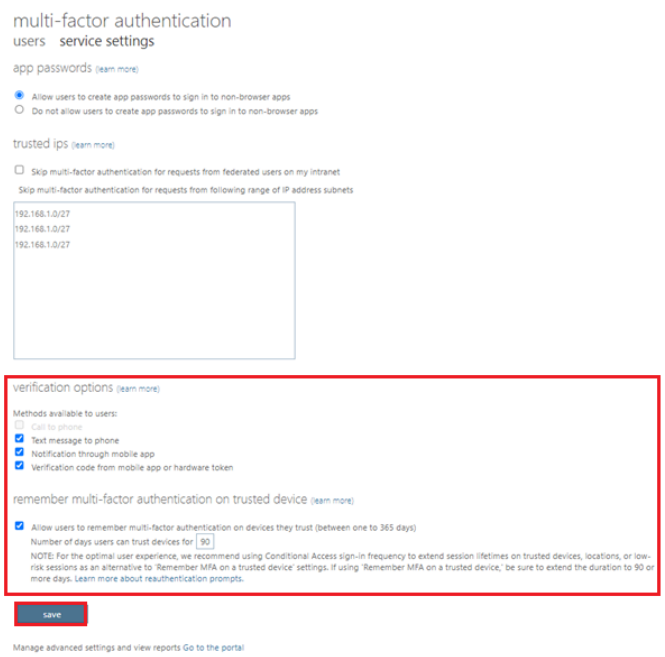


Note: Enabling multifactor authentication for this task requires a **Microsoft Entra Suite**, **Microsoft Entra ID Governance**, **or Microsoft Entra ID P2** free trail or license which in my case necessitated using a different account to complete, so the UI in following images will slightly differ.

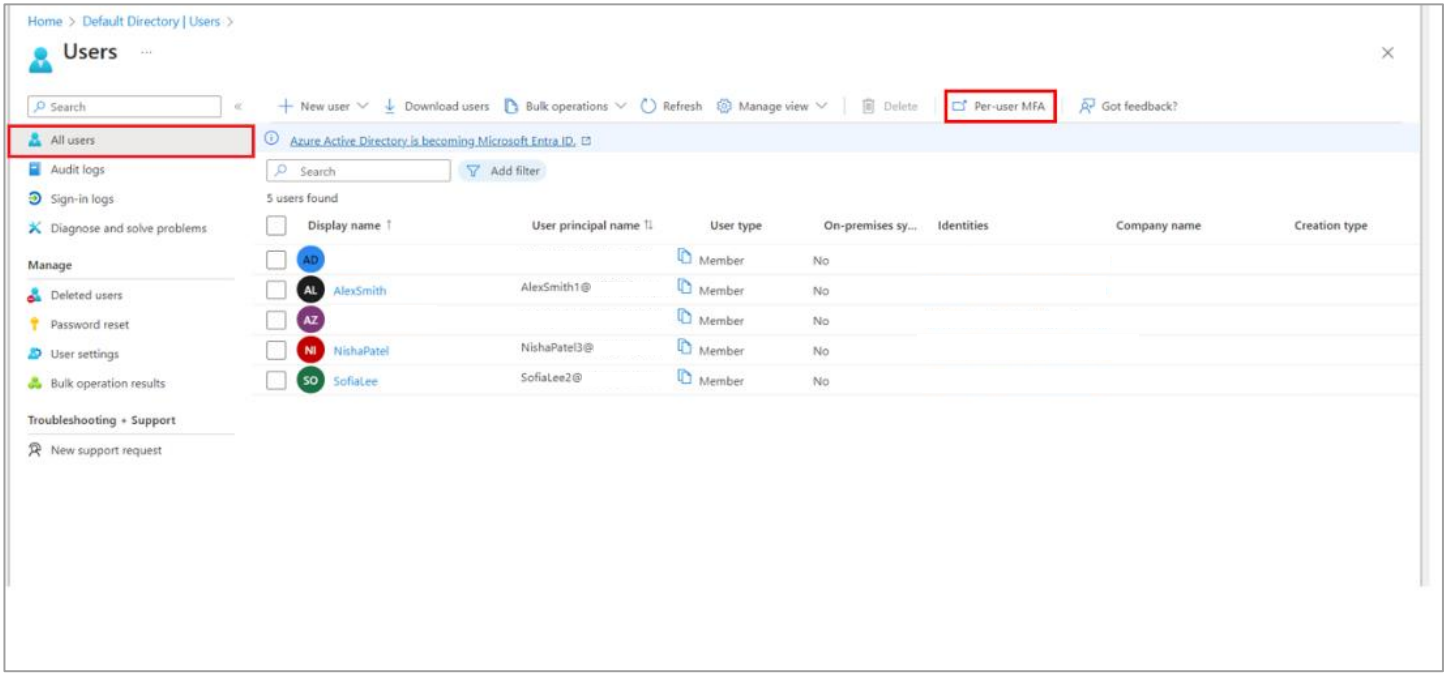
3. On the Multifactor authentication page, under the Configure section, we select **Additional cloud-based multifactor authentication settings**.



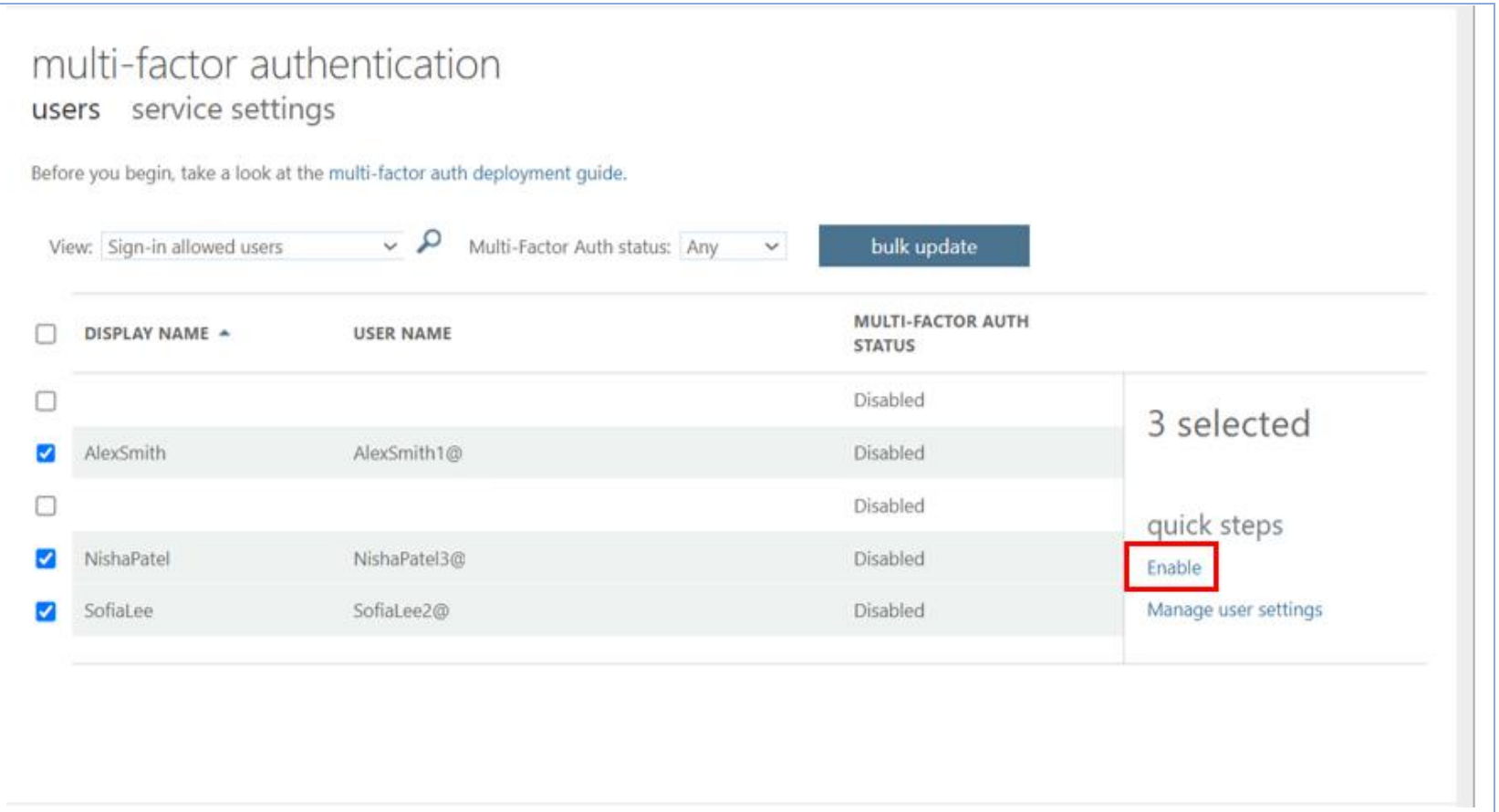
4. On the multi-factor authentication service settings page, under verification options, we check the boxes of the MFA options we desire.
5. Under remember multi-factor authentication on trusted device, we select the Allow users to remember multi-factor authentication on devices they trust (between one to 365 days) checkbox, and click on **Save**.



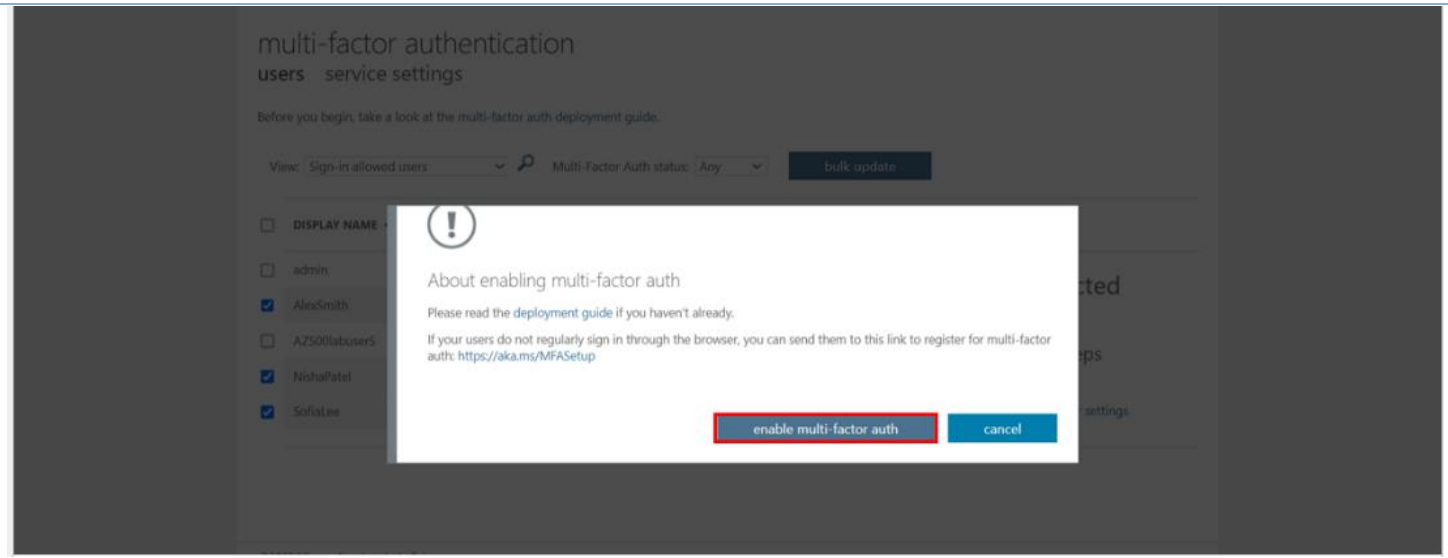
6. We then navigate back to the **Default Directory** page, select **Users** under the *Manage* blade, and then click on **Per-user MFA**.



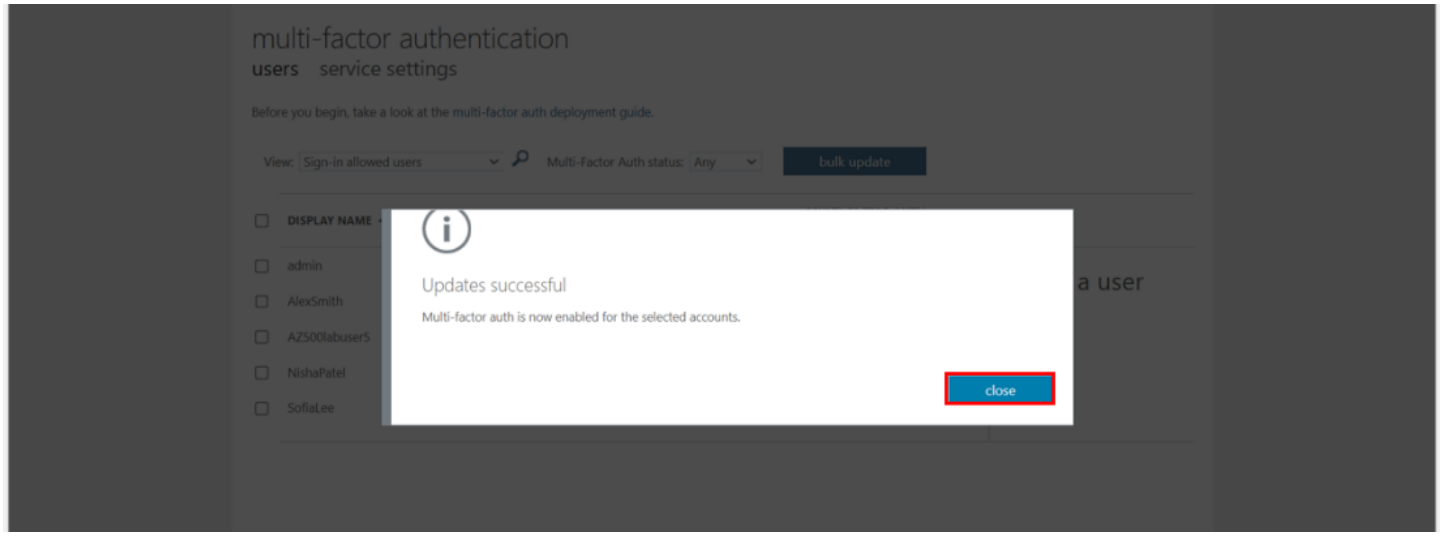
7. On the **multi-factor authentication users** page, we tick the checkboxes beside the three users created earlier: **AlexSmith**, **SofiaLee**, and **NishaPatel**.
8. We then click on **Enable** which is under **quick steps** to the right.



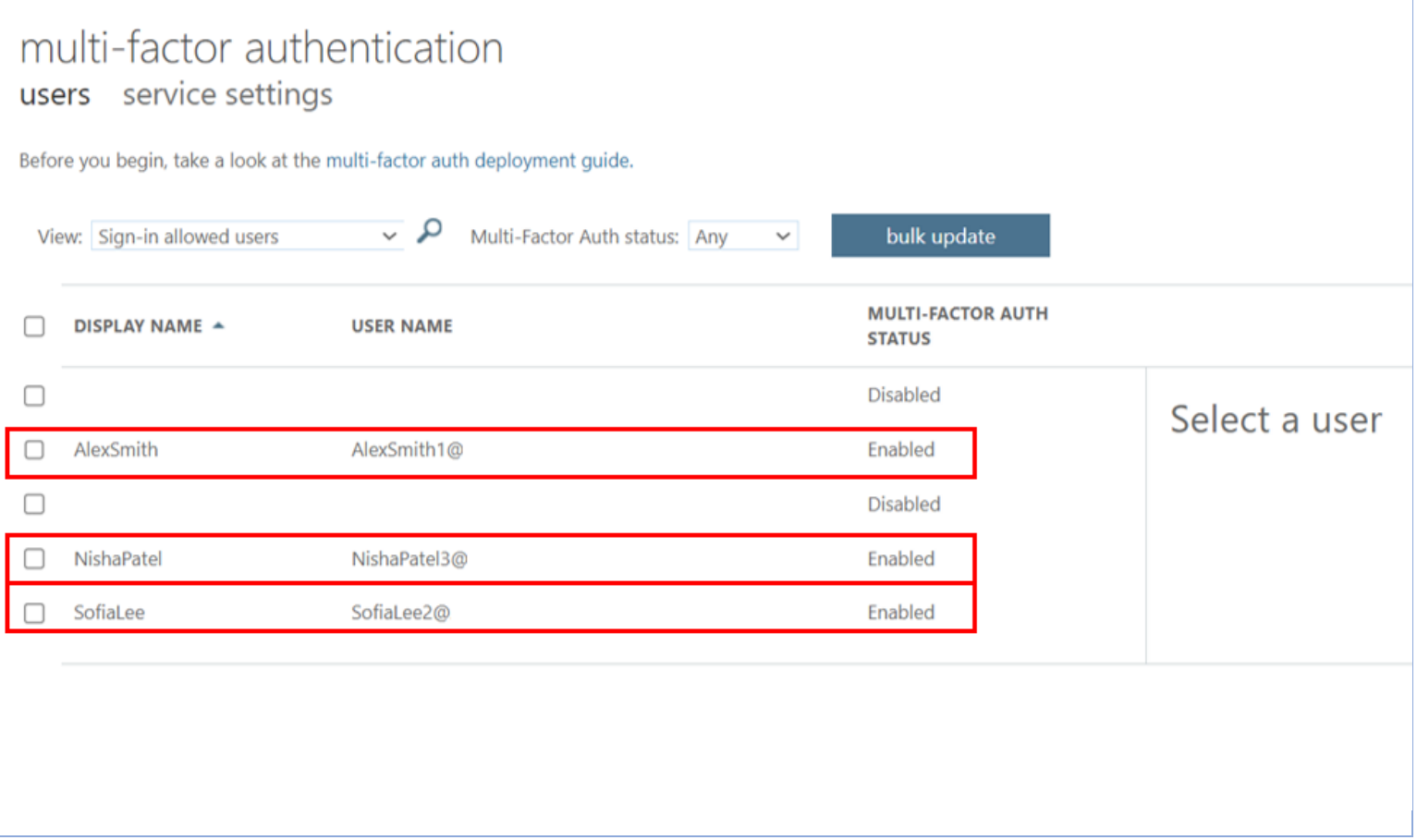
9. A pop-up will appear to ask us to confirm our decision, and we select **enable multi-factor auth**.



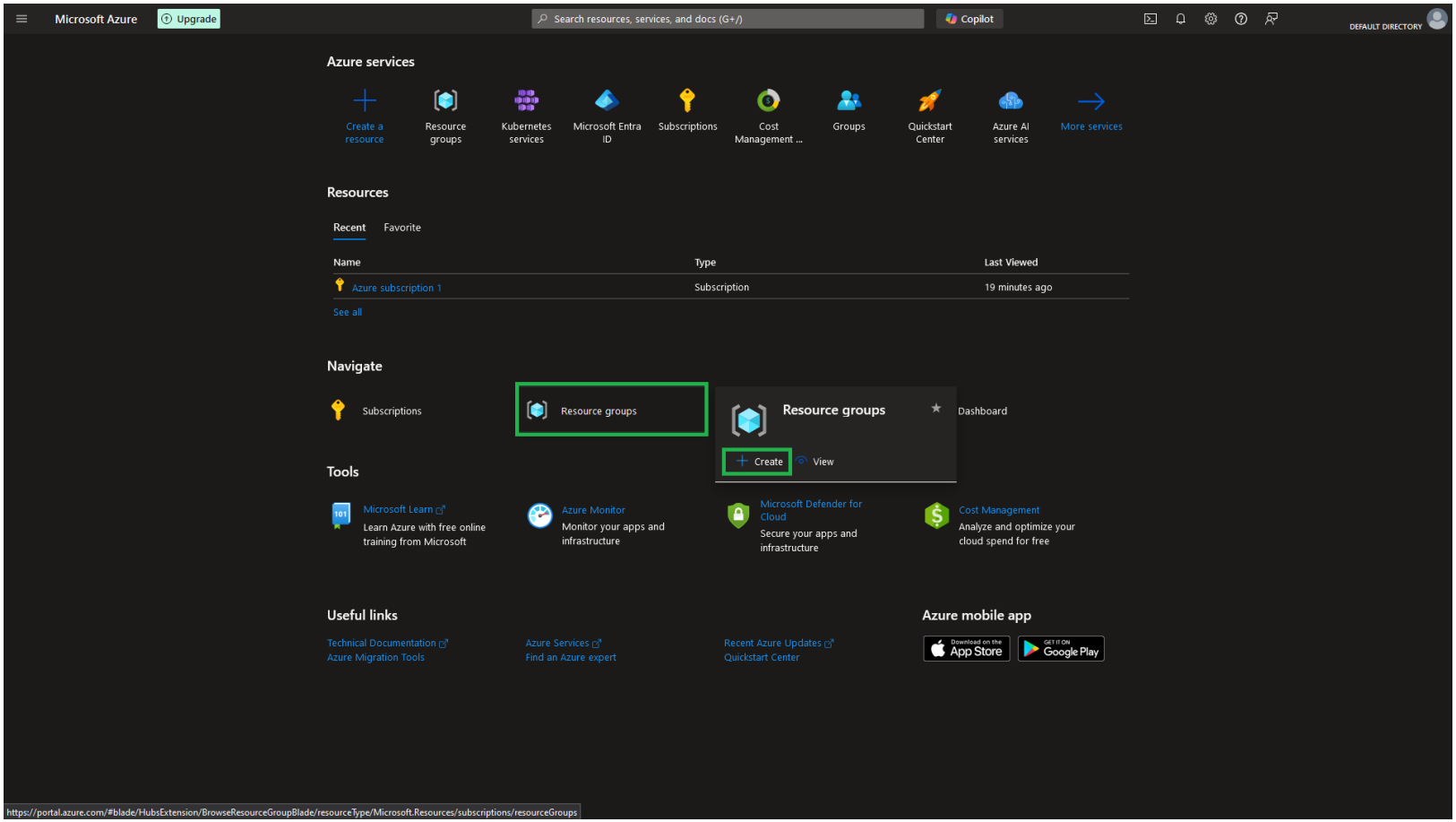
10. Another pop-up will appear stating that updates were successful which we can dismiss by clicking **Close**



11. We can then view the results and confirm that multi-factor authentication has been enabled for all three users

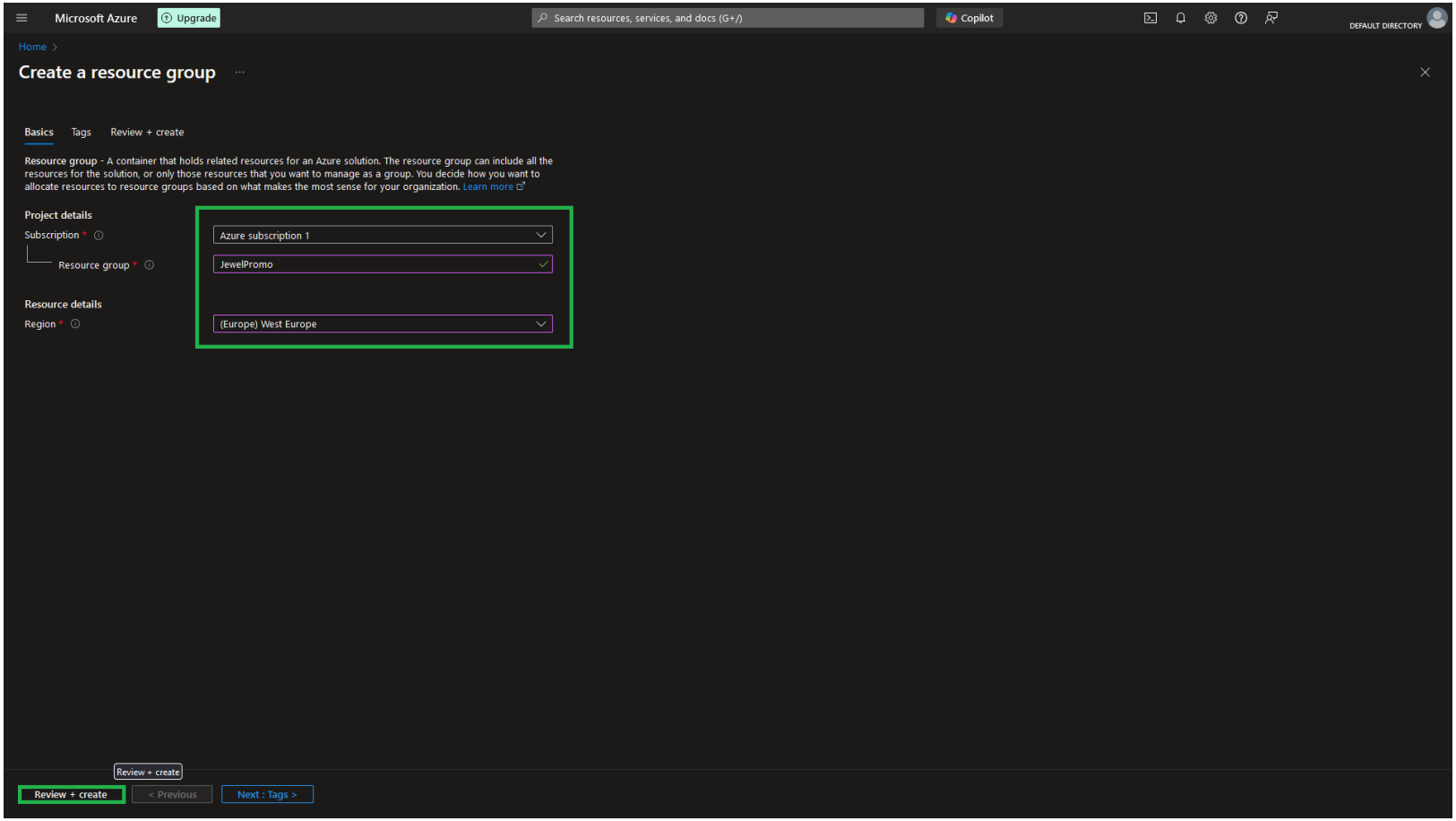


Task 2: Upload an image to a Storage account container, create a Blob shared access signature (SAS) URL for the image, and assign the Storage Blob Data Contributor role to the group members.

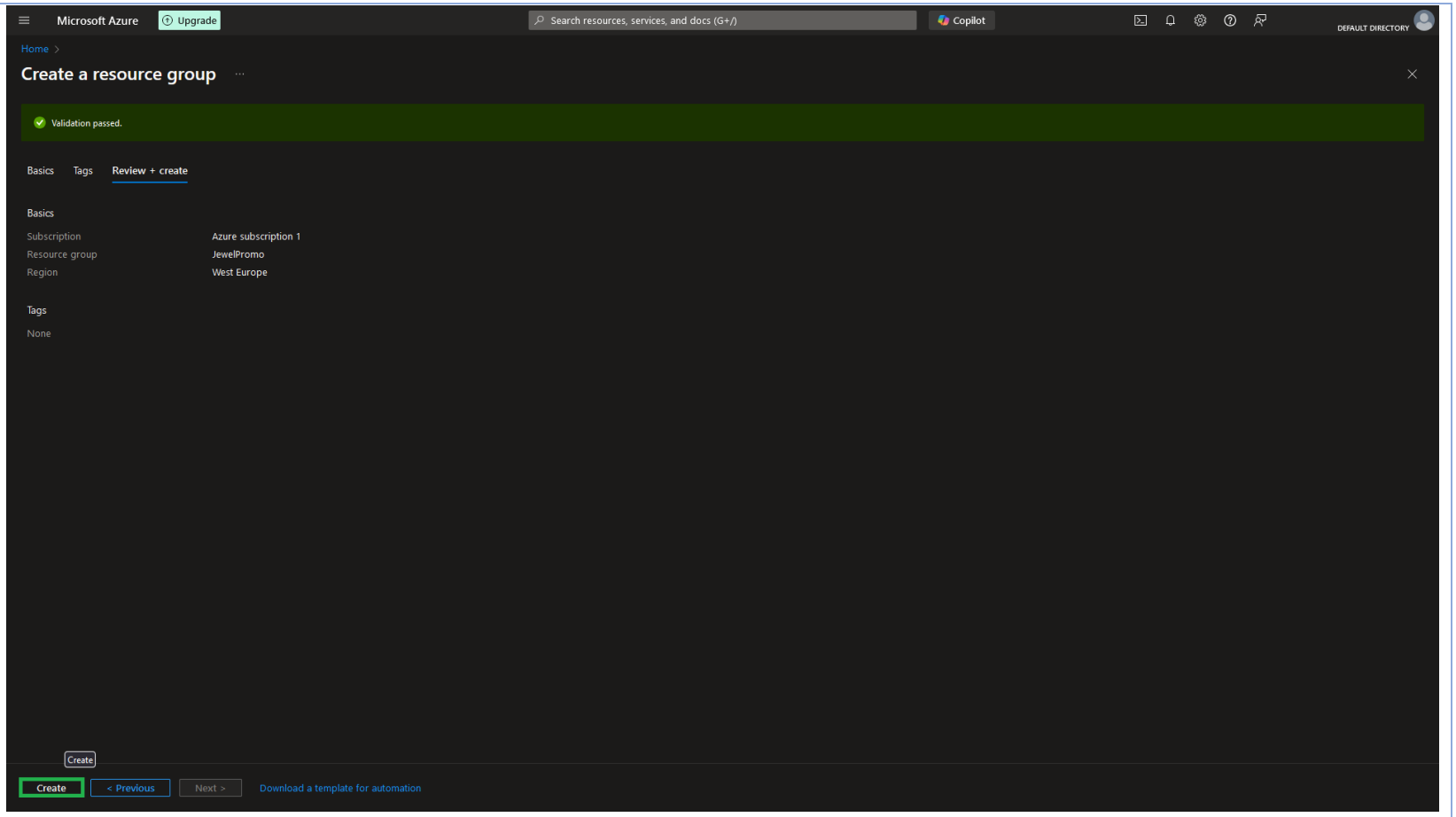
Activity	Key evidence
Activity 1: Create a resource group, a Storage account, and a container.	1. After signing in to the Azure Portal, we hover over **Resource groups** and click on **Create**. **Note:** This can also be achieved by selecting **Create a resource** and using the *Search services and marketplace* search box to search for "resource group".  2. On the **Create a resource group** page, on the **Basics** tab, we then input the following information:

Field	Value
Subscription	Select the current Azure subscription.
Resource group	Enter the resource group name **JewelPromo**.
Region	Select the region closest to you, considering latency and availability.

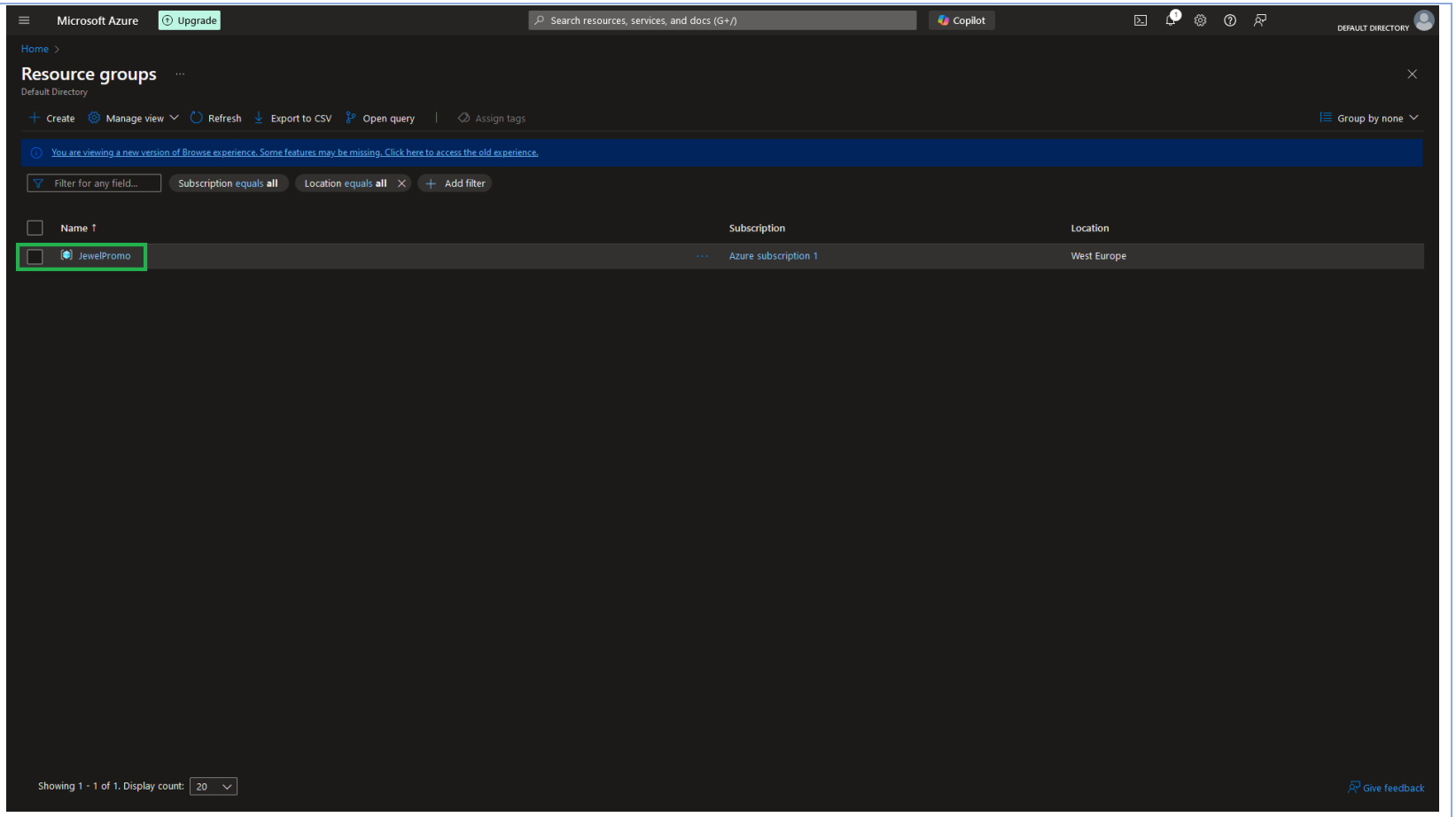
3. Click on **Review + create**



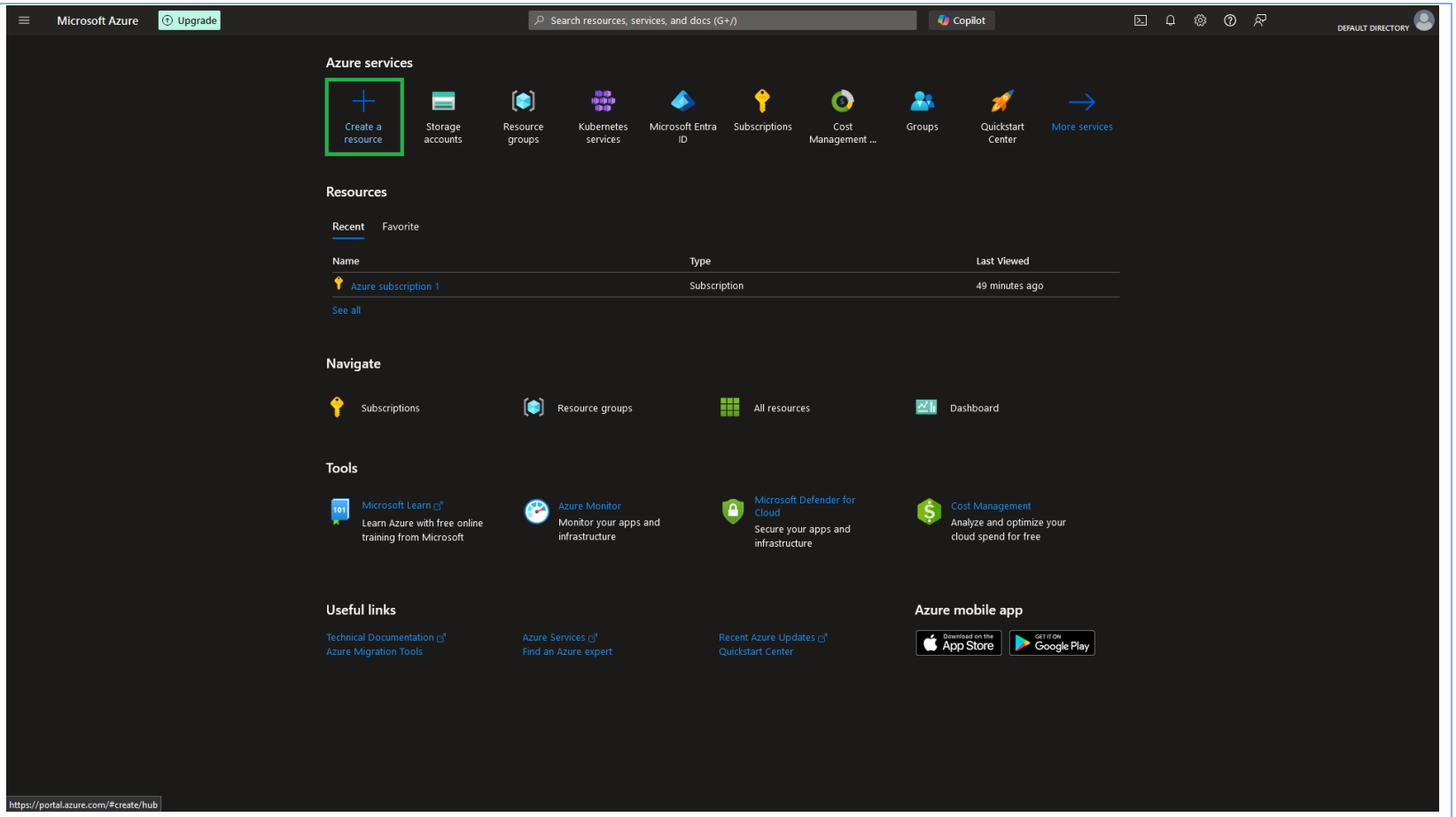
4. Select **Create**, after confirming all details are correct.



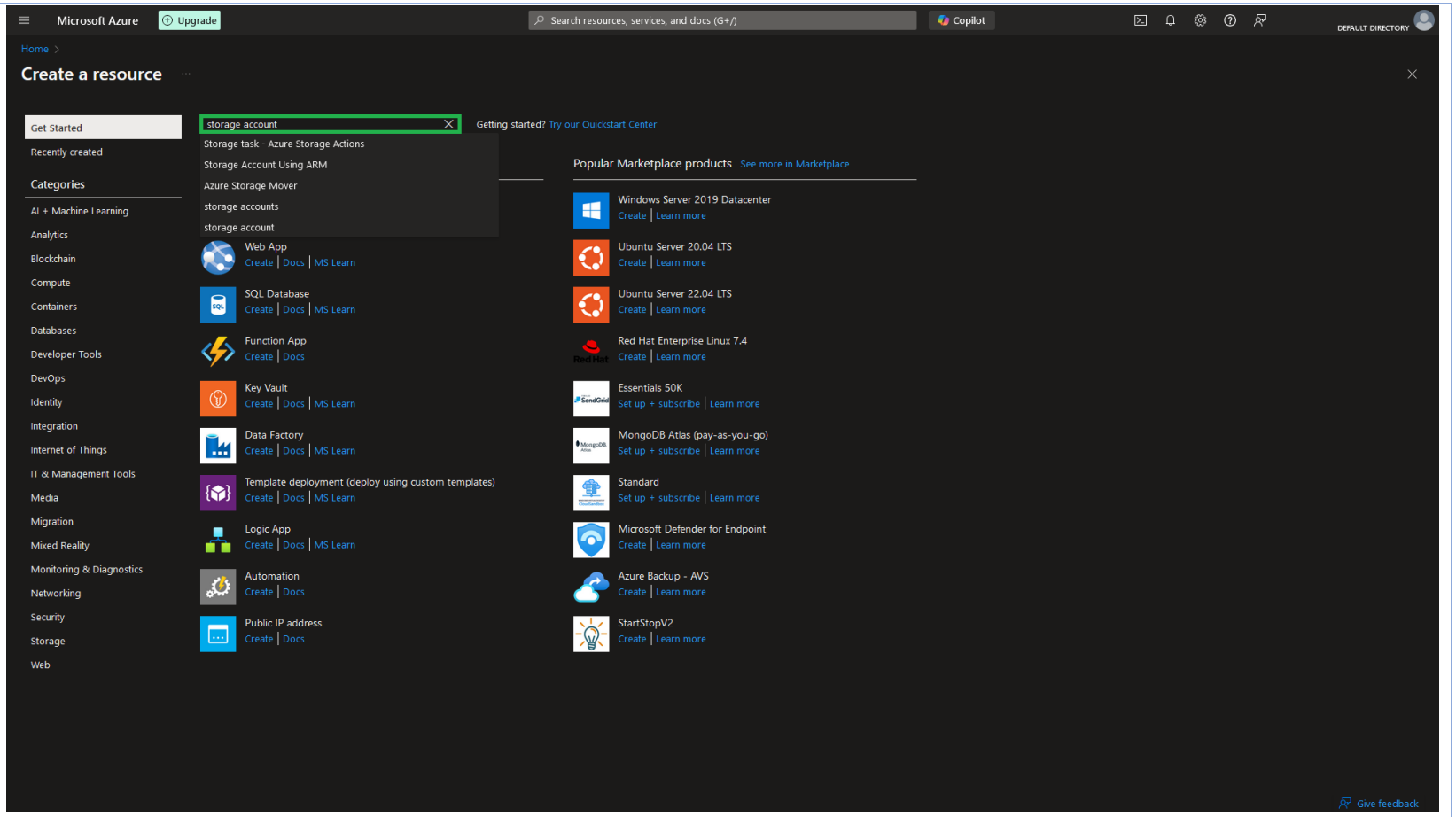
5. We will receive a notification that the resource group had been created, but we can make sure by going into the **Resource Group** page and checking for our newly created resource group.



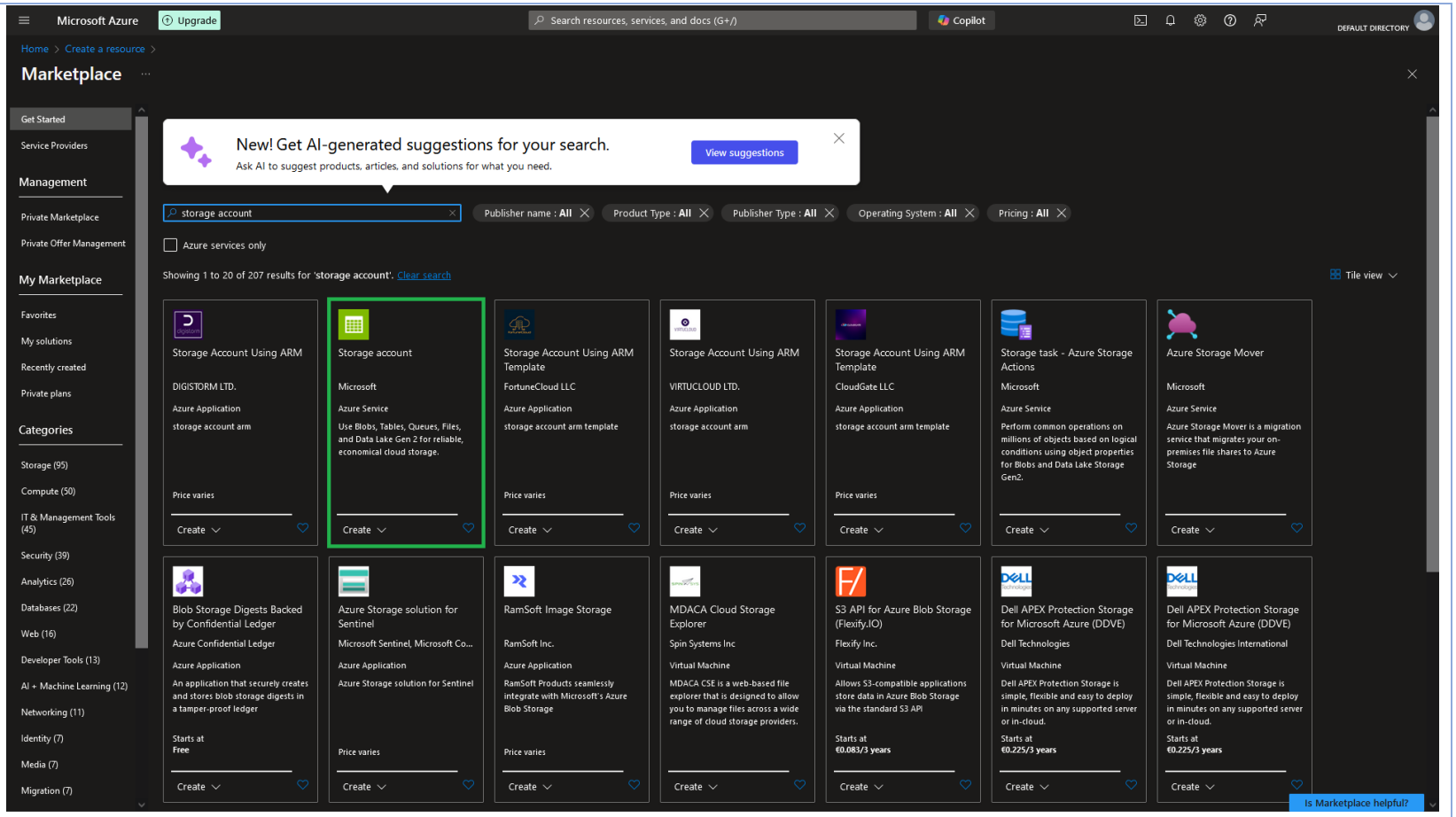
6. To create a storage account, we can either go to the **Storage accounts** page and click on **Create**, or use the **Marketplace** page. Let's go to the **Marketplace** page by clicking on **Create a resource**.



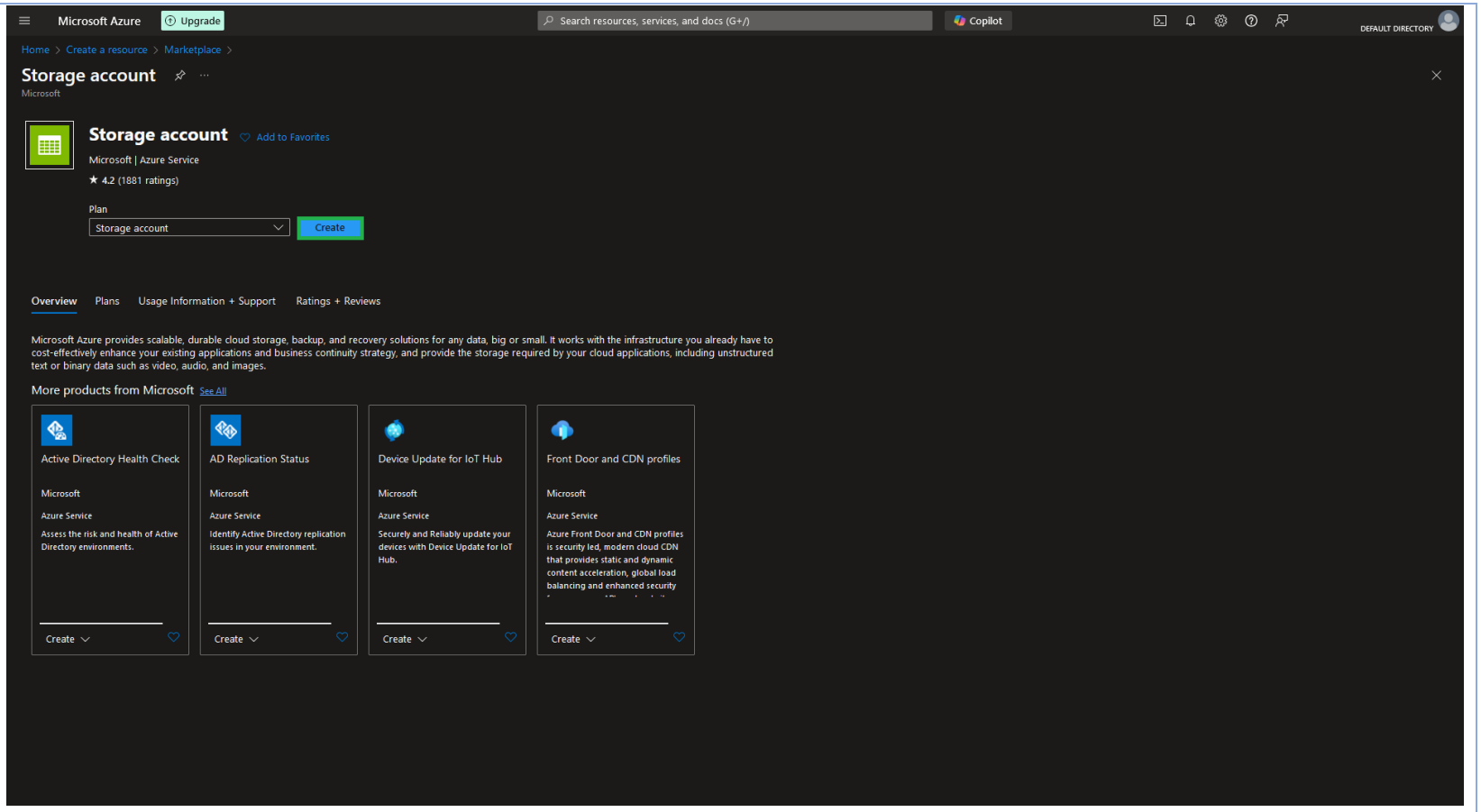
7. We then type in “storage account” in the *Search services and marketplace* search box.



8. This will take us to the **Marketplace** page where we will click on the **Storage account** result.



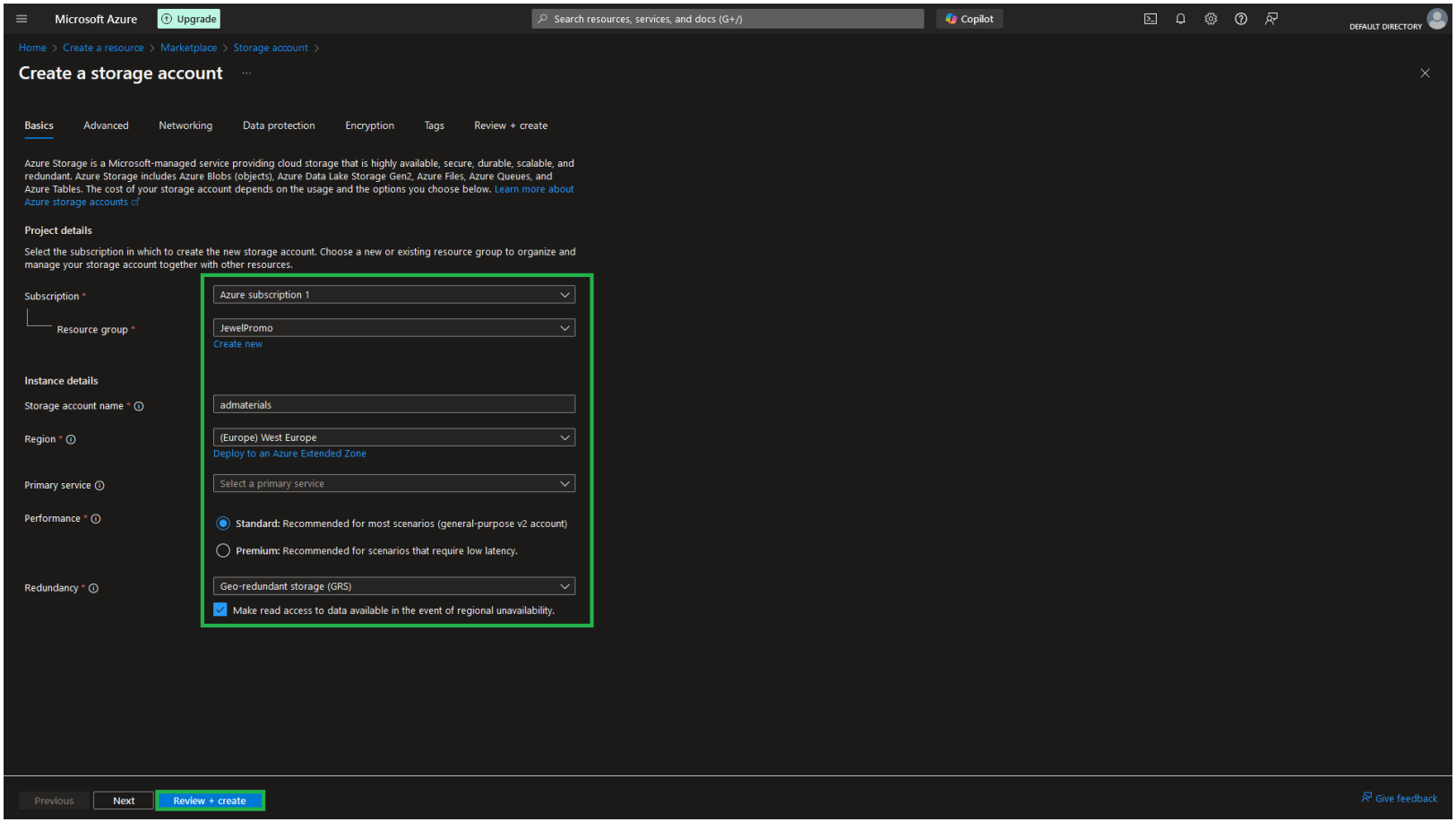
9. On the next page we click on **Create**.



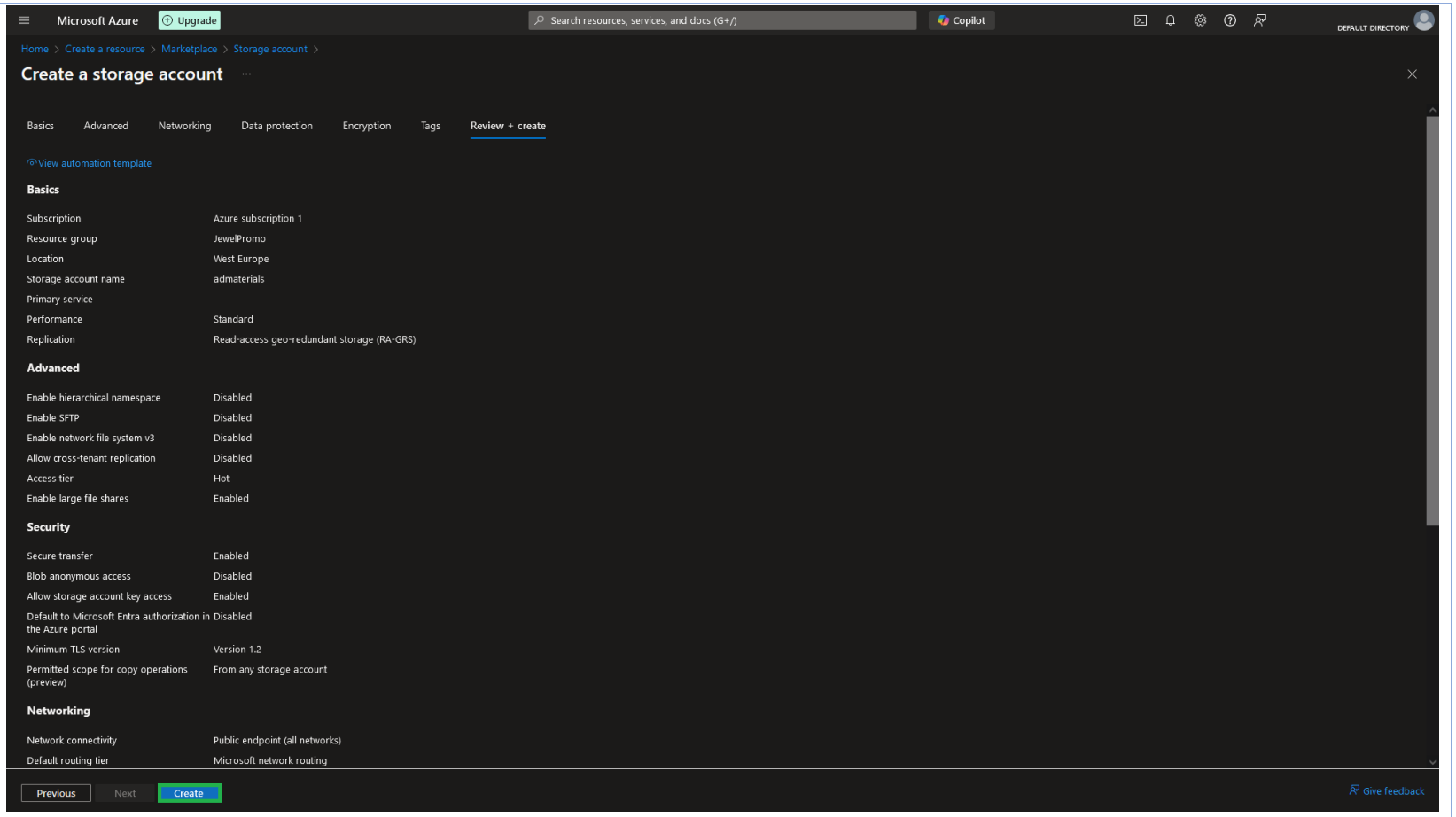
10. This will take us to the **Create a storage account** page, where we will input the following configuration information into the **Basics** tab, and select **Review + Create**.

Field	**Value**
Subscription	Select the Azure subscription for the new storage account.
Resource group	Select **JewelPromo**.
Storage account name	Enter the storage account name, **advtstorage**. **Note:** Storage account name must be globally unique
Region	Select the same region as the resource group we created earlier.
Performance	Select **Standard: Recommended for most scenarios (general-purpose v2 account)**.
Redundancy	Select **Geo-redundant storage (GRS)**.

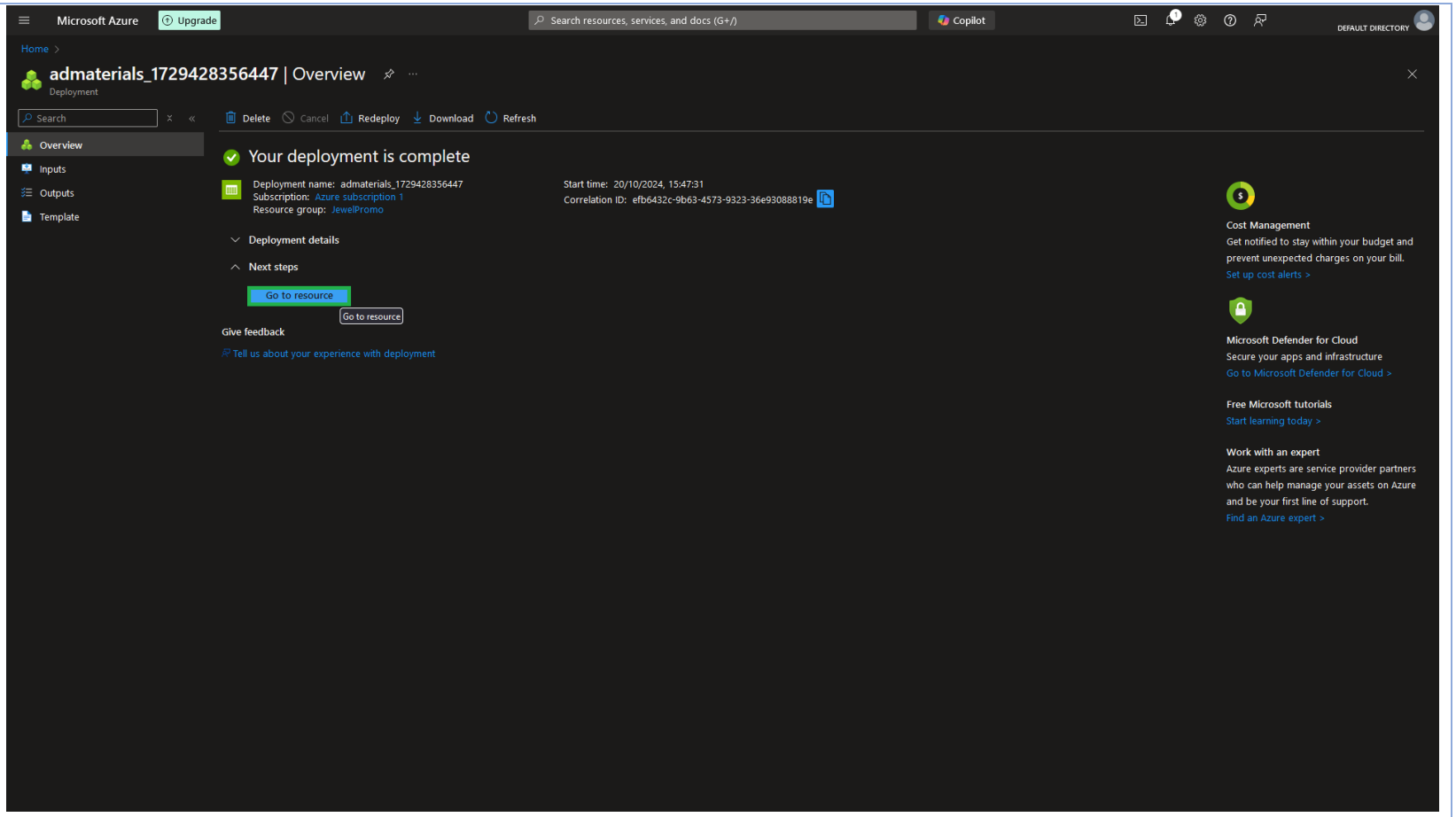
	Note: Selecting this option replicates the data to a datacenter in a different region. Ensure that the **Make read access to data available in the event of regional unavailability** checkbox is selected.



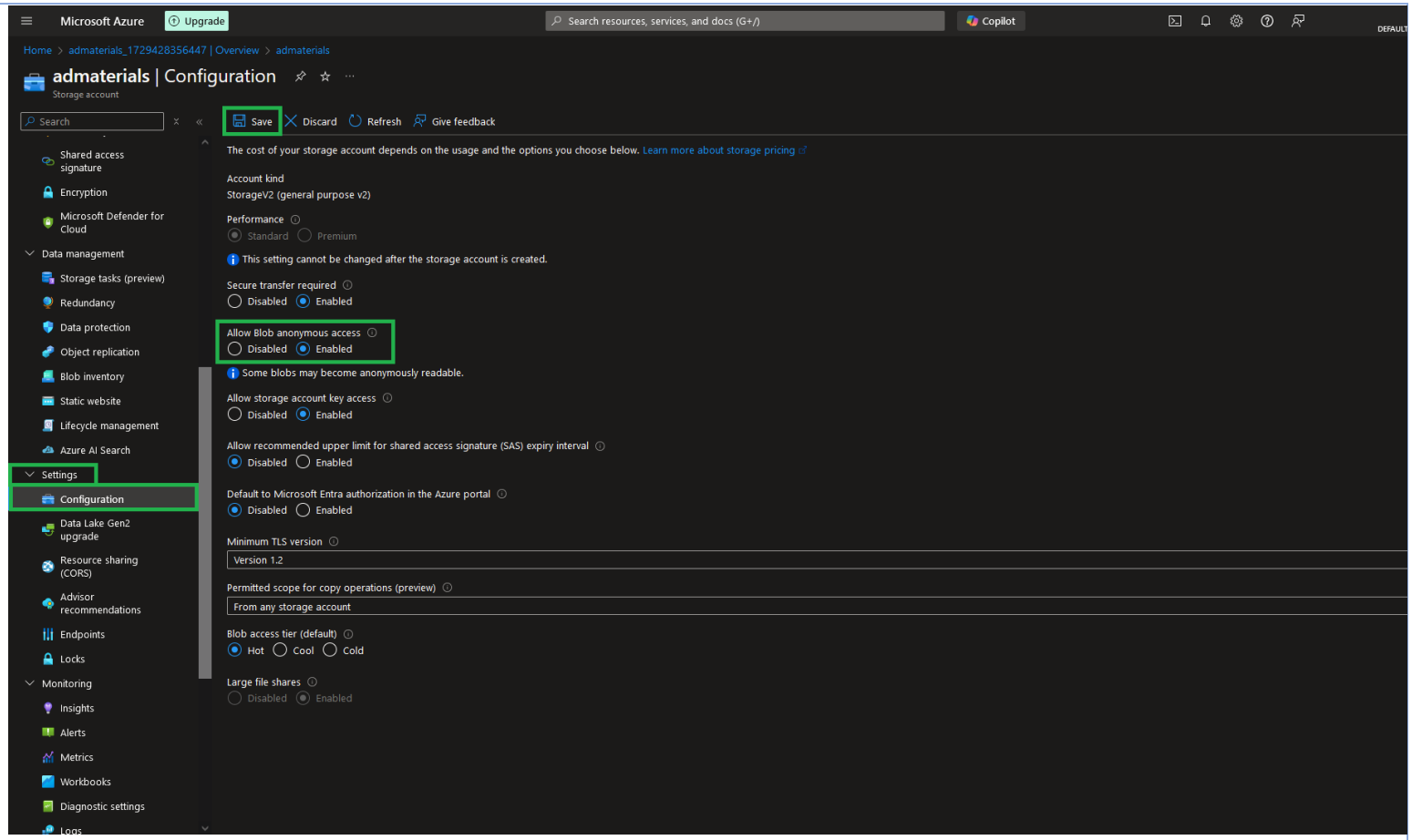
11. We then click on **Create** to deploy the storage account.



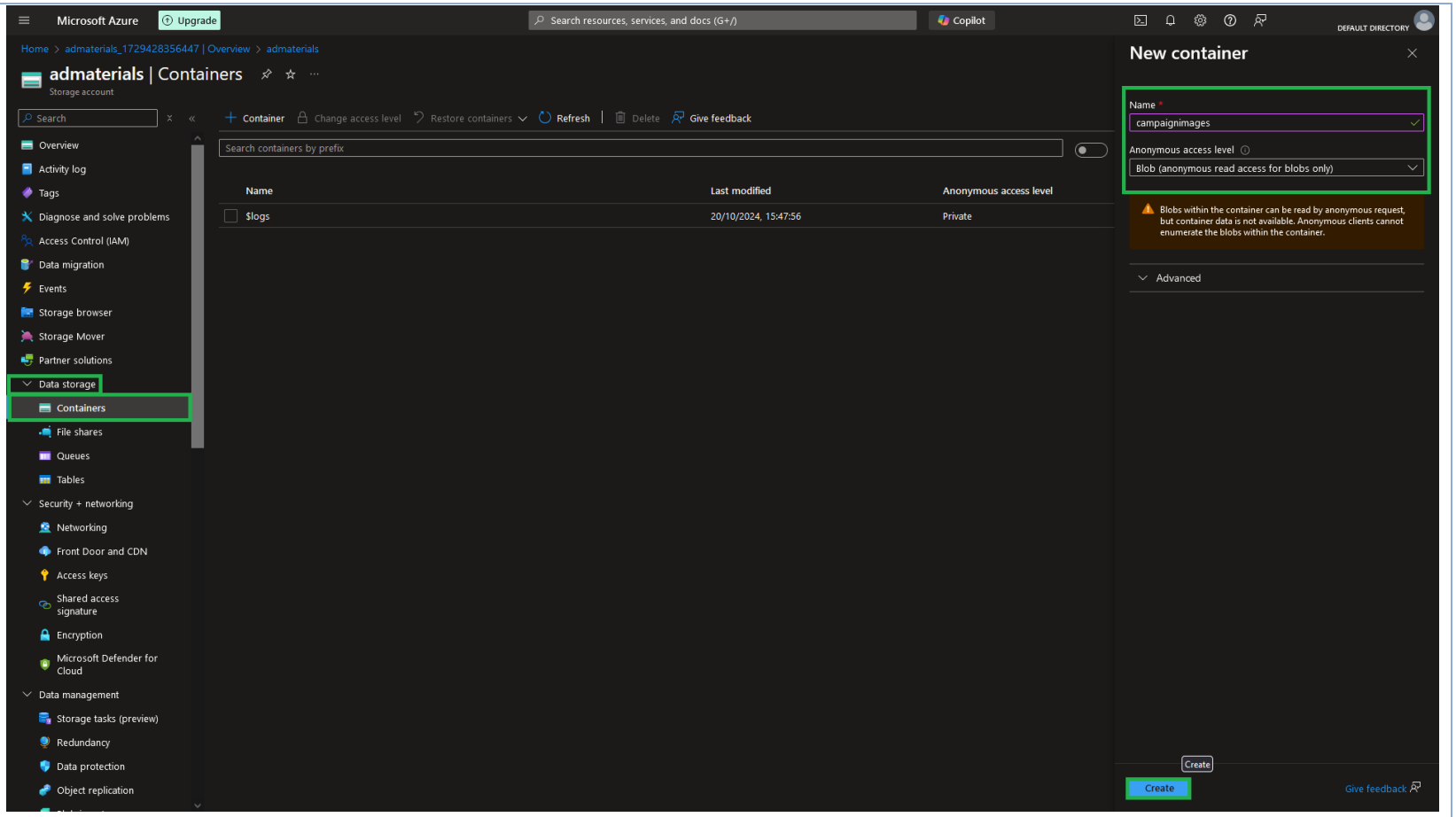
12. It will take some time for the storage account to deploy. Once it is ready, we click on **Go to resource**.



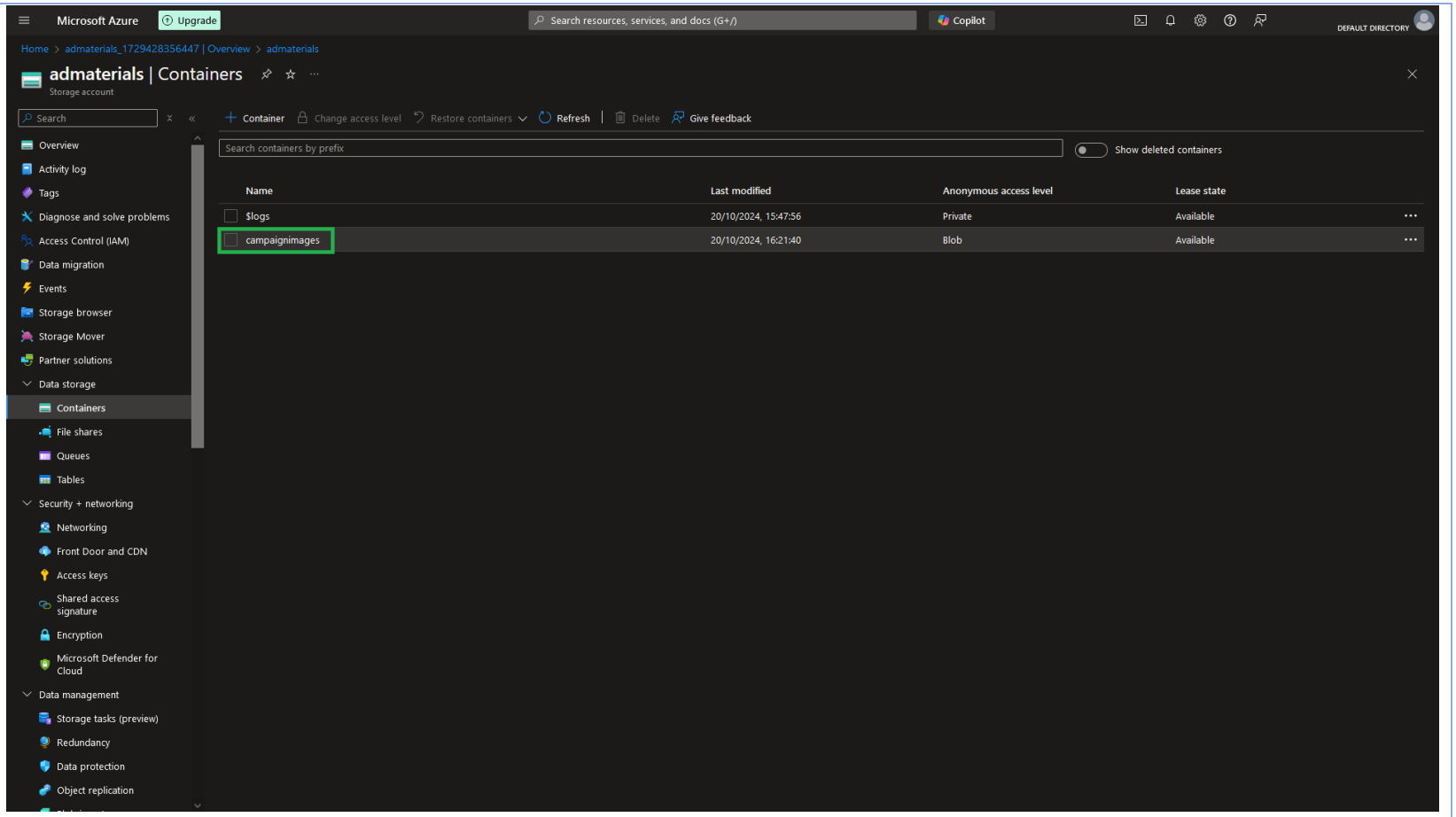
13. Anonymous access to storage accounts is disabled by default. To enable it, we first go to **Configuration** under the *Settings* blade, select the **Enable** radio button under **Allow Blob anonymous access,** and confirm changes by clicking on **Save**.

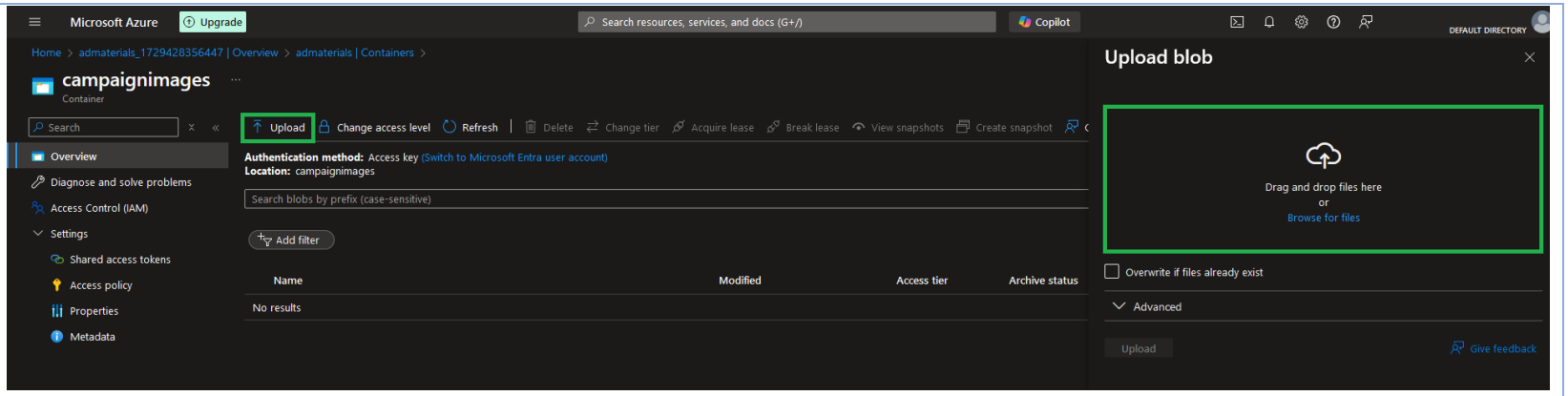


14. We then select **Containers** under the *Data storage* blade.
15. On the **Containers** page, we click on **Container** to create a new container**.**
16. On the **New container** wizard, we enter a name for our new container, such as **campaignimages**. From the **Public access level** dropdown list, which should now no longer be grayed out, we select **Blob (anonymous read access for blobs only)**.
17. We then click on **Create** to create the container.

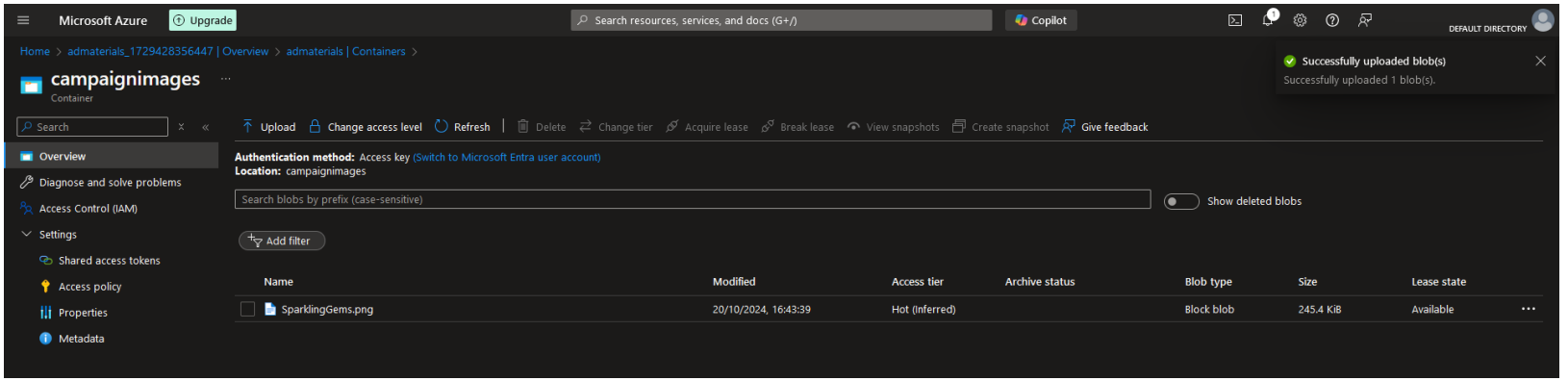


18. The container can now be viewed on the **Containers** page.

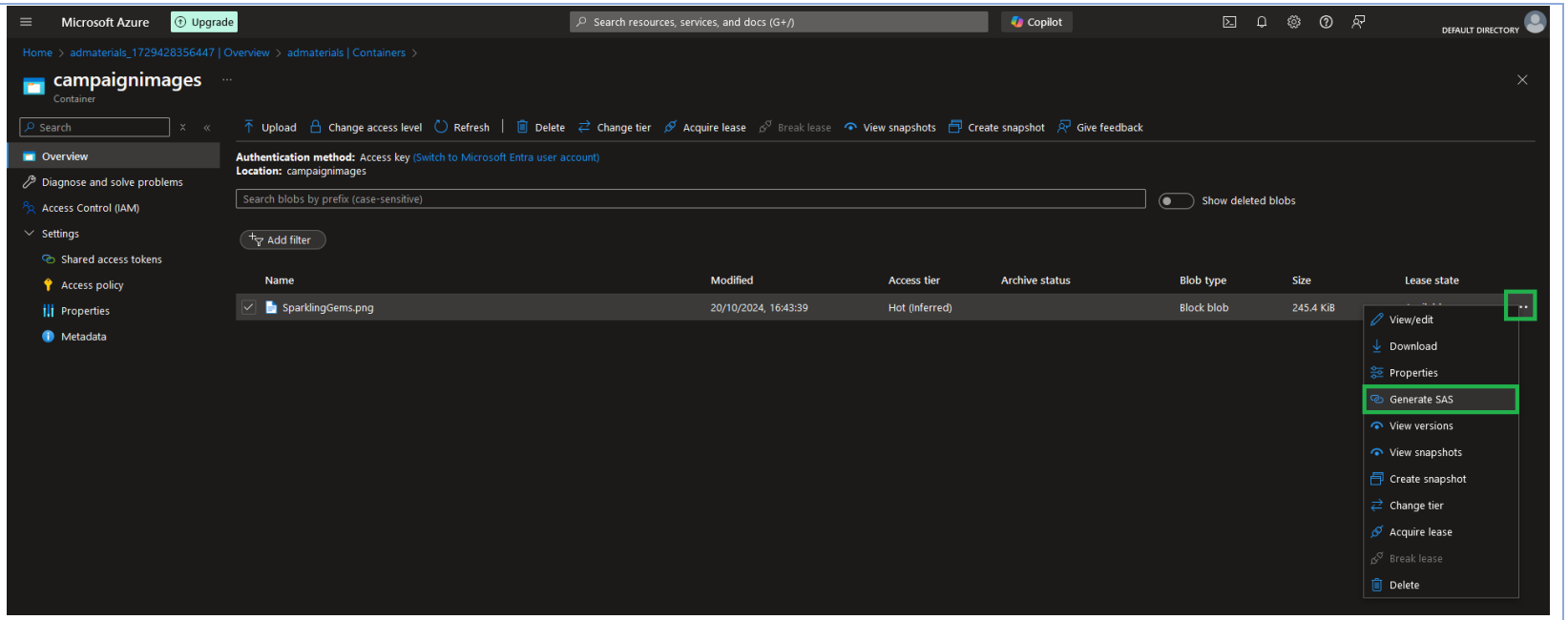
	
Activity 2: Upload an image to the container in the Storage account and create a Blob SAS URL for the image.	1. We now click on the newly created container called **campaignimages**, select the **Upload** button to open the **Upload blob** wizard, and add the SparklingGems.png to the container.



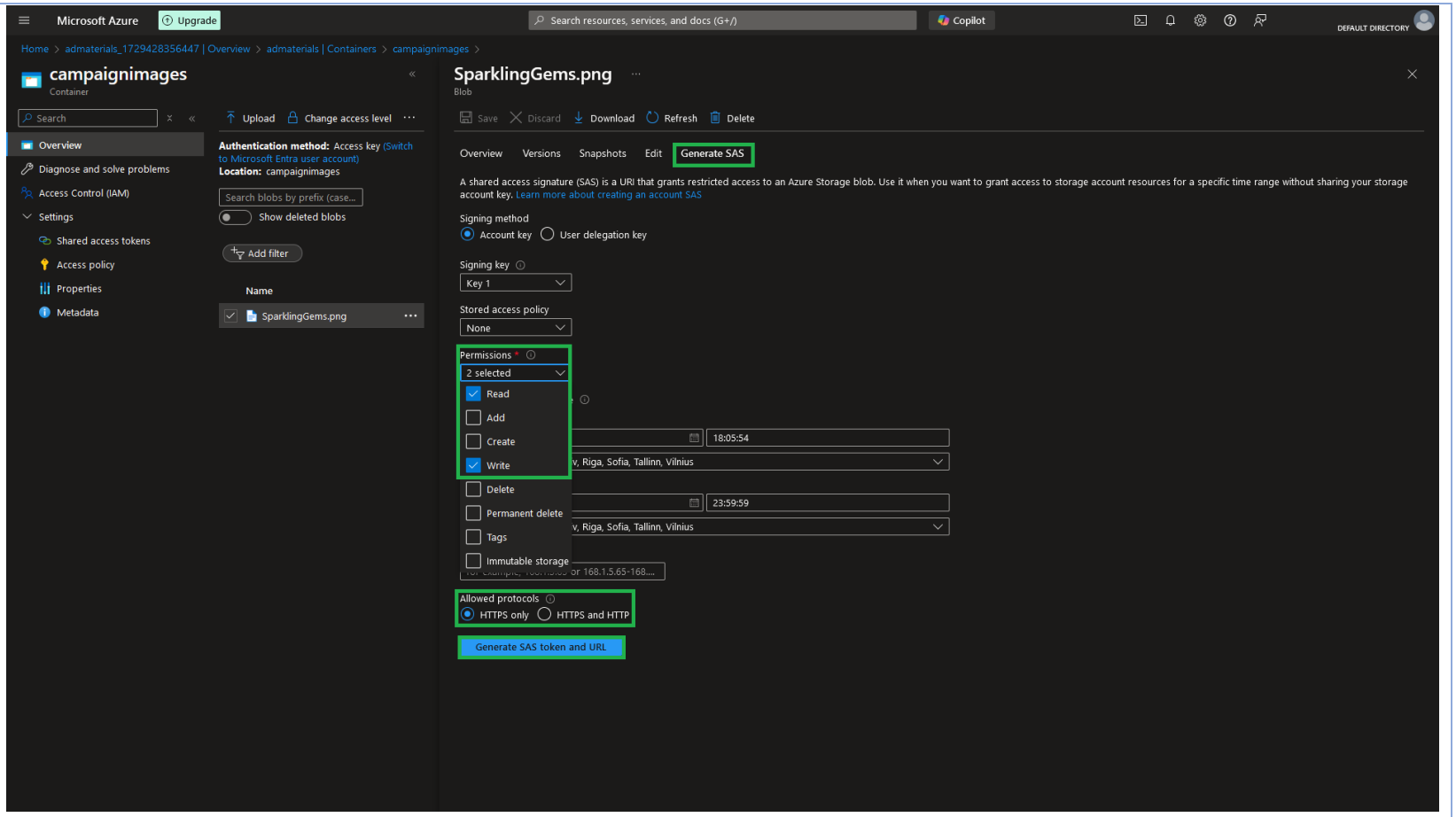
2. After adding the image, we click on **Upload** and it should successfully appear within the container.



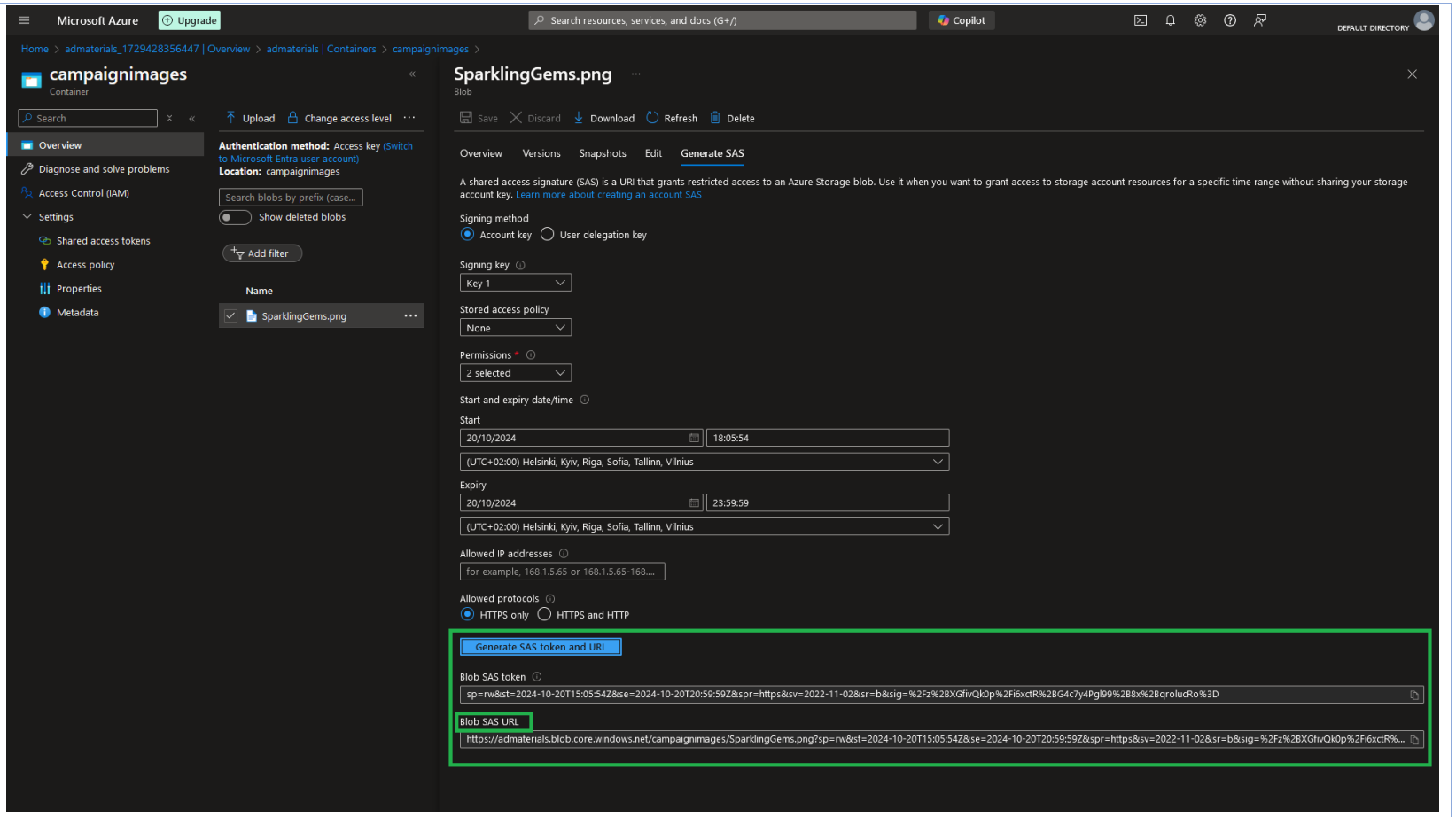
3. To generate the SAS, we click on the **ellipsis (...)** next to the SparklingGems.png file, and select **Generate SAS** from the dropdown menu.



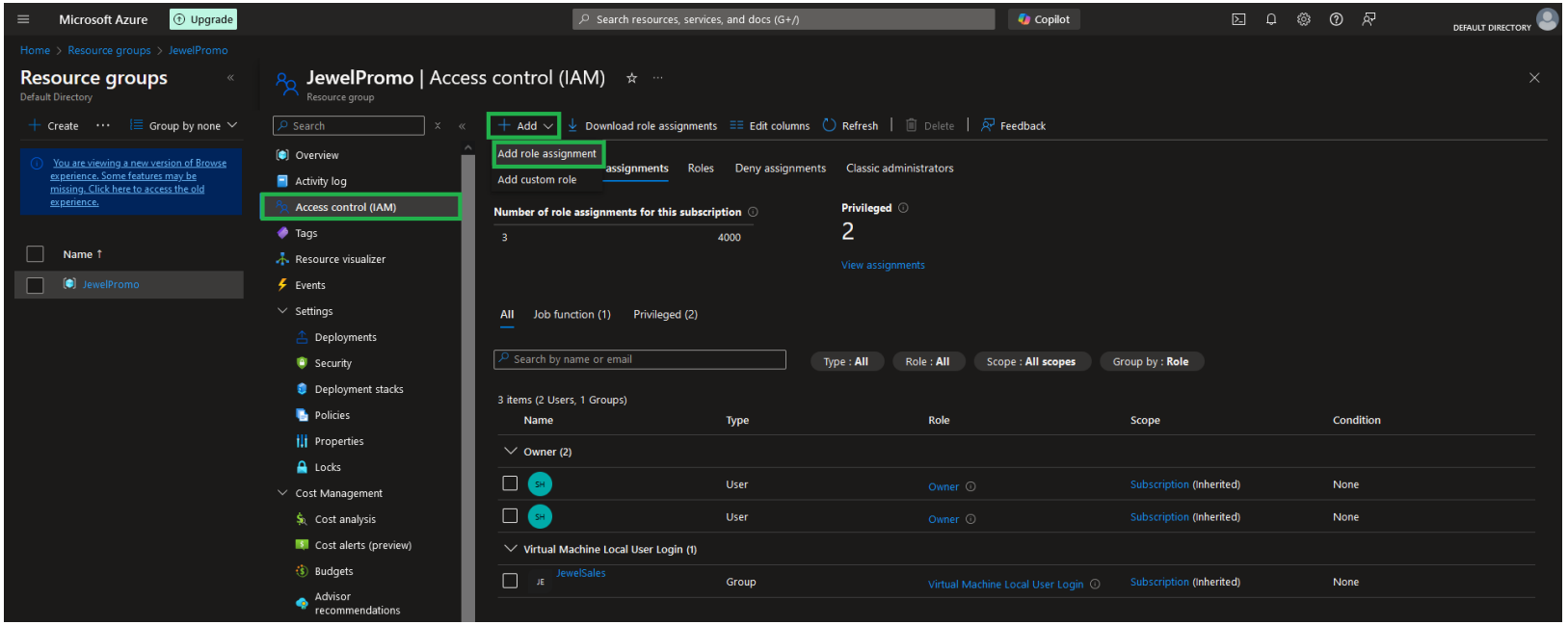
4. We then go to the **Generate SAS** tab of the windows that pops up and click on **Permissions**, enabling Read and Write permissions for the file. We then make sure that **HTTPS only** is selected under **Allowed protocols**.
5. We then confirm our selection by clicking on **Generate SAS token and URL**.



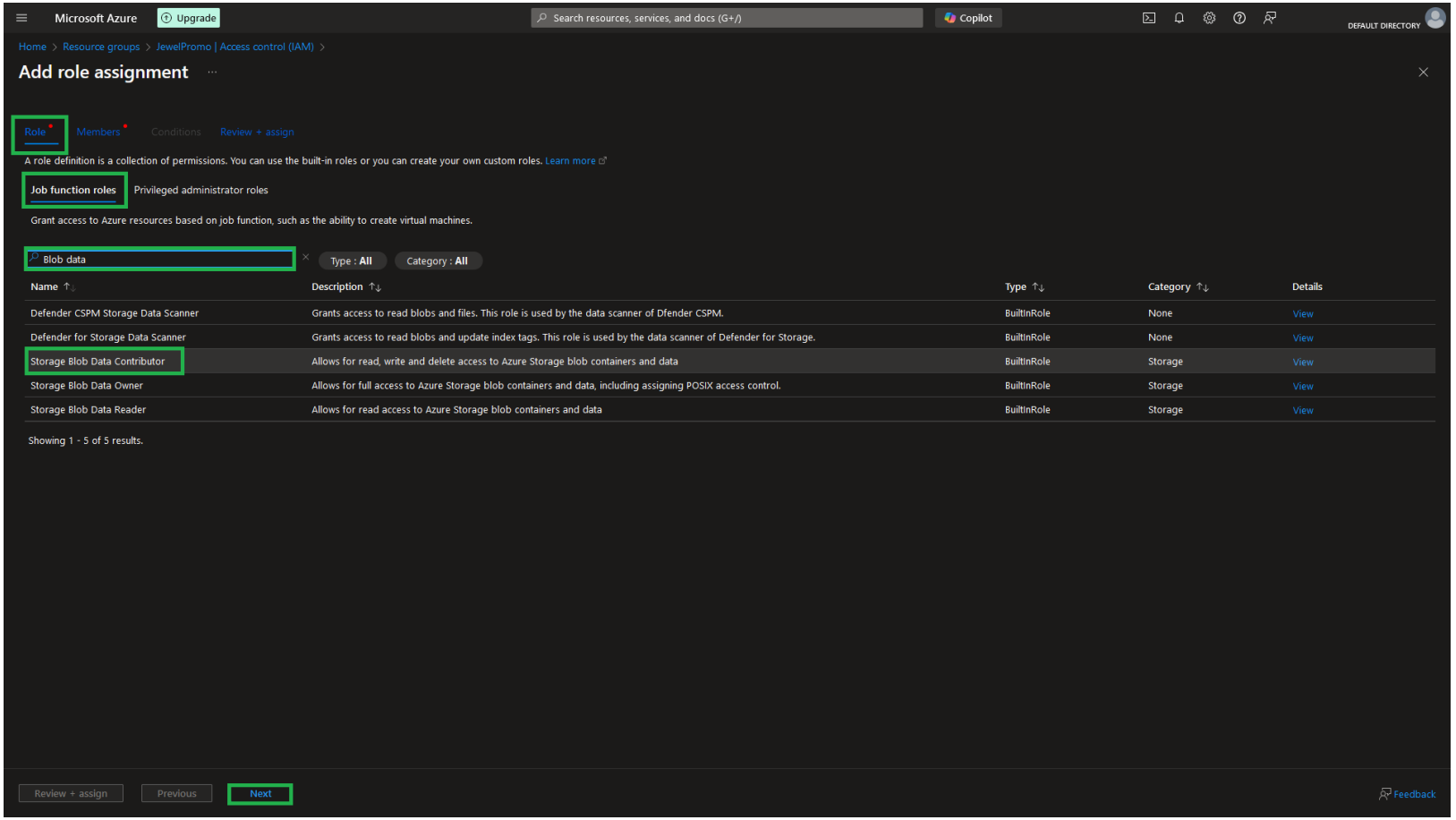
6. The **Blob SAS token** and the **Blob SAS URL** appear in the bottom area of the wizard. We then copy the **Blob SAS URL**, and save it for later use.

<table>
<tr>
<td></td>
<td> 

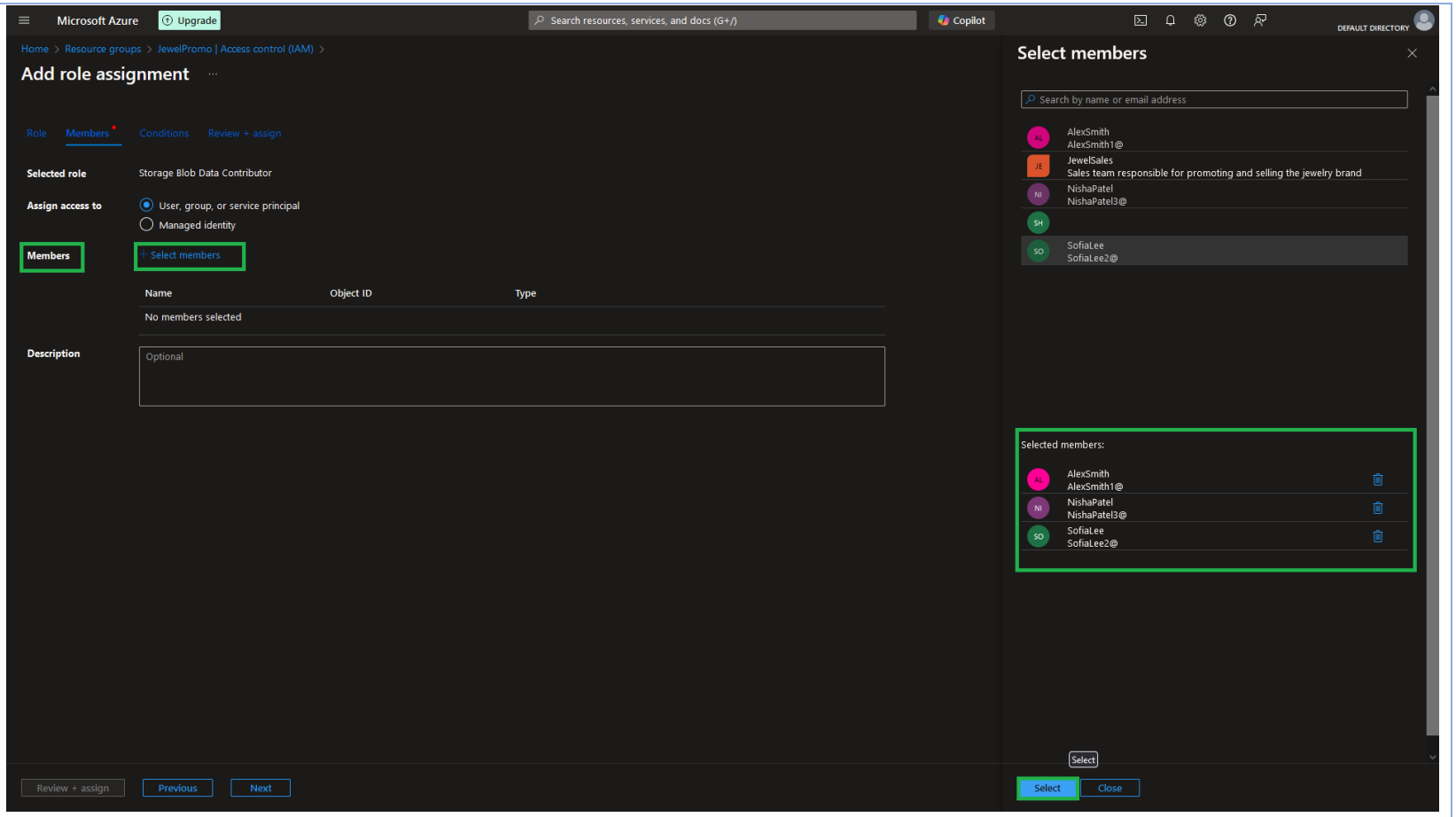
Note: This is the only time we can see and copy the SAS URL.</td>
</tr>
<tr>
<td>Activity 3: Assign the Storage Blob Data Contributor role to the group members.</td>
<td>1. We then navigate to the Resource Groups page from the Azure portal and select the JewelPromo resource group.
2. Then, we click on Access control (IAM) and select the Role assignments tab which shows us our existing role assignments.
3. Since no Storage Blob Data Contributor role exists, we select Add and choose Add role assignment.</td>
</tr>
</table>



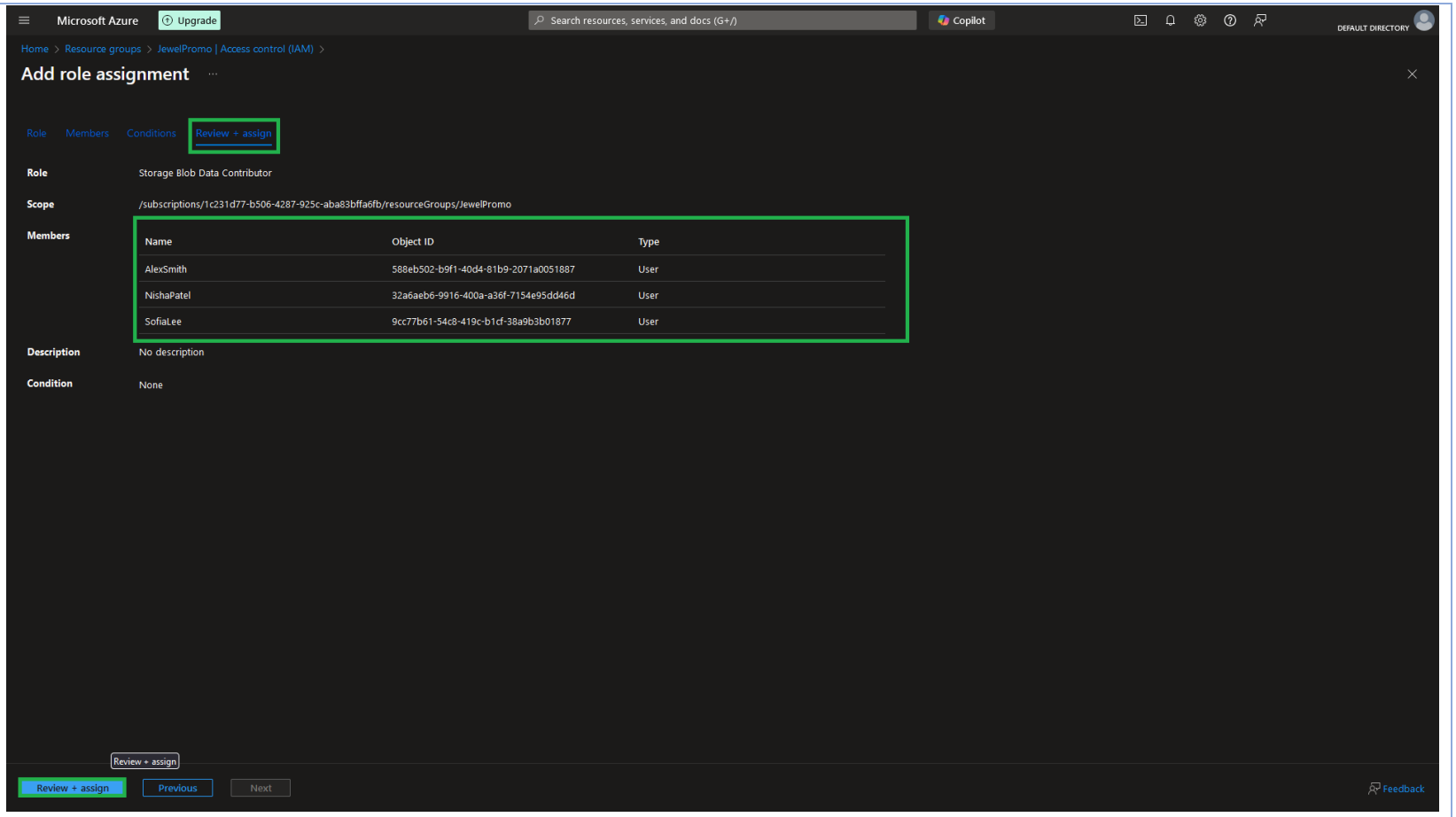
4. On the **Role** tab of the **Add role assignment menu**, on the **Job function roles** tab, in the search box, we search for and select **Storage Blob Data Contributor**, and confirm our selection by clicking on **Next**.



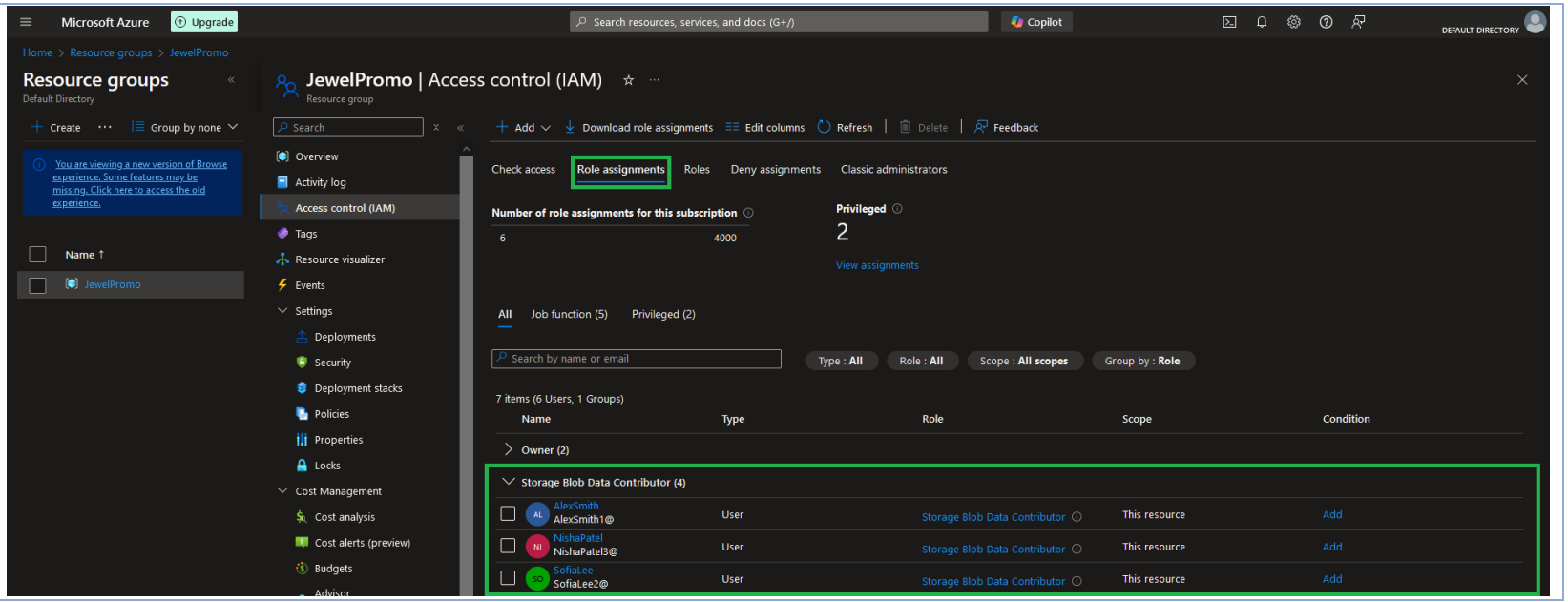
5. On the **Members** tab, in the **Members** section, we choose **Select members**. In the wizard that will pop-up, we choose three users that were created earlier: **AlexSmith**, **SofiaLee**, and **NishaPatel**, and then click on **Select** to confirm our choice.



6. We then on **Review + assign** which will take us to the **Review + assign** tab where we have to once again click on **Review + assign** to assign the roles

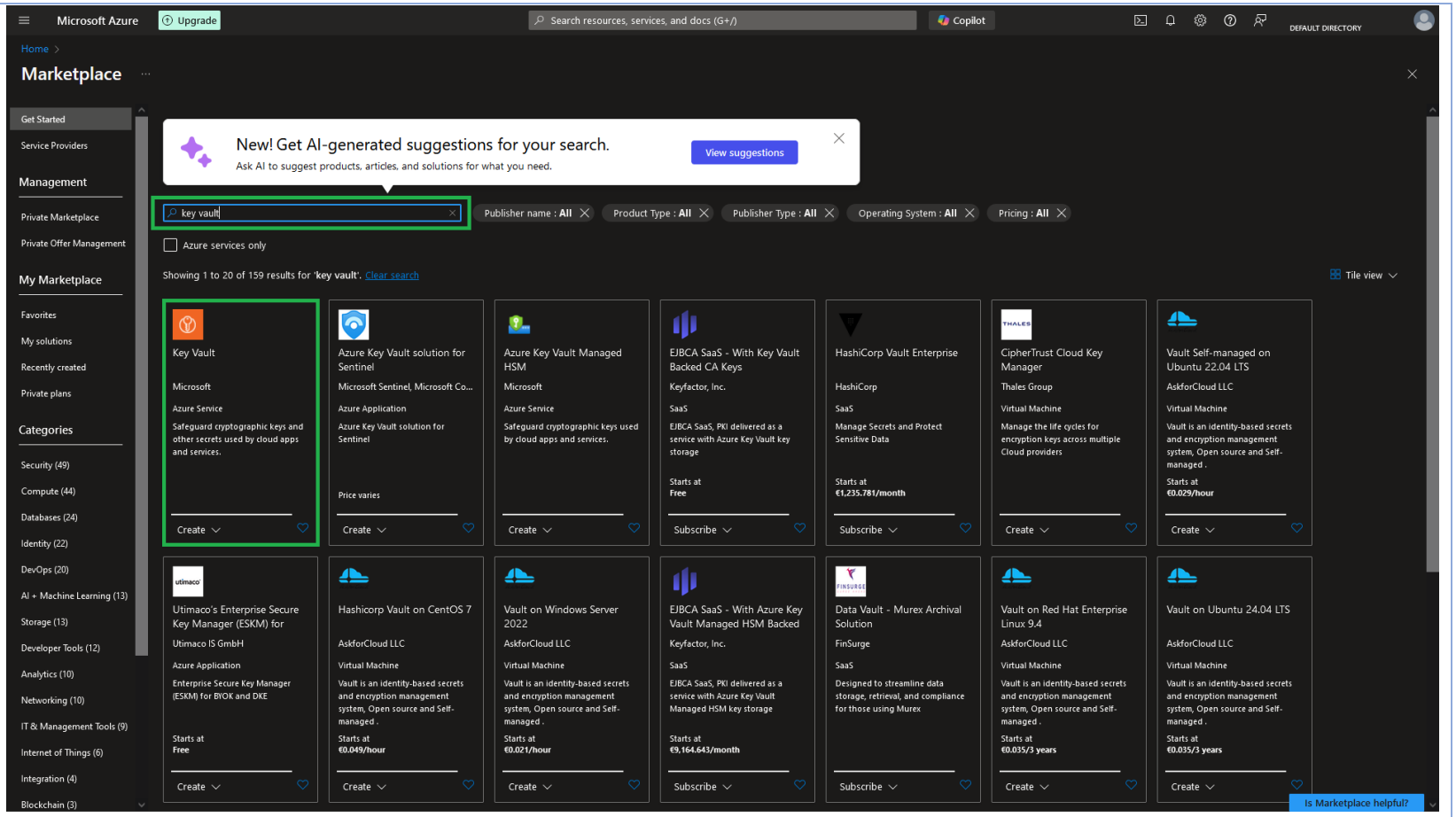


7. This action will take us back to the **Access control (IAM)** menu where on the **Role assignments** tab, we should now be able to see that the users **AlexSmith**, **SofiaLee**, and **NishaPatel** are assigned the **Storage Blob Data Contributor** role.

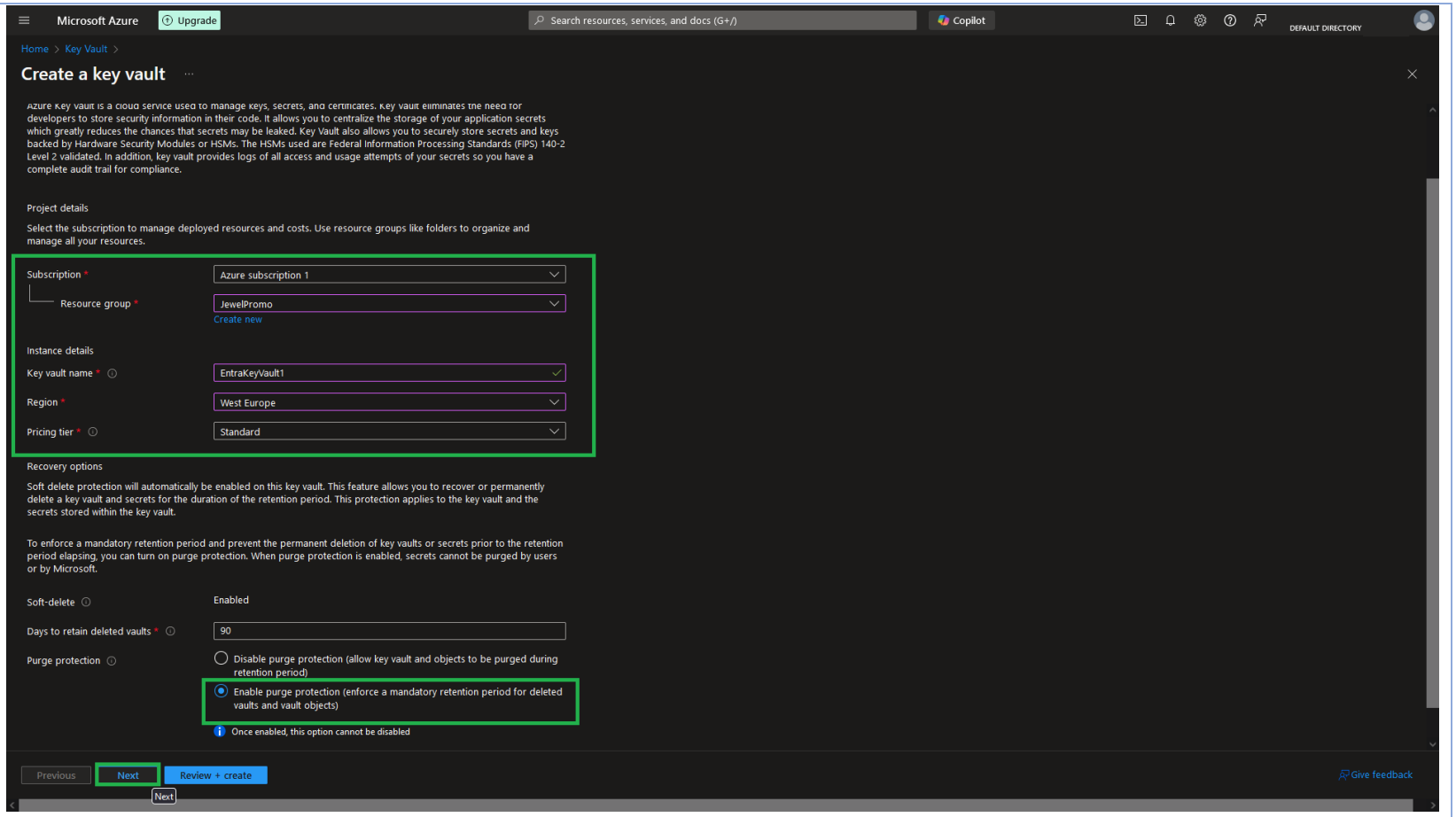
Task 3: Create a Key Vault and a managed identity and encrypt the Storage account using customer-managed keys.

Activity	Key evidence
Activity 1: Create a Key Vault and a managed identity and assign key permissions to the managed identity.	1. From the Azure Portal, we select **Create a resource** to go to the **Marketplace** page where we type “key vault” into the *Search services and marketplace* search box, and then click on **Key Vault** from the results.

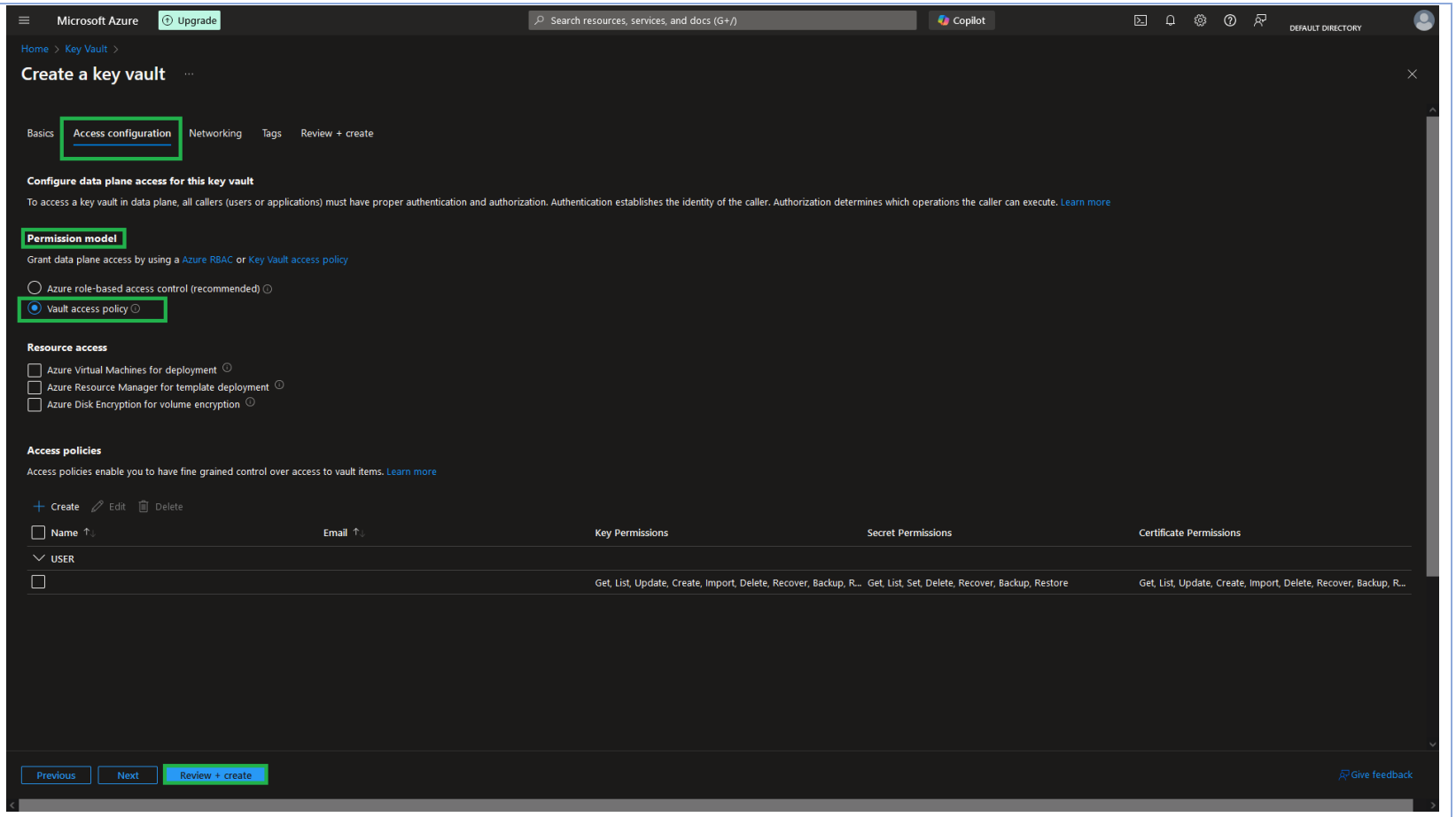


2. On the **Key Vault** page, we then click on **Create** which should open **the Create a key vault** page where we input the following configuration on the **Basics** tab, and then click on **Next**.

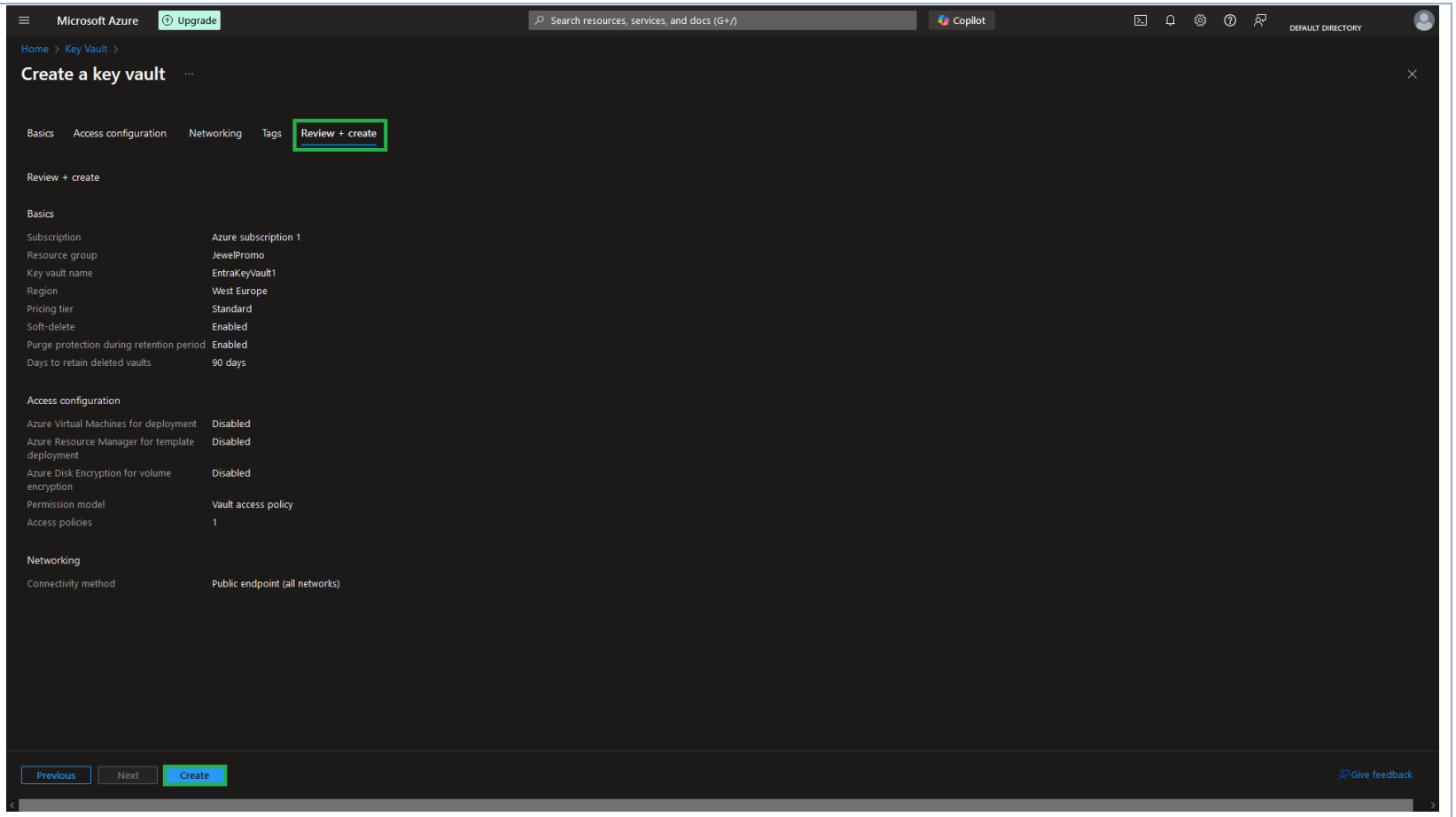
Field	**Value**
Subscription	Select an Azure subscription.
Resource group	Select **JewelPromo**.
Key vault name	Enter a key vault name, **EntraKeyVault1**.
Region	Select the same region as previous resources
Pricing tier	Select **Standard**.
Purge protection	Select **Enable purge protection (enforce a mandatory retention period for deleted vaults and vault objects)**.



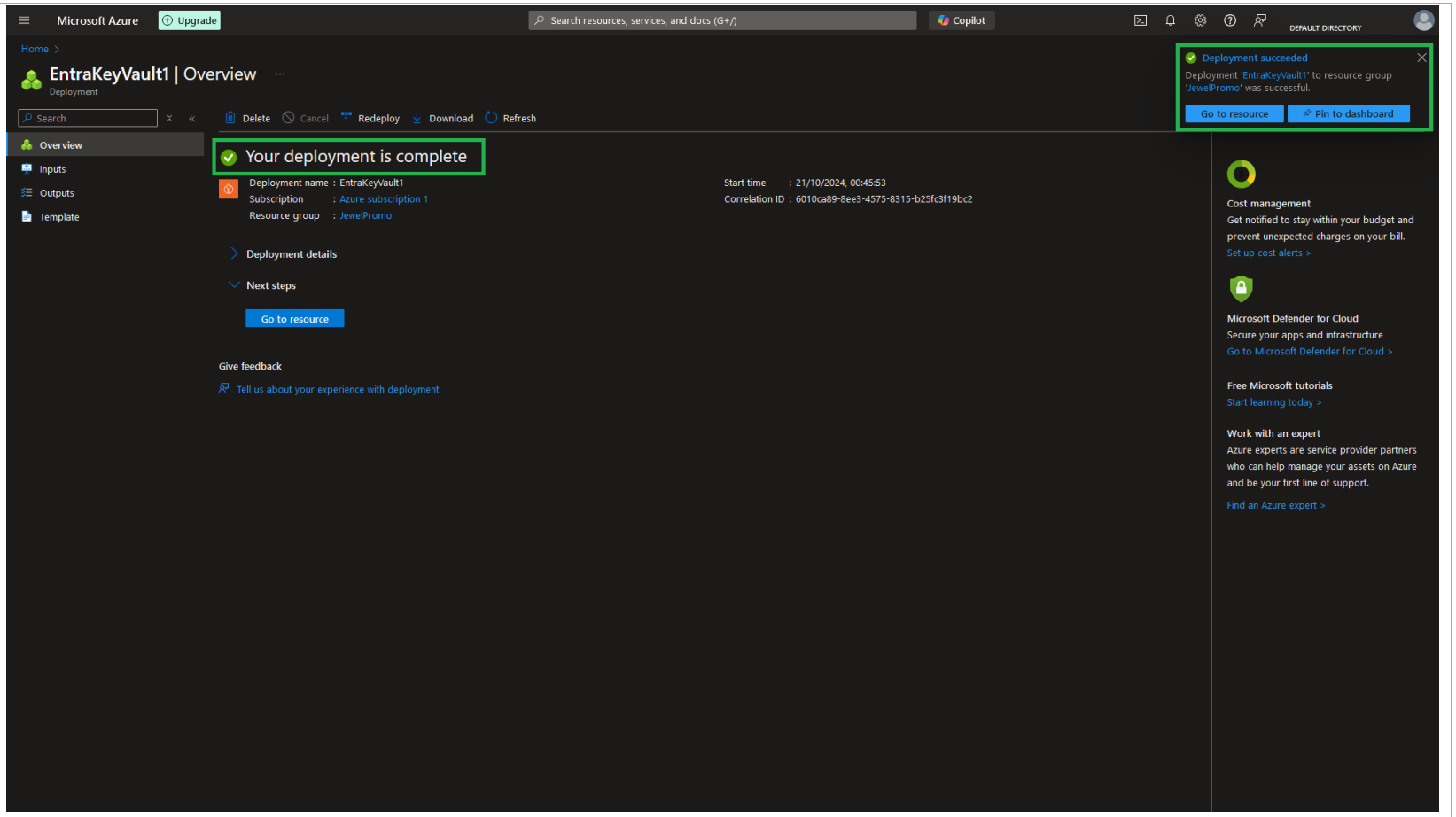
3. On the **Access configuration** tab, in the **Permission model** section, we select the **Vault access policy** radio button, and then click on **Review + Create**.



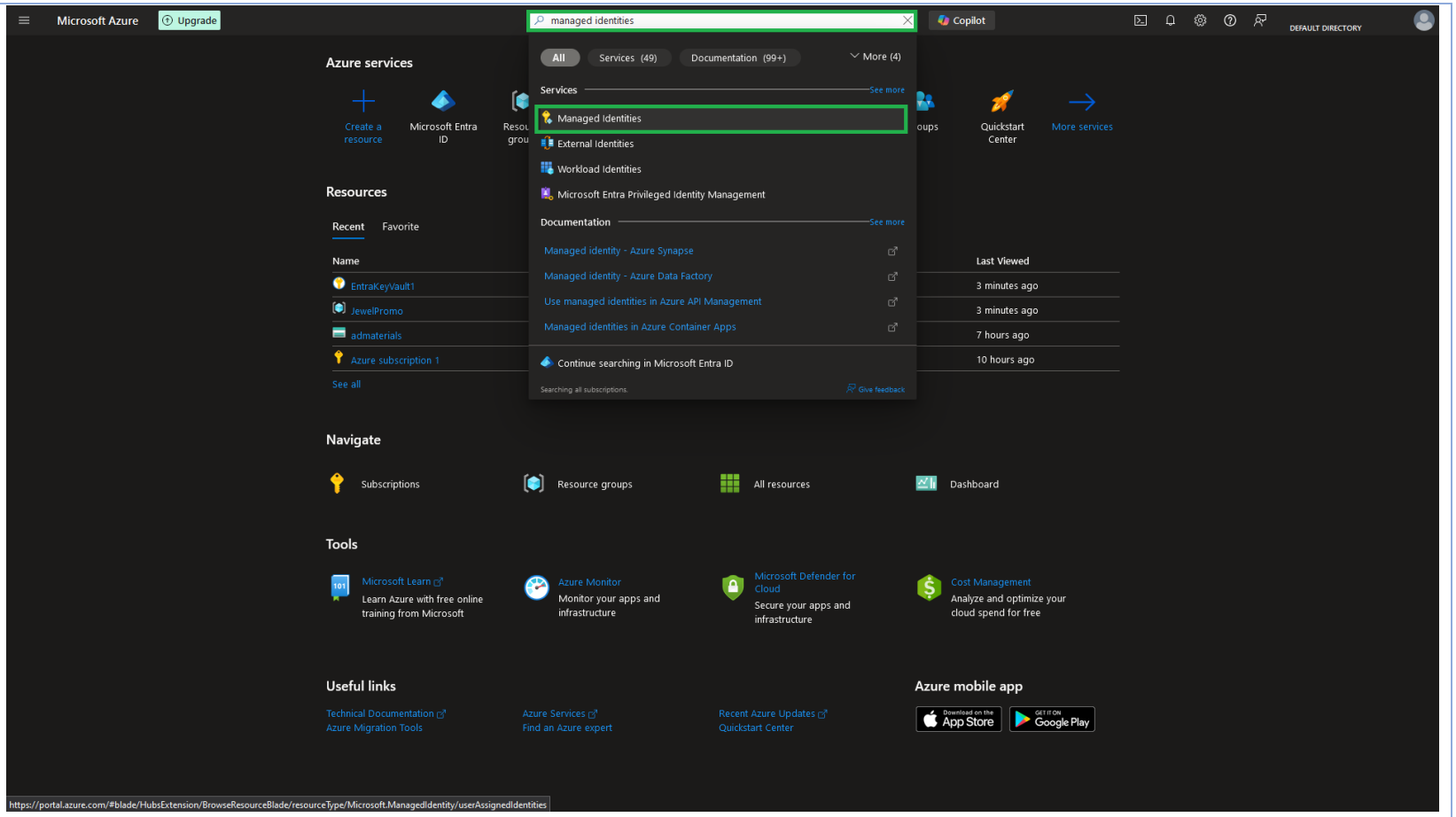
4. On the **Review + create** tab, we review the details, and click on **Create** to deploy the key vault.



5. After a short time, we will be notified that our deployment is complete.

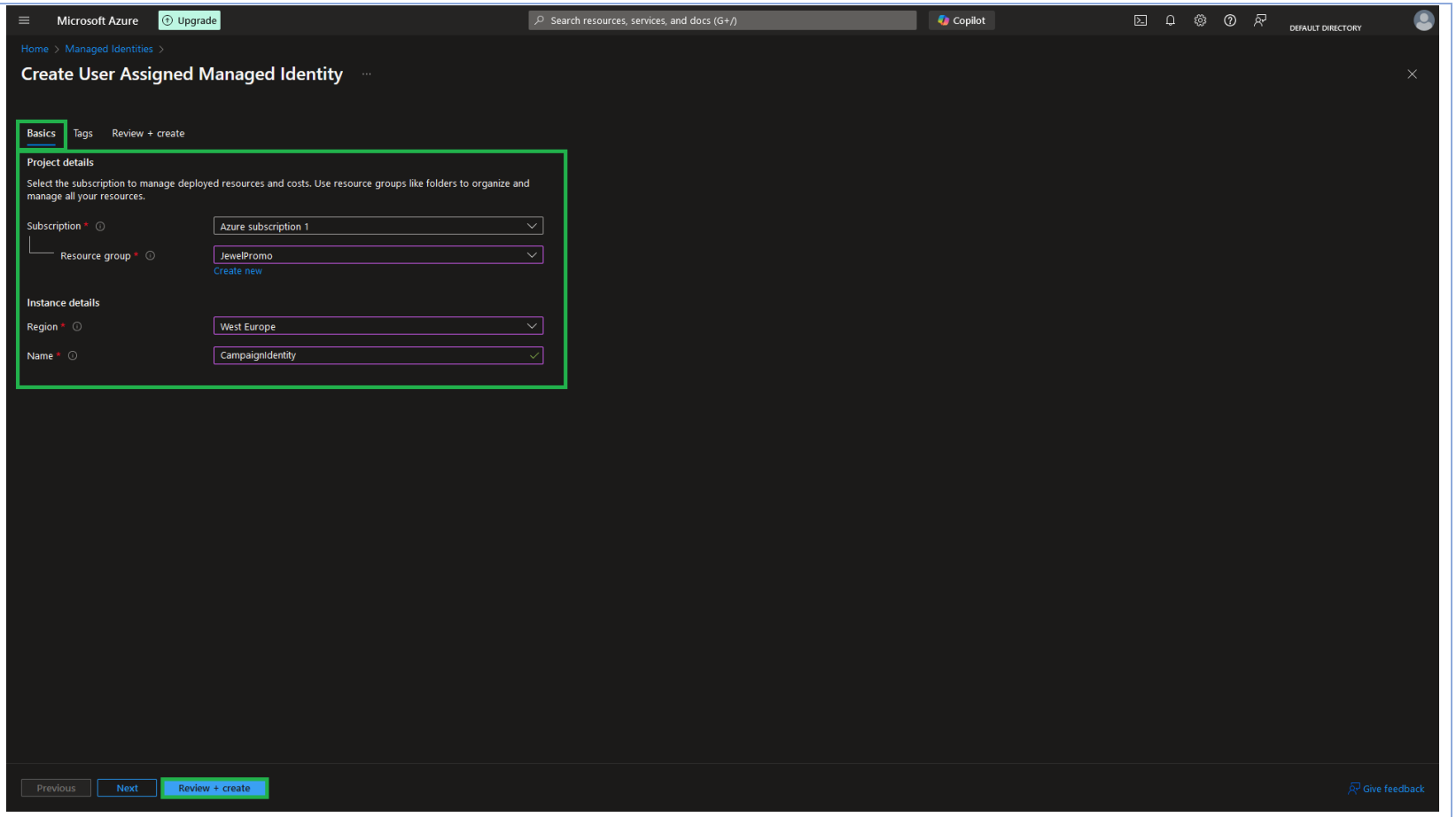


6. We then go back to the Azure Portal home page, and type “managed identities” into the search box.

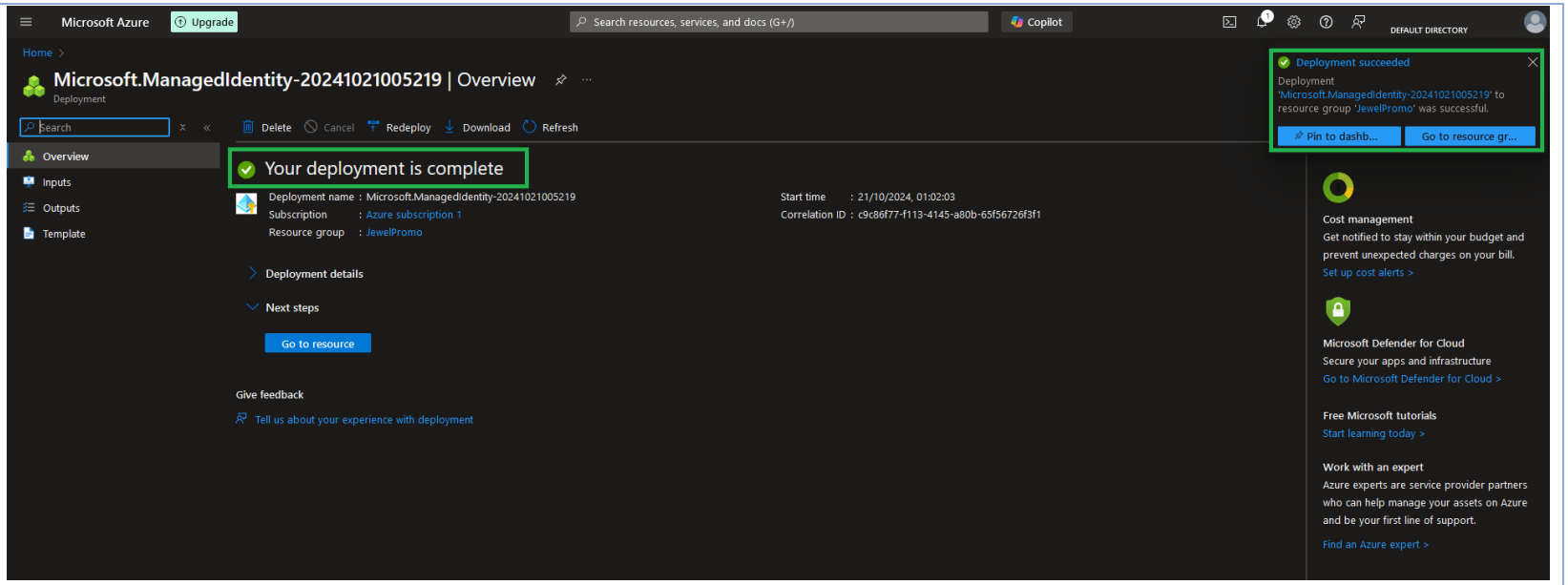


7. On the **Managed Identities** page, we then select **Create** which takes us to the **Create User Assigned Managed Identity** page where we specify the following information into the **Basics** tab, and click on **Review + create**.

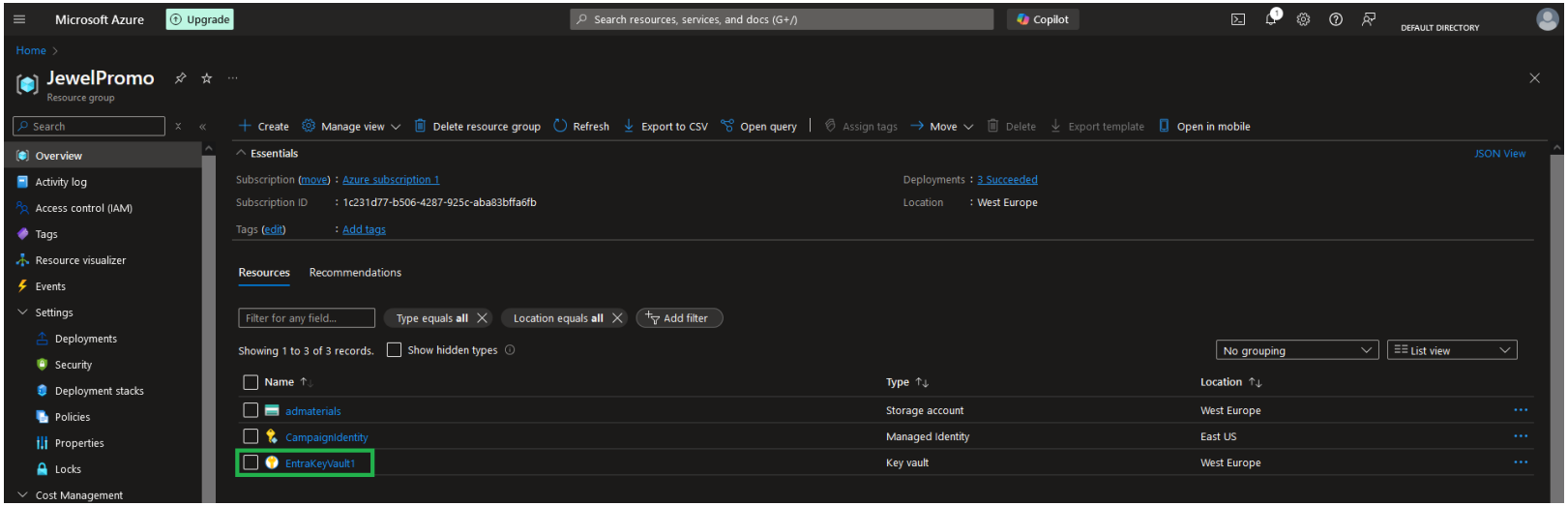
Field	**Value**
Subscription	Select an Azure subscription.
Resource group	Select **JewelPromo**.
Region	Select the same region as previous resources.
Name	Enter a unique name, such as **CampaignIdentity**.



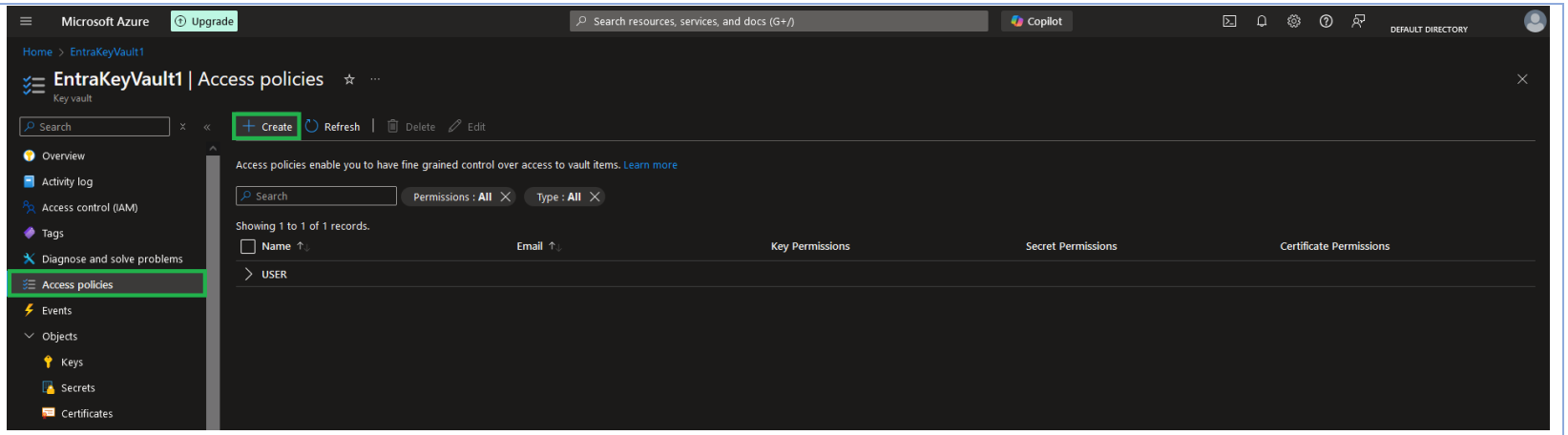
8. On the **Review + create** tab, review the details, click on **Create,** and wait for the notification that the deployment of the managed identity is complete.



9. Next, we navigate to the resource group **JewelPromo** where we deployed **EntraKeyVault1**, and click on it to access its menu.

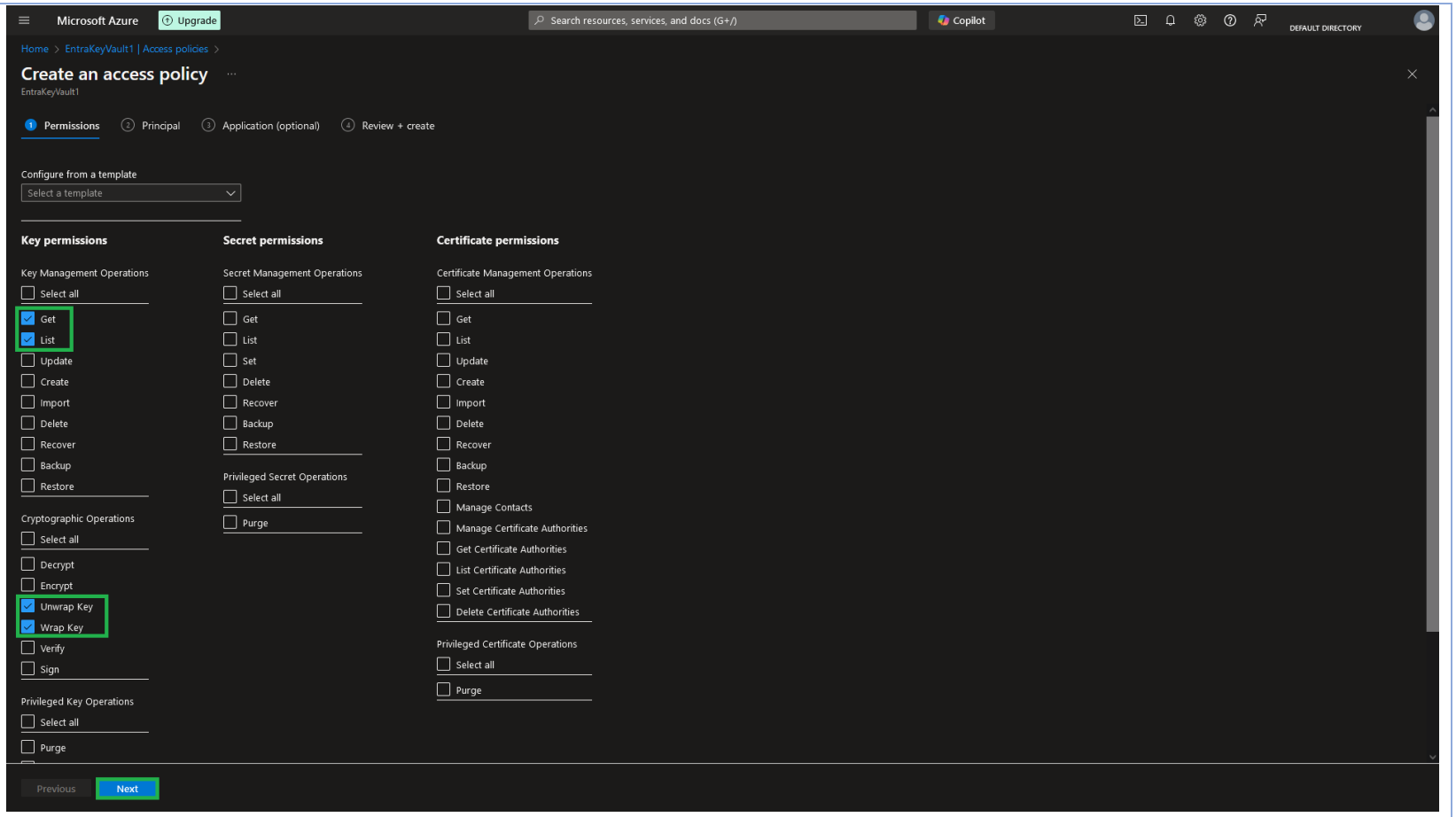


10. From the selected Key Vault's menu, we select **Access policies** and, on the **Access policies** page, click on **Create.**

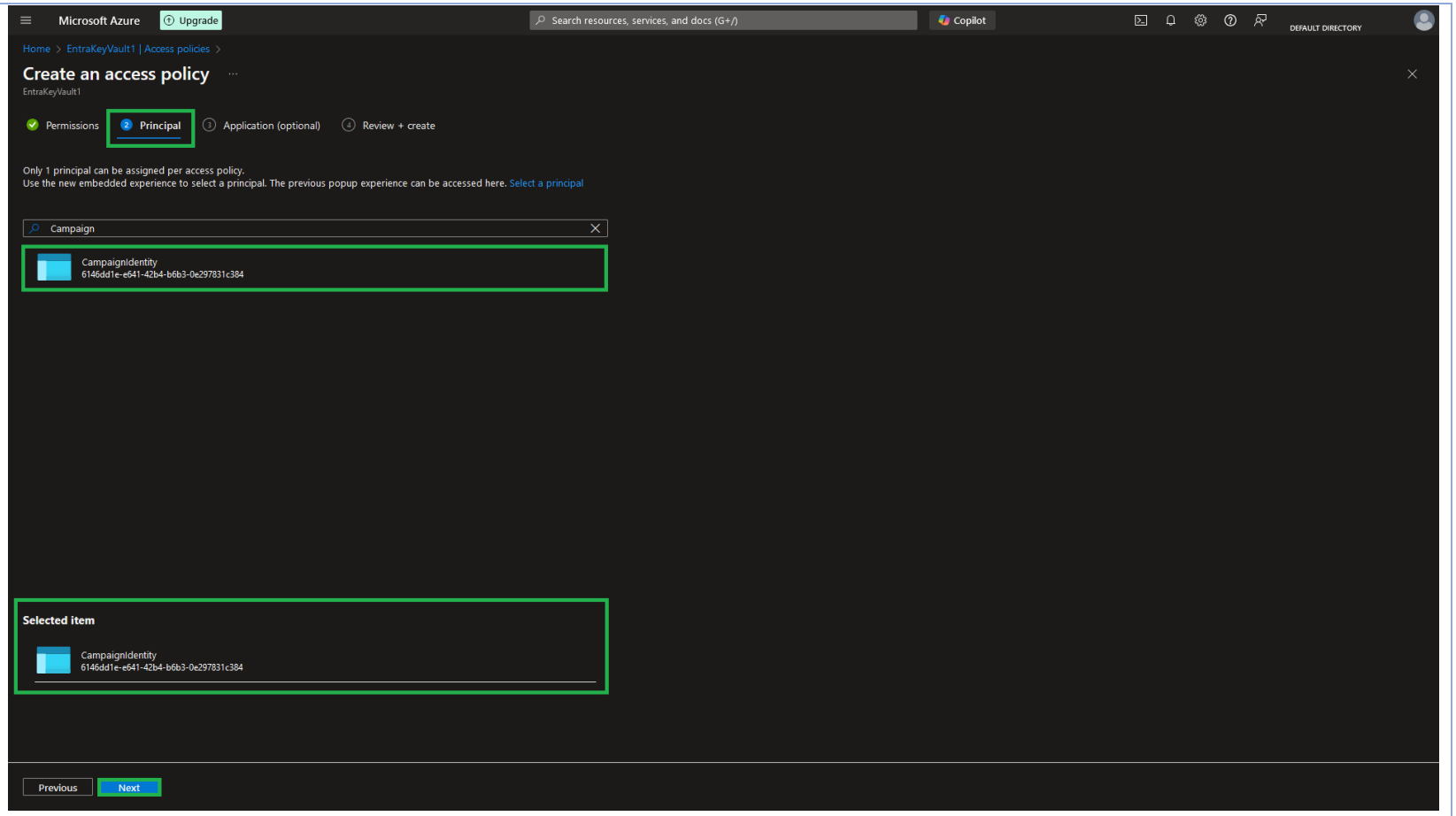


11. On the **Create an access policy** page, we assign the following permissions, and then click on the **Next** button:

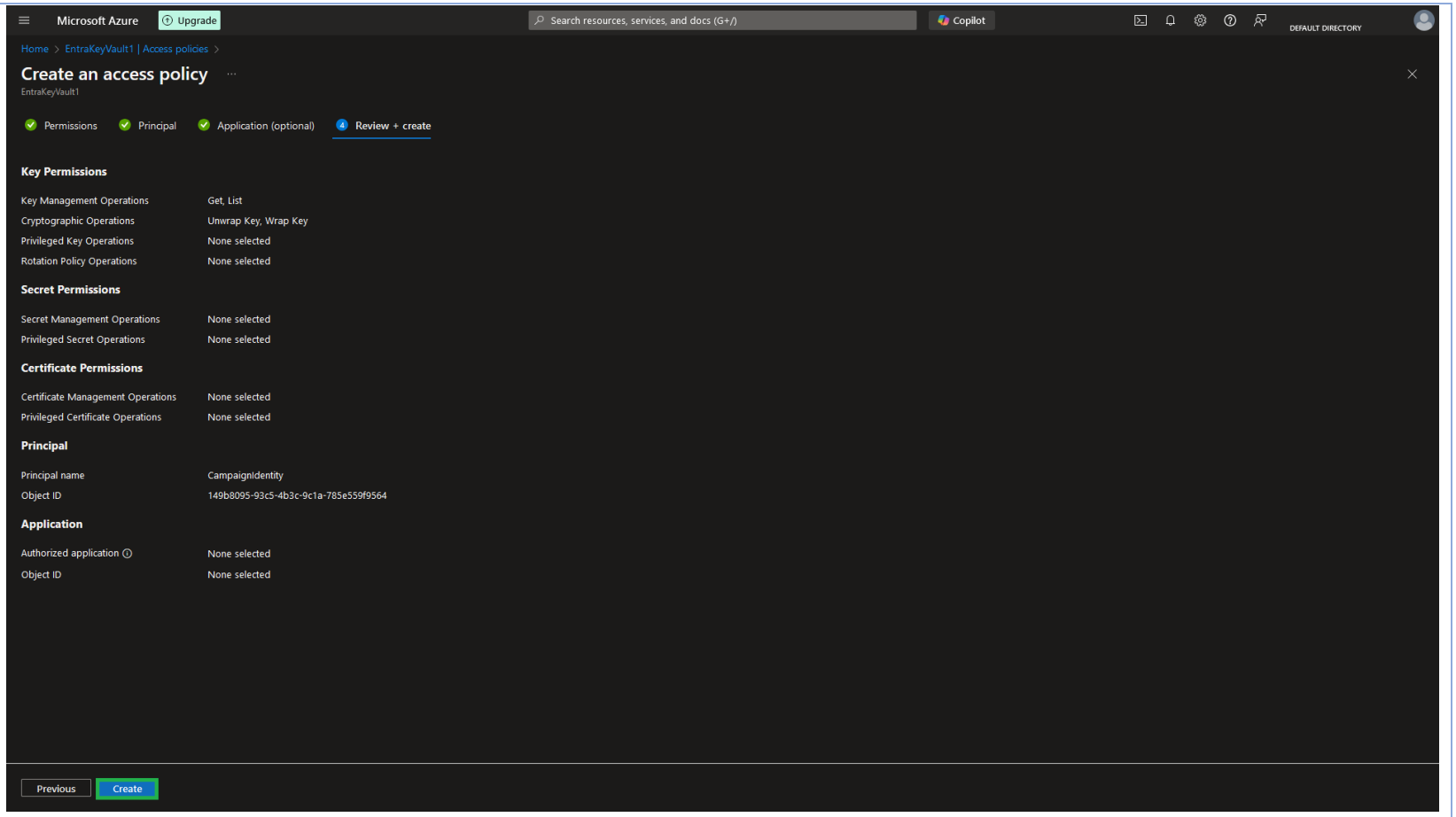
- Under **Key Management Operations**, select **Get** and **List**.
- Under **Cryptographic Operations**, select **Unwrap Key** and **Wrap Key**.



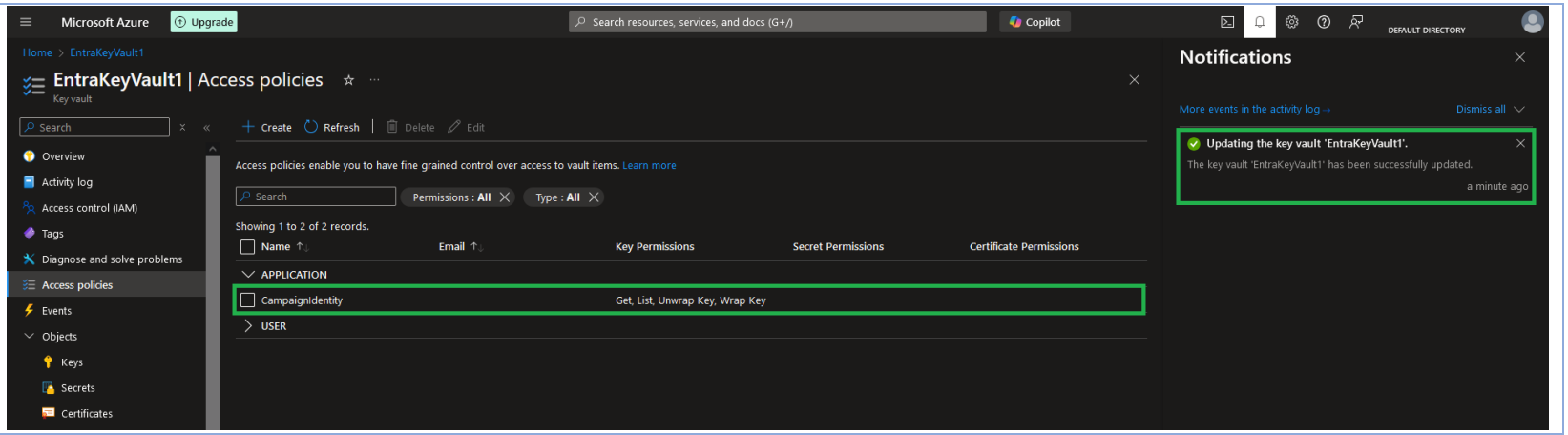
12. On the **Principal** tab, we select the created managed identity, **CampaignIdentity**, and click on **Next**.

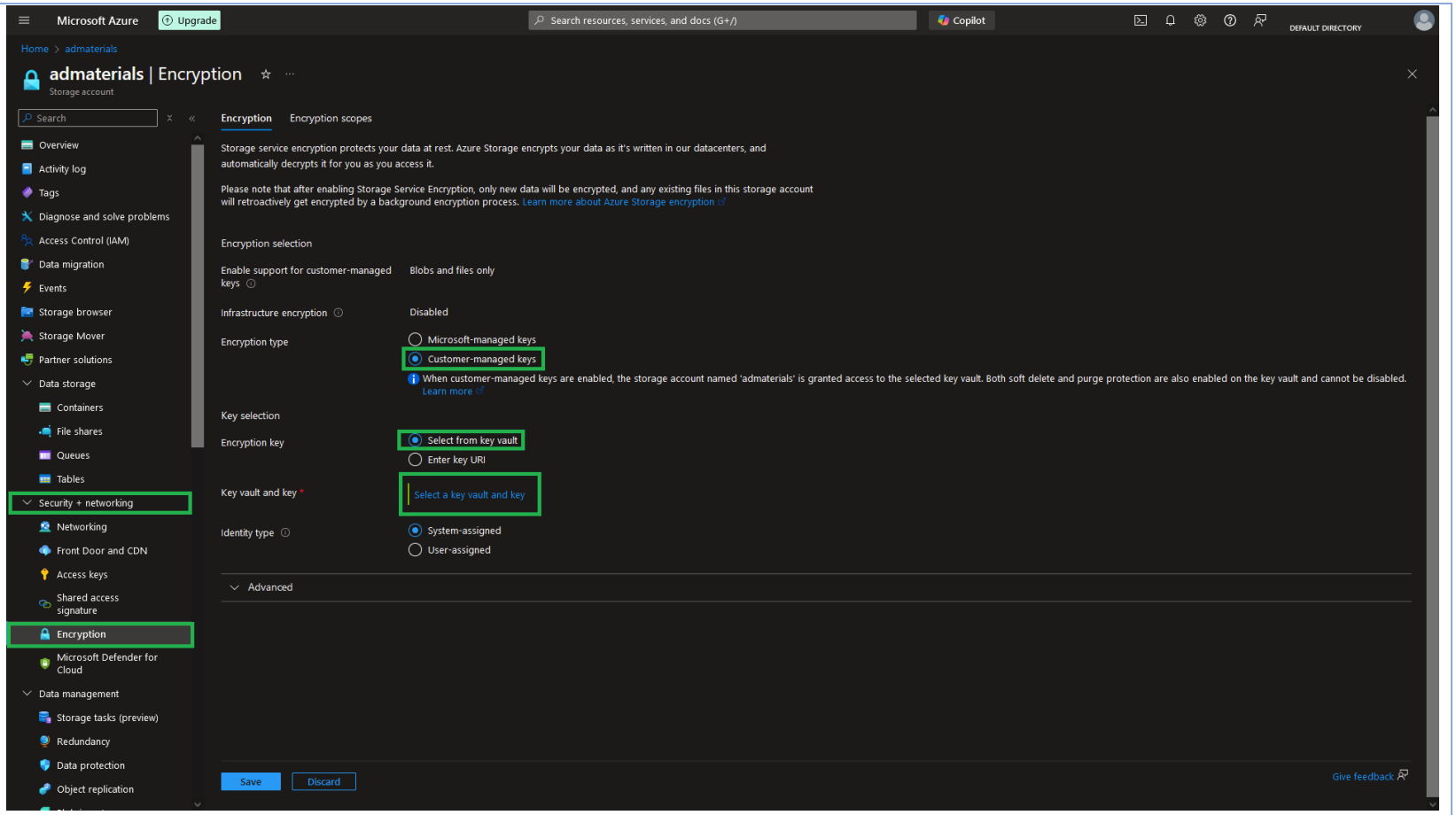


13. We then skip the **Application (optional)** tab by clicking on **Next**, and then select **Create** on the **Review + create** tab.

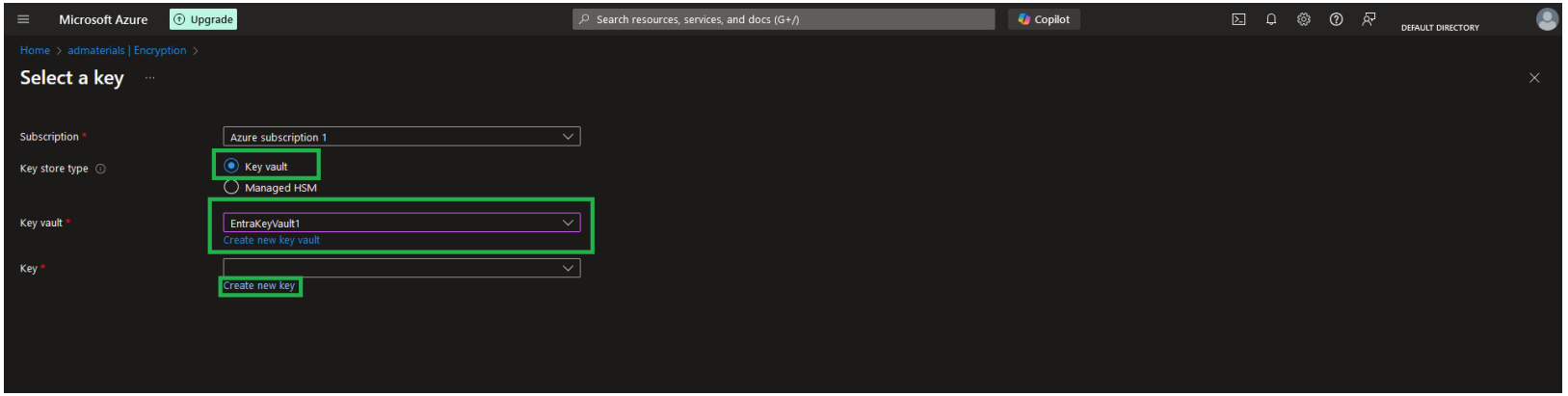


14. On the Key Vault's **Access policies** page, we can now view the key permissions assigned to our new managed identity.

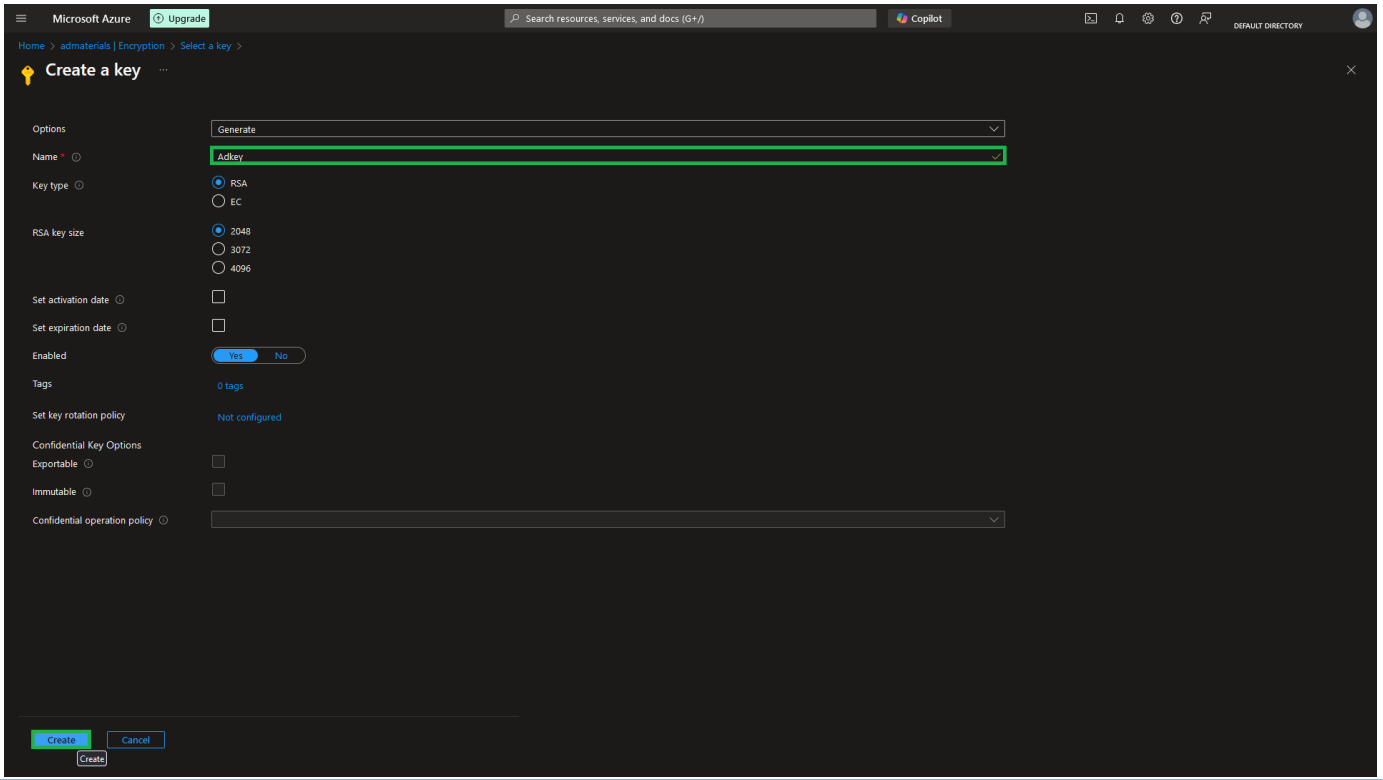
	
Activity 2: Encrypt the Storage account using customer-managed keys.	1. We navigate to our storage account, **adstorage**, and select **Encryption** from the storage account's menu, under the *Security + networking* blade. 2. On the **Encryption** page, we go to the **Encryption** tab and select the **Customer-managed keys radio button** in the **Encryption type** field. 3. Under the **Key selection** section, in the **Encryption key** field, we select the **Select from key vault** radio button, and then in the **Key vault and key** field, choose **Select a key vault and key**.



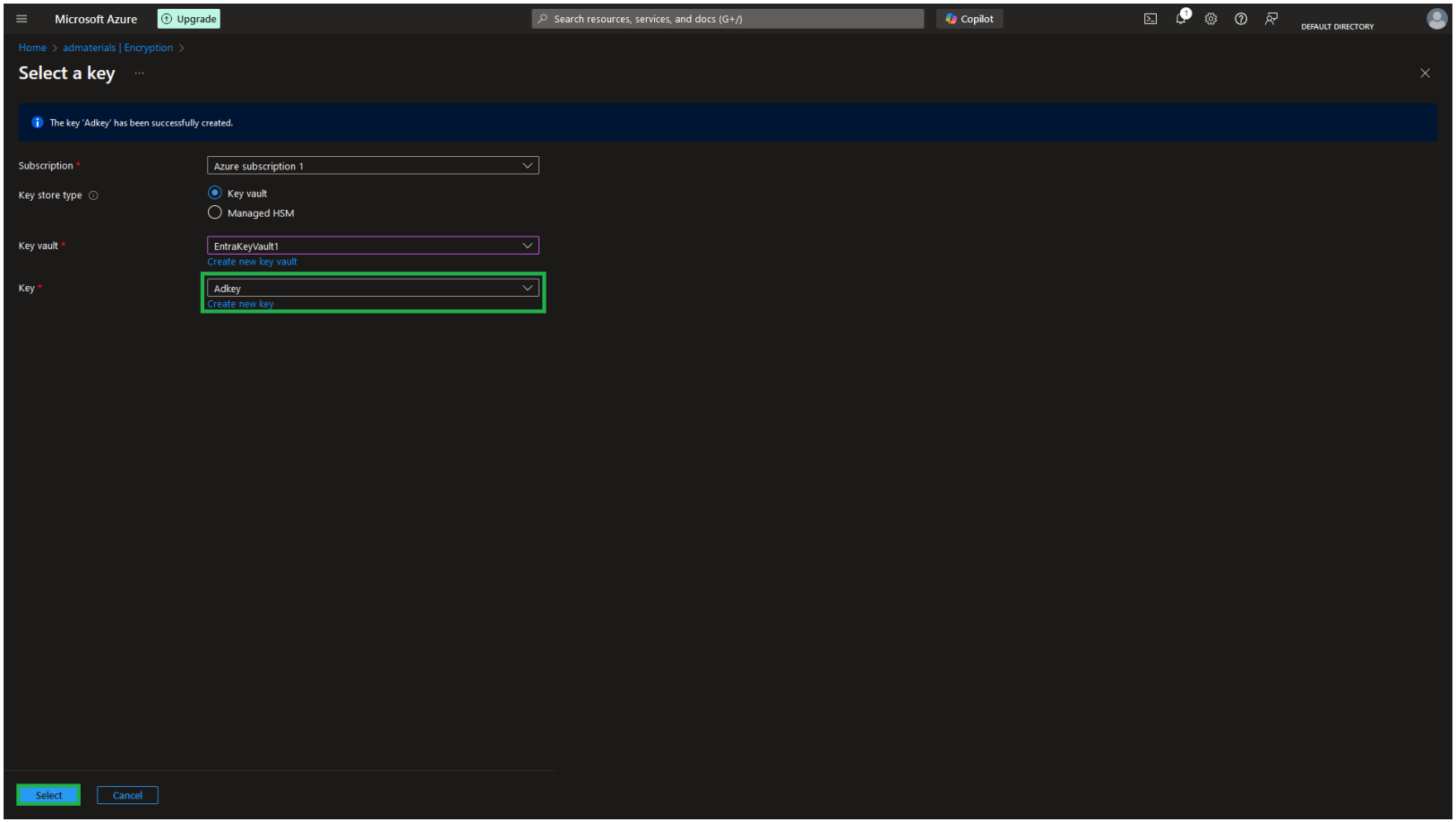
4. On the **Select a key page**, the subscription is automatically populated.
5. In the **Key store type** field, we select the **Key vault** radio button, and then select **EntraKeyVault1** from the dropdown list in the **Key vault field**.
6. Next, in the **Key** field, we click on **Create new key**.



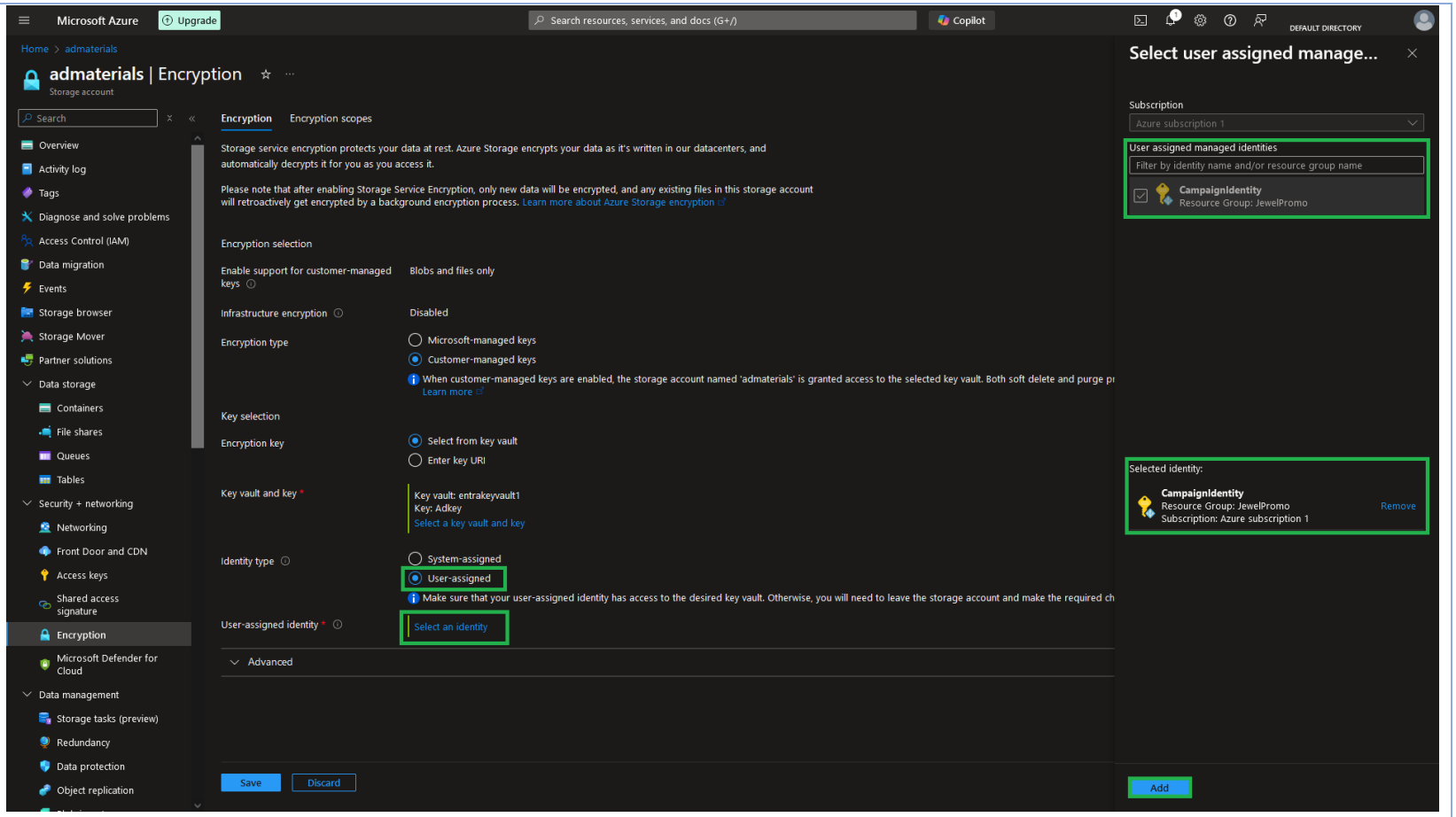
7. On the **Create a key** page, in the **Name** field, we will enter the name, **AdKey**, leave the other options to their defaults, and select **Create**.



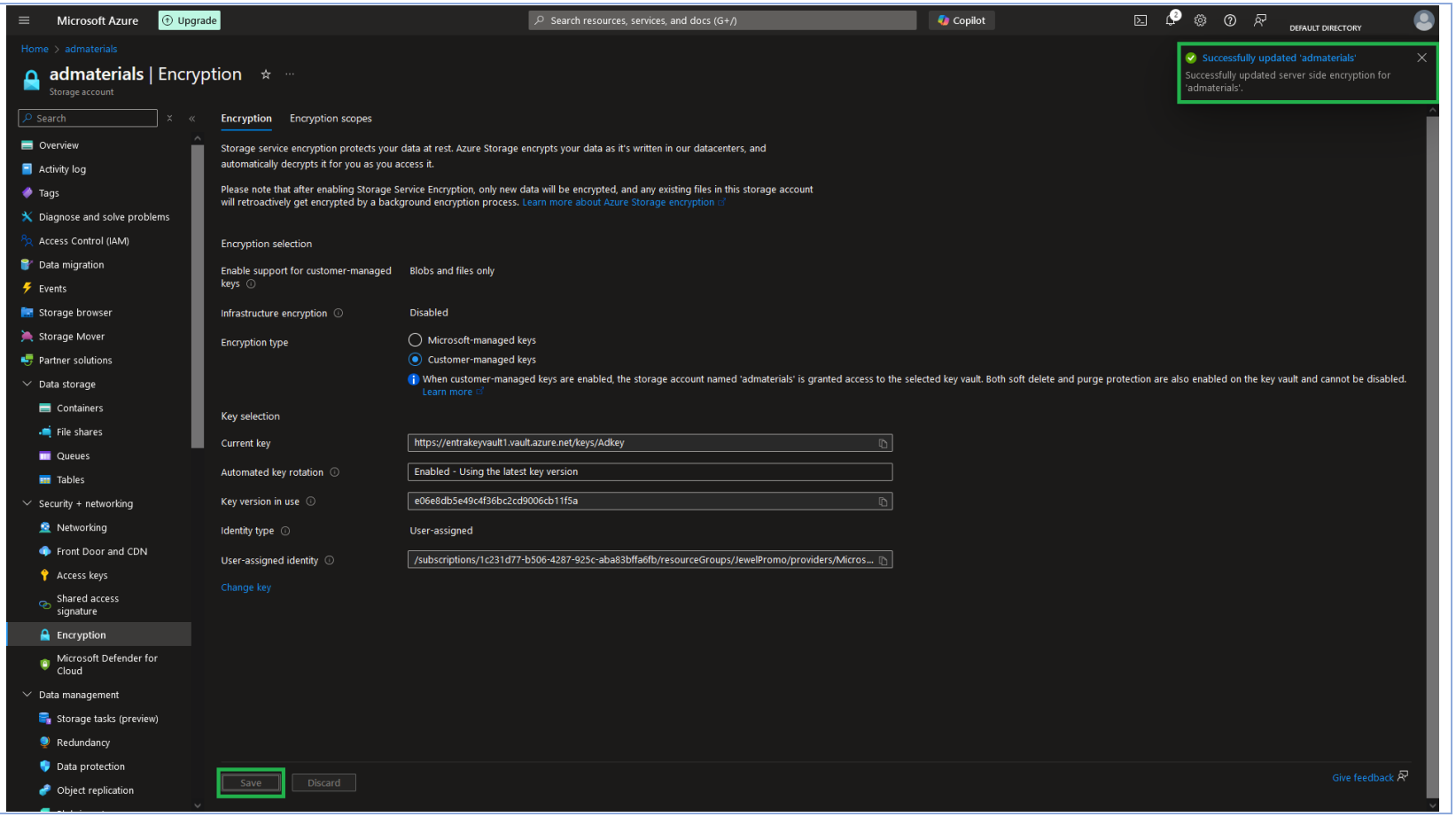
8. Then, on the **Select a key** page, choose **Select** as the key, **AdKey**, is automatically added to the **Key** field



9. Back on the **Encryption** page, in the Identity type field, we select the **User-assigned** radio button, and click on **Select an identity** which will prompt the **Select user assigned managed identity** wizard.
10. We then search for and select **CampaignIdentity** in the **User assigned managed identities field**, and then click on **Add**.

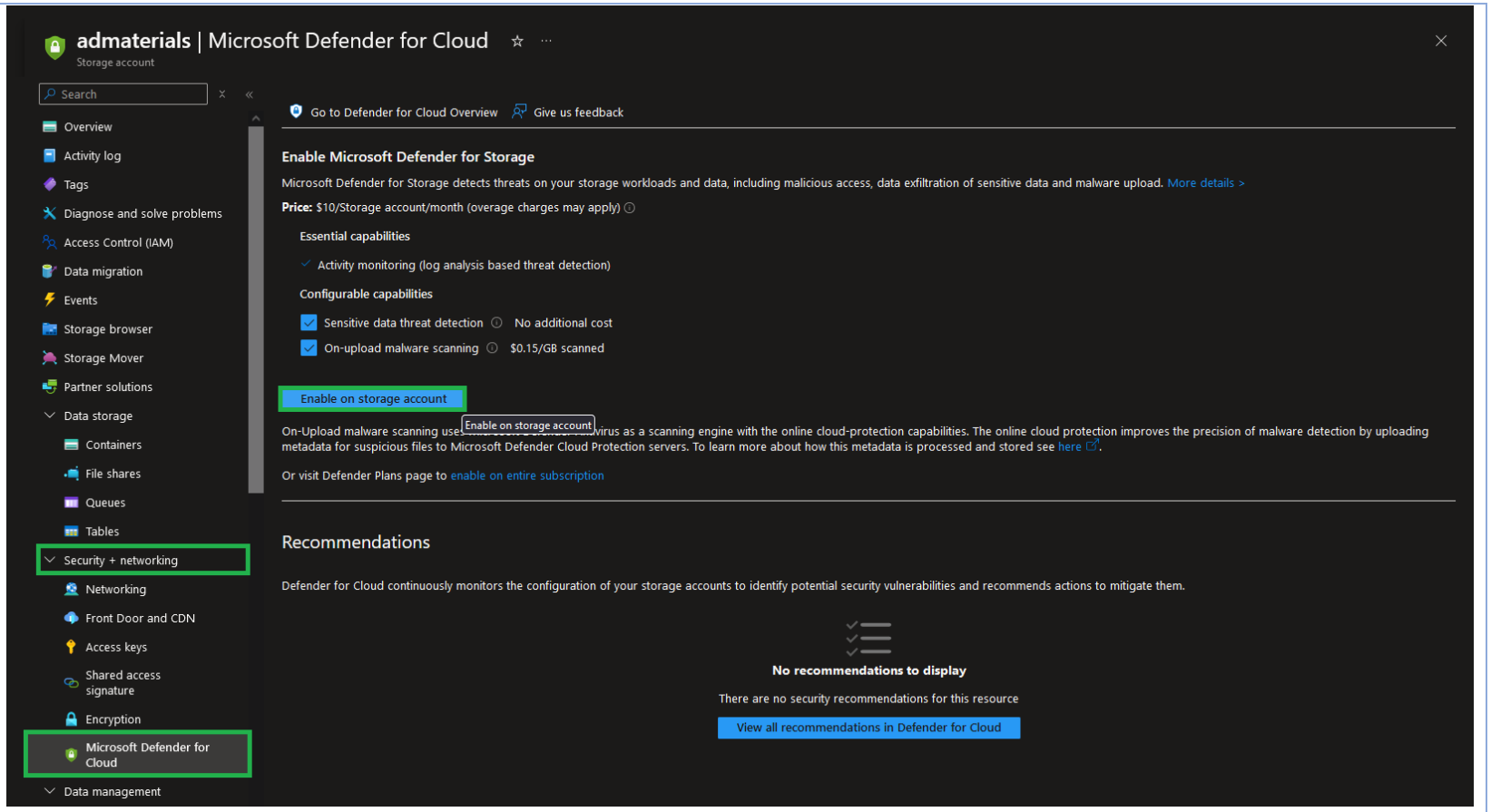


11. Then, the **Encryption** page, select **Save** and check for the notification which confirms that the storage account is successfully encrypted using customer-managed keys.

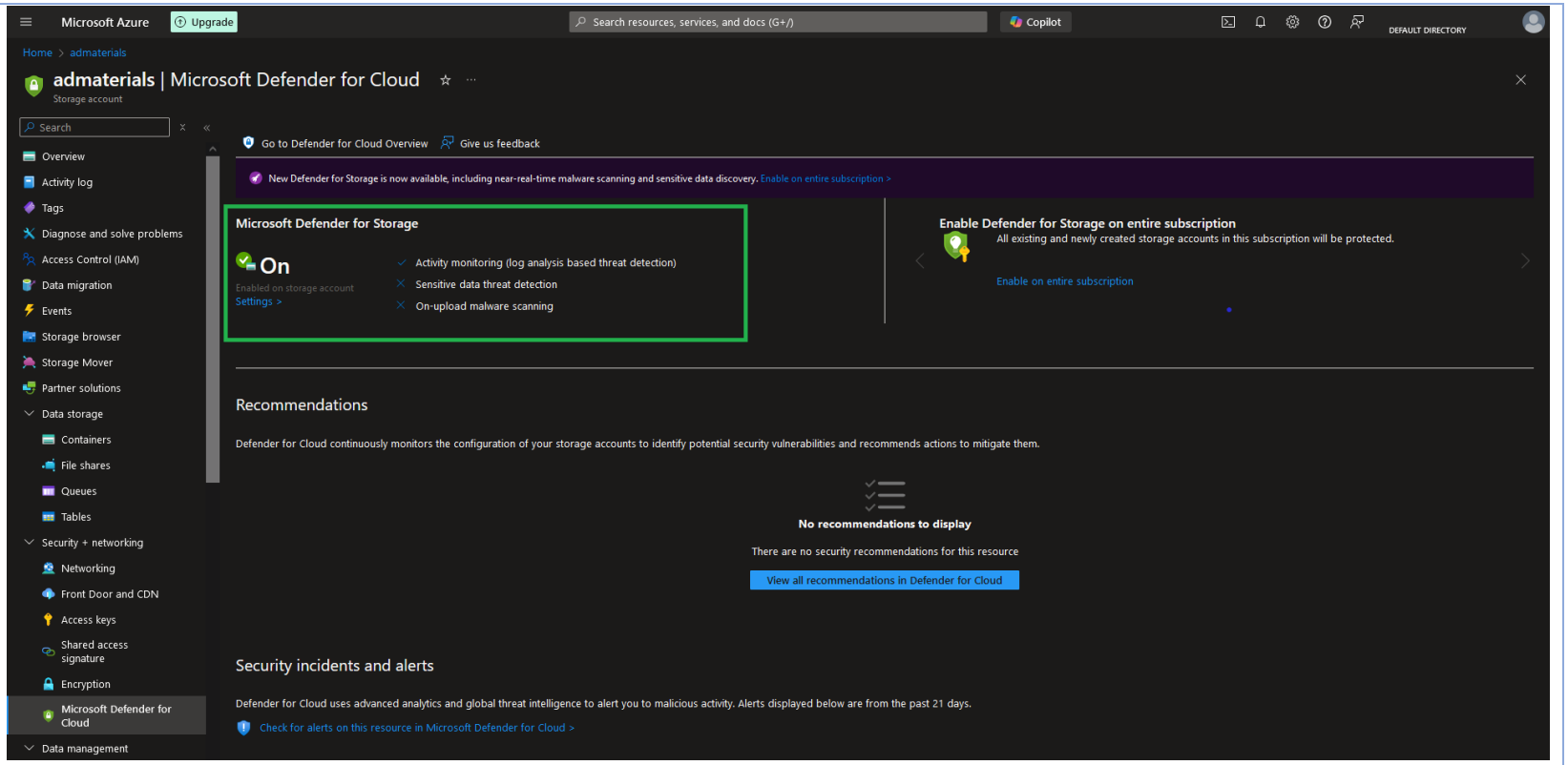


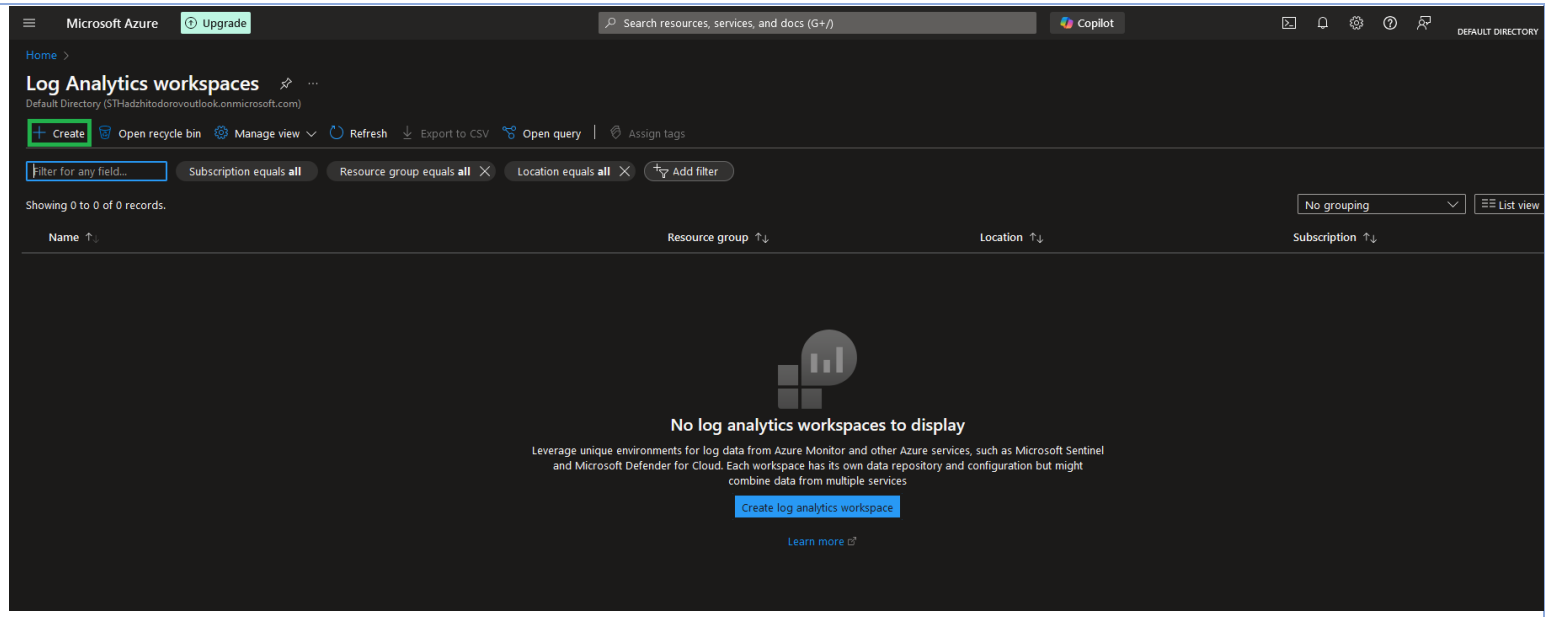
Task 4: Secure the Storage account using Microsoft Defender and Log Analytics workspace.

Activity	Key evidence
Activity 1: Enable Microsoft Defender for Storage for the Storage account.	1. We navigate to the **admaterials** storage account page, select **Microsoft Defender for Cloud** under *the Security + Networking* blade, and click on the **Enable on storage account** button.

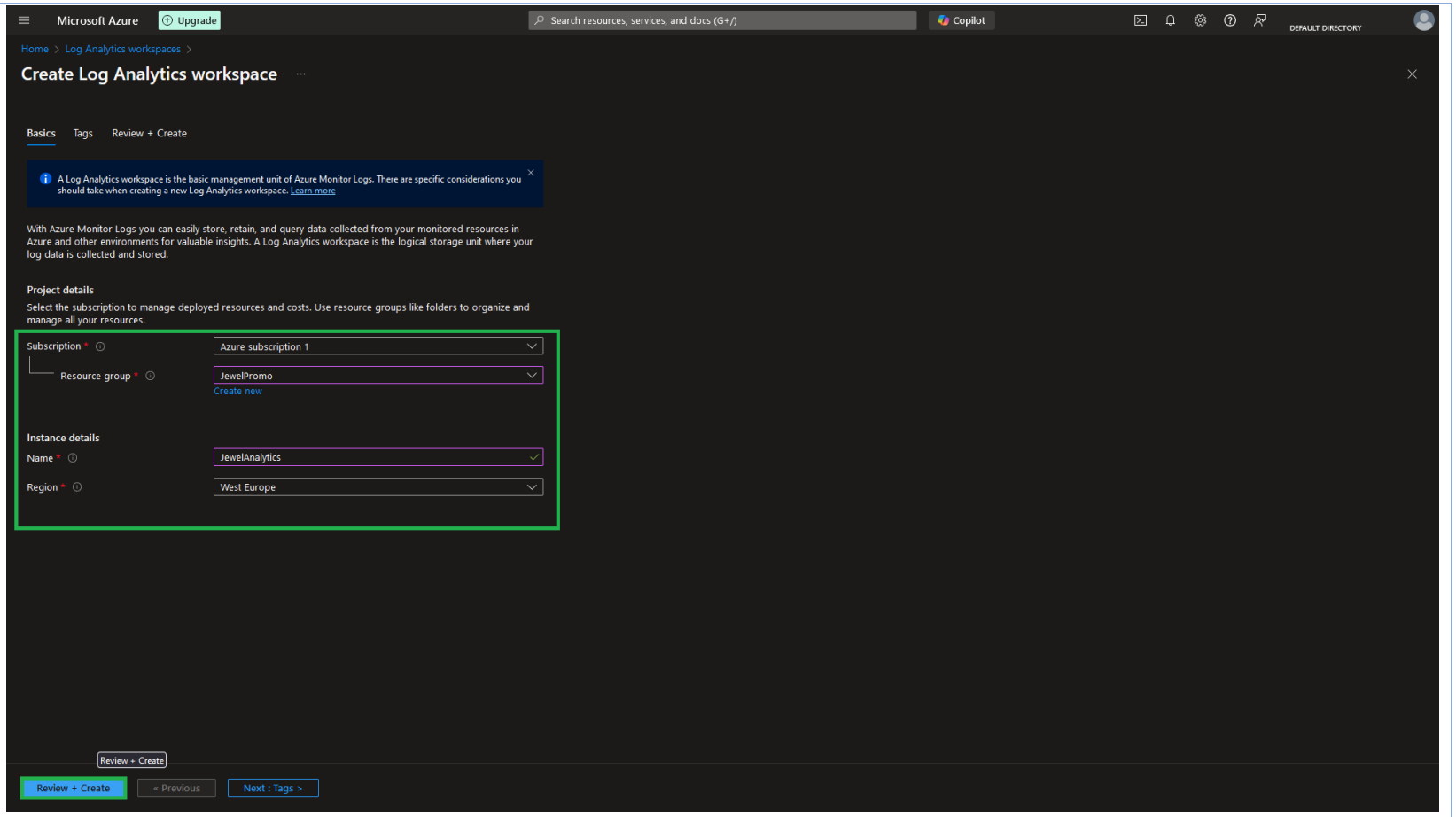


2. Now that **Microsoft Defender for Storage is enabled**, it's on status is visible on the **Defender for Cloud** page.

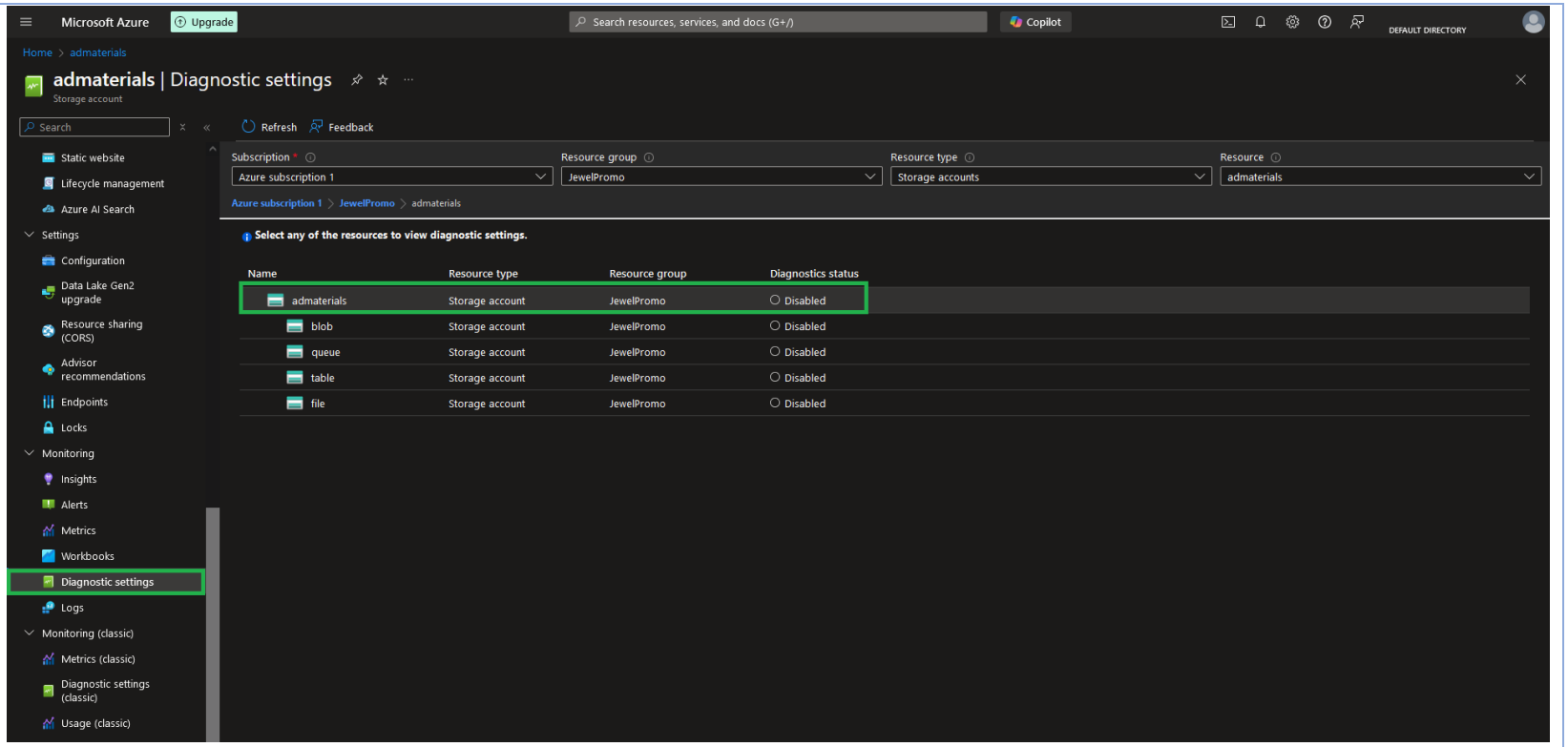
	
Activity 2: Configure diagnostic settings to send data to the Log Analytics workspace.	1. We need to create a **Log Analytics workspace** which is done by inputting “log analytics workspaces” in the search bar and going to the **Log Analytics workspaces** page where we then click on **Create**.



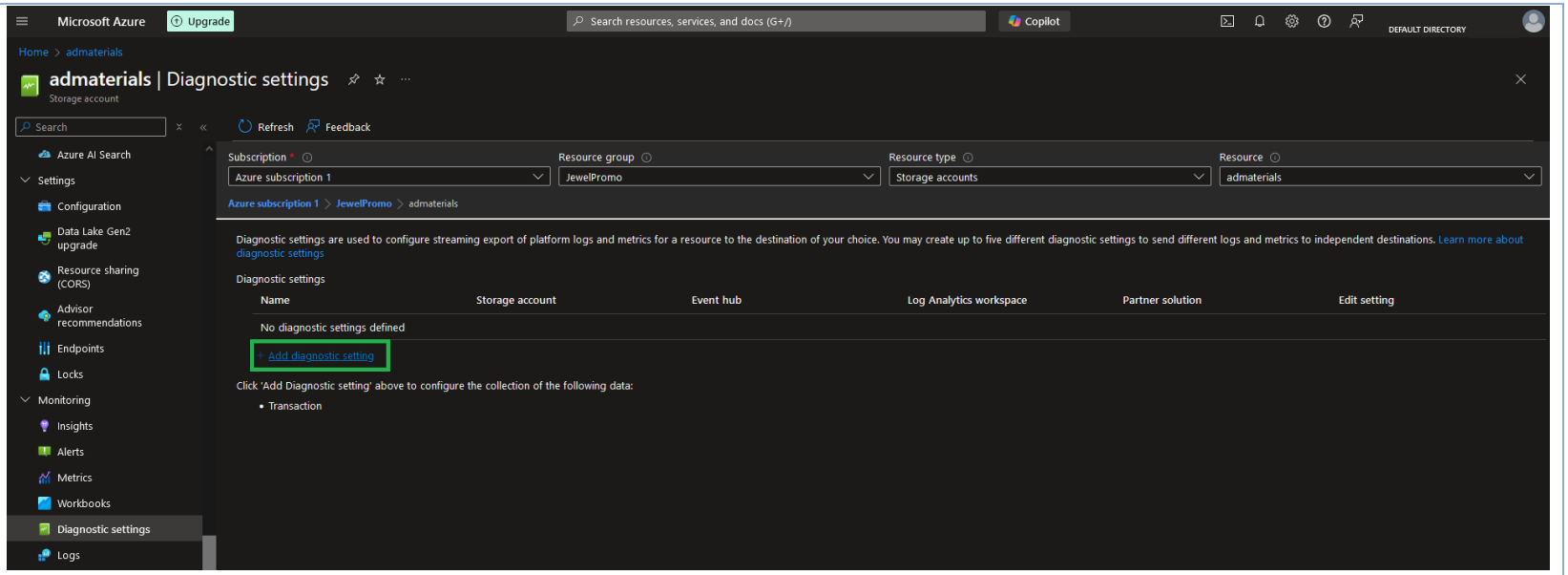
2. We then create a new **Log Analytics workspace** named **JewelAnalytics** in the **JewelPromo** resource group and wait the deployment to complete.



3. We then click on **Diagnostic settings** under the *Monitoring blade* on the storage account page, and select **admaterials** from the list of resources.

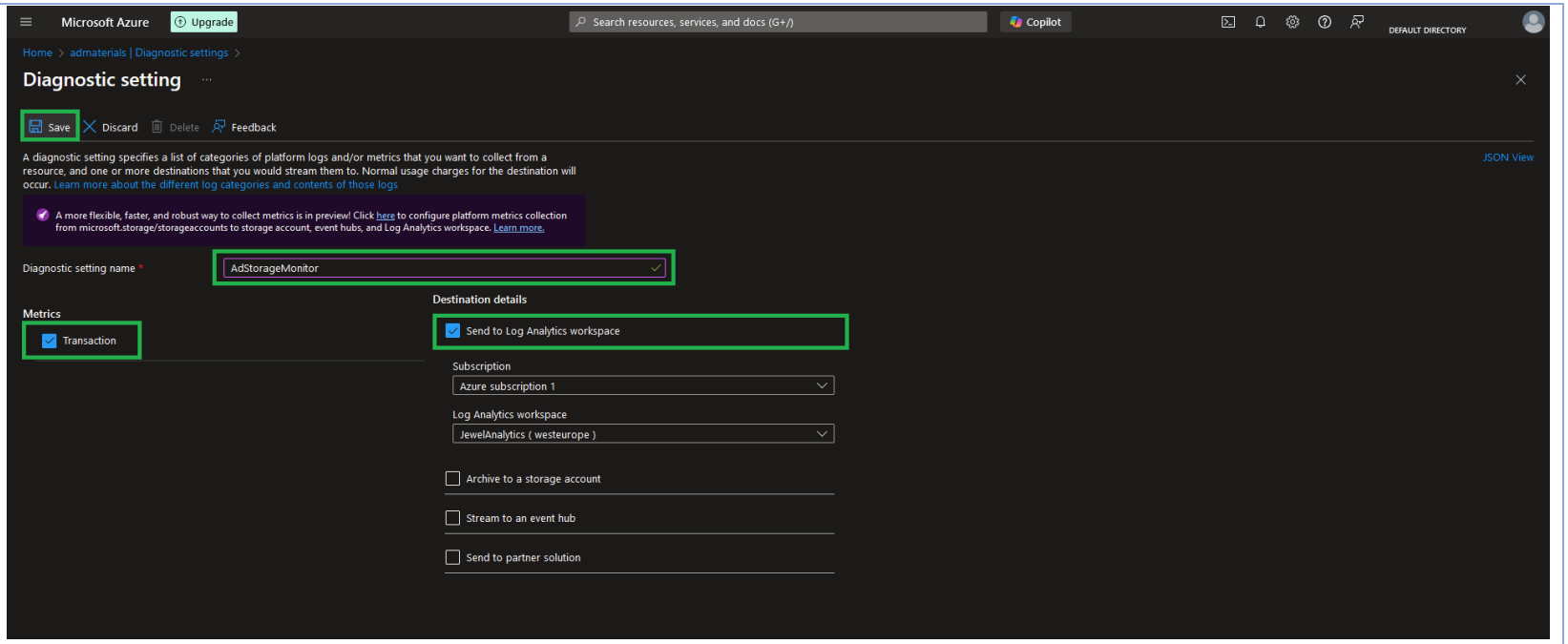


4. On the **Diagnostic settings** page, we select **Add diagnostic setting**.

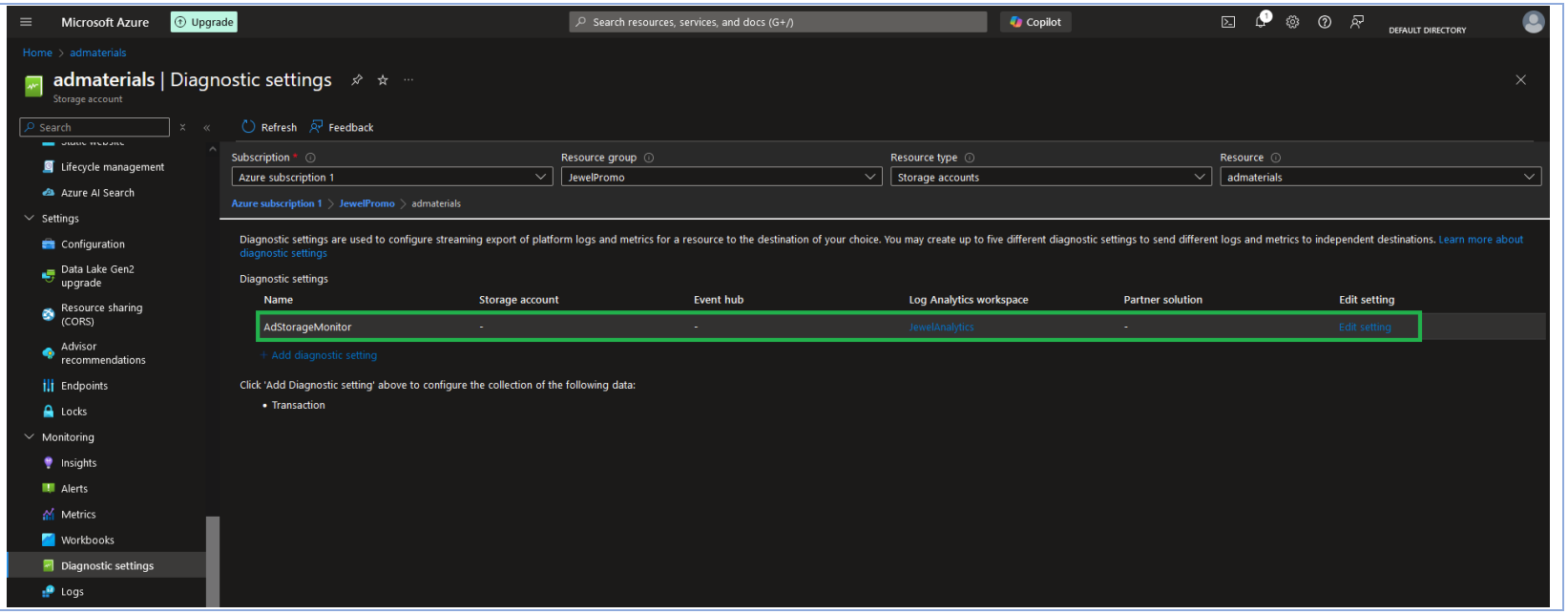


5. We then specify the following information, and click on **Save**.

Field	**Value**
Diagnostic setting name	Enter the diagnostic setting name, **AdStorageMonitor**.
Destination details	Select the **Send to Log Analytics workspace** checkbox.
Metrics	Select the **Transaction** checkbox.

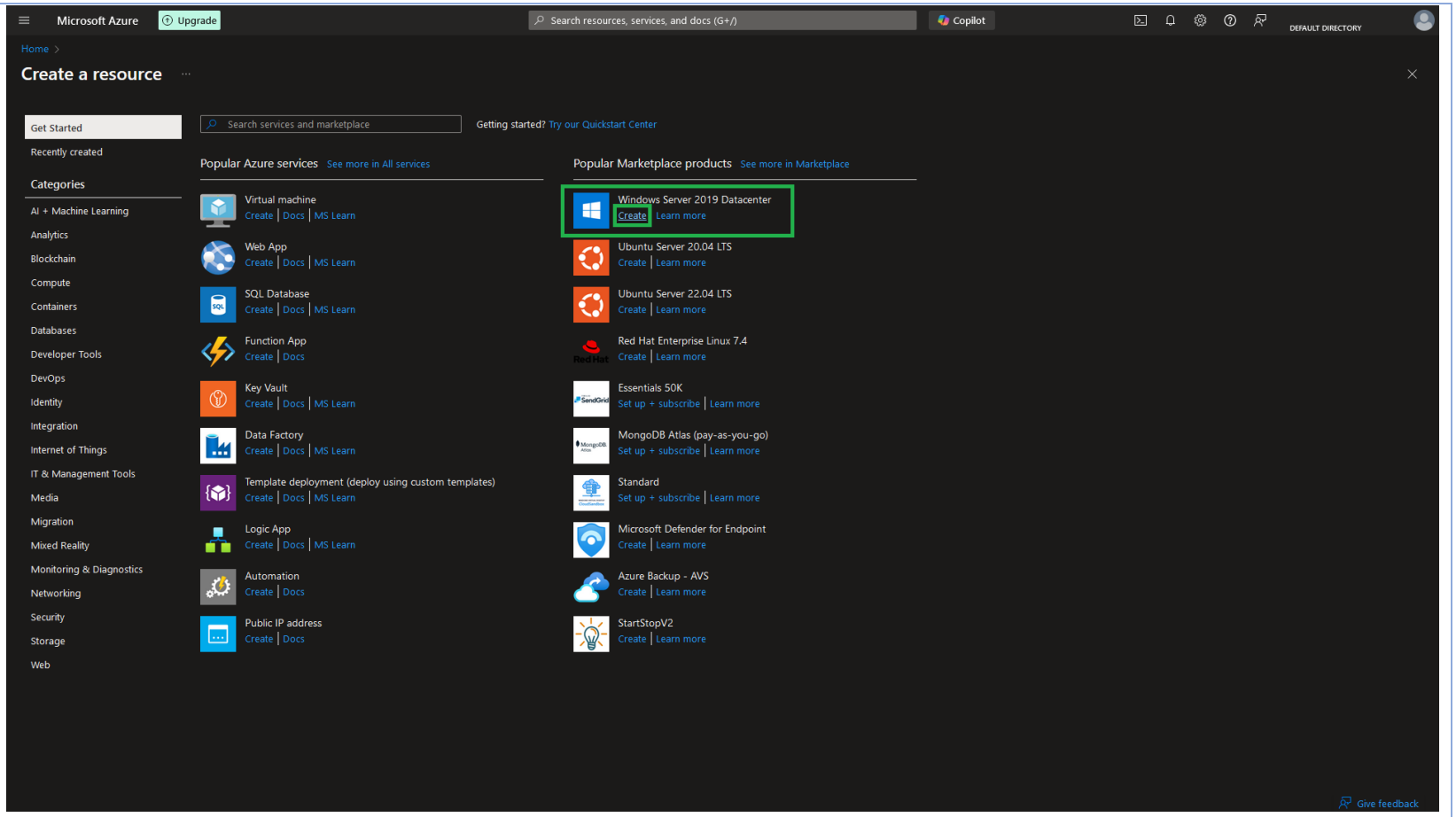


6. We should then receive a notification that the **AdStorageMonitor** diagnostic setting has been added and be able to view it on the **Diagnostic settings** page.

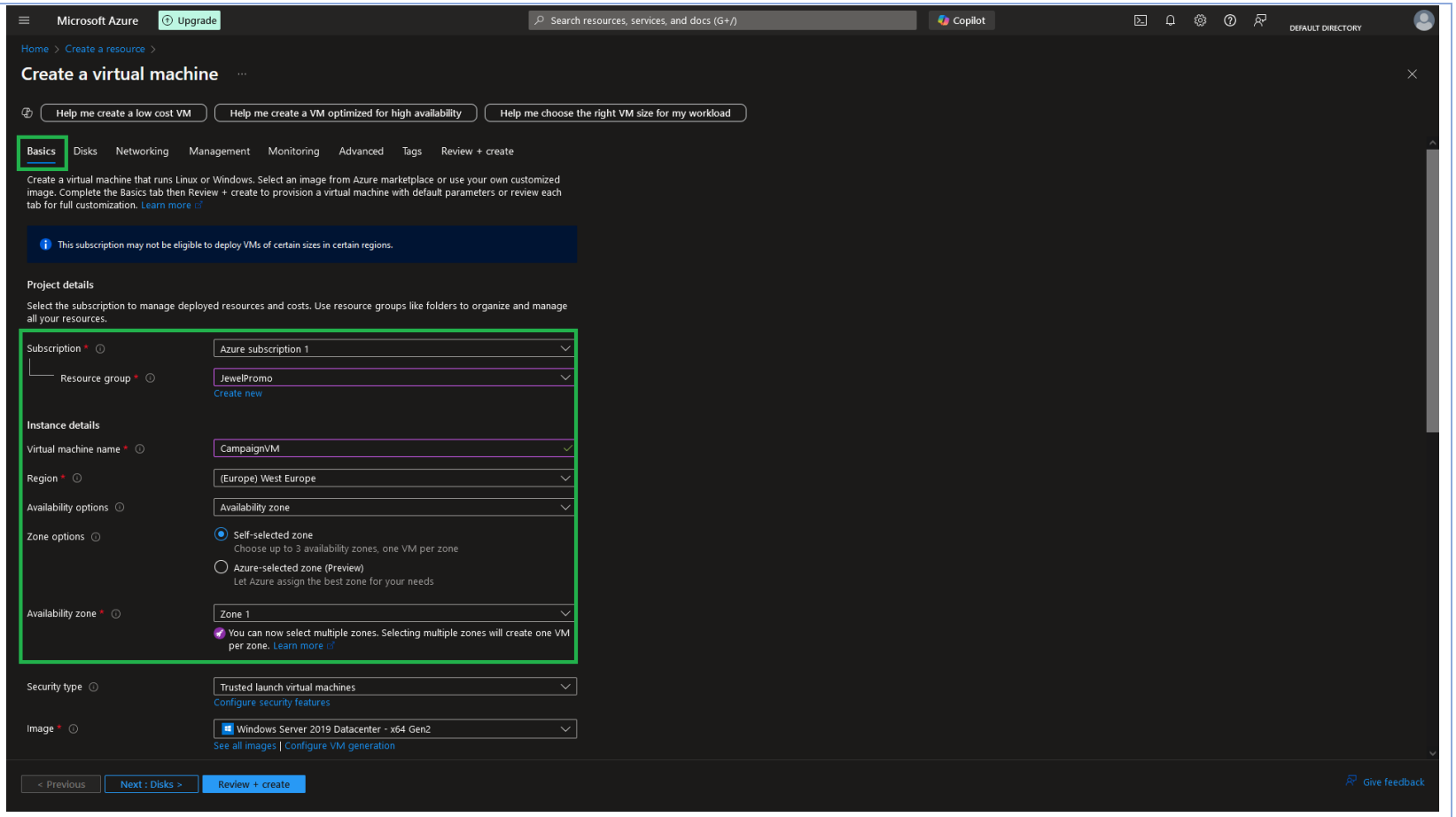
Task 5: View the image using a Blob SAS URL on a virtual machine.

Activity	Key evidence
Activity 1: Create a Windows Server 2019 Datacenter virtual machine.	1. We login to the Azure Portal and click on **Create a resource** to open the **Marketplace** page where we select Create under **Windows Server 2019 Datacenter**.

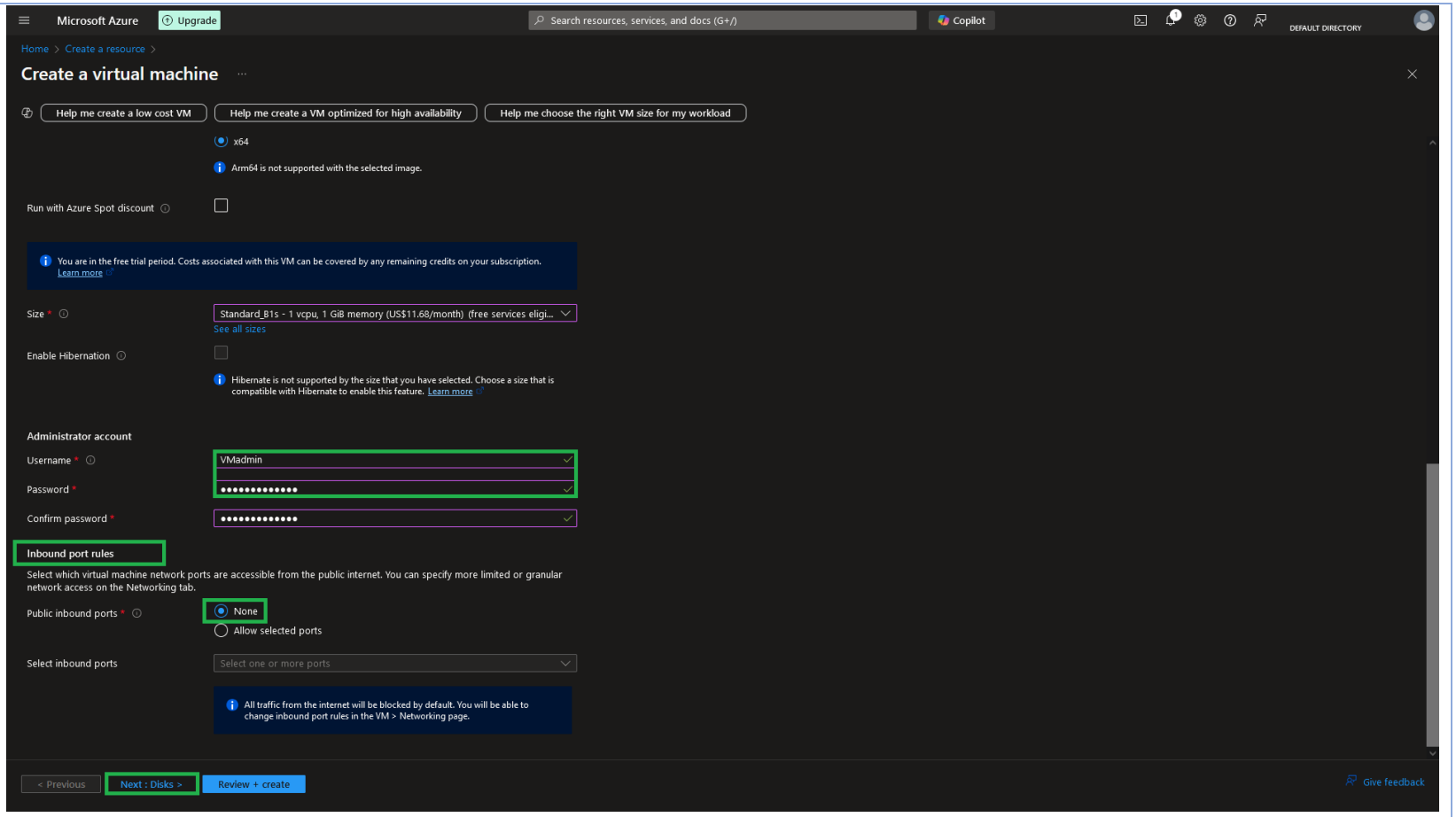


2. On the **Create a virtual machine** page, on the **Basics** tab, we then input the following information:

Field	**Value**
Subscription	Select an Azure subscription.
Resource group	Select **JewelPromo**.
Virtual machine name	Enter a unique VM name, such as **CampaignVM**.
Region	Select the same region as our other resources
Availability options	Select **Availability zone**.
Availability zone	Select **Zones 1**.

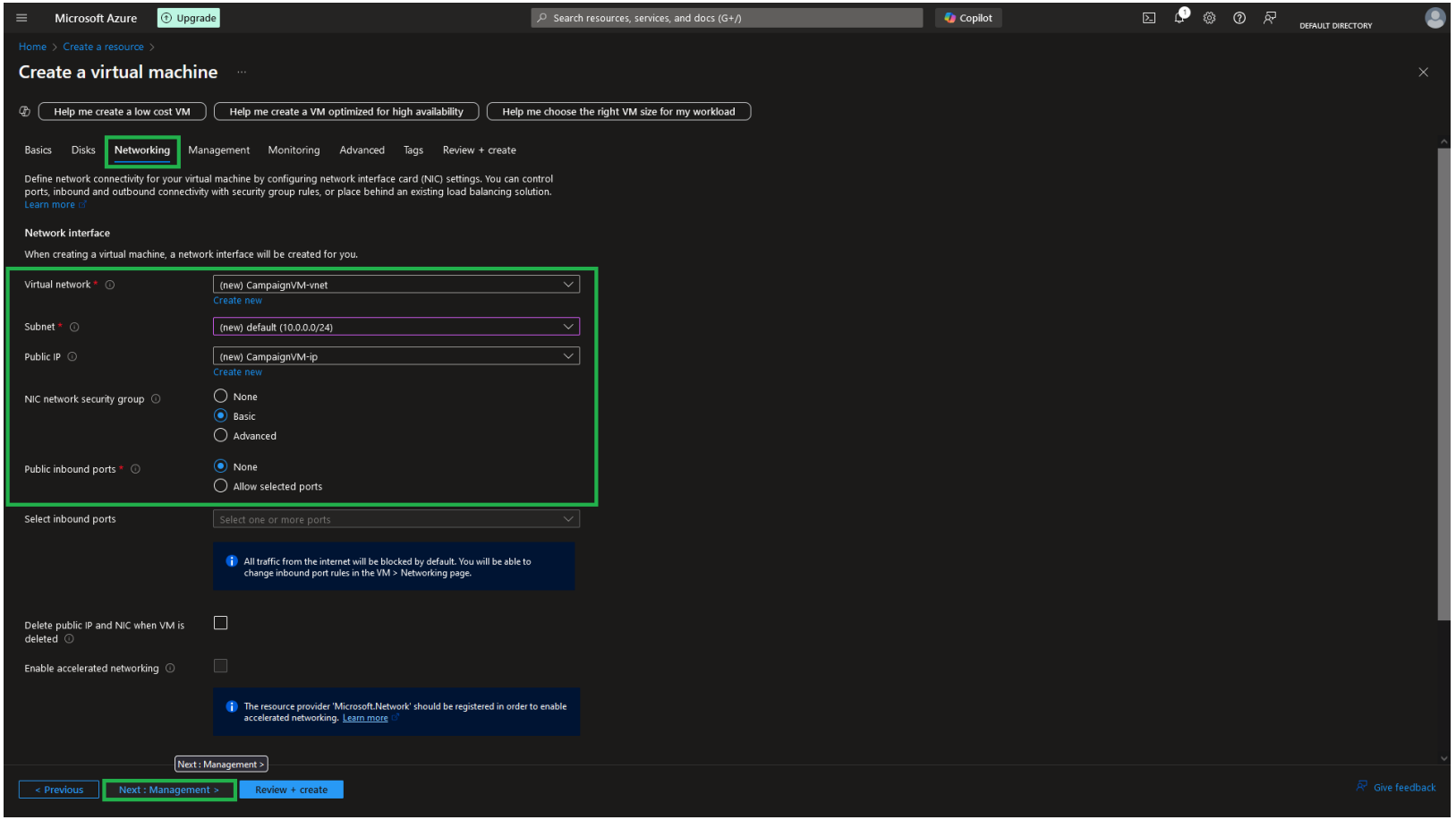


3. We scroll down and, under the **Administrator account** section, enter the **Username** and **Password**.
4. Then, under the **Inbound port rules** section, in the **Public inbound ports** field, select the **None** radio button and click on **Next: Disks**.

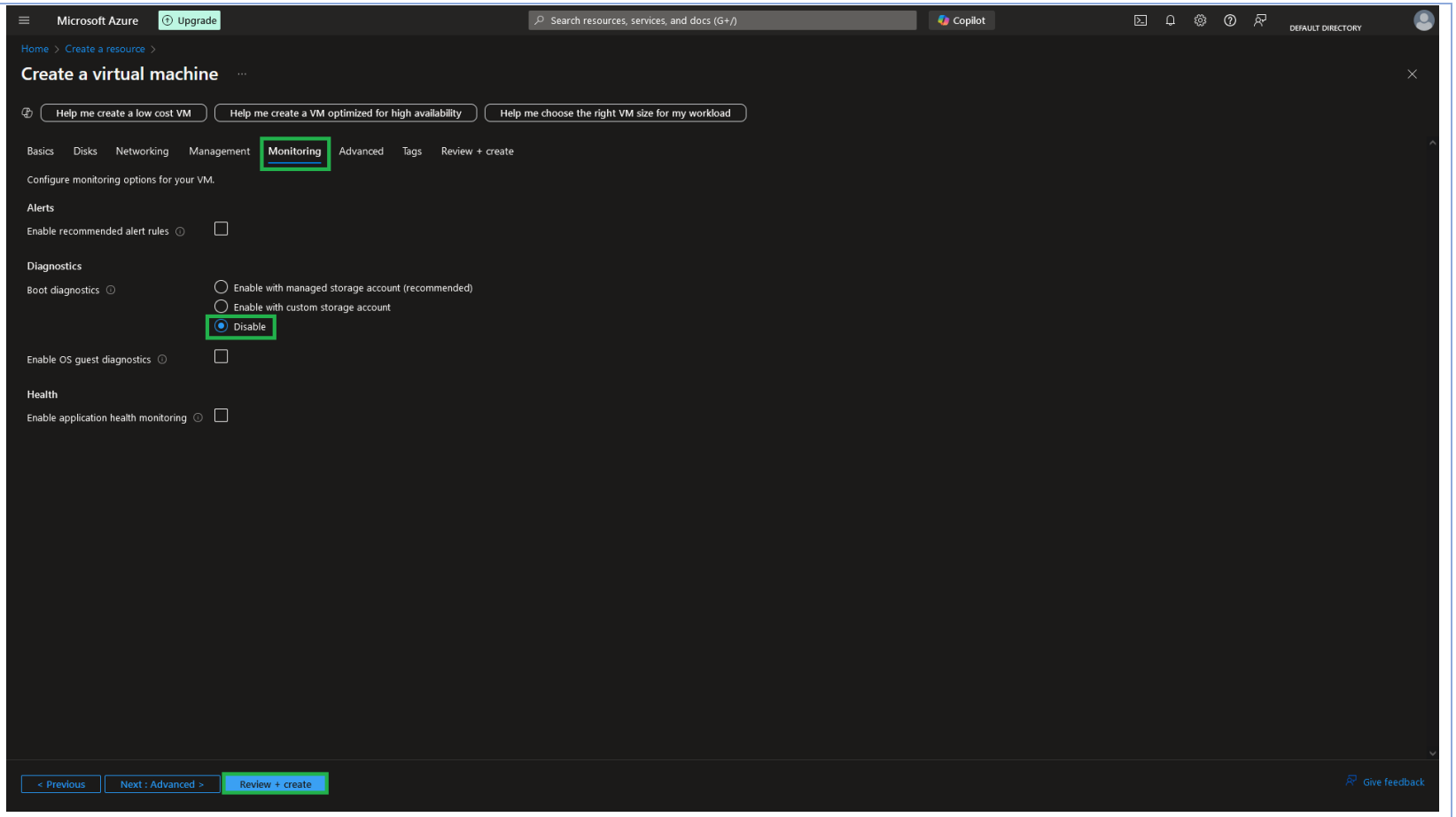


5. On the **Disks** tab, we retain the default settings, and select **Next: Networking**.
6. On the **Networking** tab, under the **Network interface** section, we specify the following information and click on **Next: Management**:

Field	**Value**
Virtual network	Select **(new) CampaignVM-vnet**.
Subnet	Select **(new) default (10.0.0.0/24)**.
Public inbound ports	Select **None**.

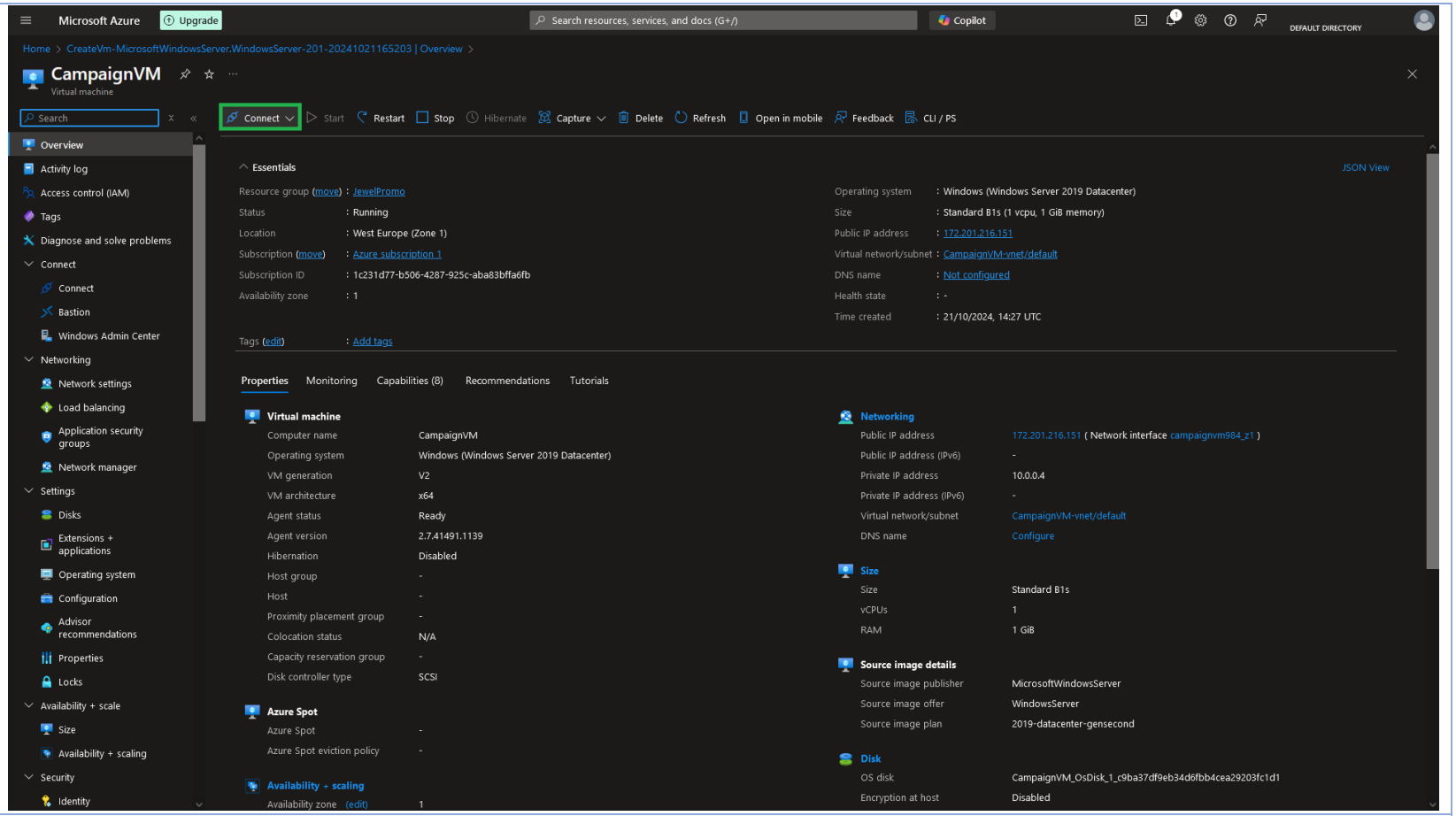


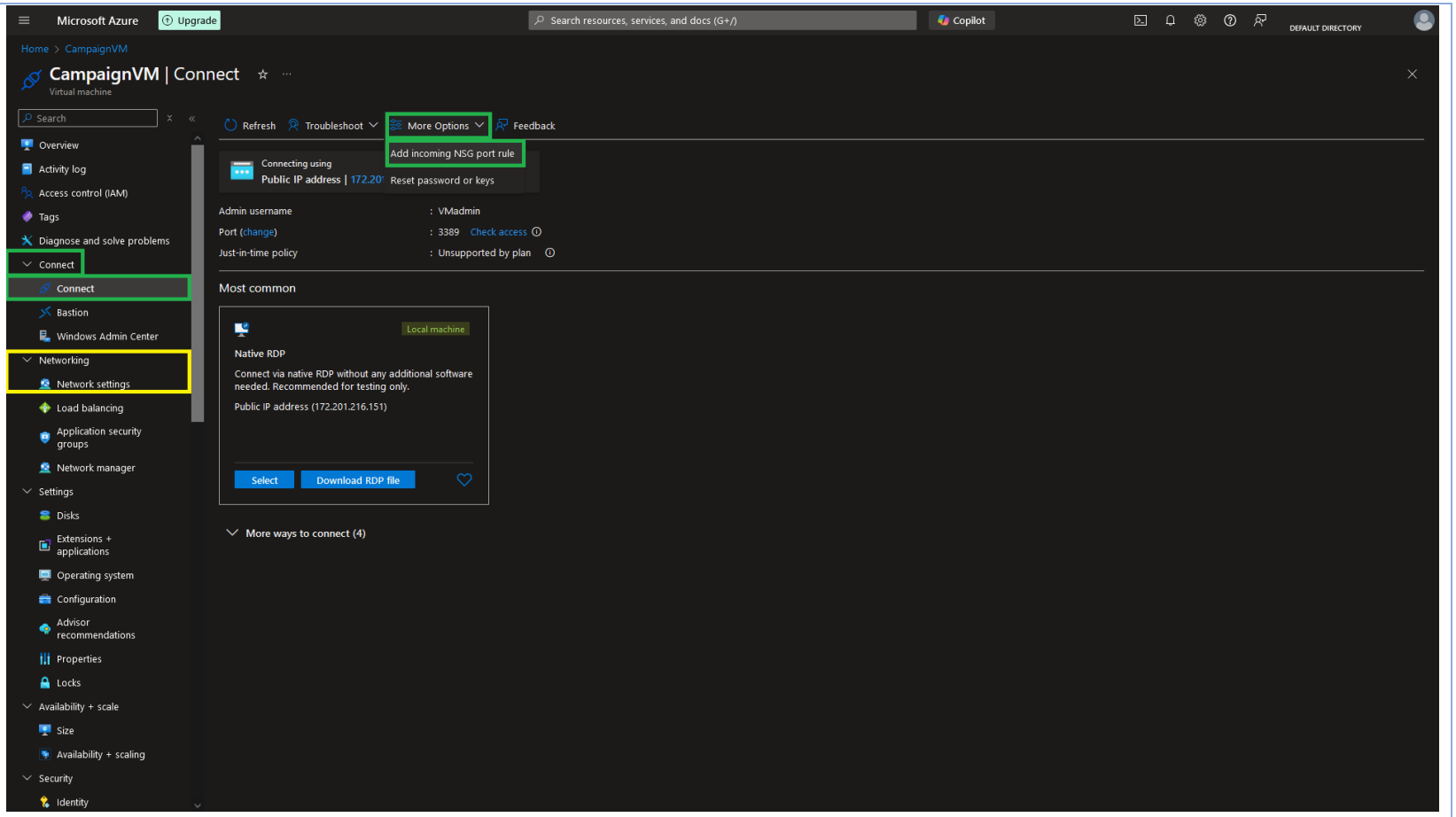
7. On the **Management** tab, we also retain the default settings, and select **Next: Monitoring**.
8. On the **Monitoring** tab, under the **Diagnostics** section, in the **Boot diagnostics** field, select the **Disable** radio button and then click on **Review + create**.



9. On the **Review + create** page, we check our configuration, and then click on **Create** to create a virtual machine
10. After the deployment is complete, we click on **Go to resource** and select **Connect** on the newly created virtual machine's **Overview** page. We then download the RDP file.

Note: At this point we cannot connect to the VM because the RDP port is blocked. We first need to allow RDP traffic with an **inbound network security group rule for port 3389**.

	
Activity 2: Add a network security group rule to allow inbound traffic on port 3389 for our virtual machine.	1. The fastest way to add the incoming network security group rule is to select **More Options** on the **Connect** page click on **Add incoming NSG port rule.** **Note:** This can also be done in **Network settings** under the *Networking* blade.

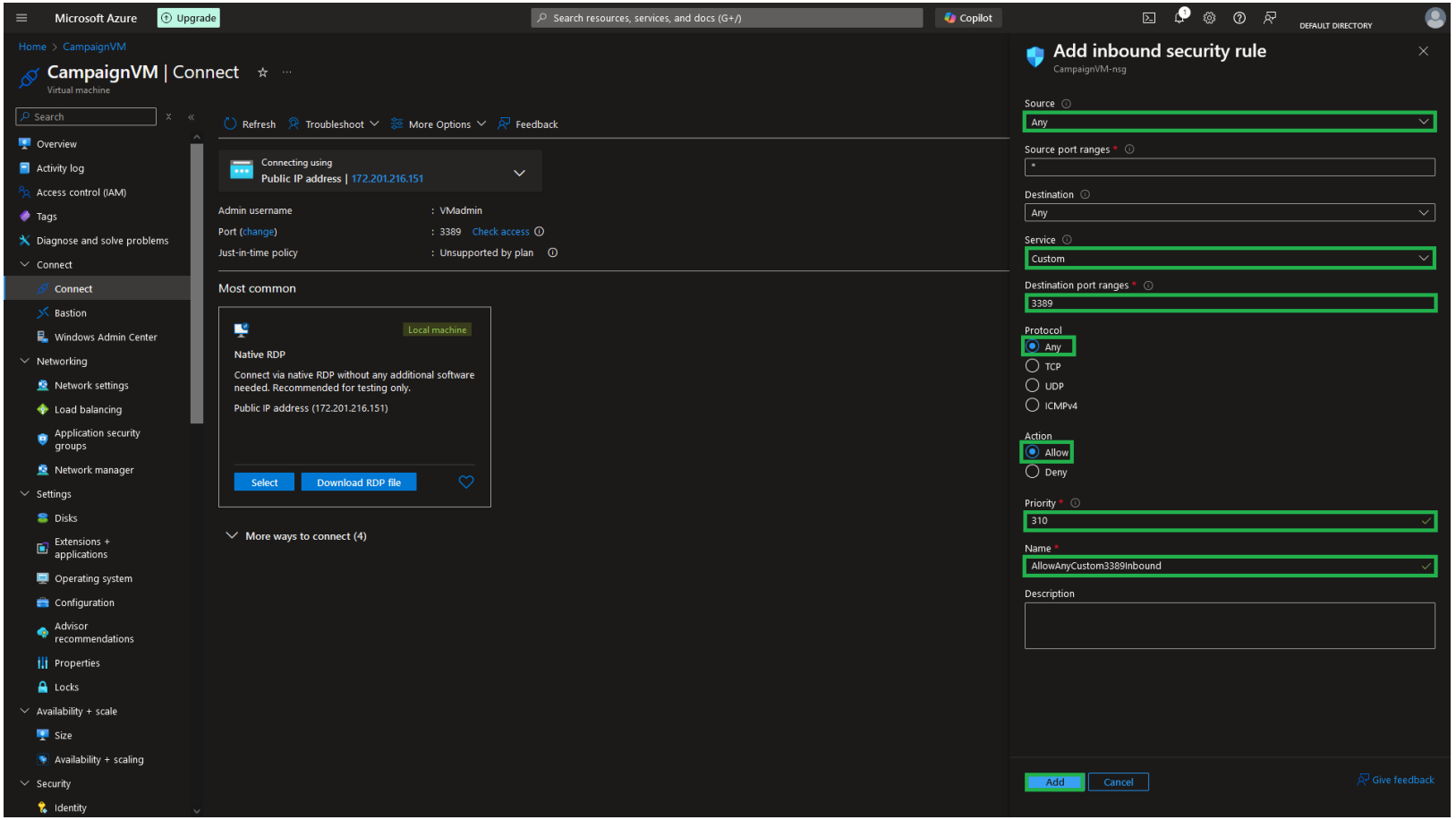


2. In the **Add inbound security rule** wizard, specify the following information and click on **Add**:

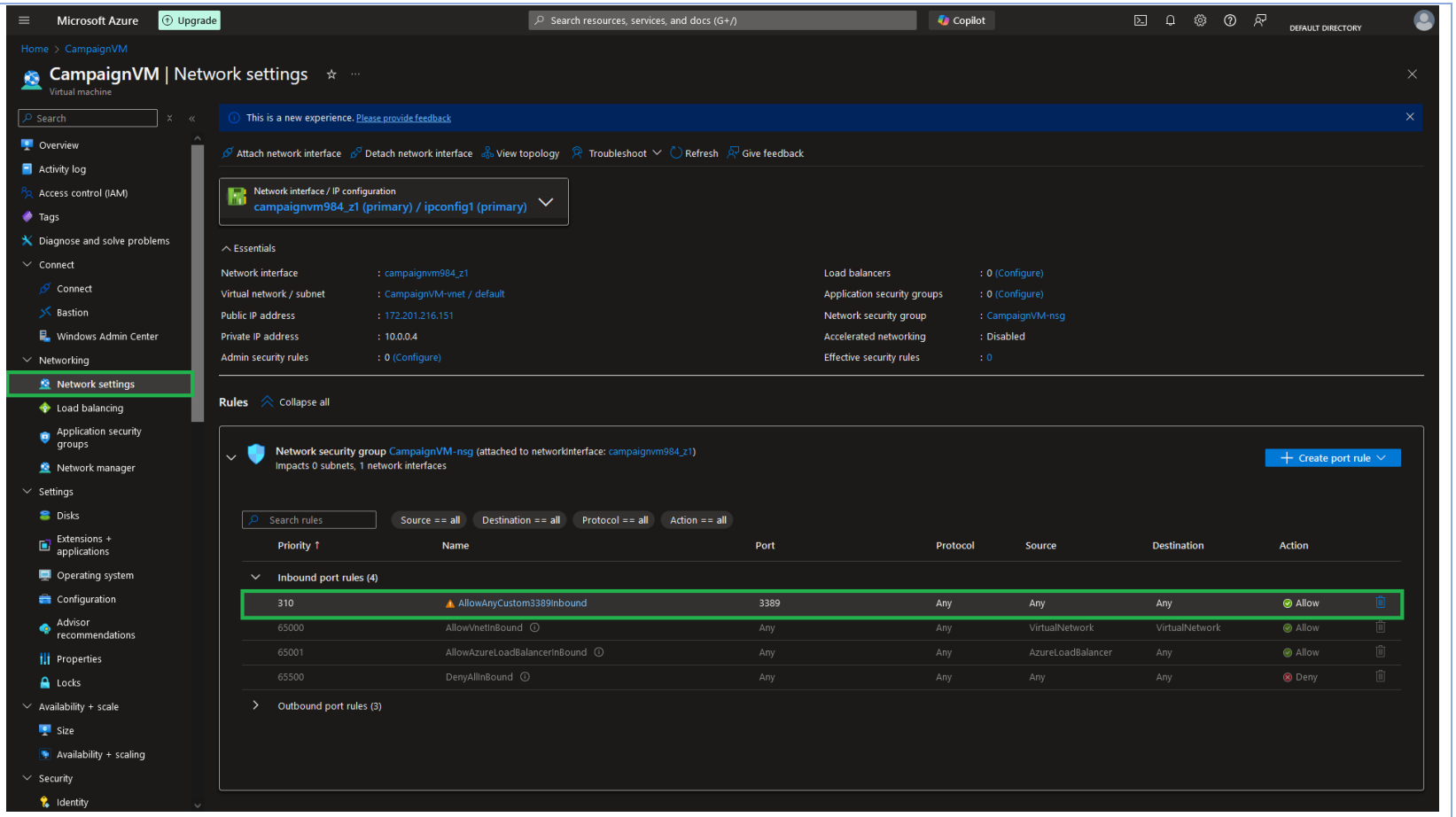
Note: This rule will only allow IP addresses on **port 3389.**

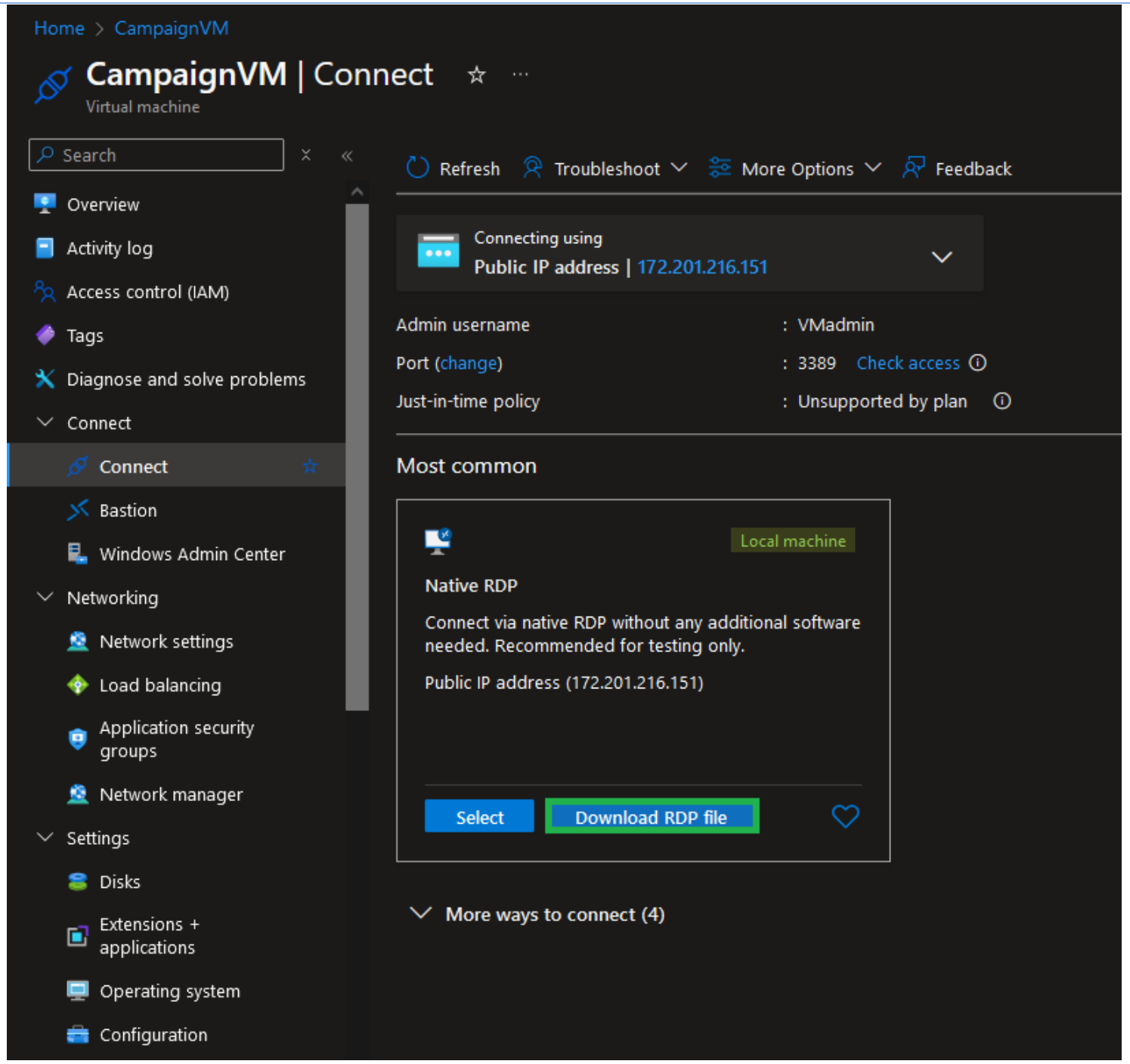
Field	**Value**
Source	Any
Service	Custom
Destination port ranges	3389
Protocol	Any

Action	Allow
Priority	310
Name	AllowAnyCustom3389Inbound

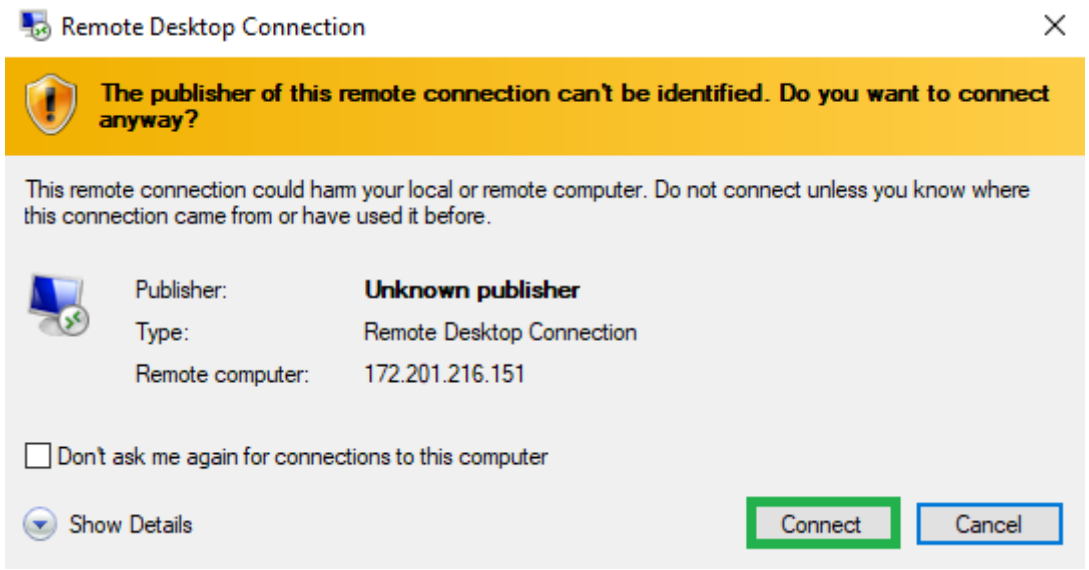


3. We can now see our new NSG rule in the **Network Settings** page on the **Inbound port rules** dropdown section.

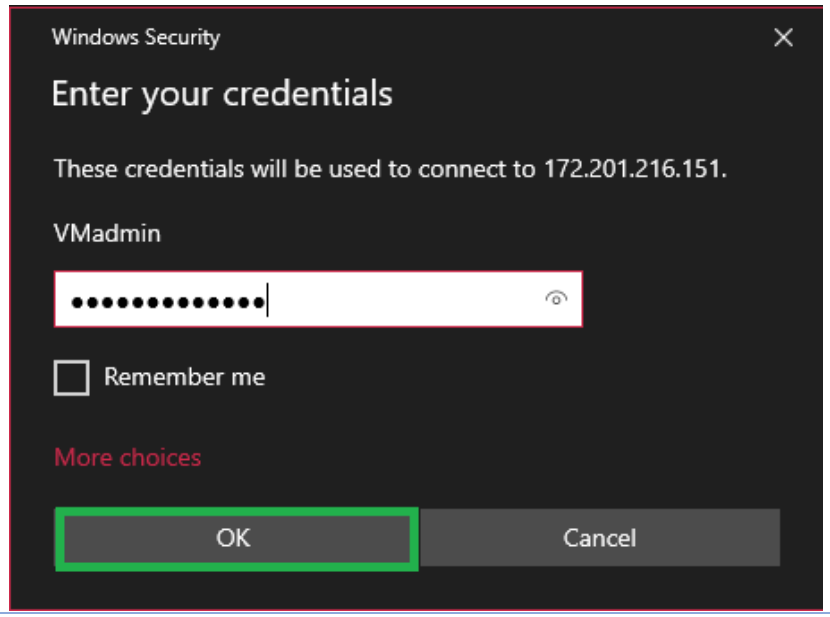
	
Activity 3: Verify access to the image as an administrator using the Blob SAS URL.	1. We can now go back to the **Connect** page and download the RDP file to test our configuration.


Home > CampaignVM
CampaignVM | Connect
Virtual machine
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Connect
Connect
Bastion
Windows Admin Center
Networking
Network settings
Load balancing
Application security groups
Network manager
Settings
Disks
Extensions + applications
Operating system
Configuration
Refresh
Troubleshoot
More Options
Feedback
Connecting using
Public IP address | 172.201.216.151
Admin username : VMadmin
Port (change) : 3389 Check access
Just-in-time policy : Unsupported by plan
Most common
Local machine
Native RDP
Connect via native RDP without any additional software needed. Recommended for testing only.
Public IP address (172.201.216.151)
Select
Download RDP file
More ways to connect (4)

2. When we open the file a **Remote Desktop Connection** pop-up window will appear where we will click on **Connect**.

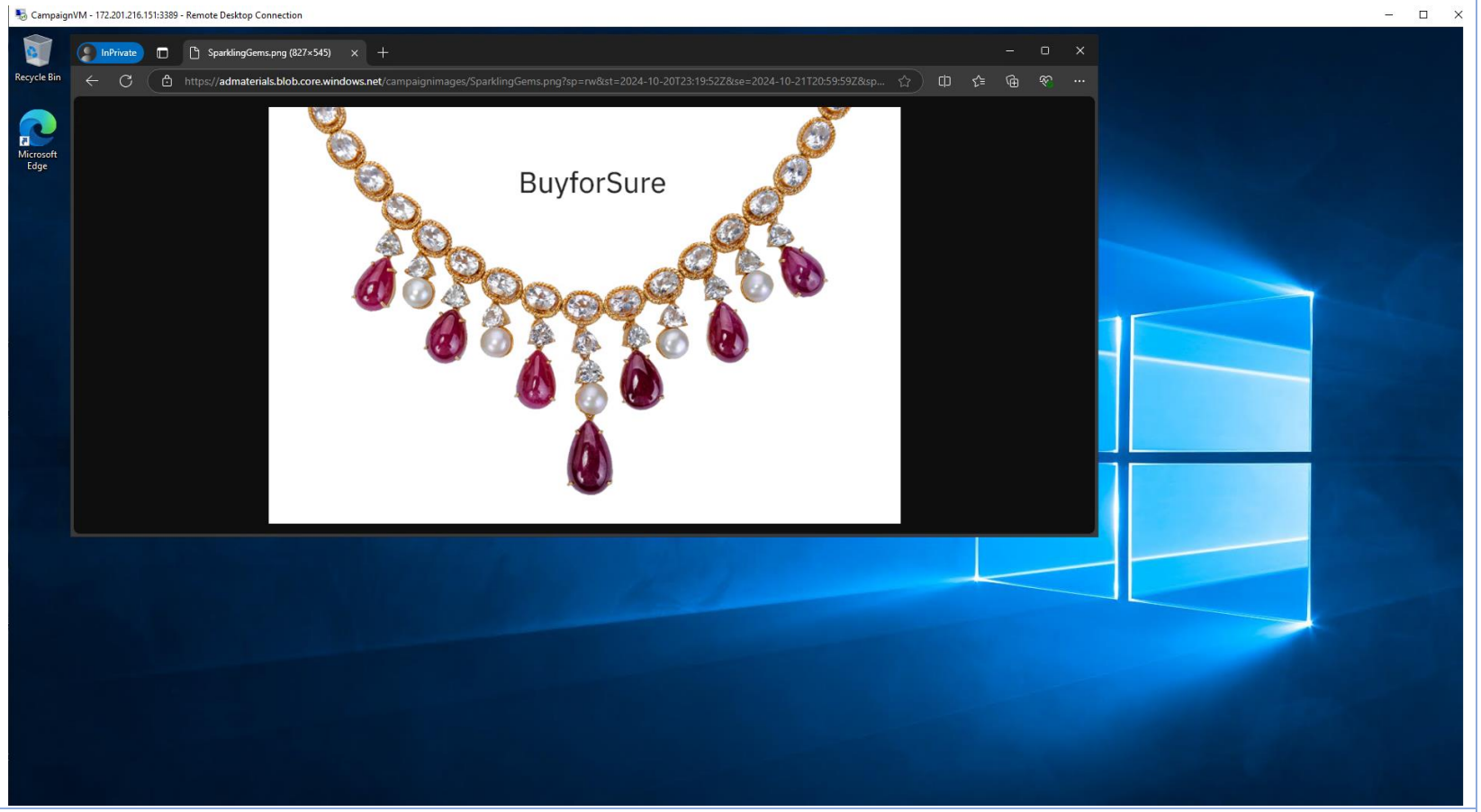


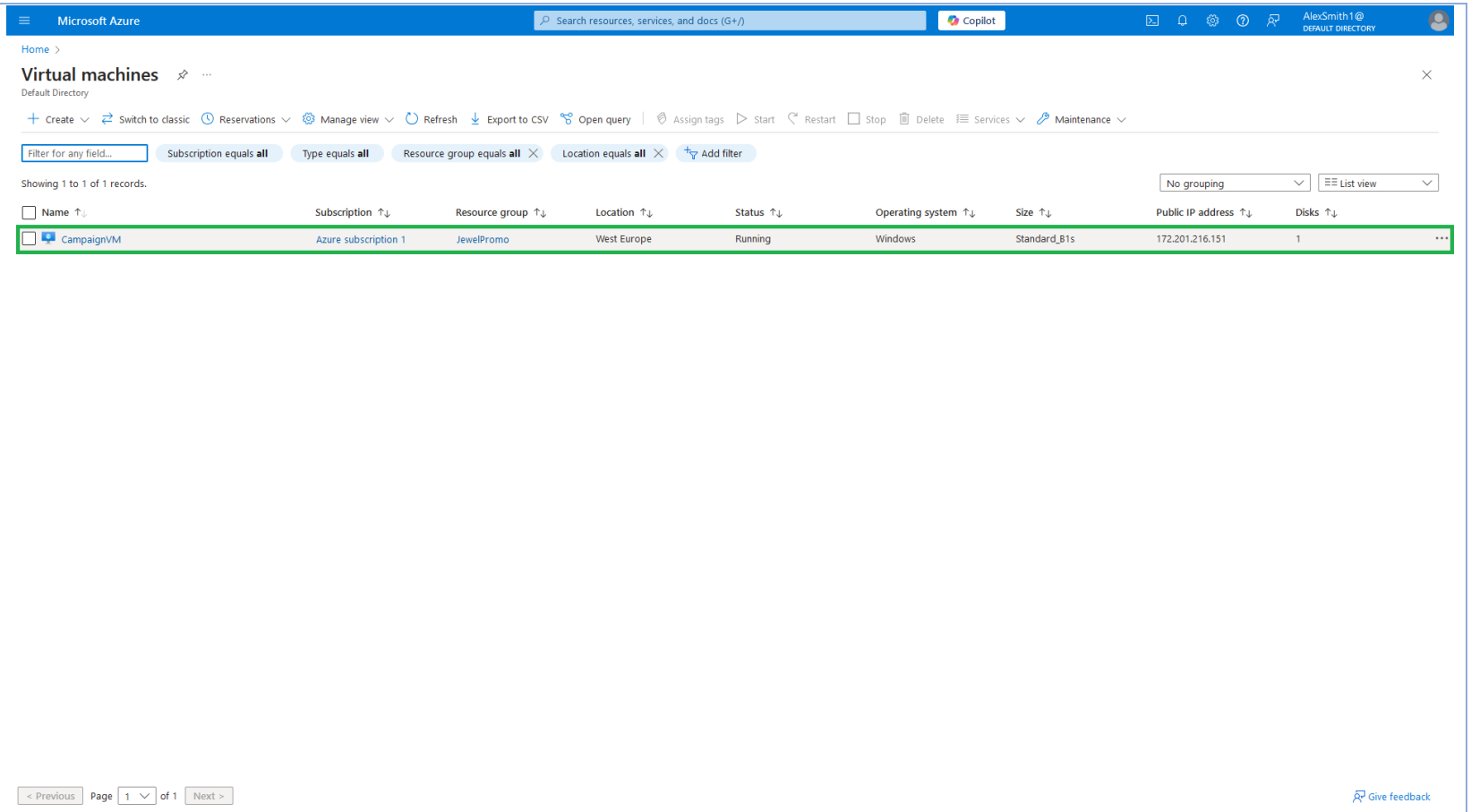
3. Then, on the **Enter your credentials** pop-up window, enter the **Username** and **Password**, and select **OK**.



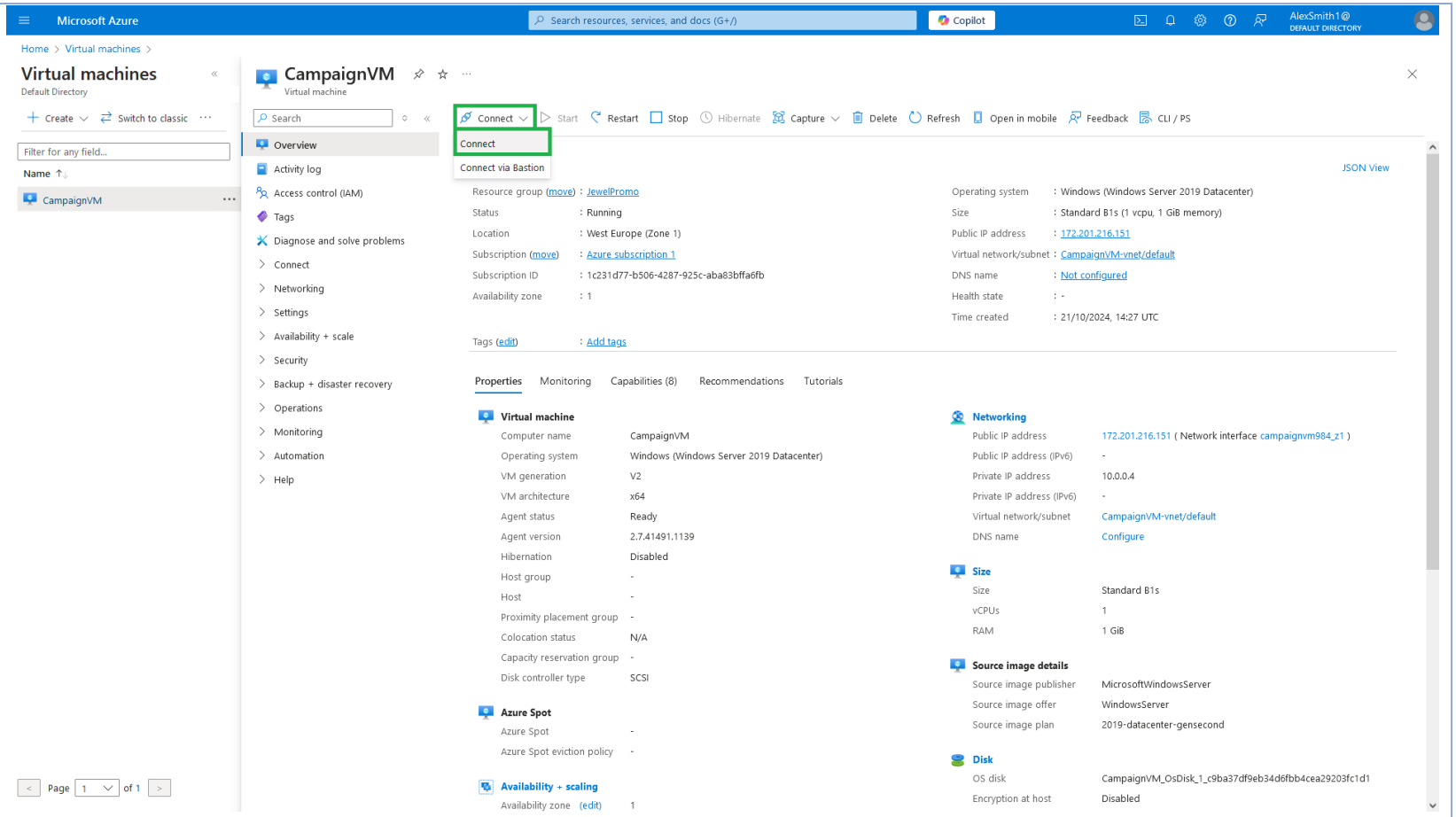
4. Next, on the **Remote Desktop Connection** pop-up window, we click on **Yes** to verify the identity of the virtual machine and finish logging on.

5. The virtual machine screen will be displayed.
6. When it loads, we open a browser and paste the **Blob SAS URL** that we saved earlier during Task 2, Activity 2. This will load the **SparklingGems.png** image stored in our **campaignimages** container within our encrypted **admaterials** storage account.

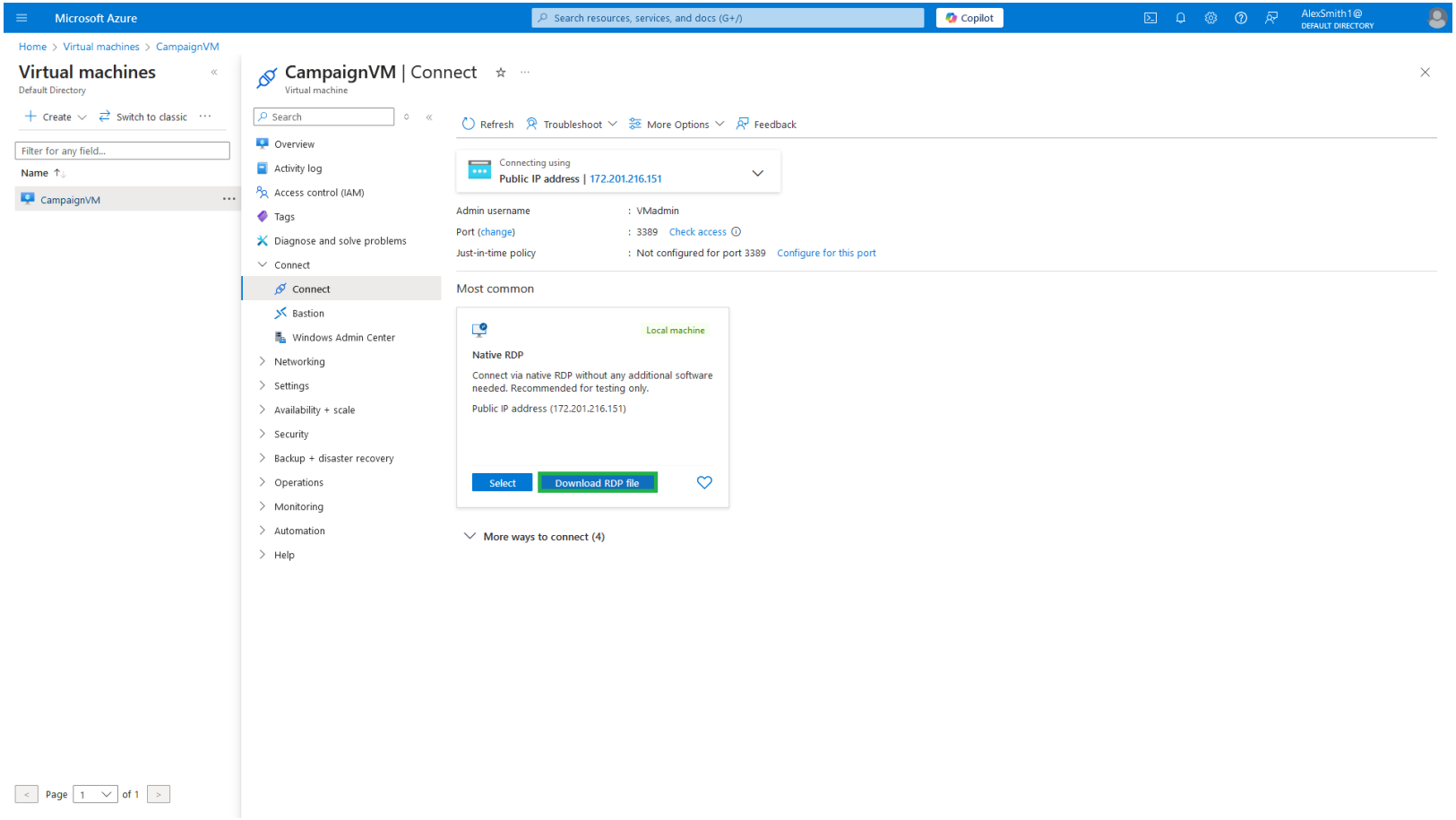
	
Activity 4: Access the image as a sales team member using the Blob SAS URL.	1. We first log in using the credentials of one of our three test users, for example, **AlexSmith**, and go to the **Virtual Machines** page.



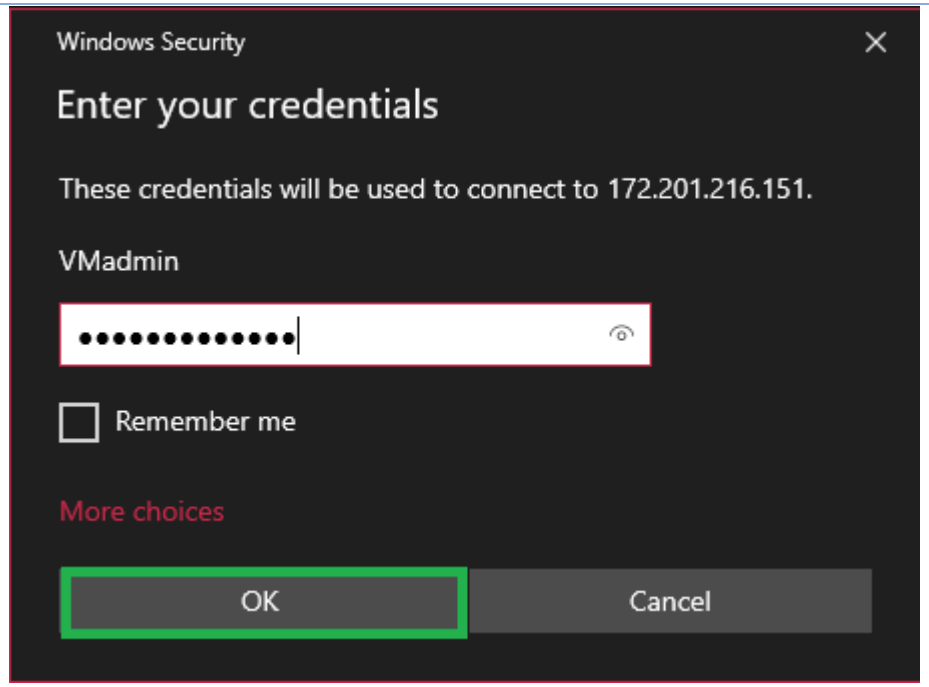
2. Clicking on the Virtual Machine will take us to its **Overview** page where we will select the **Connect** button.



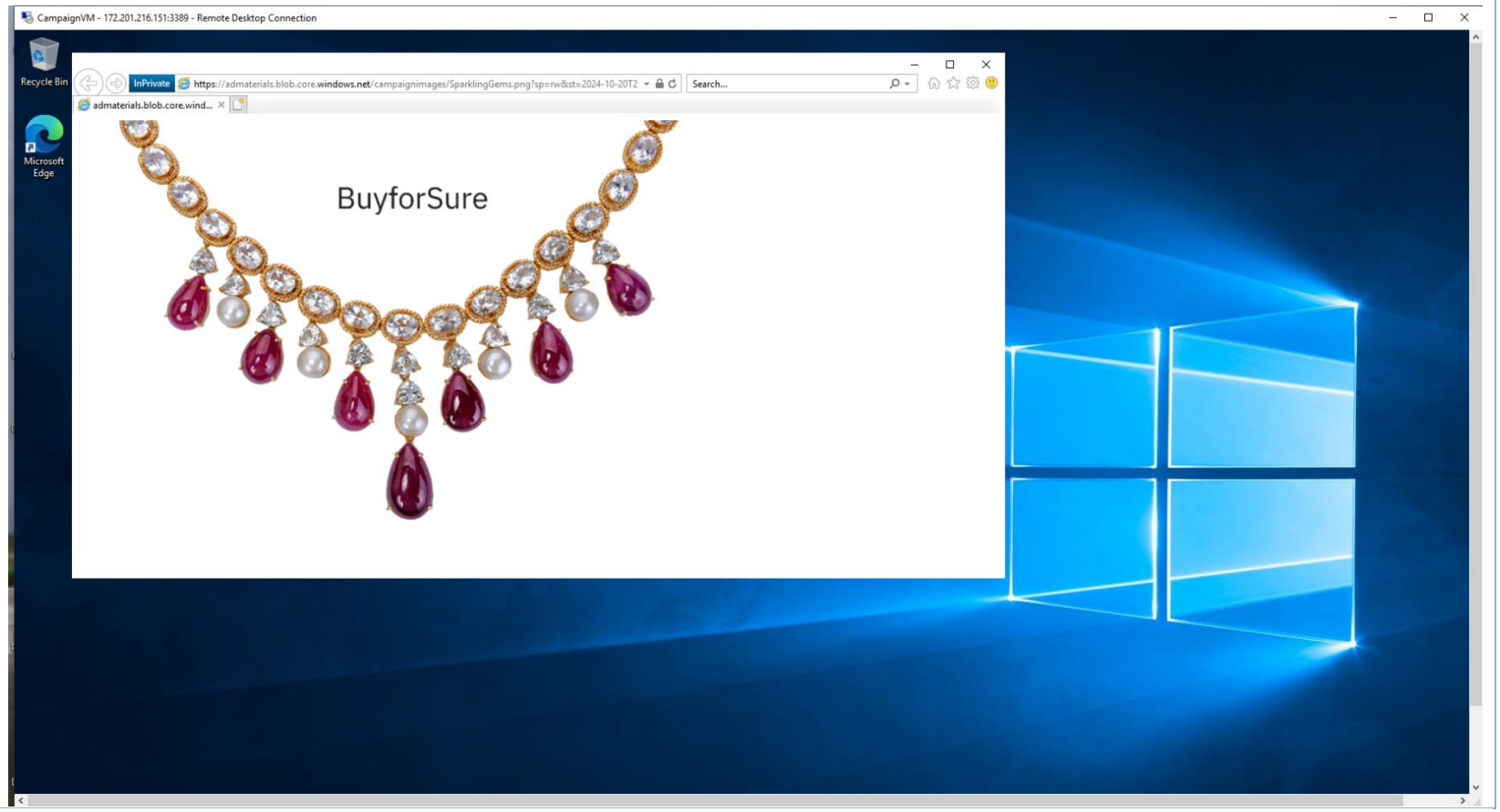
3. On the **Connect** page, we then choose **Download RDP File** in the **Native RDP** section.



4. When the **Remote Desktop Connection** pop-up window appears, we click on Connect and then login with the VMadmin credentials just like before.



5. We open a browser in the virtual machine and paste the **Blob SAS URL** to view the **SparklingGems.png** image.


CampaignVM - 172.201.216.151:3389 - Remote Desktop Connection
Recycle Bin
Microsoft Edge
InPrivate
https://admaterials.blob.core.windows.net/campaignimages/SparklingGems.png?sp=rw&st=2024-10-20T2
Search...
admaterials.blob.core.wind...
BuyforSure