

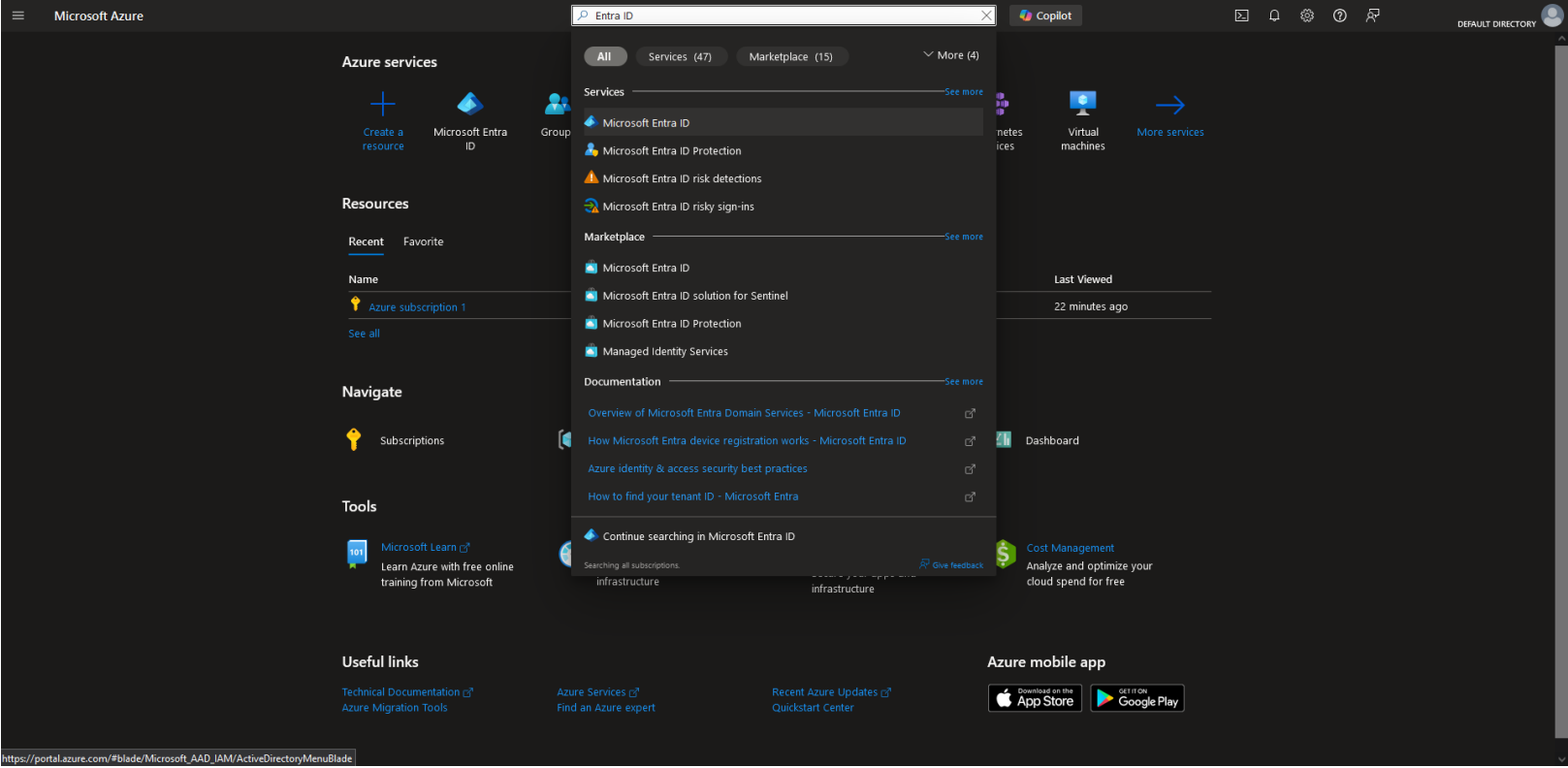
Azure Security Capstone Project

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” (<i>formerly, Azure Active Directory</i>) into the search box.  The screenshot shows the Microsoft Azure portal interface. A search bar at the top center contains the text 'Entra ID'. Below the search bar, a dropdown menu displays search results categorized into 'Services', 'Marketplace', and 'Documentation'. Under 'Services', the first result is 'Microsoft Entra ID', which is highlighted. Other results include 'Microsoft Entra ID Protection', 'Microsoft Entra ID risk detections', and 'Microsoft Entra ID risky sign-ins'. Under 'Marketplace', results include 'Microsoft Entra ID', 'Microsoft Entra ID solution for Sentinel', and 'Microsoft Entra ID Protection'. Under 'Documentation', results include 'Overview of Microsoft Entra Domain Services - Microsoft Entra ID', 'How Microsoft Entra device registration works - Microsoft Entra ID', 'Azure identity & access security best practices', and 'How to find your tenant ID - Microsoft Entra'. At the bottom of the dropdown, there is a link to 'Continue searching in Microsoft Entra ID'. The background of the portal shows various Azure services and resources, including 'Azure subscription 1' and 'Microsoft Learn'. 2. On the Default Directory page, select Users under the <i>Manage</i> blade.

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

Home >

Default Directory | Overview

Overview | Preview features | Diagnose and solve problems | Manage

- Overview
- Preview features
- Diagnose and solve problems
- Manage
 - Users**
 - Groups
 - External identities
 - Roles and administrators
 - Administrative units
 - Delegated admin partners
 - Enterprise applications
 - Devices
 - App registrations
 - Identity Governance
 - Application proxy
 - Custom security attributes
 - Licenses
 - Cross-tenant synchronization
 - Microsoft Entra Connect
 - Custom domain names
 - Mobility (MDM and

Microsoft Entra has a simpler, integrated experience for managing all your Identity and Access Management needs. Try the new Microsoft Entra admin center!

Overview | Monitoring | Properties | Recommendations | Setup guides

Search your tenant

Basic information

Name	Default Directory	Users	1
Tenant ID		Groups	0
Primary domain		Applications	0
License	Microsoft Entra ID Free	Devices	0

Alerts

Service Change to Microsoft Entra Connect

We are making security-related service changes to Microsoft Entra Connect Sync and Connect Health. Upgrade to the latest version to avoid any feature disruptions.

[Learn more](#)

Migrate to the converged Authentication methods policy

Please migrate your authentication methods off the legacy MFA and SSPR policies by September 2025 to avoid any service impact.

[Learn more](#)

My feed

Try Microsoft Entra admin center

Secure your identity environment with Microsoft Entra ID, permissions management and more.

[Go to Microsoft Entra](#)

Global Administrator

[View role information](#)

[View profile](#)

Secure Score for Identity

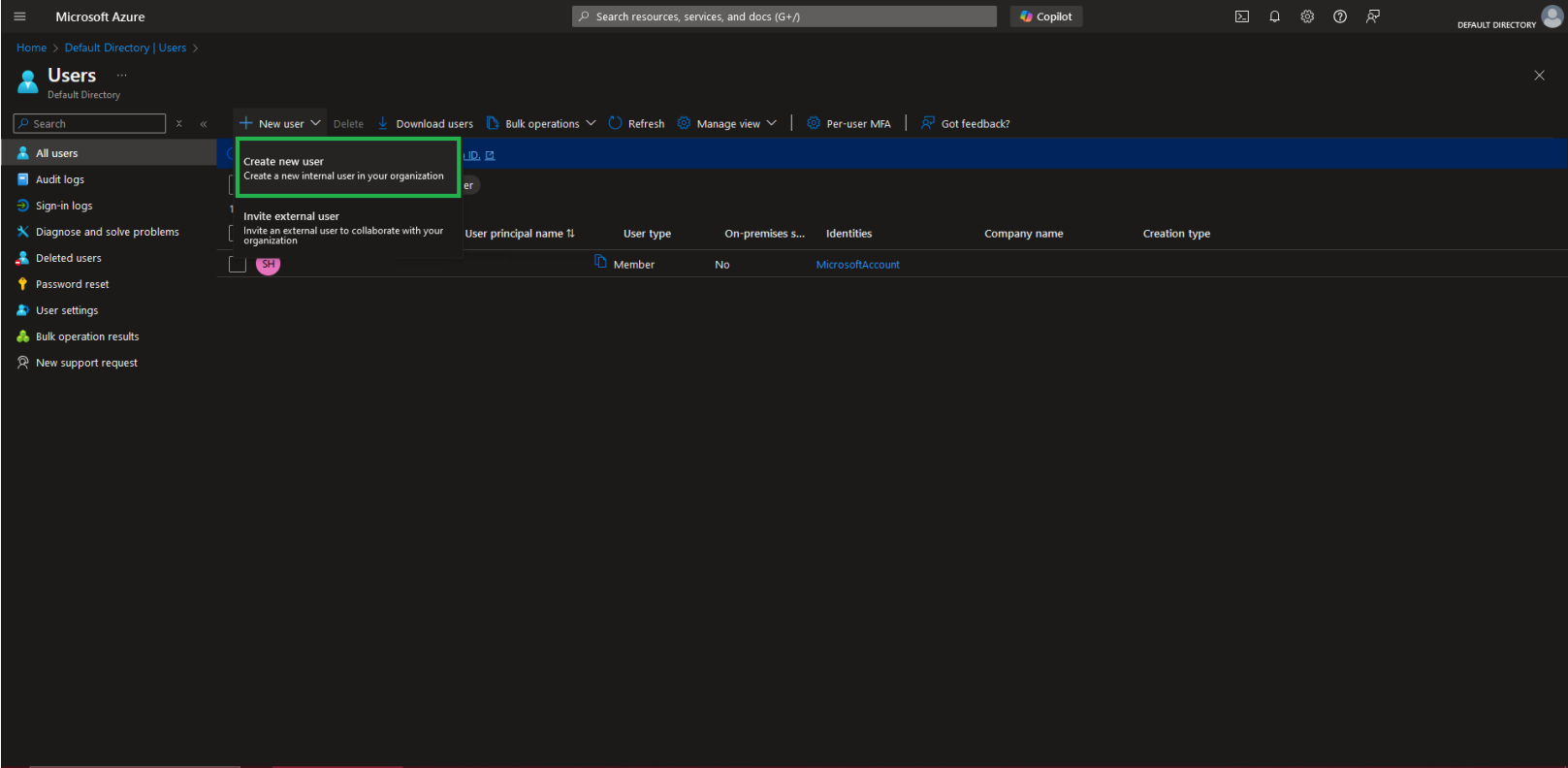
N/A

Secure score updates can take up to 48 hours.

[View secure score](#)

https://portal.azure.com/#view/Microsoft-AAD-IAM/ActiveDirectoryMenuBlade/~/_/Users

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.

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

Home > Default Directory | Users > Users >

Create new user

Create a new internal user in your organization

Basics Properties Assignments Review + create

Create a new user in your organization. This user will have a user name like `alice@contoso.com`. [Learn more](#)

Identity

User principal name * @ [Domain not listed? Learn more](#)

Mail nickname *

Display name *

Password * [Auto-generate password](#)

Account enabled ☒

[Review + create](#) < Previous Next: Properties >

[Give feedback](#)

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**

Microsoft Azure

Search resources, services, and docs (G+/)

Copilot

Home > Default Directory | Users > Users >

Create new user

Create a new internal user in your organization

Basics Properties Assignments Review + create

Basics

User principal name	AlexSmith1@
Display name	AlexSmith
Mail nickname	AlexSmith1
Password	••••••••
Account enabled	Yes

Properties

User type	Member
-----------	--------

Assignments

Administrative units

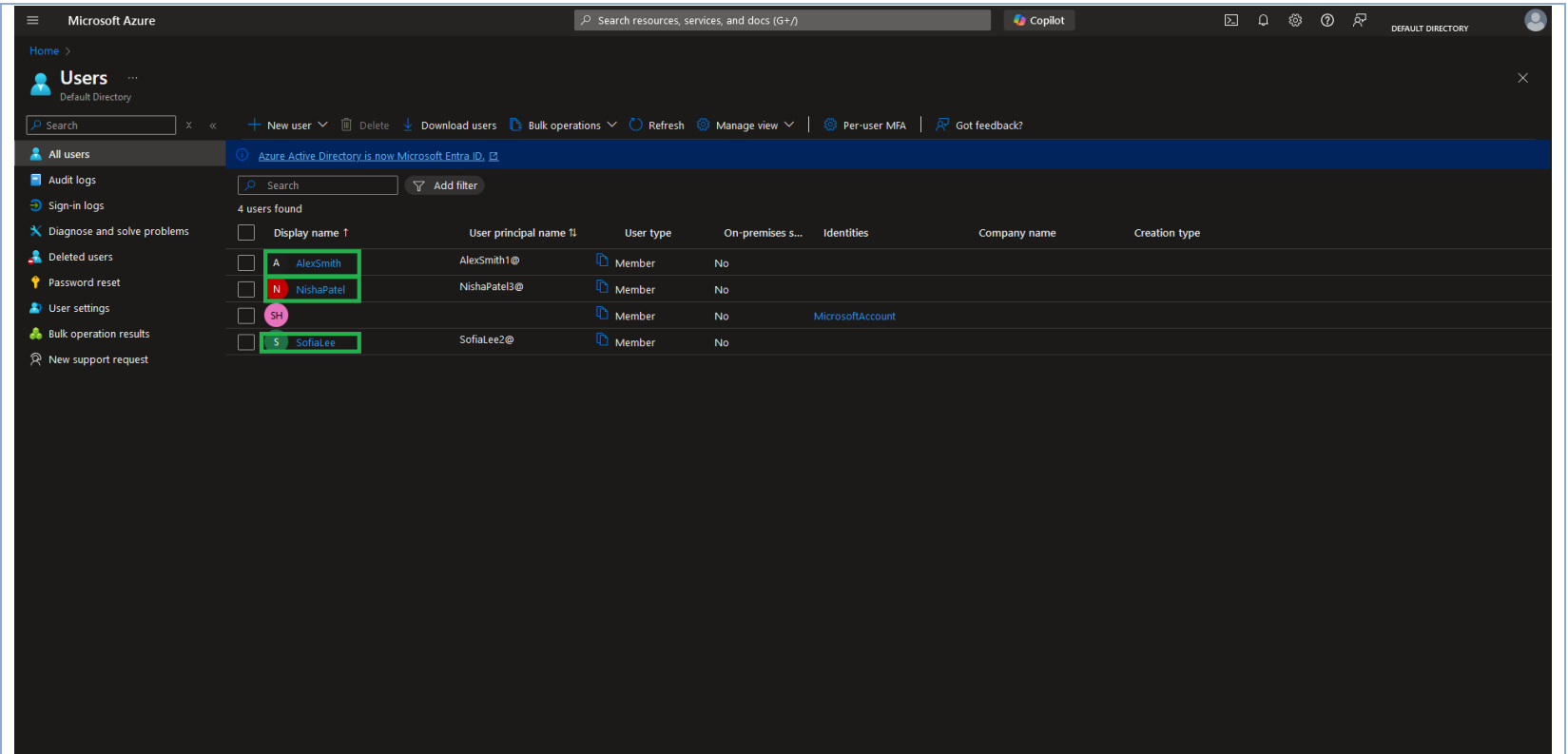
Groups

Roles

Create < Previous Next >

Give feedback

- The process is then repeated for users **SofiaLee** and **NishaPatel**.
- 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.

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

Home >

Default Directory | Overview

Overview | Preview features | Diagnose and solve problems | Manage | Users | **Groups** | External Identities | Roles and administrators | Administrative units | Delegated admin partners | Enterprise applications | Devices | App registrations | Identity Governance | Application proxy | Custom security attributes | Licenses | Cross-tenant synchronization | Microsoft Entra Connect | Custom domain names | Mobility (MDM and

Microsoft Entra has a simpler, integrated experience for managing all your Identity and Access Management needs. Try the new Microsoft Entra admin center.

Overview | Monitoring | Properties | Recommendations | Setup guides

Search your tenant

Basic information

Name	Default Directory	Users	4
Tenant ID		Groups	0
Primary domain		Applications	0
License	Microsoft Entra ID Free	Devices	0

Alerts

Service Change to Microsoft Entra Connect

We are making security-related service changes to Microsoft Entra Connect Sync and Connect Health. Upgrade to the latest version to avoid any feature disruptions.

[Learn more](#)

Migrate to the converged Authentication methods policy

Please migrate your authentication methods off the legacy MFA and SSPR policies by September 2025 to avoid any service impact.

[Learn more](#)

My feed

Try Microsoft Entra admin center

Secure your identity environment with Microsoft Entra ID, permissions management and more.

Global Administrator

[View role information](#)

[View profile](#)

Secure Score for Identity

N/A

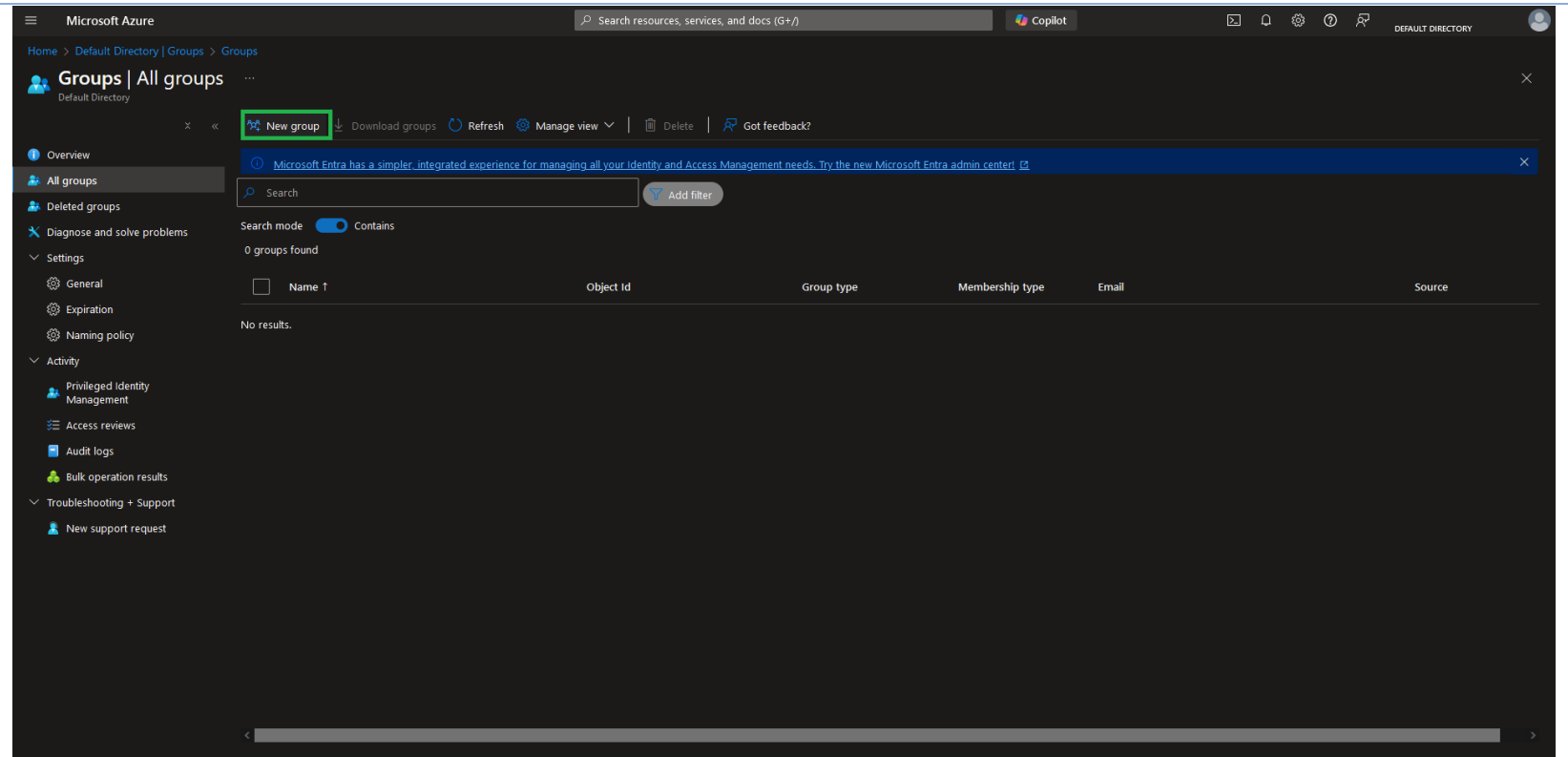
Secure score updates can take up to 48 hours.

[View secure score](#)

[Go to Microsoft Entra](#)

https://portal.azure.com/#view/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/~/_/Groups

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**.

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

Home > Default Directory | Groups > Groups | All groups >

New Group

Got feedback?

Group type * ⓘ
Microsoft 365

Group name * ⓘ
JewelSales

Group email address * ⓘ
JewelSales @STHadzhitodorovoutlook.onmicrosoft.com

Group description ⓘ
Sales team responsible for promoting and selling the jewelry brand

Membership type ⓘ
Assigned

Use group sensitivity labels in Microsoft Entra ID to classify and protect Microsoft 365 groups. [Learn more about assigning sensitivity labels in Microsoft Entra ID.](#)

Owners
No owners selected

Members
No members selected

Create

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

The screenshot shows the 'New Group' wizard in the Microsoft Azure portal. The interface is dark-themed. At the top, there's a navigation bar with 'Microsoft Azure', a search bar, and a 'Copilot' button. Below the navigation bar, the breadcrumb trail is 'Home > Default Directory | Groups > Groups | All groups >'. The main heading is 'New Group'. Below this, there's a 'Got feedback?' link. The form fields are as follows:

- Group type:** Microsoft 365
- Group name:** JewelSales
- Group email address:** JewelSales (with a dropdown showing @STHadzhitoDorovoutlook.onmicrosoft.com)
- Group description:** Sales team responsible for promoting and selling the jewelry brand
- Membership type:** Assigned

Below the form fields, there's a blue information box with a question mark icon and the text: 'Use group sensitivity labels in Microsoft Entra ID to classify and protect Microsoft 365 groups. [Learn more about assigning sensitivity labels in Microsoft Entra ID.](#)'

Under the 'Owners' section, it says '1 owner selected'. Below that, the 'Members' section is highlighted with a green box. It contains the text 'No members selected'.

At the bottom of the form, there's a blue 'Create' button.

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

Add members

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@

Selected (3)

 Reset

	AlexSmith AlexSmith1@	
	NishaPatel NishaPatel3@	
	SofiaLee SofiaLee2@	

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.

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

Home > Default Directory | Groups > Groups

Groups | All groups

Default Directory

⌕ New group ⬇ Download groups ↻ Refresh ⚙ Manage view | 🗑 Delete | 🗨 Got feedback?

Overview

All groups

Deleted groups

Diagnose and solve problems

Settings

- General
- Expiration
- Naming policy

Activity

- Privileged Identity Management
- Access reviews
- Audit logs
- Bulk operation results

Troubleshooting + Support

- New support request

Microsoft Entra has a simpler, integrated experience for managing all your identity and Access Management needs. Try the new Microsoft Entra admin center. [🔗](#)

Search

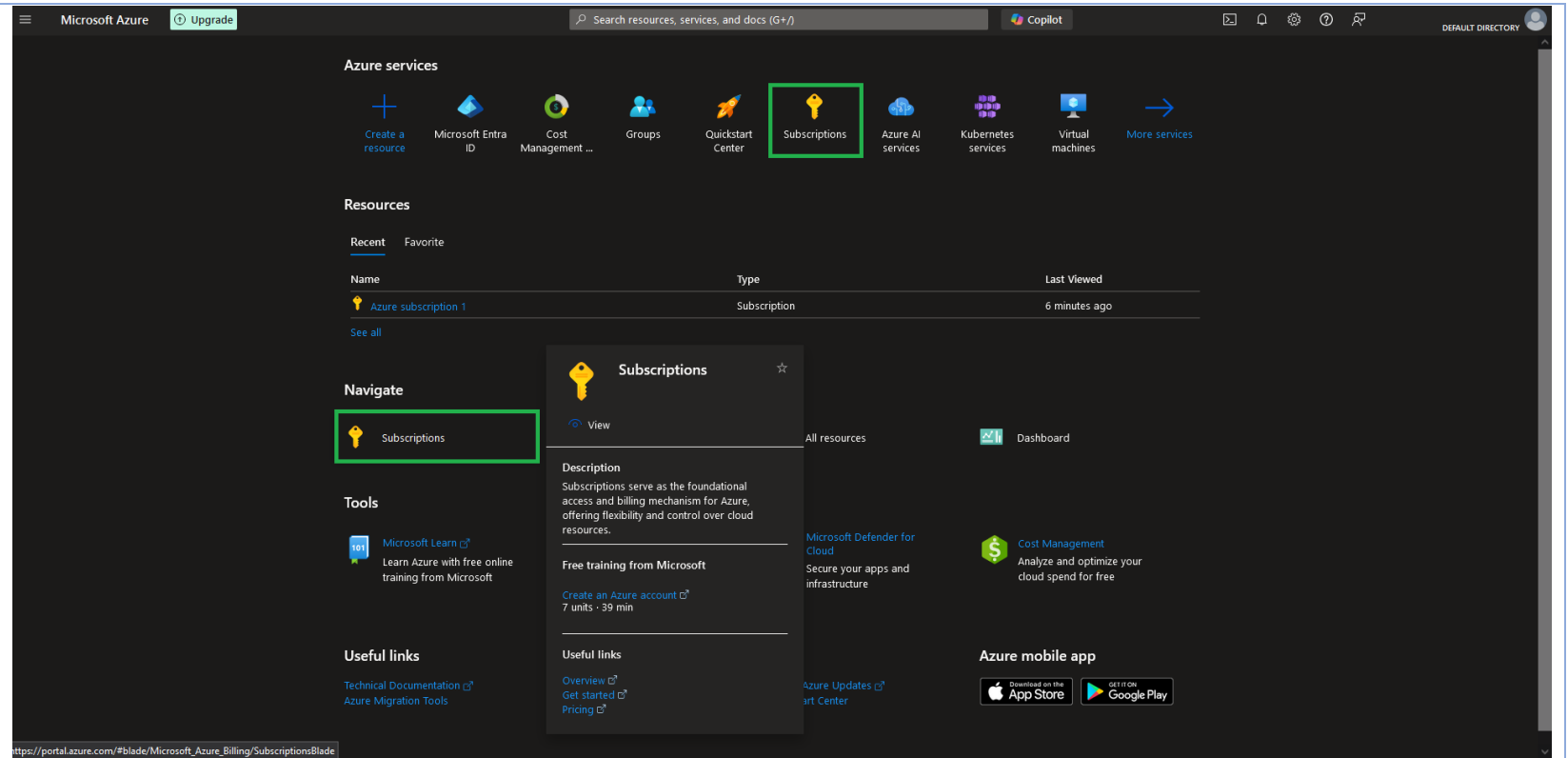
Add filter

Search mode: Contains

1 group found

☐	Name ↑	Object Id	Group type	Membership type	Email	Source
☐	 JewelSales	7651f958-a91e-489c-b6cb-52170893d78d	Microsoft 365	Assigned	JewelSales@	Cloud

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



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

Microsoft Azure Upgrade Search resources, services, and docs (G+/) Copilot DEFAULT DIRECTORY

Home > Subscriptions >

Subscriptions

Default Directory

+ Add Manage Policies View Requests View eligible subscriptions Export to CSV

Global administrators can manage all subscriptions in this list by updating their policy setting [here](#).

View list of subscriptions for which you have role-based access control (RBAC) permissions to manage Azure resources. To view subscriptions for which you have billing access, [click here](#).

Showing subscriptions in Default Directory directory. Don't see a subscription? [Switch directories](#)

Search for any field... Subscriptions: Filtered (1 of 1) My role == all Status == all Add filter

Subscription name ↑↓	Subscription ID ↑↓	My role ↑↓	Current cost	Secure Score ↑↓	Parent management group ↑↓	Status ↑↓
Azure subscription 1	1c231d77-b506-4287-925c-aba83bffa6fb	Owner		-	Tenant Root Group	Active

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

Microsoft Azure Upgrade

Search resources, services, and docs (G+)

Copilot

Home > Subscriptions > Azure subscription 1

Subscriptions

Default Directory

+ Add Manage Policies ...

Global administrators can manage all subscriptions in this list by updating their policy setting [here](#).

View list of subscriptions for which you have role-based access control (RBAC) permissions to manage Azure resources. To view subscriptions for which you have billing access, [click here](#).

Showing subscriptions in Default Directory directory. Don't see a subscription? [Switch directories](#)

Subscriptions: Filtered (1 of 1)

My role == all

Status == all

+ Add filter

Subscription name ↑↓

Azure subscription 1 ...

Azure subscription 1 | Access control (IAM)

Subscription

Search

+ Add Download role assignments Edit columns Refresh Delete Feedback

Add role assignment

Add co-administrator **Add role assignment**

Add custom role

of August 31, 2024, [Azure classic administrator roles](#) (along with Azure classic resources, Azure Service Manager) are retired and are no longer supported. If you still have active Co-Administrator or Service Administrator, [convert these roles to Azure RBAC immediately](#). [Learn more](#)

Check access Role assignments Roles Deny assignments ⚠ Classic administrators

My access

View my level of access to this resource.

[View my access](#)

Check access

Review the level of access a user, group, service principal, or managed identity has to this resource. [Learn more](#)

[Check access](#)

Grant access to this resource

Grant access to resources by assigning a role. [Learn more](#)

[Add role assignment](#)

View access to this resource

View the role assignments that grant access to this and other resources. [Learn more](#)

[View](#)

View deny assignments

View the role assignments that have been denied access to specific actions at this scope. [Learn more](#)

[View](#)

Create a custom role

Create a custom role for Azure resources with your own set of permissions to meet the specific needs of your organization. [Learn more](#)

[Add](#)

New! Permissions Management

Discover, monitor and remediate unused permissions in your Azure environment with Microsoft Entra Permissions Management. [Learn more](#)

[Get started](#)

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**.

Microsoft Azure Upgrade Search resources, services, and docs (G+/) Copilot

Home > Subscriptions > Azure subscription 1 | Access control (IAM)

Add role assignment

Role Members Conditions Review + assign

A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles. [Learn more](#)

Job function roles Privileged administrator roles

Grant access to Azure resources based on job function, such as the ability to create virtual machines.

Virtual Machine Type: All Category: All

Name	Description	Type	Category	Details
Azure Stack HCI Connected InfraVMs	Role of Arc integration for Azure Stack HCI Infrastructure Virtual Machines.	BuiltInRole	None	View
Classic Virtual Machine Contributor	Lets you manage classic virtual machines, but not access to them, and not the virtual network or storage account they're connected to.	BuiltInRole	Compute	View
Desktop Virtualization Power On Contributor	Provide permission to the Azure Virtual Desktop Resource Provider to start virtual machines.	BuiltInRole	None	View
Desktop Virtualization Power On Off Contributor	Provide permission to the Azure Virtual Desktop Resource Provider to start and stop virtual machines.	BuiltInRole	None	View
Desktop Virtualization Virtual Machine Contributor	This role is in preview and subject to change. Provide permission to the Azure Virtual Desktop Resource Provider to create, delete, update, start, and stop ...	BuiltInRole	None	View
DevTest Labs User	Lets you connect, start, restart, and shutdown your virtual machines in your Azure DevTest Labs.	BuiltInRole	DevOps	View
Service Fabric Cluster Contributor	Manage your Service Fabric Cluster resources. Includes clusters, application types, application type versions, applications, and services. You will need additi...	BuiltInRole	None	View
Virtual Machine Administrator Login	View Virtual Machines in the portal and login as administrator	BuiltInRole	Compute	View
Virtual Machine Contributor	Lets you manage virtual machines, but not access to them, and not the virtual network or storage account they're connected to.	BuiltInRole	Compute	View
Virtual Machine Data Access Administrator (preview)	Manage access to Virtual Machines by adding or removing role assignments for the Virtual Machine Administrator Login and Virtual Machine User Login r...	BuiltInRole	None	View
Virtual Machine Local User Login	View Virtual Machines in the portal and login as a local user configured on the arc server	BuiltInRole	None	View
Virtual Machine User Login	View Virtual Machines in the portal and login as a regular user.	BuiltInRole	Compute	View

Showing 1 - 12 of 12 results.

Review + assign Previous **Next** Feedback

- Then, on the **Add role assignment**, we select the **User, group, or service principal** radio button in the **Assign access to** section
- 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.

Microsoft Azure Upgrade

Home > Azure subscription 1 | Access control (IAM) >

Add role assignment

Role: Members

Selected role: Virtual Machine Administrator Login

Assign access to: ☒ User, group, or service principal ☐ Managed identity

Members: [+ Select members](#)

Name	Object ID	Type
No members selected		

Description: Optional

[Review + assign](#) [Previous](#) [Next](#)

Select members

Search by name or email address

- AlexSmith
AlexSmith1@
- JewelSales
Sales team responsible for promoting and selling the jewelry brand**
- NishaPatel
NishaPatel3@
- SofiaLee
SofiaLee2@

Selected members:

- JewelSales
Sales team responsible for promoting and selling the jewelry brand**

[Select](#) [Close](#)

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

Microsoft Azure Upgrade

Search resources, services, and docs (G+)

Copilot

Home > Azure subscription 1 | Access control (IAM) >

Add role assignment

Role **Members** Conditions Review + assign

Selected role Virtual Machine Administrator Login

Assign access to ☒ User, group, or service principal ☐ Managed identity

Members + Select members

Name	Object ID	Type
JewelSales	7651f958-a91e-489c-b6cb-52170893d7...	Group

Description Optional

Review + assign Previous **Next**

Feedback

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

Microsoft Azure

Upgrade

Search resources, services, and docs (G+)

Copilot

📄 🔔 ⚙️ ⓘ 👤

DEFAULT DIRECTORY

Home > Azure subscription 1 | Access control (IAM) >

Add role assignment

✕

RoleMembersConditionsReview + assign

RoleVirtual Machine Administrator Login

Scope/subscriptions/1c231d77-b506-4287-925c-aba83bffa6fb

Members

Name	Object ID	Type
JewelSales	7651f958-a91e-489c-b6cb-52170893d78d	Group

DescriptionNo description

Review + assign

Previous

Next

Feedback

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

Microsoft Azure Upgrade

Search resources, services, and docs (G+)

Copilot

DEFAULT DIRECTORY

Home > Azure subscription 1

Azure subscription 1 | Access control (IAM)

Subscription

Search

+ Add Download role assignments Edit columns Refresh Delete Feedback

OverviewActivity logAccess control (IAM)TagsDiagnose and solve problemsSecurityEventsCost ManagementCost analysisCost alertsBudgetsAdvisor recommendationsBillingBilling profile invoicesSettingsProgrammatic deploymentBilling propertiesResource groupsResourcesPreview featuresUsage + quotasPoliciesMy permissionsResource providersDeploymentsDeployment stacksResource locks

Added Role assignment
JewelSales was added as Virtual Machine Administrator Login for Azure subscription 1.

Action required: As of August 31, 2024, Azure classic administrator roles (along with Azure classic resources, Azure Service Manager) are retired and are no longer supported. If you still have active Co-Administrator or Service Administrator role assignments, convert these roles to Azure RBAC immediately. Learn more

Check accessRole assignmentsRolesDeny assignmentsClassic administrators

Number of role assignments for this subscription74000Privileged3View assignments

AllJob function (1)Privileged (3)

Search by name or emailType: AllRole: AllScope: All scopesGroup by: Role

4 items (3 Users, 1 Groups)

Name	Type	Role	Scope	Condition
> Owner (3)				
Virtual Machine Administrator Login (1)				
☐ JE JewelSales	Group	Virtual Machine Administrator Login	This resource	None

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.

Microsoft Azure Upgrade Search resources, services, and docs (G+/) Copilot

Home > **Default Directory | Overview**

Diagnose and solve problems Manage Manage tenants What's new Preview features Got feedback?

Manage

- Users
- Groups
- External identities
- Roles and administrators
- Administrative units
- Delegated admin partners
- Enterprise applications
- Devices
- App registrations
- Identity Governance
- Application proxy
- Custom security attributes
- Licenses
- Cross-tenant synchronization
- Microsoft Entra Connect
- Custom domain names
- Mobility (MDM and WIP)
- Password reset
- User settings

Properties

Security

Monitoring

Microsoft Entra has a simpler, integrated experience for managing all your Identity and Access Management needs. Try the new Microsoft Entra admin center.

Overview Monitoring Properties Recommendations Setup guides

Search your tenant

Basic information

Name	Default Directory	Users	4
Tenant ID		Groups	1
Primary domain		Applications	0
License	Microsoft Entra ID Free	Devices	0

Alerts

- Service Change to Microsoft Entra Connect**
We are making security-related service changes to Microsoft Entra Connect Sync and Connect Health. Upgrade to the latest version to avoid any feature disruptions.
[Learn more](#)
- Migrate to the converged Authentication methods policy**
Please migrate your authentication methods off the legacy MFA and SSPR policies by September 2025 to avoid any service impact.
[Learn more](#)

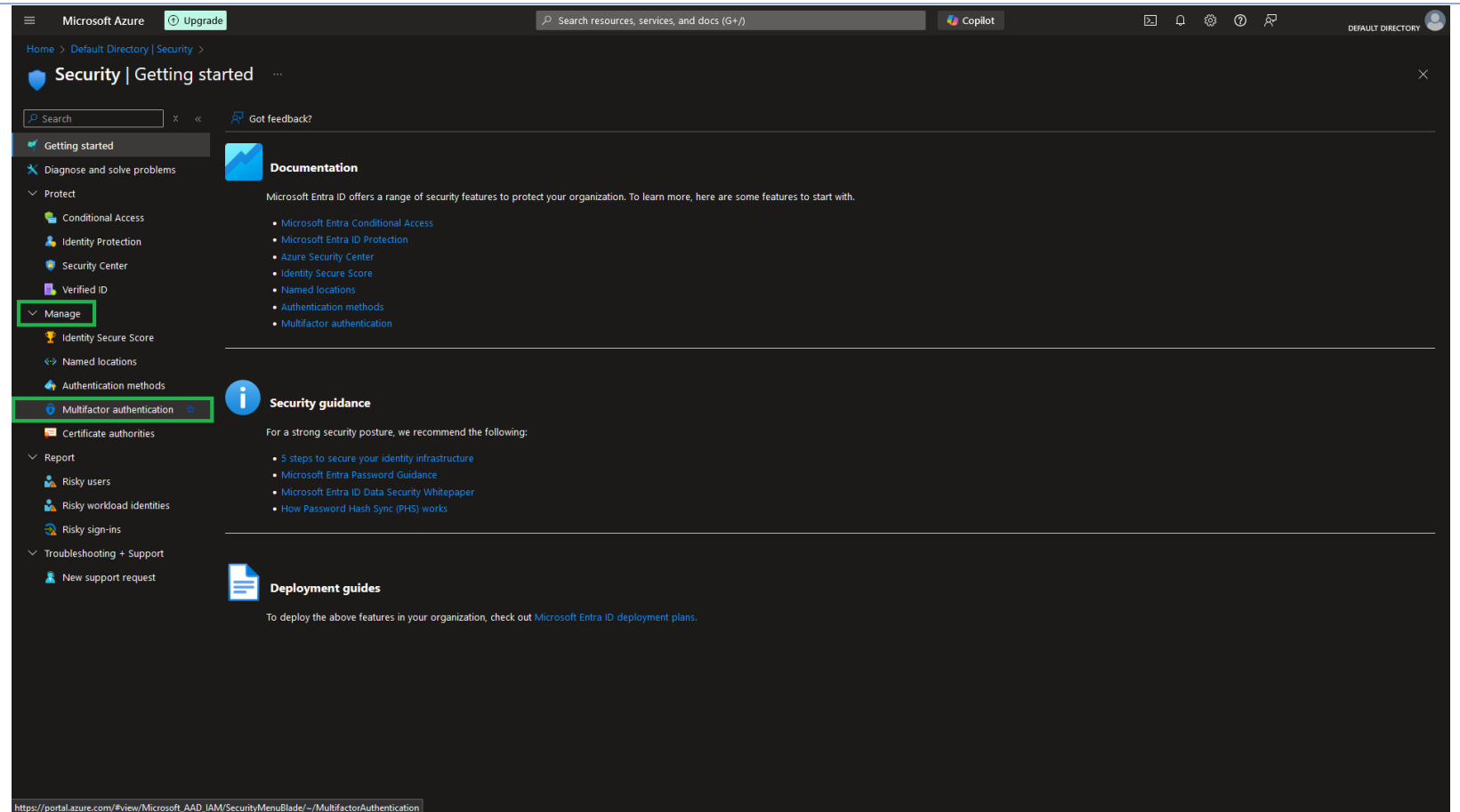
My feed

- Try Microsoft Entra admin center**
Secure your identity environment with Microsoft Entra ID, permissions management and more.
[Go to Microsoft Entra](#)
- Sibil Hadzhitodorov**
37f434e8-3aed-475d-89e5-c3fc7f999098
Global Administrator
[View role information](#)
[View profile](#)
- Secure Score for Identity**
0.00%
Secure score updates can take up to 48 hours.
[View secure score](#)

Microsoft Entra Connect
Not enabled
Sync has never run
[Go to Microsoft Entra Connect](#)

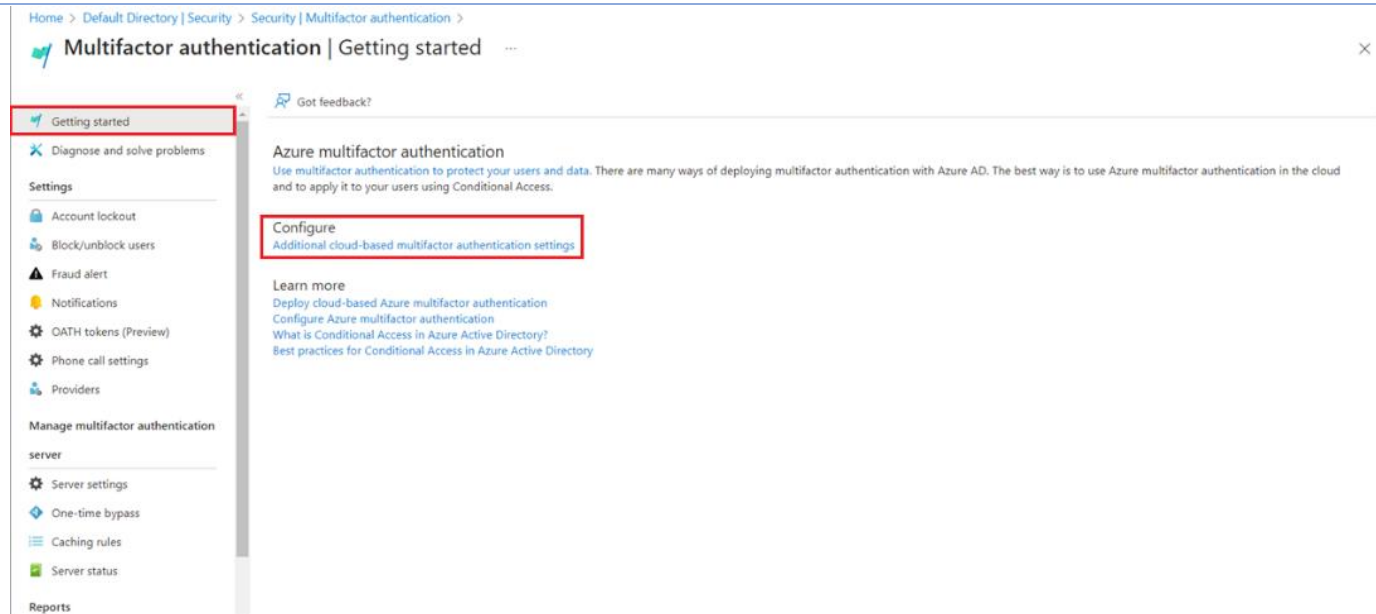
https://portal.azure.com/#view/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade~/Security

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 trial 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**.

multi-factor authentication
users service settings

app passwords [\(learn more\)](#)

- ☒ Allow users to create app passwords to sign in to non-browser apps
☐ Do not allow users to create app passwords to sign in to non-browser apps

trusted ips [\(learn more\)](#)

- ☐ Skip multi-factor authentication for requests from federated users on my intranet
Skip multi-factor authentication for requests from following range of IP address subnets

192.168.1.0/27
192.168.1.0/27
192.168.1.0/27

verification options [\(learn more\)](#)

Methods available to users:

- ☐ Call to phone
☒ Text message to phone
☒ Notification through mobile app
☒ Verification code from mobile app or hardware token

remember multi-factor authentication on trusted device [\(learn more\)](#)

- ☒ Allow users to remember multi-factor authentication on devices they trust (between one to 365 days)

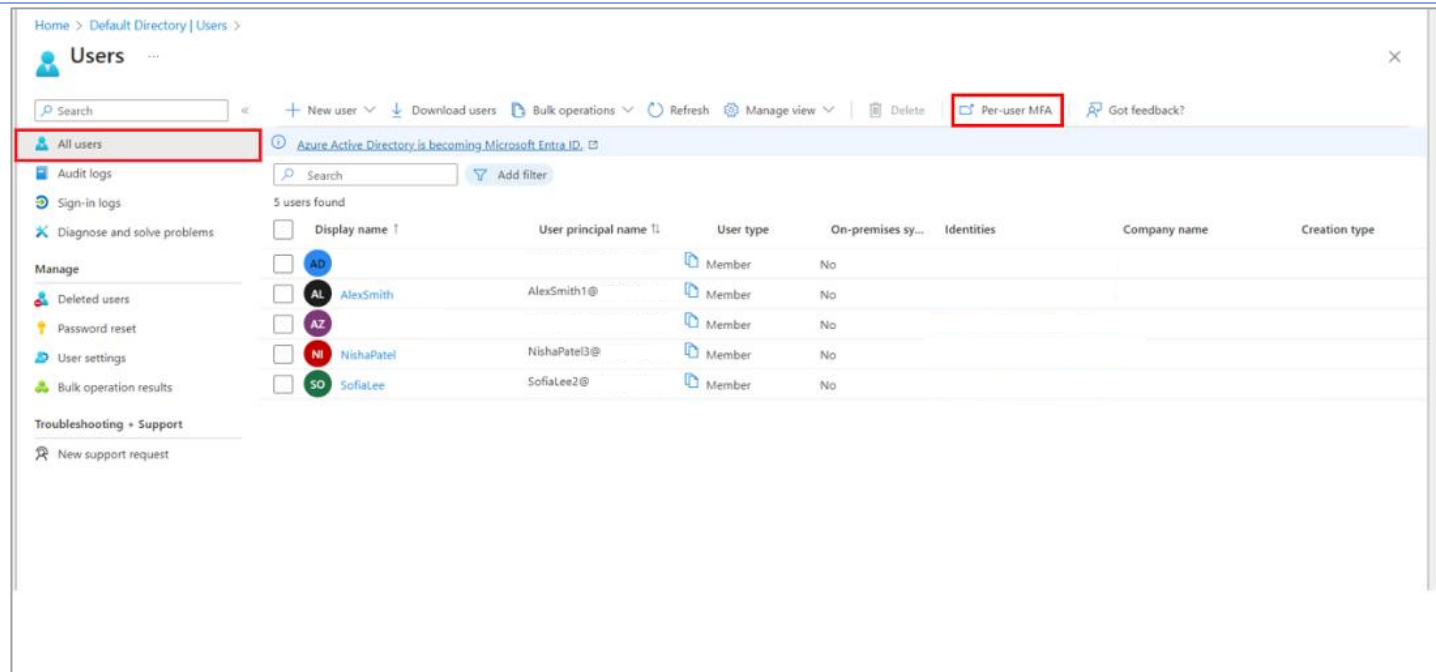
Number of days users can trust devices for

NOTE: For the optimal user experience, we recommend using Conditional Access sign-in frequency to extend session lifetimes on trusted devices, locations, or low-risk sessions as an alternative to 'Remember MFA on a trusted device' settings. If using 'Remember MFA on a trusted device,' be sure to extend the duration to 90 or more days. [Learn more about reauthentication prompts.](#)

Save

Manage advanced settings and view reports [Go to the portal](#)

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.

multi-factor authentication

users service settings

Before you begin, take a look at the [multi-factor auth deployment guide](#).

View: Sign-in allowed users 

Multi-Factor Auth status: Any

[bulk update](#)

☐	DISPLAY NAME 	USER NAME	MULTI-FACTOR AUTH STATUS
☐			Disabled
☒	AlexSmith	AlexSmith1@	Disabled
☐			Disabled
☒	NishaPatel	NishaPatel3@	Disabled
☒	SofiaLee	SofiaLee2@	Disabled

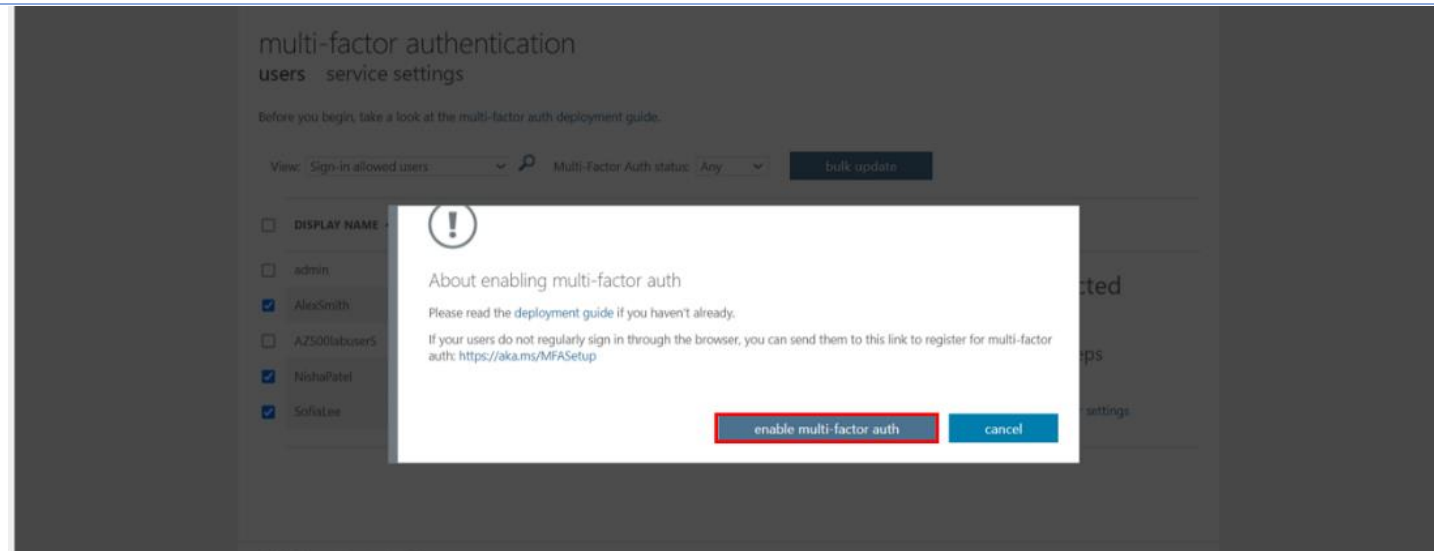
3 selected

quick steps

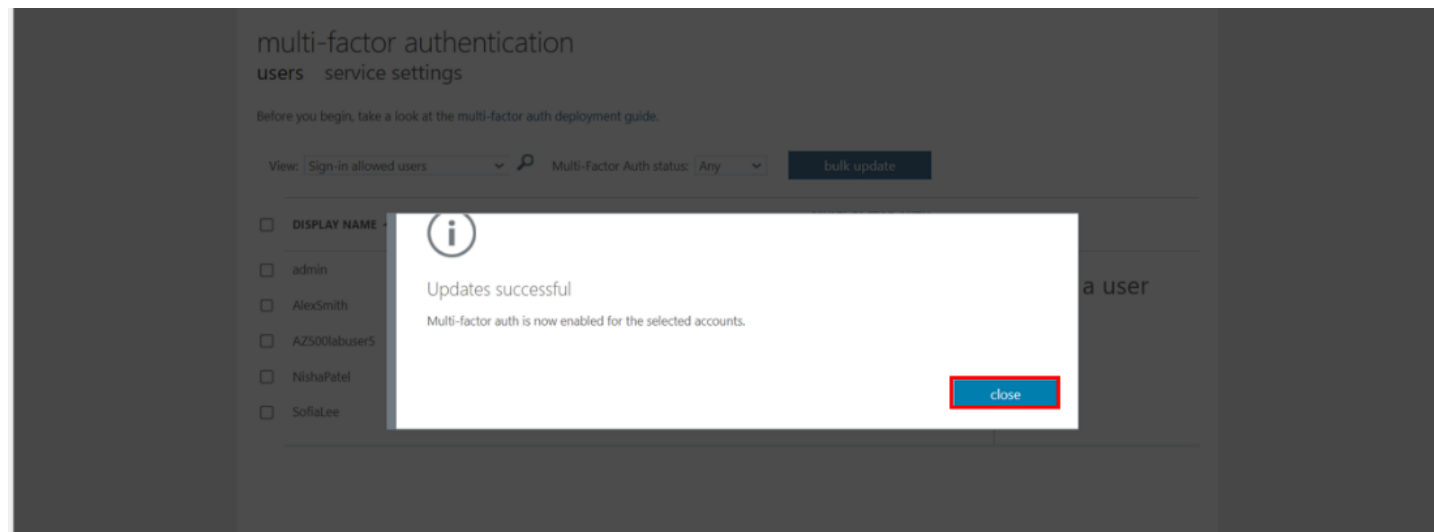
[Enable](#)

[Manage user settings](#)

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

multi-factor authentication

users service settings

Before you begin, take a look at the [multi-factor auth deployment guide](#).

View: Sign-in allowed users 

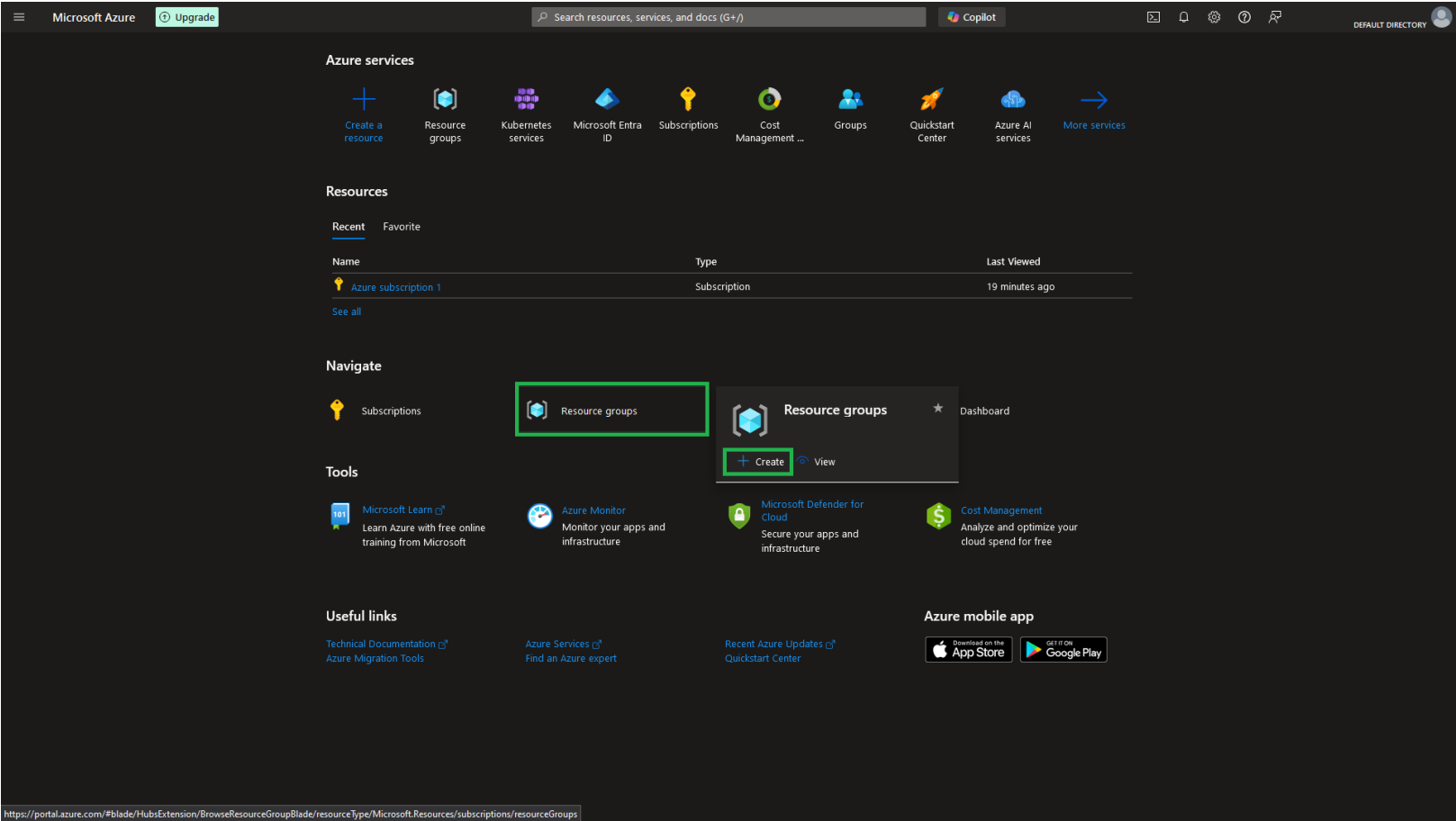
Multi-Factor Auth status: Any

bulk update

☐	DISPLAY NAME ▲	USER NAME	MULTI-FACTOR AUTH STATUS
☐			Disabled
☐	AlexSmith	AlexSmith1@	Enabled
☐			Disabled
☐	NishaPatel	NishaPatel3@	Enabled
☐	SofiaLee	SofiaLee2@	Enabled

Select a user

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.

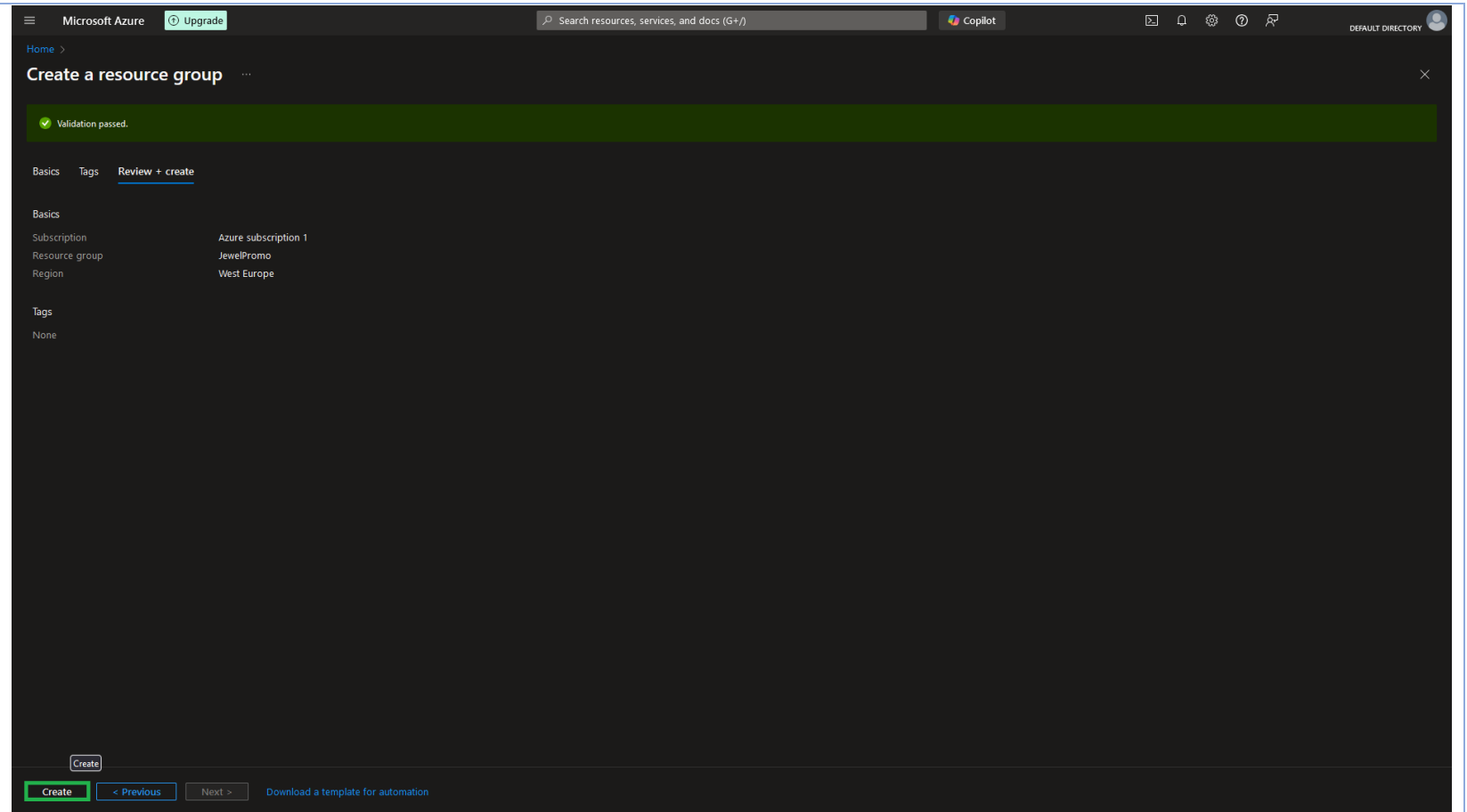
Activity	Key evidence
Activity 1: Create a resource group, a Storage account, and a container.	1. After signing in to the Azure Portal, we hover over Resource groups and click on Create. Note: This can also be achieved by selecting Create a resource and using the <i>Search services and marketplace</i> 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.

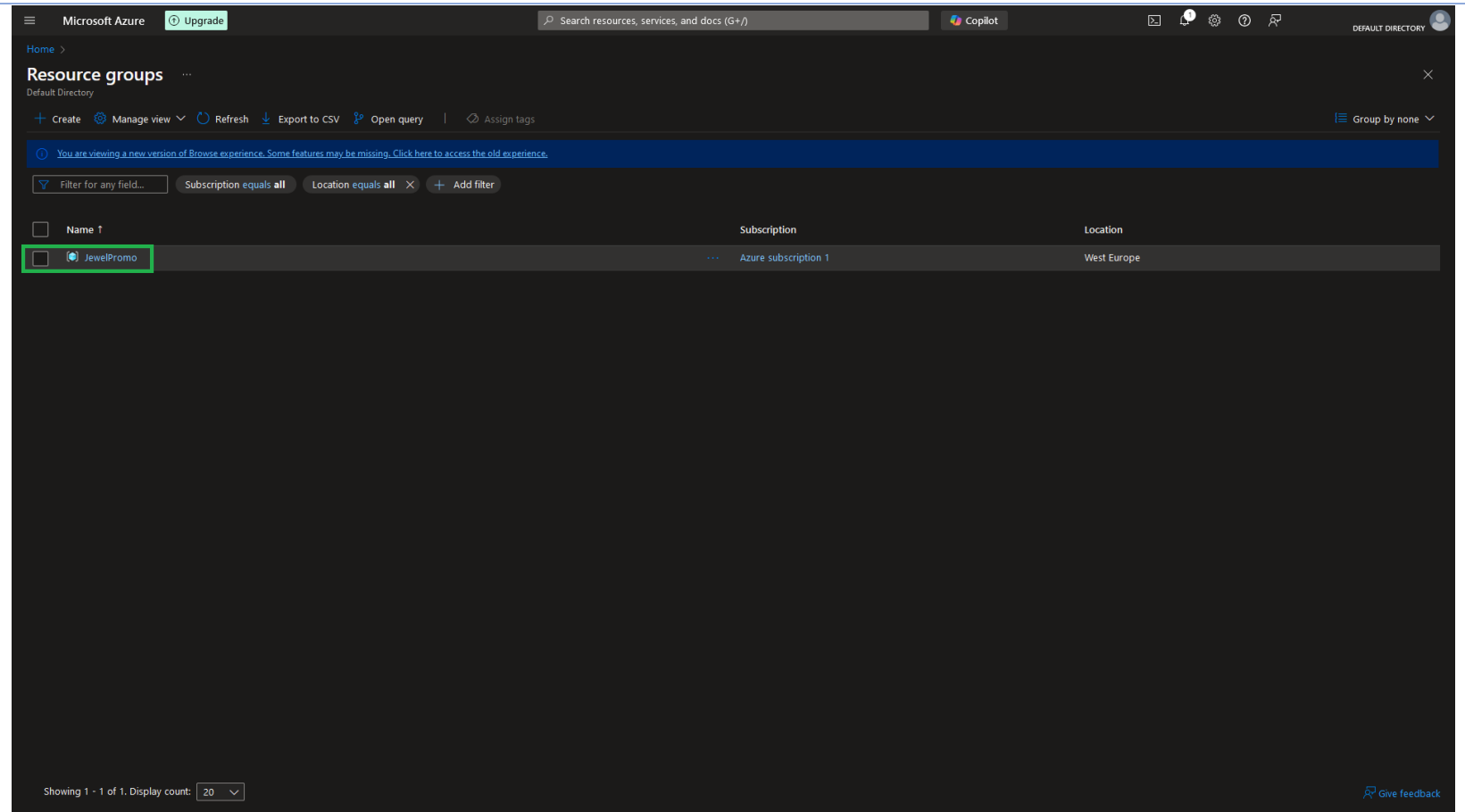
3. Click on **Review + create**

The screenshot shows the 'Create a resource group' page in the Microsoft Azure portal, specifically the 'Review + create' tab. The page has a dark theme. At the top, there's a navigation bar with 'Microsoft Azure', an 'Upgrade' button, a search bar, and a 'Copilot' button. Below the navigation bar, the page title is 'Create a resource group'. There are three tabs: 'Basics', 'Tags', and 'Review + create'. The 'Review + create' tab is active. A descriptive paragraph explains what a resource group is. Below this, there are two sections: 'Project details' and 'Resource details'. In 'Project details', 'Subscription' is set to 'Azure subscription 1' and 'Resource group' is set to 'JewelPromo'. In 'Resource details', 'Region' is set to '(Europe) West Europe'. A green rectangular box highlights these three dropdown menus. At the bottom of the page, there are three buttons: 'Review + create' (highlighted with a green border), '< Previous', and 'Next : Tags >'. A small 'Review + create' button is also visible above the main one.

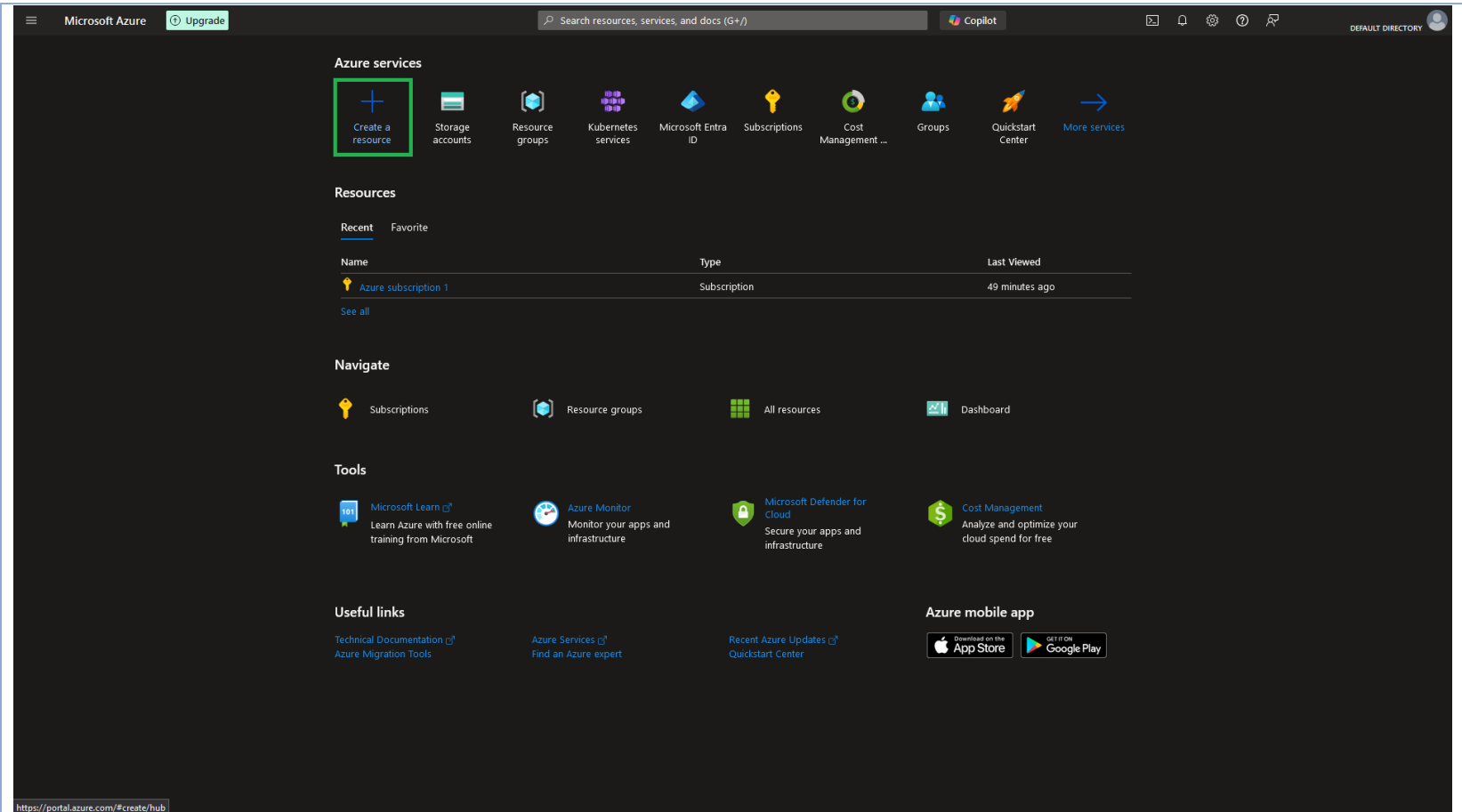
4. Select **Create**, after confirming all details are correct.



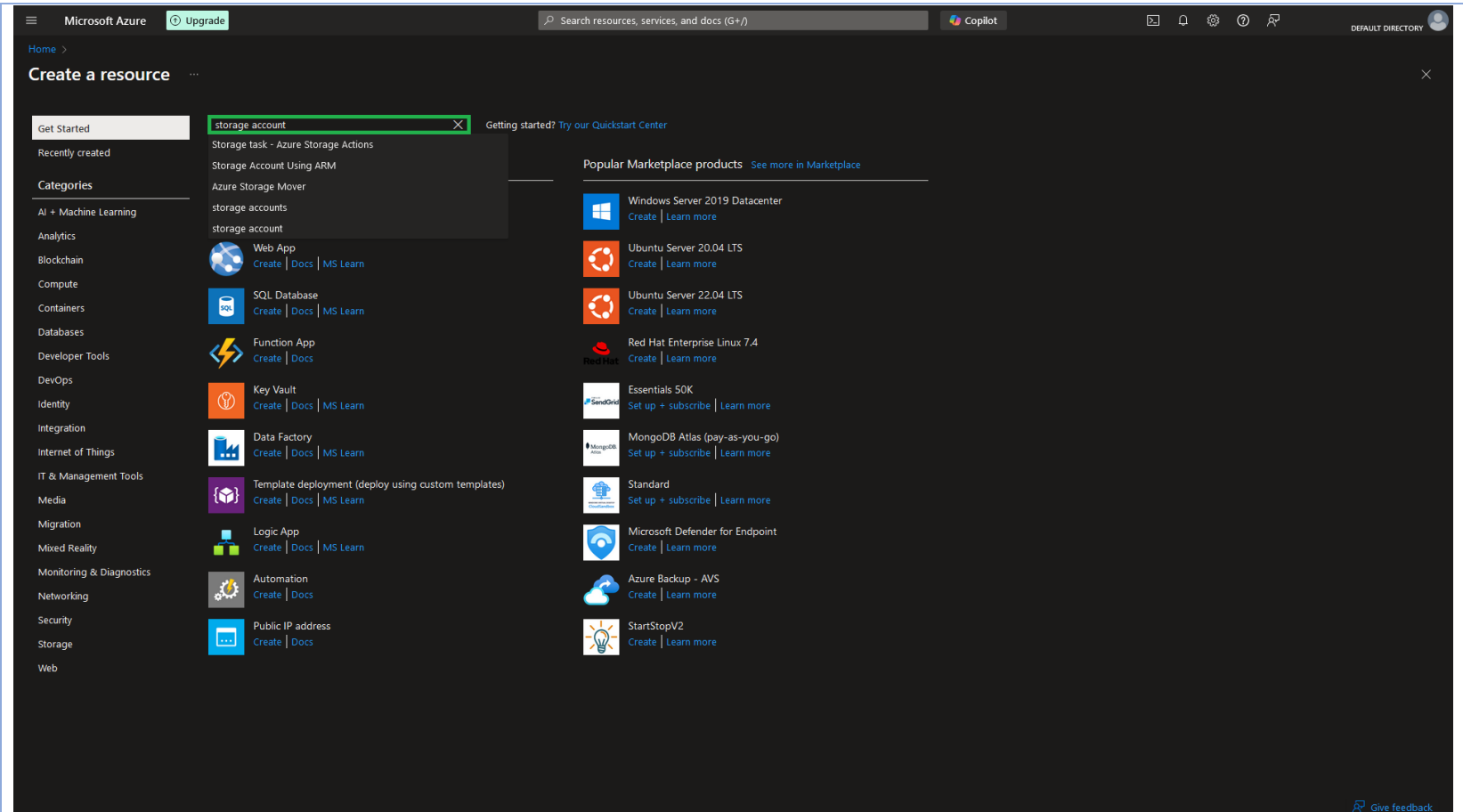
5. We will receive a notification that the resource group had been created, but we can make sure by going into the **Resource Group** page and checking for our newly created resource group.



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.

Microsoft Azure Upgrade Search resources, services, and docs (G+/) Copilot

Home > Create a resource > Marketplace

Get Started Service Providers Management Private Marketplace Private Offer Management My Marketplace Favorites My solutions Recently created Private plans Categories Storage (95) Compute (50) IT & Management Tools (45) Security (39) Analytics (26) Databases (22) Web (16) Developer Tools (13) AI + Machine Learning (12) Networking (11) Identity (7) Media (7) Migration (7)

New! Get AI-generated suggestions for your search. Ask AI to suggest products, articles, and solutions for what you need. View suggestions

storage account Publisher name: All Product Type: All Publisher Type: All Operating System: All Pricing: All

Showing 1 to 20 of 207 results for 'storage account'. Clear search

Storage Account Using ARM Template DIGISTORM LTD. Azure Application storage account arm Price varies Create

Storage account Microsoft Azure Service Use Blobs, Tables, Queues, Files, and Data Lake Gen 2 for reliable, economical cloud storage. Price varies Create

Storage Account Using ARM Template FortuneCloud LLC Azure Application storage account arm template Price varies Create

Storage Account Using ARM Template VIRTUCLLOUD LTD. Azure Application storage account arm Price varies Create

Storage Account Using ARM Template CloudGate LLC Azure Application storage account arm template Price varies Create

Storage task - Azure Storage Actions Microsoft Azure Service Perform common operations on millions of objects based on logical conditions using object properties for Blobs and Data Lake Storage Gen2. Price varies Create

Azure Storage Mover Microsoft Azure Service Azure Storage Mover is a migration service that migrates your on-premises file shares to Azure Storage. Price varies Create

Blob Storage Digests Backed by Confidential Ledger Azure Confidential Ledger Azure Application An application that securely creates and stores blob storage digests in a tamper-proof ledger. Starts at Free Create

Azure Storage solution for Sentinel Microsoft Sentinel, Microsoft Co... Azure Application Azure Storage solution for Sentinel Price varies Create

RamSoft Image Storage RamSoft Inc. Azure Application RamSoft Products seamlessly integrate with Microsoft's Azure Blob Storage. Price varies Create

MDACA Cloud Storage Explorer Spin Systems Inc. Virtual Machine MDACA CSE is a web-based file explorer that is designed to allow you to manage files across a wide range of cloud storage providers. Starts at €0.083/3 years Create

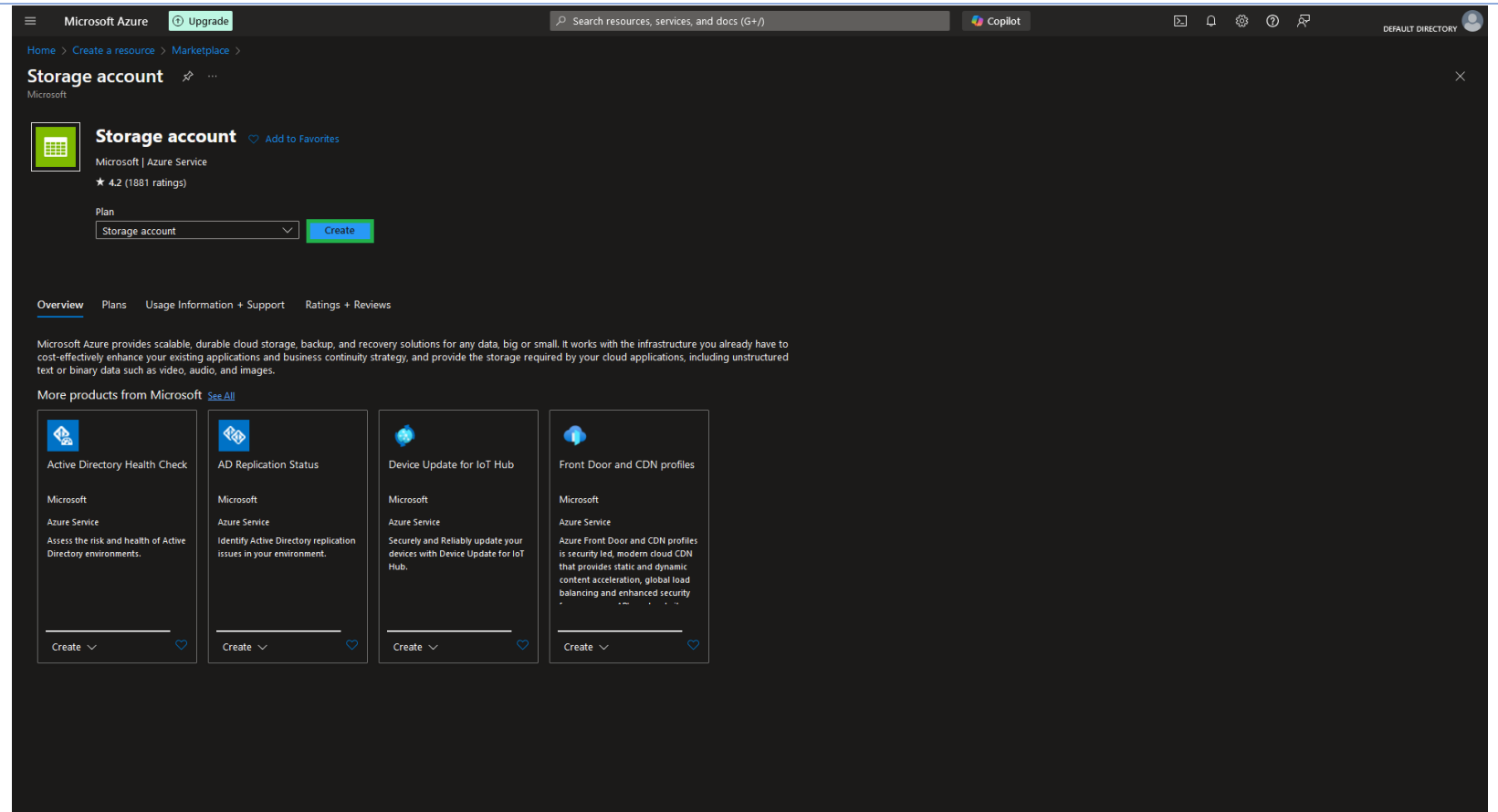
S3 API for Azure Blob Storage (Flexify.I/O) Flexify Inc. Virtual Machine Allows S3-compatible applications store data in Azure Blob Storage via the standard S3 API. Starts at €0.225/3 years Create

Dell APEX Protection Storage for Microsoft Azure (DDVE) Dell Technologies Virtual Machine Dell APEX Protection Storage is simple, flexible and easy to deploy in minutes on any supported server or in-cloud. Starts at €0.225/3 years Create

Dell APEX Protection Storage for Microsoft Azure (DDVE) Dell Technologies International Virtual Machine Dell APEX Protection Storage is simple, flexible and easy to deploy in minutes on any supported server or in-cloud. Starts at €0.225/3 years Create

Is Marketplace helpful?

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.

Microsoft Azure Upgrade

Search resources, services, and docs (G+)

Copilot

Home > Create a resource > Marketplace > Storage account >

Create a storage account

Basics Advanced Networking Data protection Encryption Tags Review + create

Azure Storage is a Microsoft-managed service providing cloud storage that is highly available, secure, durable, scalable, and redundant. Azure Storage includes Azure Blobs (objects), Azure Data Lake Storage Gen2, Azure Files, Azure Queues, and Azure Tables. The cost of your storage account depends on the usage and the options you choose below. [Learn more about Azure storage accounts](#)

Project details

Select the subscription in which to create the new storage account. Choose a new or existing resource group to organize and manage your storage account together with other resources.

Subscription * Azure subscription 1

Resource group * JewelPromo

[Create new](#)

Instance details

Storage account name * admaterials

Region * (Europe) West Europe

[Deploy to an Azure Extended Zone](#)

Primary service * Select a primary service

Performance * Standard: Recommended for most scenarios (general-purpose v2 account)

Premium: Recommended for scenarios that require low latency.

Redundancy * Geo-redundant storage (GRS)

☒ Make read access to data available in the event of regional unavailability.

Previous Next Review + create

[Give feedback](#)

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

Microsoft Azure

Upgrade

Search resources, services, and docs (G+)

Copilot

DEFAULT DIRECTORY

[Home](#) > [Create a resource](#) > [Marketplace](#) > [Storage account](#) >

Create a storage account

BasicsAdvancedNetworkingData protectionEncryptionTagsReview + create

[View automation template](#)

Basics

Subscription	Azure subscription 1
Resource group	JewelPromo
Location	West Europe
Storage account name	admaterials
Primary service	
Performance	Standard
Replication	Read-access geo-redundant storage (RA-GRS)

Advanced

Enable hierarchical namespace	Disabled
Enable SFTP	Disabled
Enable network file system v3	Disabled
Allow cross-tenant replication	Disabled
Access tier	Hot
Enable large file shares	Enabled

Security

Secure transfer	Enabled
Blob anonymous access	Disabled
Allow storage account key access	Enabled
Default to Microsoft Entra authorization in the Azure portal	Disabled
Minimum TLS version	Version 1.2
Permitted scope for copy operations (preview)	From any storage account

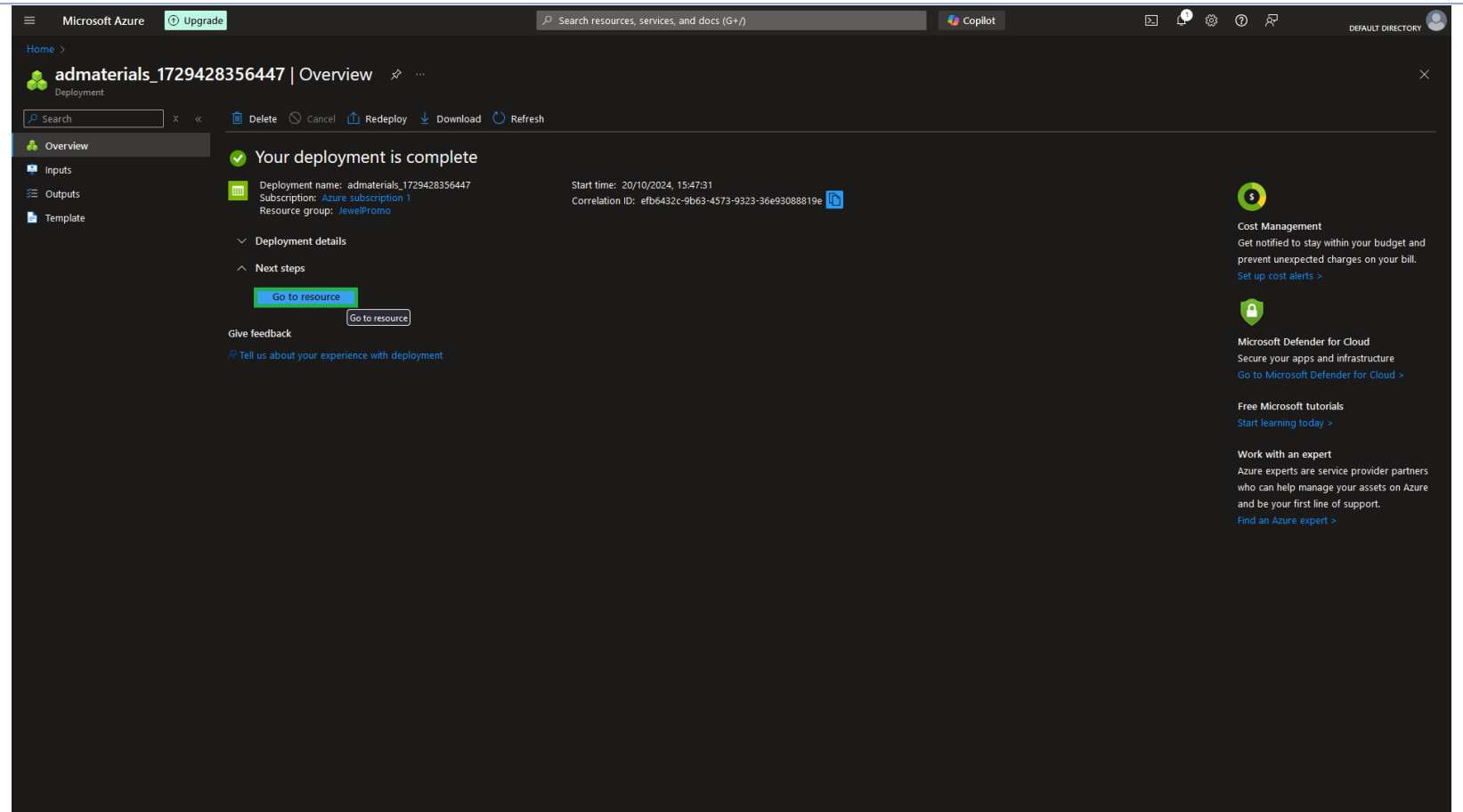
Networking

Network connectivity	Public endpoint (all networks)
Default routing tier	Microsoft network routing

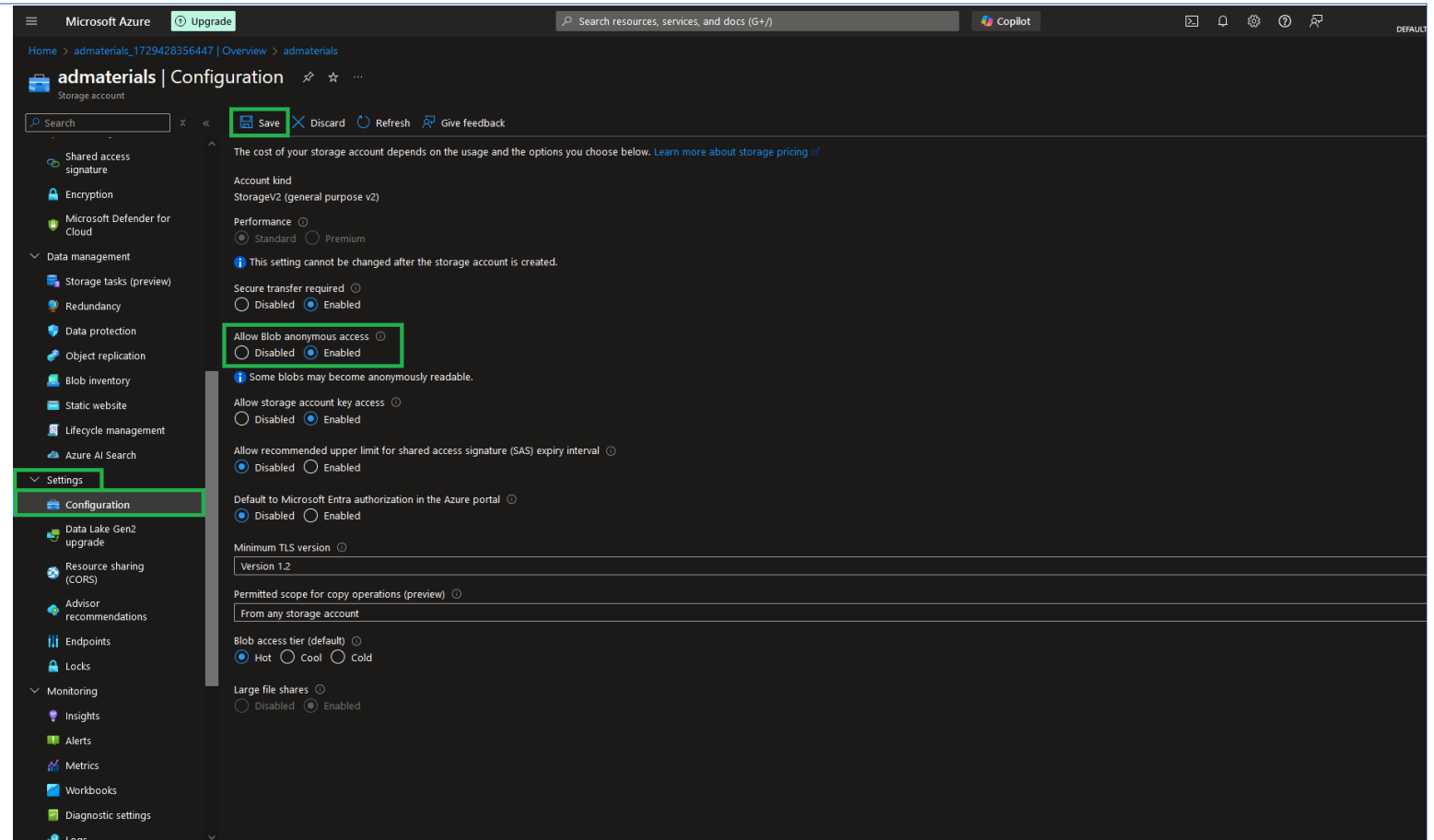
PreviousNextCreate

[Give feedback](#)

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.

Microsoft Azure Upgrade Search resources, services, and docs (G+/) Copilot

Home > admaterials_1729428356447 | Overview > admaterials

admaterials | Containers

Storage account

Search containers by prefix

Name	Last modified	Anonymous access level
☐ \$logs	20/10/2024, 15:47:56	Private

New container

Name

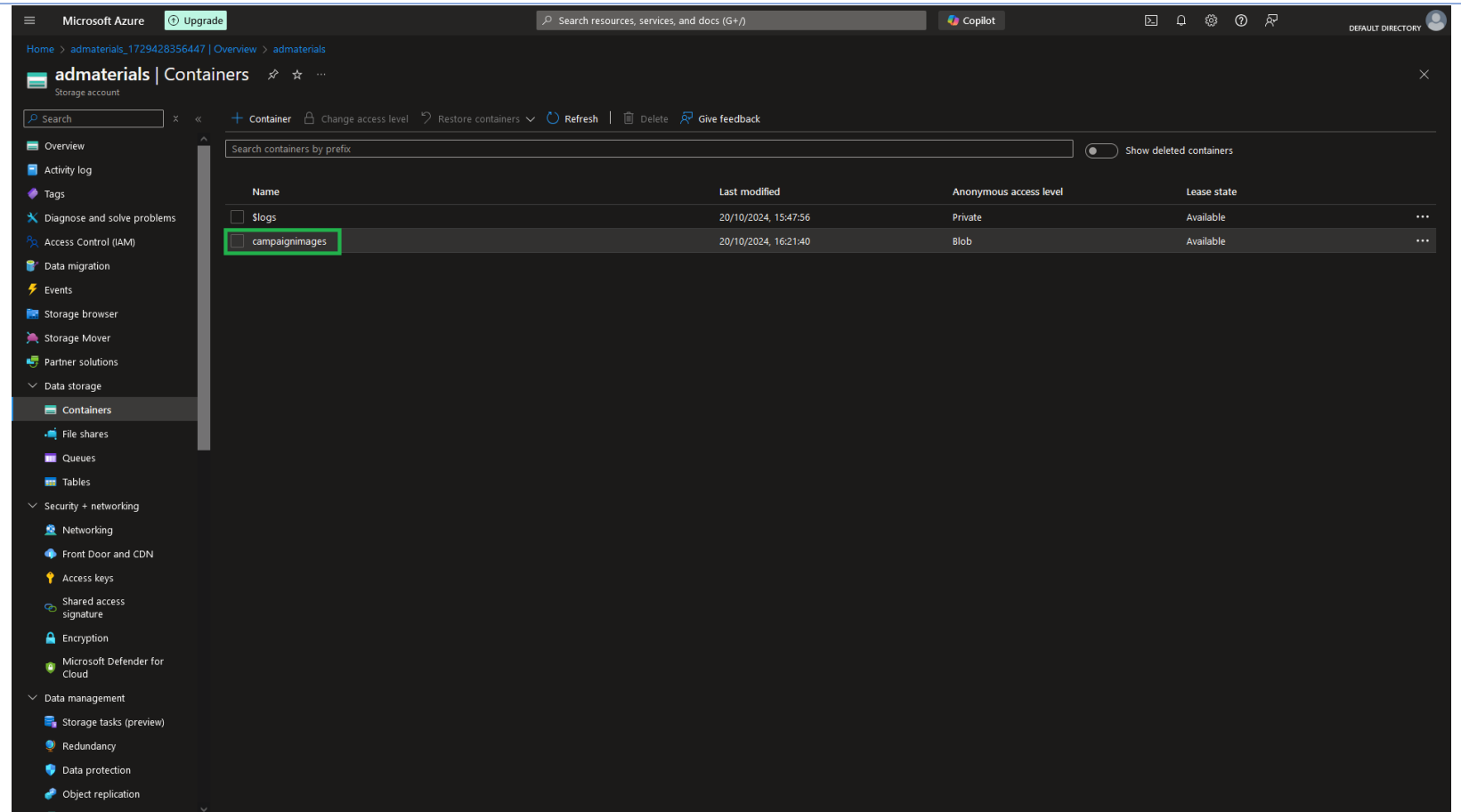
Anonymous access level

Blobs within the container can be read by anonymous request, but container data is not available. Anonymous clients cannot enumerate the blobs within the container.

Advanced

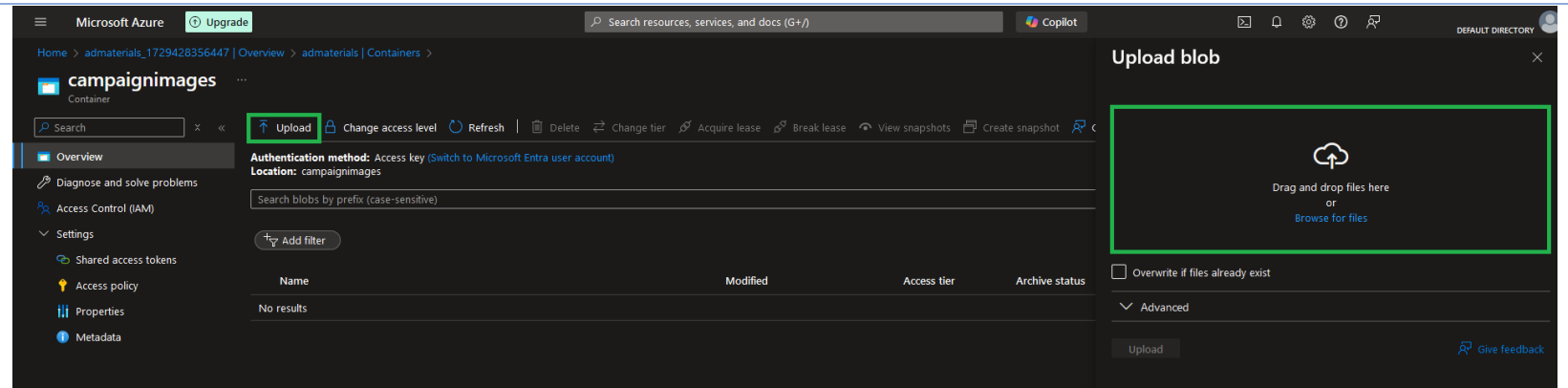
Create

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

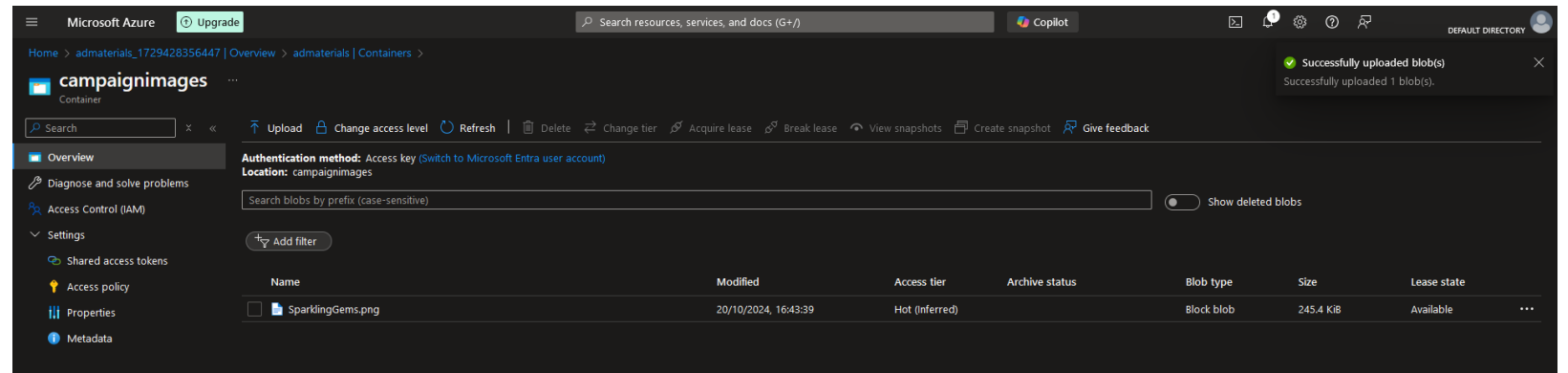


Activity 2: Upload an image to the container in the Storage account and create a Blob SAS URL for the image.

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.

Microsoft Azure Upgrade Search resources, services, and docs (G+/) Copilot

Home > admaterials_1729428356447 | Overview > admaterials | Containers >

campaignimages Container

Search x « Upload Change access level Refresh Delete Change tier Acquire lease Break lease View snapshots Create snapshot Give feedback

Overview Diagnose and solve problems Access Control (IAM) Settings Shared access tokens Access policy Properties Metadata

Authentication method: Access key (Switch to Microsoft Entra user account)
Location: campaignimages

Search blobs by prefix (case-sensitive) Show deleted blobs

Add filter

Name	Modified	Access tier	Archive status	Blob type	Size	Lease state
✓ SparklingGems.png	20/10/2024, 16:43:39	Hot (inferred)		Block blob	245.4 KiB	...

- View/edit
- Download
- Properties
- Generate SAS
- View versions
- View snapshots
- Create snapshot
- Change tier
- Acquire lease
- Break lease
- Delete

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**.

The screenshot displays the Microsoft Azure portal interface. On the left, the 'campaignimages' container is selected, showing a list of blobs with 'SparklingGems.png' highlighted. The main pane shows the 'Generate SAS' wizard for this blob. The 'Permissions' dropdown menu is open, showing 'Read' and 'Write' selected. The 'Allowed protocols' section shows 'HTTPS only' selected. The 'Generate SAS token and URL' button is visible at the bottom of the wizard.

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.

Microsoft Azure Upgrade Search resources, services, and docs (G+/) Copilot

Home > admaterials_1729428356447 | Overview > admaterials | Containers > campaignimages >

campaignimages

Container

Search Upload Change access level

Overview Diagnose and solve problems Access Control (IAM) Settings Shared access tokens Access policy Properties Metadata

Authentication method: Access key (Switch to Microsoft Entra user account) Location: campaignimages Search blobs by prefix (case...) Show deleted blobs Add filter

Name
✓ SparklingGems.png

SparklingGems.png

Blob

Save Discard Download Refresh Delete

Overview Versions Snapshots Edit **Generate SAS**

A shared access signature (SAS) is a URI that grants restricted access to an Azure Storage blob. Use it when you want to grant access to storage account resources for a specific time range without sharing your storage account key. [Learn more about creating an account SAS](#)

Signing method: ☒ Account key ☐ User delegation key

Signing key: Key 1

Stored access policy: None

Permissions: 2 selected

Start and expiry date/time

Start: 20/10/2024 18:05:54 (UTC+02:00) Helsinki, Kyiv, Riga, Sofia, Tallinn, Vilnius

Expiry: 20/10/2024 23:59:59 (UTC+02:00) Helsinki, Kyiv, Riga, Sofia, Tallinn, Vilnius

Allowed IP addresses: for example, 168.1.5.65 or 168.1.5.65-168...

Allowed protocols: ☒ HTTPS only ☐ HTTPS and HTTP

Generate SAS token and URL

Blob SAS token: sp=rw&st=2024-10-20T15:05:54Z&se=2024-10-20T20:59:59Z&spr=https&sv=2022-11-02&sr=b&sig=%2Fz%2BXGfivQk0p%2Fi6xtR%2BG4c7y4Pl99%2B8x%2BqrolucRo%3D

Blob SAS URL: <https://admaterials.blob.core.windows.net/campaignimages/SparklingGems.png?sp=rw&st=2024-10-20T15:05:54Z&se=2024-10-20T20:59:59Z&spr=https&sv=2022-11-02&sr=b&sig=%2Fz%2BXGfivQk0p%2Fi6xtR%2BG4c7y4Pl99%2B8x%2BqrolucRo%3D>

Note: This is the only time we can see and copy the SAS URL.

Activity 3: Assign the Storage Blob Data Contributor role to the group members.

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**.

Microsoft Azure Upgrade

Home > Resource groups > JewelPromo

Resource groups

Default Directory

+ Create ... Group by none

You are viewing a new version of Browse experience. Some features may be missing. Click here to access the old experience.

Name ↑

JewelPromo

JewelPromo | Access control (IAM)

Resource group

Search

+ Add Add role assignment Download role assignments Edit columns Refresh Delete Feedback

Overview Activity log Access control (IAM) Tags Resource visualizer Events Settings Deployments Security Deployment stacks Policies Properties Locks Cost Management Cost analysis Cost alerts (preview) Budgets Advisor recommendations

Number of role assignments for this subscription 3 4000

Privileged 2 View assignments

All Job function (1) Privileged (2)

Search by name or email Type: All Role: All Scope: All scopes Group by: Role

3 items (2 Users, 1 Groups)

Name	Type	Role	Scope	Condition
Owner (2)				
☐ SK	User	Owner	Subscription (inherited)	None
☐ SK	User	Owner	Subscription (inherited)	None
Virtual Machine Local User Login (1)				
☐ JE JewelSales	Group	Virtual Machine Local User Login	Subscription (inherited)	None

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**.

Microsoft Azure Upgrade

Home > Resource groups > JewelPromo | Access control (IAM) >

Add role assignment

Role Members Conditions Review + assign

A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles. [Learn more](#)

Job function roles Privileged administrator roles

Grant access to Azure resources based on job function, such as the ability to create virtual machines.

Blob data x Type: All Category: All

Name ↑	Description ↑	Type ↑	Category ↑	Details
Defender CSPM Storage Data Scanner	Grants access to read blobs and files. This role is used by the data scanner of Defender CSPM.	BuiltInRole	None	View
Defender for Storage Data Scanner	Grants access to read blobs and update index tags. This role is used by the data scanner of Defender for Storage.	BuiltInRole	None	View
Storage Blob Data Contributor	Allows for read, write and delete access to Azure Storage blob containers and data	BuiltInRole	Storage	View
Storage Blob Data Owner	Allows for full access to Azure Storage blob containers and data, including assigning POSIX access control.	BuiltInRole	Storage	View
Storage Blob Data Reader	Allows for read access to Azure Storage blob containers and data	BuiltInRole	Storage	View

Showing 1 - 5 of 5 results.

Review + assign Previous **Next** Feedback

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.

Microsoft Azure Upgrade

Search resources, services, and docs (G+)

Copilot

Home > Resource groups > JewelPromo | Access control (IAM) >

Add role assignment

Role: Members* Conditions: Review + assign

Selected role: Storage Blob Data Contributor

Assign access to: ☒ User, group, or service principal ☐ Managed identity

Members **+ Select members**

Name	Object ID	Type
No members selected		

Description: Optional

Review + assign Previous Next

Select members

Search by name or email address

- AlexSmith AlexSmith1@
- JewelSales Sales team responsible for promoting and selling the jewelry brand
- NishaPatel NishaPatel3@
- SofiaLee SofiaLee2@

Selected members:

- AlexSmith AlexSmith1@
- NishaPatel NishaPatel3@
- SofiaLee SofiaLee2@

Select Close

- 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

Microsoft Azure Upgrade Search resources, services, and docs (G+/) Copilot

Home > Resource groups > JewelPromo | Access control (IAM) >

Add role assignment

Role Members Conditions **Review + assign**

Role Storage Blob Data Contributor

Scope /subscriptions/1c231d77-b506-4287-925c-aba83bffa6fb/resourceGroups/JewelPromo

Members

Name	Object ID	Type
AlexSmith	588eb502-b9f1-40d4-81b9-2071a0051887	User
NishaPatel	32a6aeb6-9916-400a-a36f-7154e95dd46d	User
SofiaLee	9cc77b61-54c8-419c-b1cf-38a9b3b01877	User

Description No description

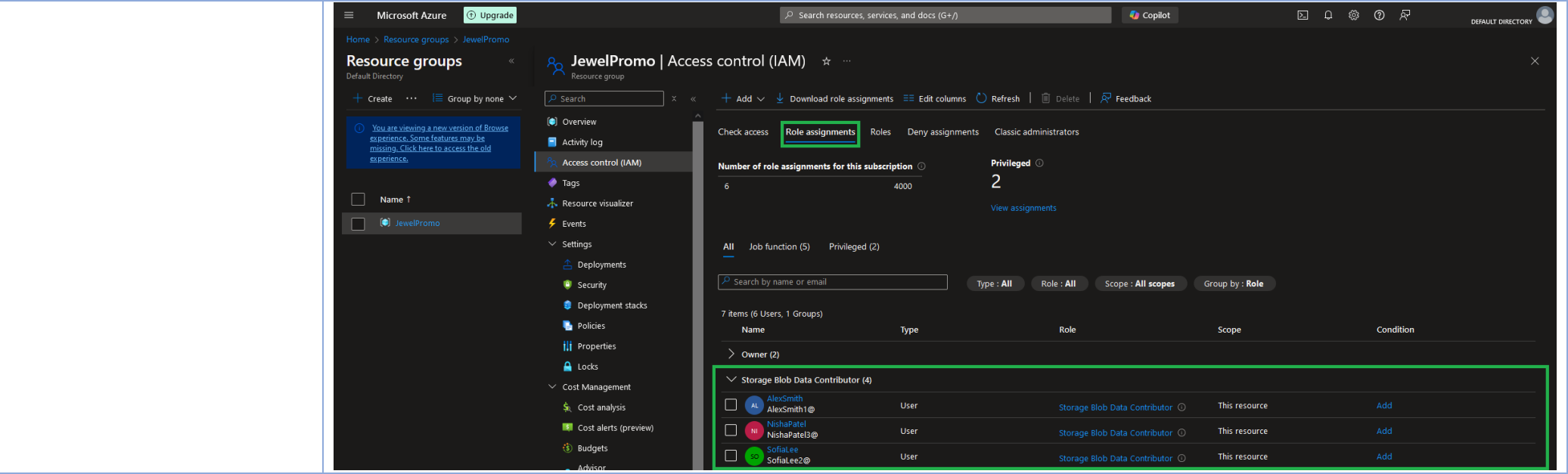
Condition None

Review + assign

Review + assign Previous Next

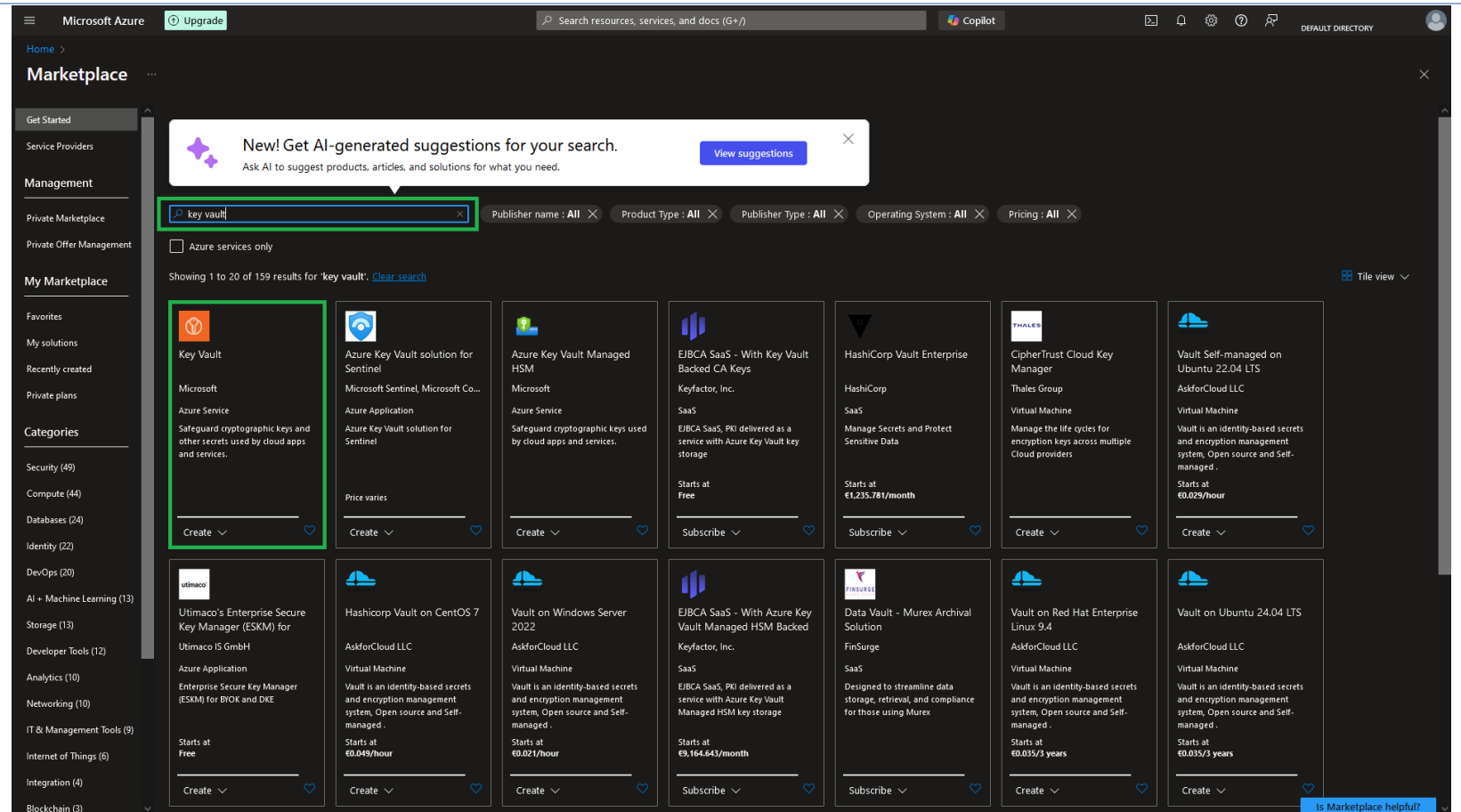
Feedback

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 <i>Search services and marketplace</i> search box, and then click on Key Vault from the results.



- 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) .

Microsoft Azure Upgrade Search resources, services, and docs (G+/) Copilot

Home > Key Vault >

Create a key vault

Azure Key Vault is a cloud service used to manage keys, secrets, and certificates. Key Vault eliminates the need for developers to store security information in their code. It allows you to centralize the storage of your application secrets which greatly reduces the chances that secrets may be leaked. Key Vault also allows you to securely store secrets and keys backed by Hardware Security Modules or HSMs. The HSMs used are Federal Information Processing Standards (FIPS) 140-2 Level 2 validated. In addition, Key Vault provides logs of all access and usage attempts of your secrets so you have a complete audit trail for compliance.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * Azure subscription 1

Resource group * JewelPromo

[Create new](#)

Instance details

Key vault name * EntraKeyVault1

Region * West Europe

Pricing tier * Standard

Recovery options

Soft delete protection will automatically be enabled on this key vault. This feature allows you to recover or permanently delete a key vault and secrets for the duration of the retention period. This protection applies to the key vault and the secrets stored within the key vault.

To enforce a mandatory retention period and prevent the permanent deletion of key vaults or secrets prior to the retention period elapsing, you can turn on purge protection. When purge protection is enabled, secrets cannot be purged by users or by Microsoft.

Soft-delete ☐ Enabled

Days to retain deleted vaults * 90

Purge protection ☐ Disable purge protection (allow key vault and objects to be purged during retention period)

☒ Enable purge protection (enforce a mandatory retention period for deleted vaults and vault objects)

Once enabled, this option cannot be disabled

Previous Next Review + create

Next

[Give feedback](#)

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**.

Microsoft Azure Upgrade

Search resources, services, and docs (G+)

Copilot

Home > Key Vault >

Create a key vault

Basics Access configuration Networking Tags Review + create

Configure data plane access for this key vault

To access a key vault in data plane, all callers (users or applications) must have proper authentication and authorization. Authentication establishes the identity of the caller. Authorization determines which operations the caller can execute. [Learn more](#)

Permission model

Grant data plane access by using a [Azure RBAC](#) or [Key Vault access policy](#)

☐ Azure role-based access control (recommended) ⓘ

☒ Vault access policy ⓘ

Resource access

☐ Azure Virtual Machines for deployment ⓘ

☐ Azure Resource Manager for template deployment ⓘ

☐ Azure Disk Encryption for volume encryption ⓘ

Access policies

Access policies enable you to have fine grained control over access to vault items. [Learn more](#)

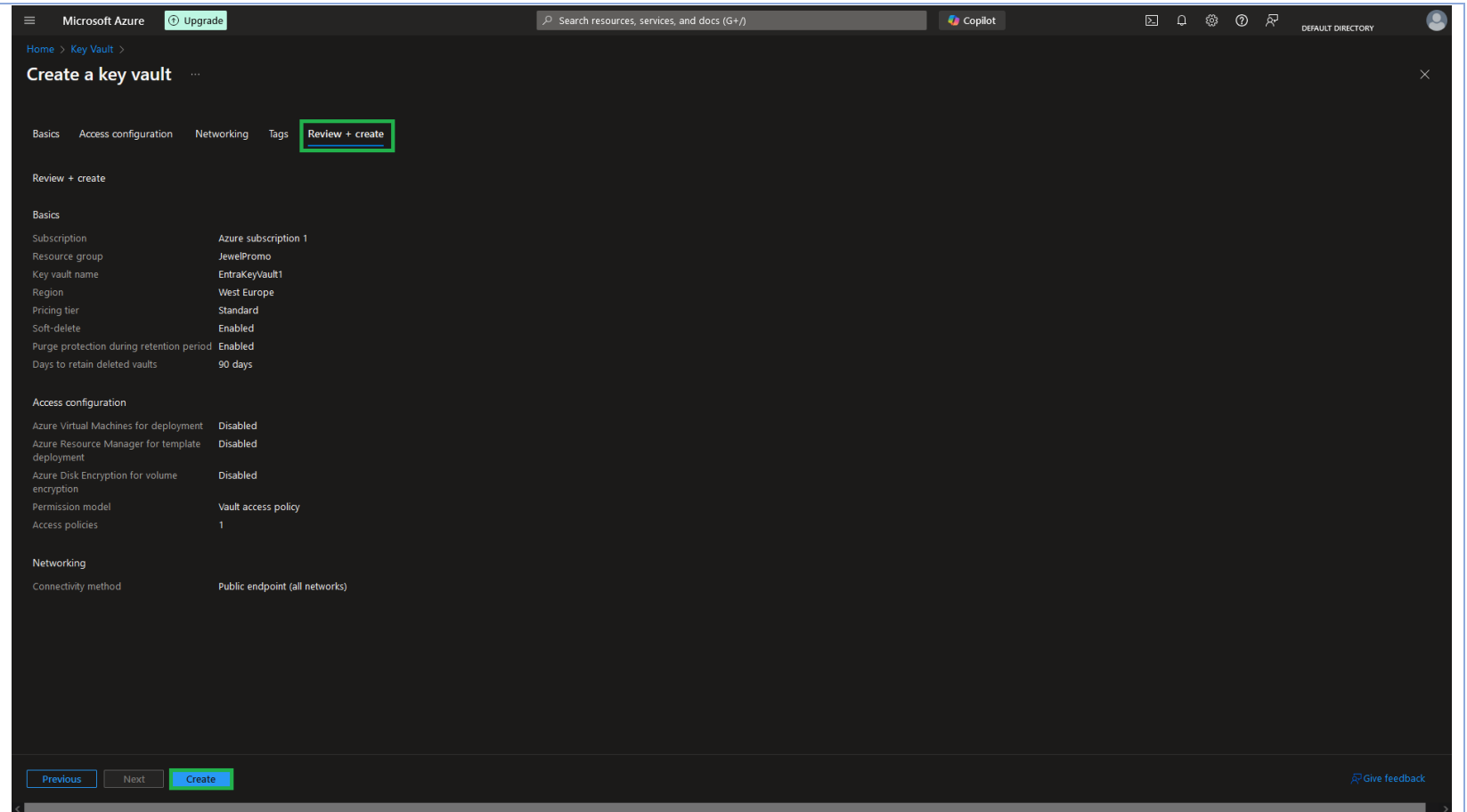
+ Create Edit Delete

☐ Name ↑	Email ↑	Key Permissions	Secret Permissions	Certificate Permissions
✓ USER				
☐		Get, List, Update, Create, Import, Delete, Recover, Backup, R...	Get, List, Set, Delete, Recover, Backup, Restore	Get, List, Update, Create, Import, Delete, Recover, Backup, R...

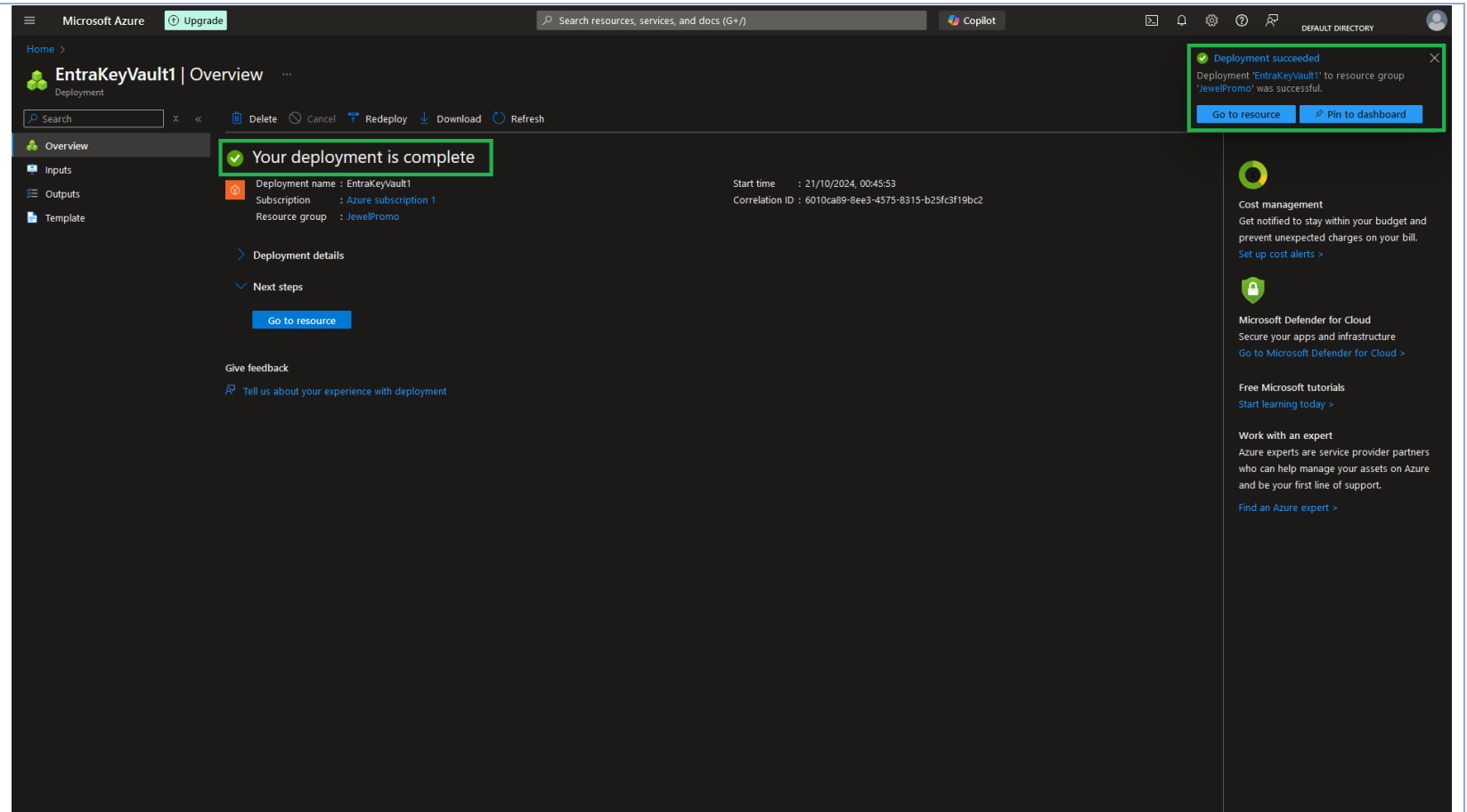
Previous Next Review + create

[Give feedback](#)

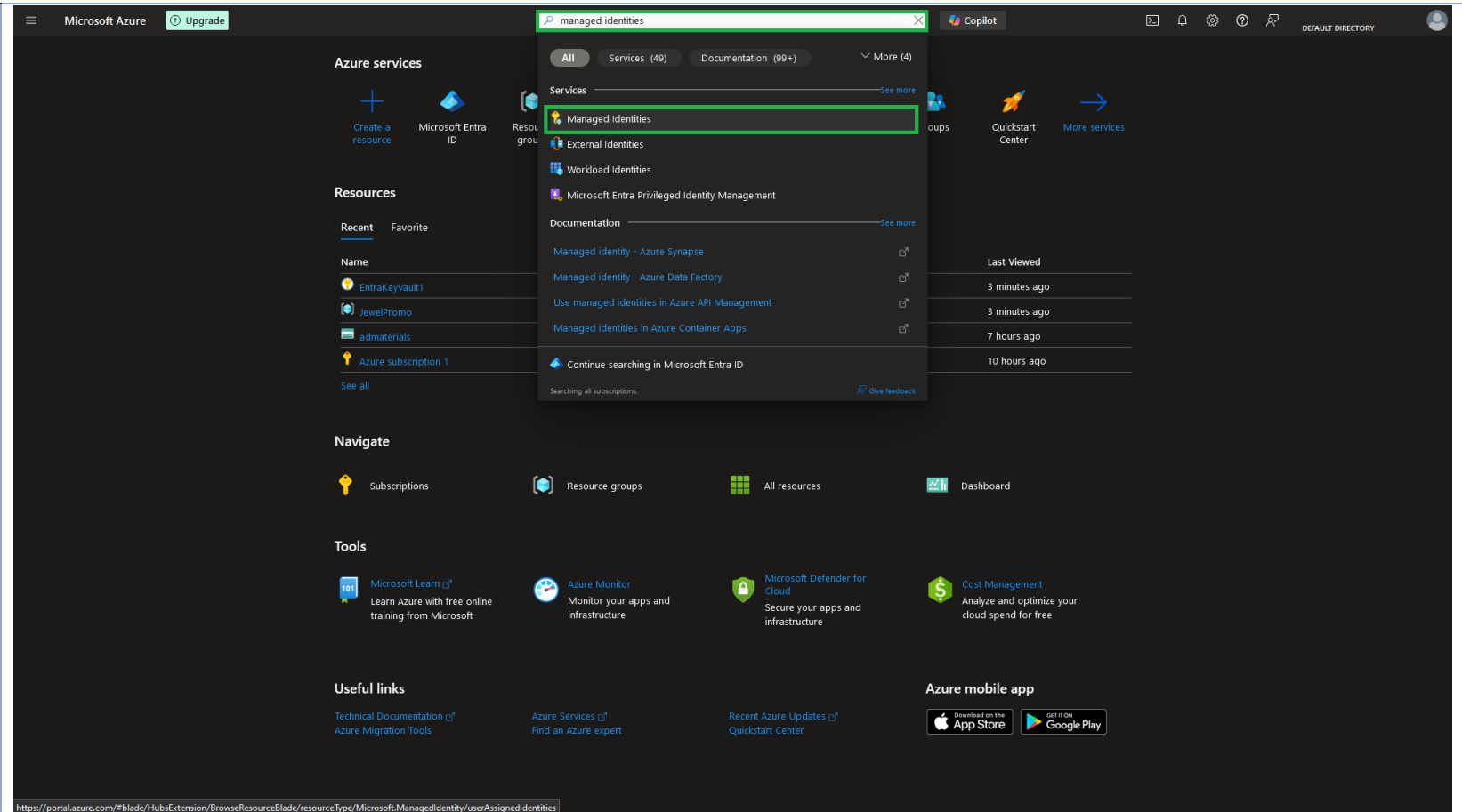
4. On the **Review + create** tab, we review the details, and click on **Create** to deploy the key vault.



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 .

Microsoft Azure Upgrade

Search resources, services, and docs (G+)

Copilot

Home > Managed Identities >

Create User Assigned Managed Identity

Basics Tags Review + create

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * Azure subscription 1

Resource group * JewelPromo [Create new](#)

Instance details

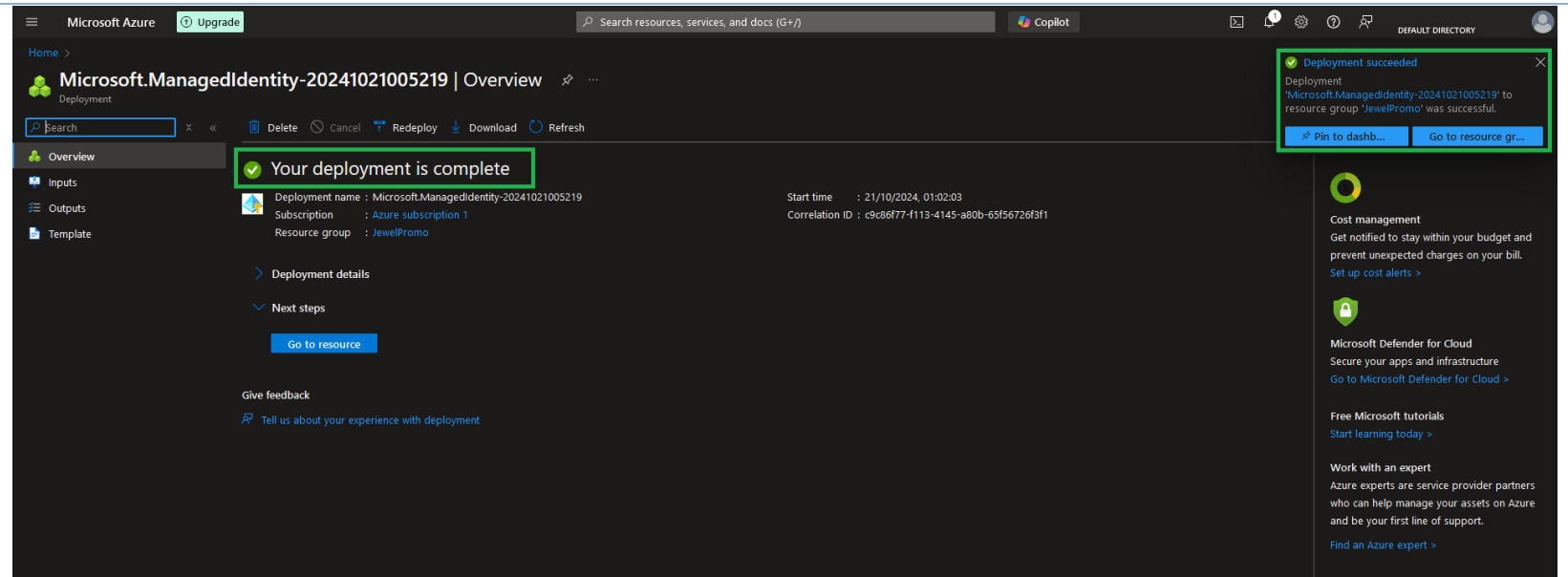
Region * West Europe

Name * CampaignIdentity

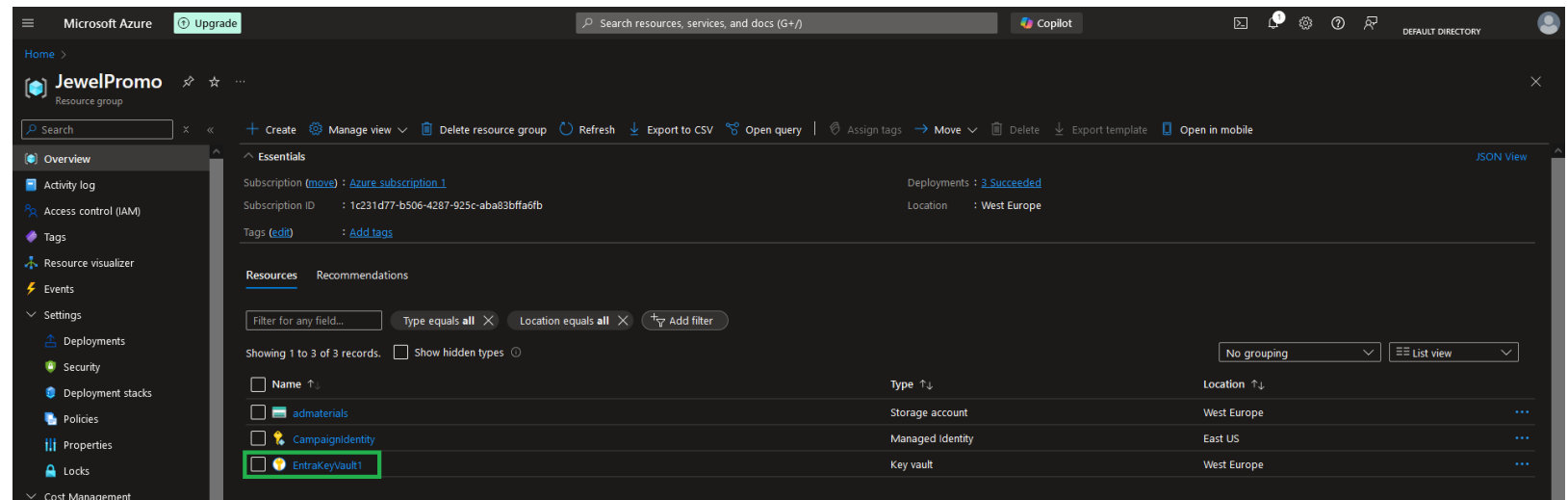
Previous Next Review + create

[Give feedback](#)

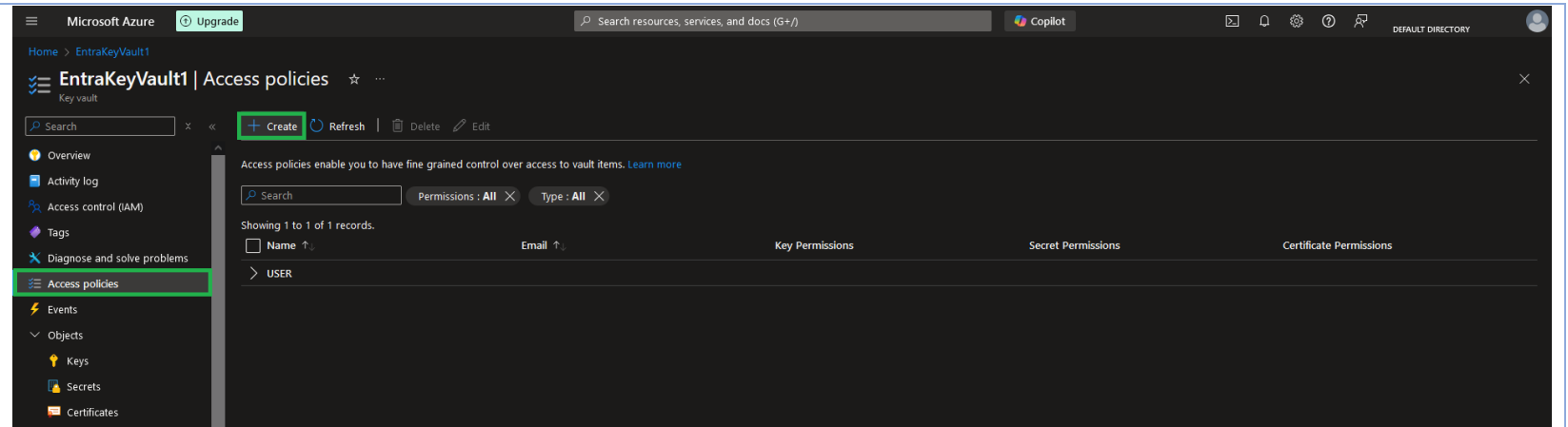
8. On the **Review + create** tab, review the details, click on **Create**, and wait for the notification that the deployment of the managed identity is complete.



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**.

Microsoft Azure Upgrade

Search resources, services, and docs (G+)

Copilot

Home > EntraKeyVault1 | Access policies >

Create an access policy

EntraKeyVault1

1 Permissions 2 Principal 3 Application (optional) 4 Review + create

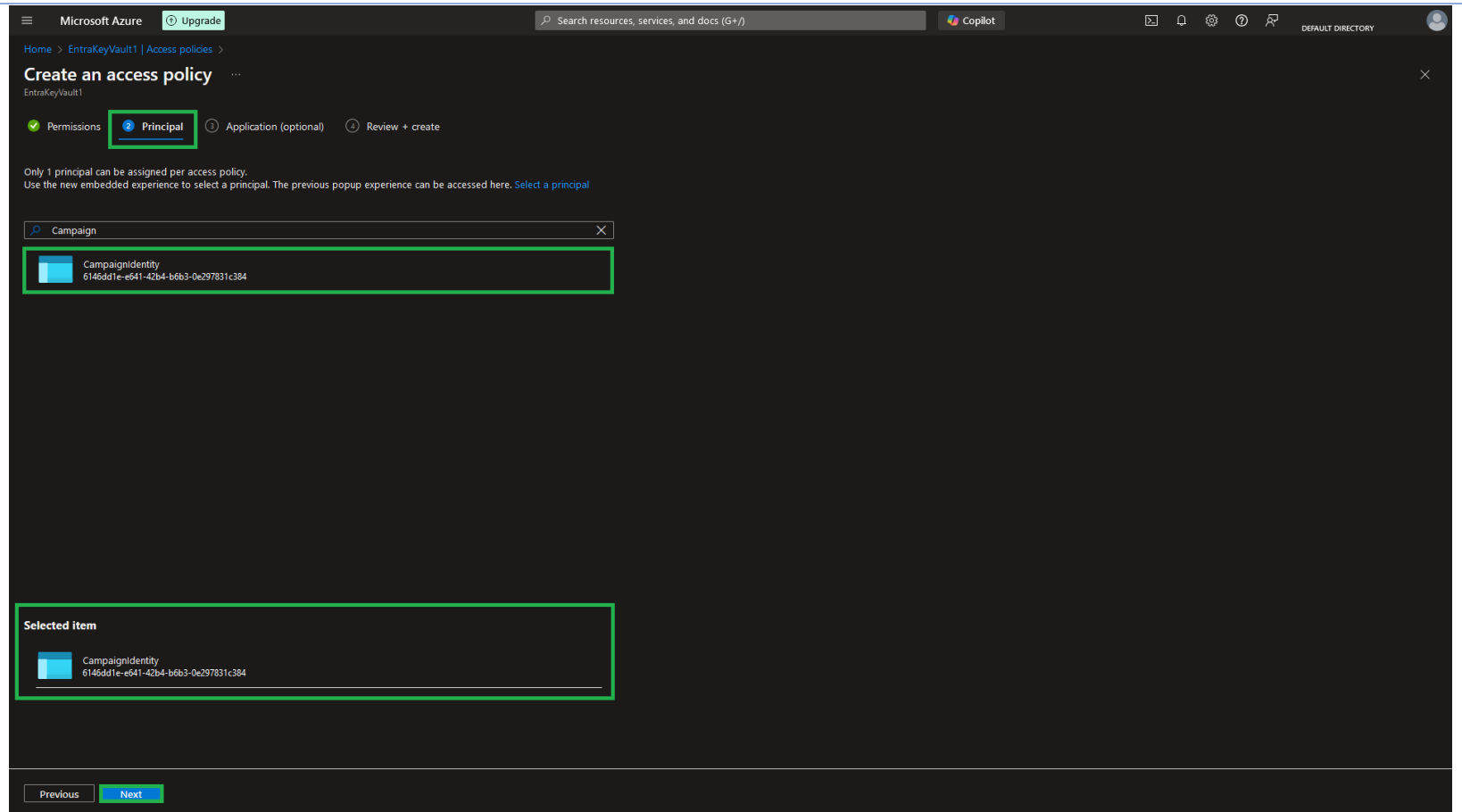
Configure from a template

Select a template

Key permissions	Secret permissions	Certificate permissions
Key Management Operations	Secret Management Operations	Certificate Management Operations
☐ Select all	☐ Select all	☐ Select all
☒ Get	☐ Get	☐ Get
☒ List	☐ List	☐ List
☐ Update	☐ Set	☐ Update
☐ Create	☐ Delete	☐ Create
☐ Import	☐ Recover	☐ Import
☐ Delete	☐ Backup	☐ Delete
☐ Recover	☐ Restore	☐ Recover
☐ Backup		☐ Backup
☐ Restore	Privileged Secret Operations	☐ Restore
	☐ Select all	☐ Manage Contacts
Cryptographic Operations	☐ Purge	☐ Manage Certificate Authorities
☐ Select all		☐ Get Certificate Authorities
☐ Decrypt		☐ List Certificate Authorities
☐ Encrypt		☐ Set Certificate Authorities
☒ Unwrap Key		☐ Delete Certificate Authorities
☒ Wrap Key		
☐ Verify		Privileged Certificate Operations
☐ Sign		☐ Select all
Privileged Key Operations		☐ Purge
☐ Select all		
☐ Purge		

Previous Next

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.

Microsoft Azure Upgrade

Search resources, services, and docs (G+)

Copilot

Home > EntraKeyVault1 | Access policies >

Create an access policy

EntraKeyVault1

Permissions Principal Application (optional) Review + create

Key Permissions

Key Management Operations	Get, List
Cryptographic Operations	Unwrap Key, Wrap Key
Privileged Key Operations	None selected
Rotation Policy Operations	None selected

Secret Permissions

Secret Management Operations	None selected
Privileged Secret Operations	None selected

Certificate Permissions

Certificate Management Operations	None selected
Privileged Certificate Operations	None selected

Principal

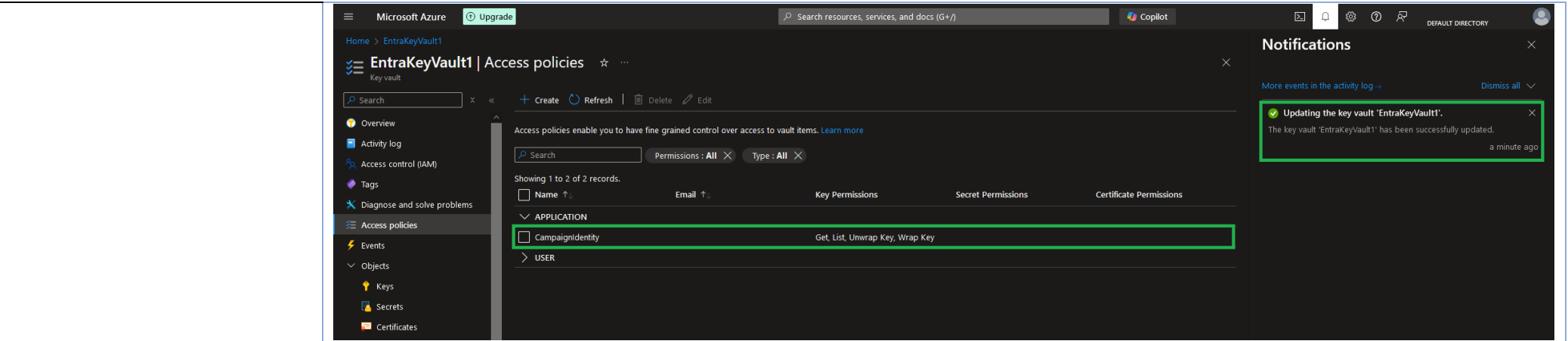
Principal name	CampaignIdentity
Object ID	149b8095-93c5-4b3c-9c1a-785e559f9564

Application

Authorized application	None selected
Object ID	None selected

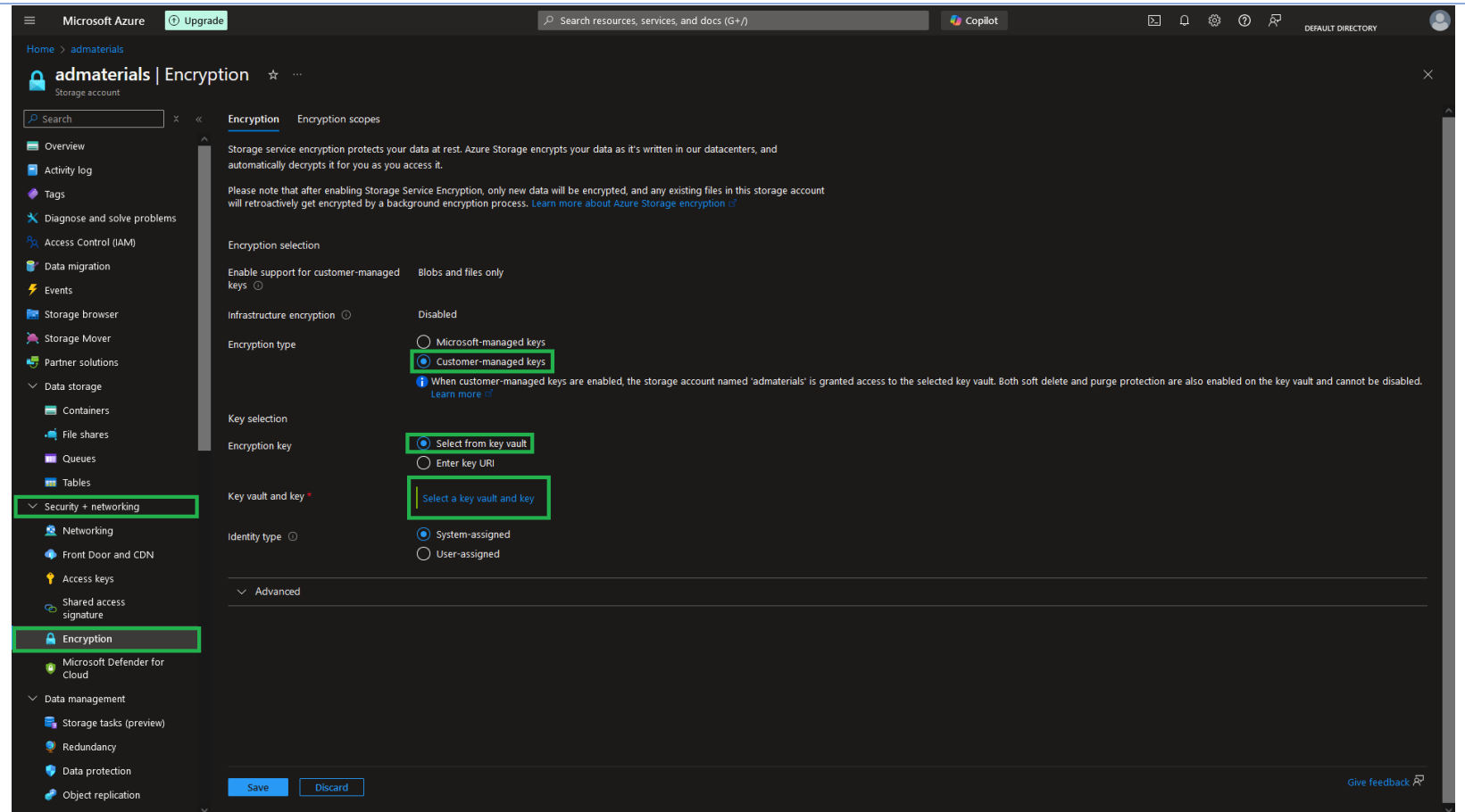
Previous Create

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**.

Microsoft Azure Upgrade

Search resources, services, and docs (G+/)

Copilot

Home > admaterials | Encryption >

Select a key

Subscription * Azure subscription 1

Key store type ○

☒ Key vault

☐ Managed HSM

Key vault * EntraKeyVault1

Create new key vault

Key * 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**.

Microsoft Azure Upgrade

Search resources, services, and docs (G+/)

Copilot

Home > admaterials | Encryption > Select a key >

Create a key

Options Generate

Name * Adkey

Key type ○

☒ RSA

☐ EC

RSA key size

☒ 2048

☐ 3072

☐ 4096

Set activation date ○

☐

Set expiration date ○

☐

Enabled Yes No

Tags 0 tags

Set key rotation policy Not configured

Confidential Key Options

Exportable ○

☐

Immutable ○

☐

Confidential operation policy ○

Create Cancel

Create

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

Microsoft Azure Upgrade

Search resources, services, and docs (G+)

Copilot

Home > admaterials | Encryption >

Select a key

The key "Adkey" has been successfully created.

Subscription * Azure subscription 1

Key store type ○ ☒ Key vault ☐ Managed HSM

Key vault * EntraKeyVault1
Create new key vault

Key * Adkey
Create new key

Select Cancel

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**.

The screenshot displays the Microsoft Azure portal interface for configuring encryption on a storage account named 'admaterials'. The left sidebar shows the navigation menu with 'Encryption' selected. The main content area is titled 'Encryption' and includes a search bar, a list of services, and a detailed configuration page. The configuration page is divided into several sections: 'Encryption selection', 'Key selection', 'Identity type', and 'User-assigned identity'. The 'User-assigned' identity type is selected, and a 'Select an identity' button is highlighted. A sidebar on the right shows the 'Select user assigned managed...' dialog with 'CampaignIdentity' selected. The 'Save' button is at the bottom.

Microsoft Azure Upgrade Search resources, services, and docs (G+/) Copilot DEFAULT DIRECTORY

Home > admaterials

admaterials | Encryption Storage account

Search Encryption Encryption scopes

Overview Activity log Tags Diagnose and solve problems Access Control (IAM) Data migration Events Storage browser Storage Mover Partner solutions Data storage Containers File shares Queues Tables Security + networking Networking Front Door and CDN Access keys Shared access signature Encryption Microsoft Defender for Cloud Data management Storage tasks (preview) Redundancy Data protection Object replication

Storage service encryption protects your data at rest. Azure Storage encrypts your data as it's written in our datacenters, and automatically decrypts it for you as you access it.

Please note that after enabling Storage Service Encryption, only new data will be encrypted, and any existing files in this storage account will retroactively get encrypted by a background encryption process. [Learn more about Azure Storage encryption](#)

Encryption selection

Enable support for customer-managed keys: Blobs and files only

Infrastructure encryption: Disabled

Encryption type: Microsoft-managed keys (selected) Customer-managed keys

When customer-managed keys are enabled, the storage account named 'admaterials' is granted access to the selected key vault. Both soft delete and purge protection are required. [Learn more](#)

Key selection

Encryption key: Select from key vault (selected) Enter key URI

Key vault and key: Key vault: entrakeyvault1 Key: Adkey [Select a key vault and key](#)

Identity type: System-assigned (selected) User-assigned (selected)

Make sure that your user-assigned identity has access to the desired key vault. Otherwise, you will need to leave the storage account and make the required changes.

User-assigned identity: Select an identity

Advanced

Save Discard

Select user assigned managed...

Subscription: Azure subscription 1

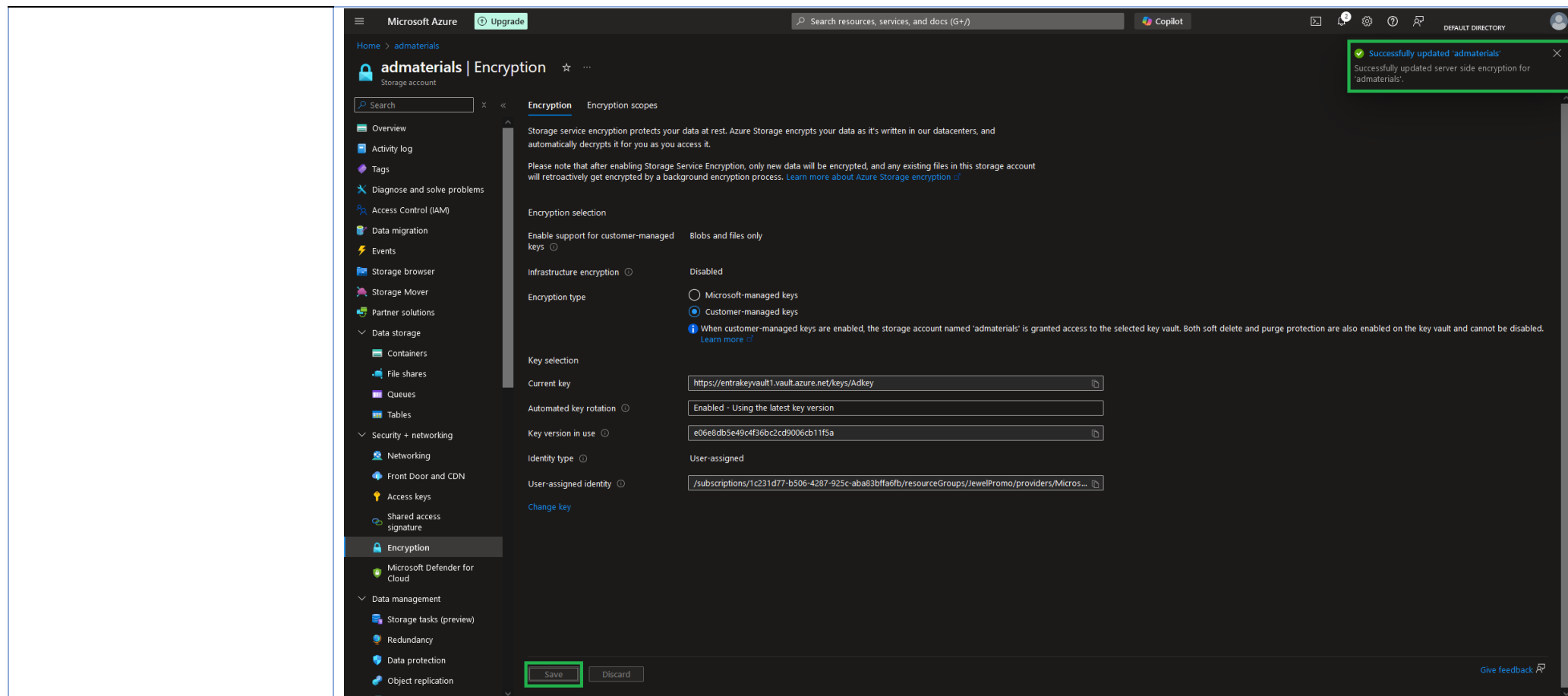
User assigned managed identities: Filter by identity name and/or resource group name

CampaignIdentity Resource Group: JewelPromo

Selected identity: CampaignIdentity Resource Group: JewelPromo Subscription: Azure subscription 1 Remove

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 <i>the Security + Networking</i> blade, and click on the Enable on storage account button.

admaterials | Microsoft Defender for Cloud

Storage account

Search

Overview

Activity log

Tags

Diagnose and solve problems

Access Control (IAM)

Data migration

Events

Storage browser

Storage Mover

Partner solutions

Data storage

Containers

File shares

Queues

Tables

Security + networking

Networking

Front Door and CDN

Access keys

Shared access signature

Encryption

Microsoft Defender for Cloud

Data management

Go to Defender for Cloud Overview

Give us feedback

Enable Microsoft Defender for Storage

Microsoft Defender for Storage detects threats on your storage workloads and data, including malicious access, data exfiltration of sensitive data and malware upload. [More details >](#)

Price: \$10/Storage account/month (overage charges may apply)

Essential capabilities

Activity monitoring (log analysis based threat detection)

Configurable capabilities

Sensitive data threat detection No additional cost

On-upload malware scanning \$0.15/GB scanned

Enable on storage account

On-Upload malware scanning uses [Enable on storage account](#) virus as a scanning engine with the online cloud-protection capabilities. The online cloud protection improves the precision of malware detection by uploading metadata for suspicious files to Microsoft Defender Cloud Protection servers. To learn more about how this metadata is processed and stored see [here](#).

Or visit Defender Plans page to [enable on entire subscription](#)

Recommendations

Defender for Cloud continuously monitors the configuration of your storage accounts to identify potential security vulnerabilities and recommends actions to mitigate them.

✓

✓

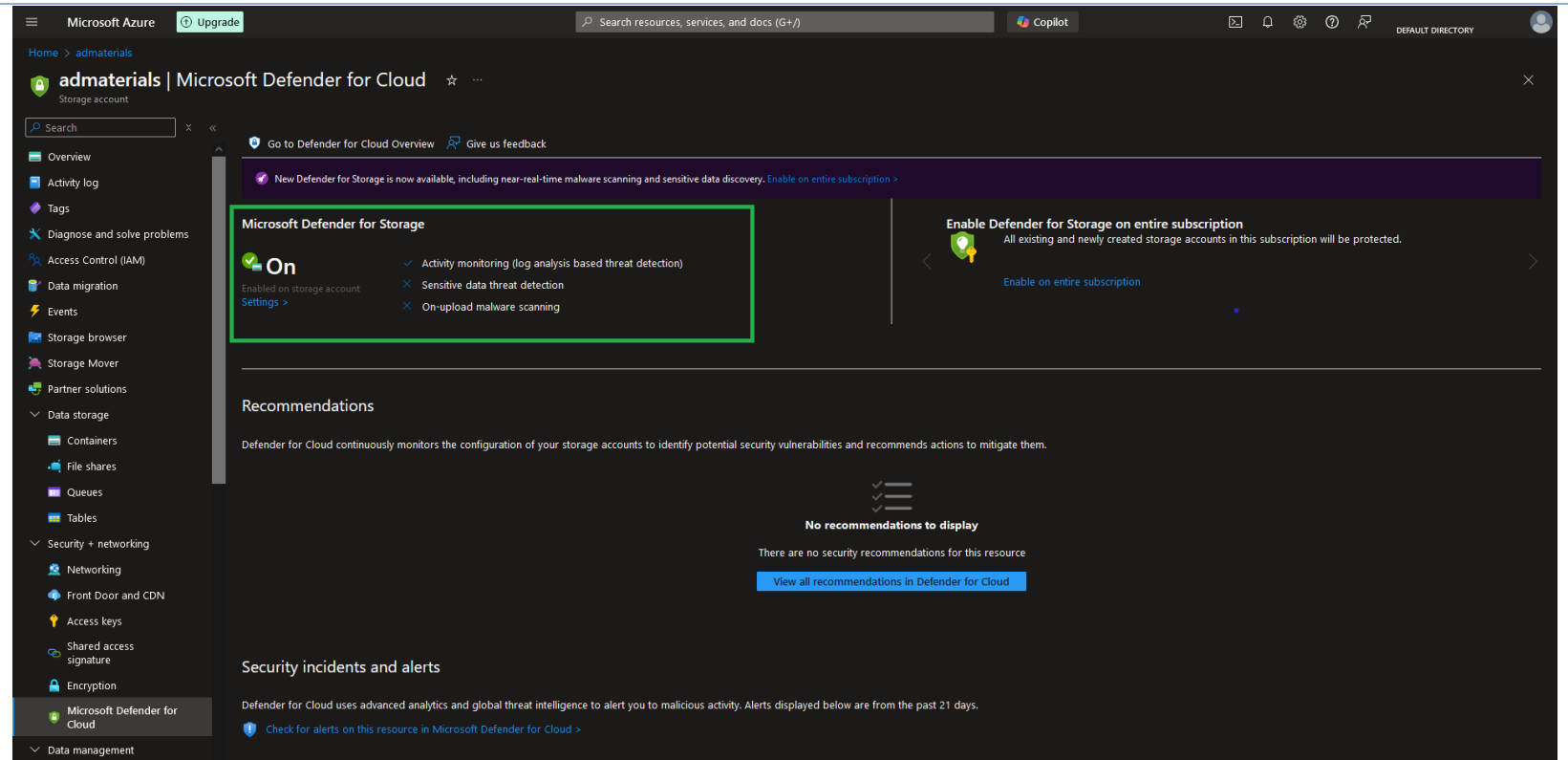
✓

No recommendations to display

There are no security recommendations for this resource

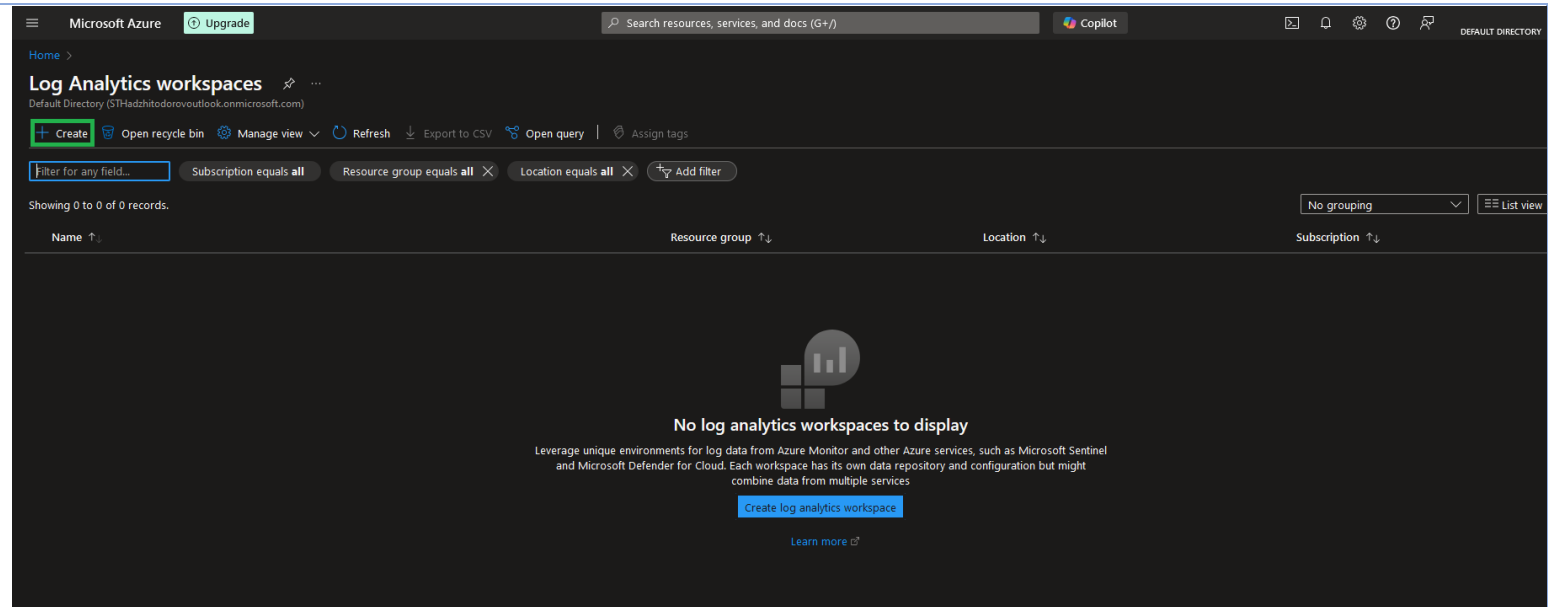
View all recommendations in Defender for Cloud

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.

Microsoft Azure Upgrade

Search resources, services, and docs (G+)

Copilot

Home > Log Analytics workspaces >

Create Log Analytics workspace

Basics Tags Review + Create

i A Log Analytics workspace is the basic management unit of Azure Monitor Logs. There are specific considerations you should take when creating a new Log Analytics workspace. [Learn more](#)

With Azure Monitor Logs you can easily store, retain, and query data collected from your monitored resources in Azure and other environments for valuable insights. A Log Analytics workspace is the logical storage unit where your log data is collected and stored.

Project details
Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * Azure subscription 1

Resource group * JewelPromo [Create new](#)

Instance details

Name * JewelAnalytics

Region * West Europe

Review + Create

Review + Create < Previous Next : Tags >

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

Microsoft Azure Upgrade Search resources, services, and docs (G+/) Copilot

Home > admaterials

admaterials | Diagnostic settings

Storage account

Search Refresh Feedback

Subscription: Azure subscription 1 Resource group: JewelPromo Resource type: Storage accounts Resource: admaterials

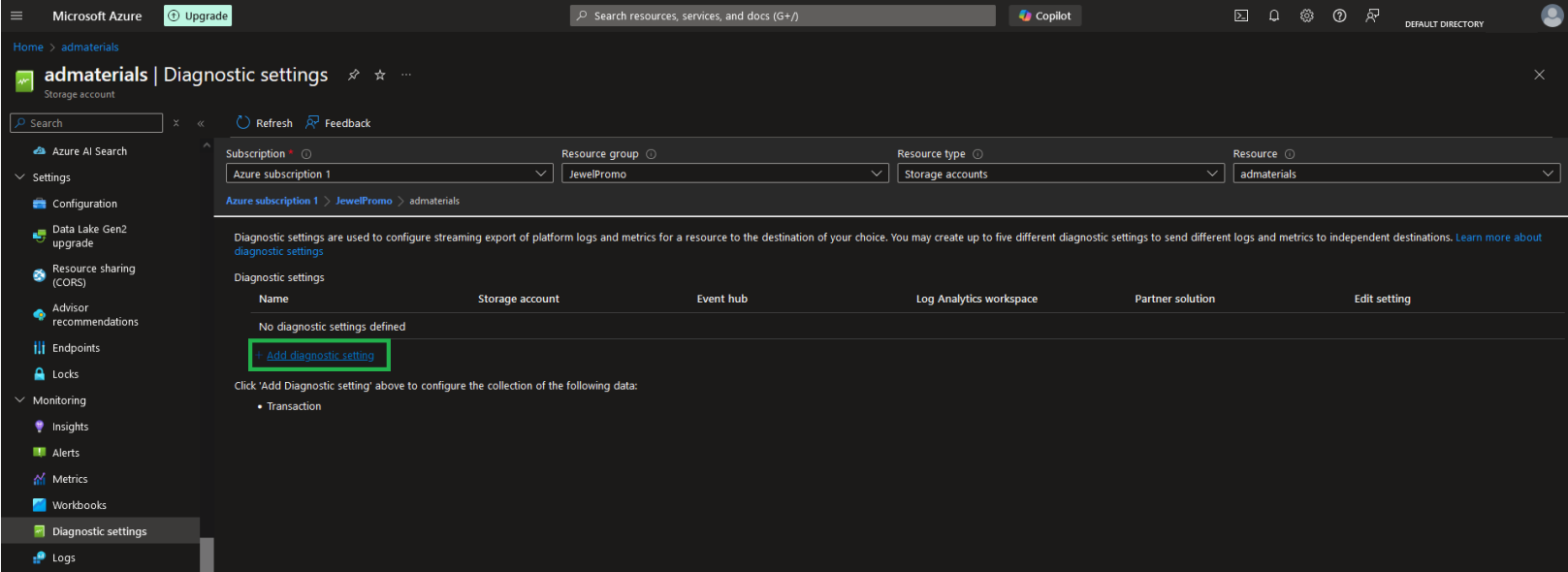
Azure subscription 1 > JewelPromo > admaterials

Select any of the resources to view diagnostic settings.

Name	Resource type	Resource group	Diagnostics status
admaterials	Storage account	JewelPromo	☐ Disabled
blob	Storage account	JewelPromo	☐ Disabled
queue	Storage account	JewelPromo	☐ Disabled
table	Storage account	JewelPromo	☐ Disabled
file	Storage account	JewelPromo	☐ Disabled

Diagnostic settings

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.

Microsoft Azure Upgrade Search resources, services, and docs (G+/) Copilot

Home > admaterials | Diagnostic settings >

Diagnostic setting

Save Discard Delete Feedback

A diagnostic setting specifies a list of categories of platform logs and/or metrics that you want to collect from a resource, and one or more destinations that you would stream them to. Normal usage charges for the destination will occur. [Learn more about the different log categories and contents of those logs](#)

A more flexible, faster, and robust way to collect metrics is in preview! Click [here](#) to configure platform metrics collection from microsoft.storage/storageaccounts to storage account, event hubs, and Log Analytics workspace. [Learn more](#)

Diagnostic setting name * AdStorageMonitor ✓

Metrics

☒ Transaction

Destination details

☒ Send to Log Analytics workspace

Subscription

Azure subscription 1

Log Analytics workspace

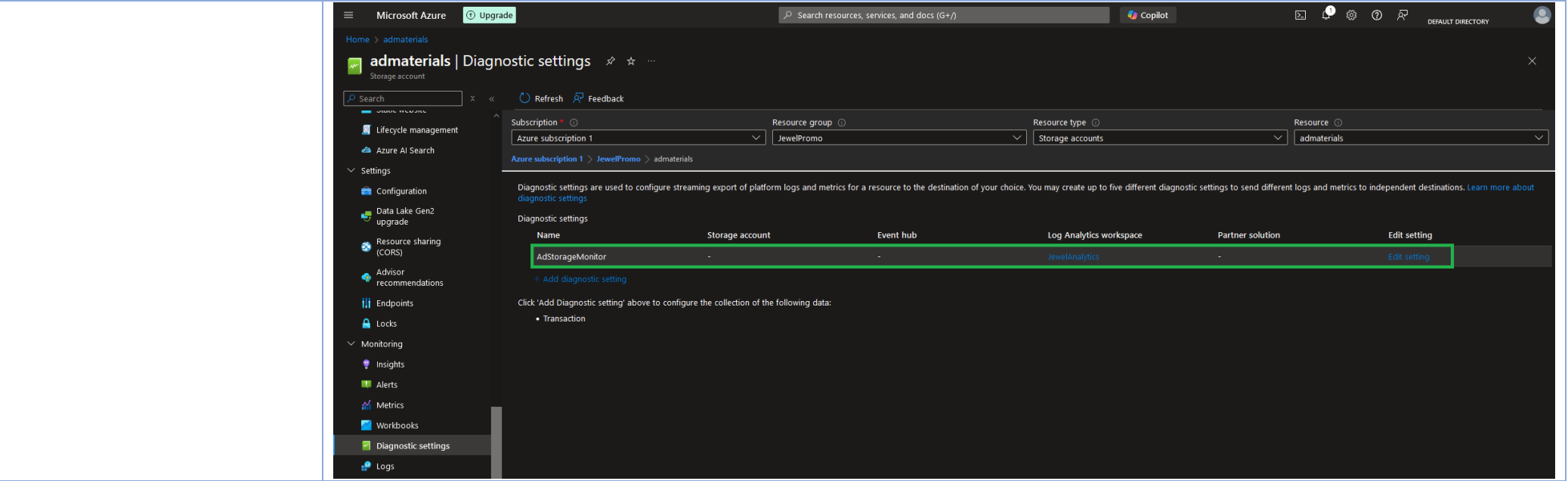
JewelAnalytics (westeurope)

☐ Archive to a storage account

☐ Stream to an event hub

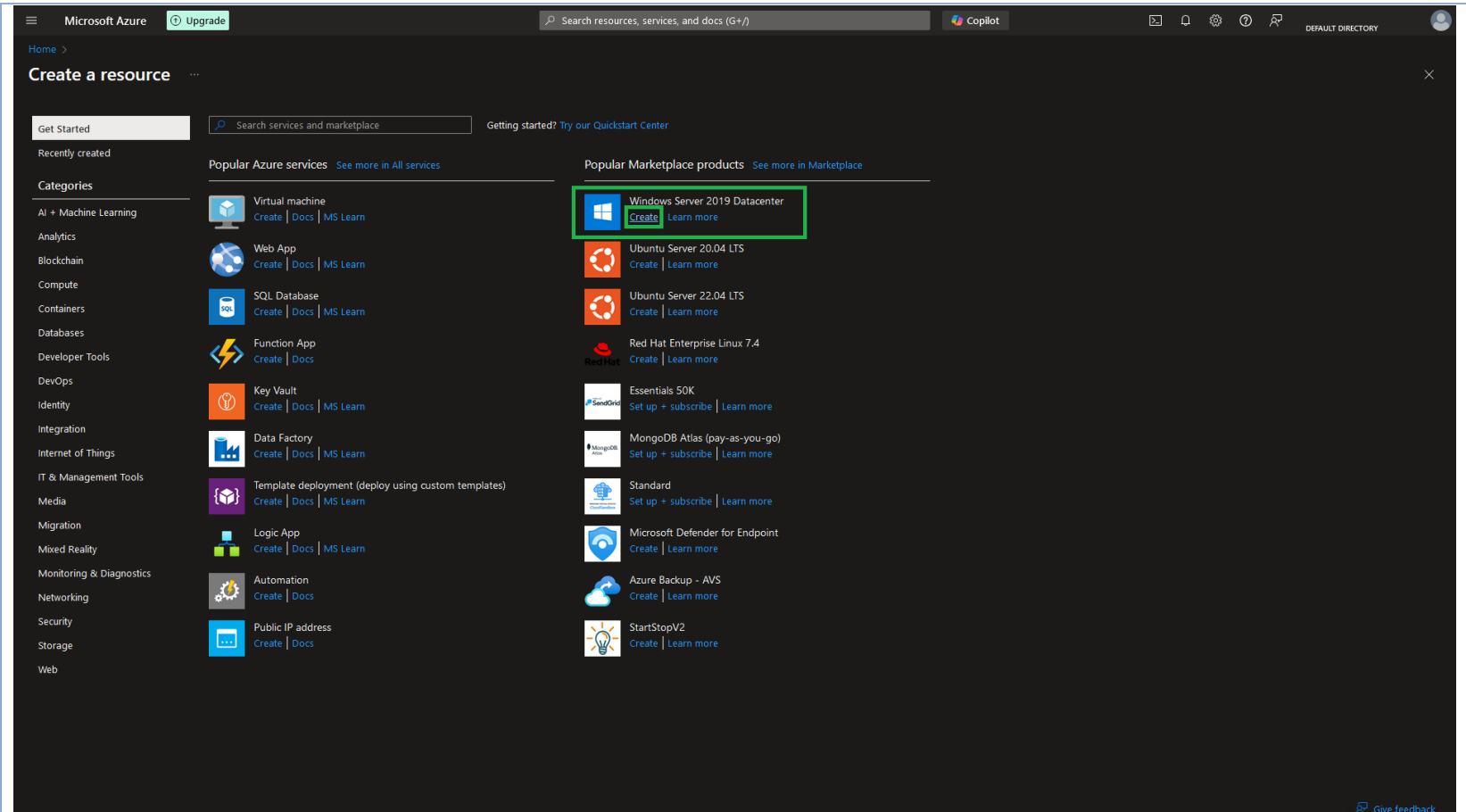
☐ Send to partner solution

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 .

Microsoft Azure Upgrade Search resources, services, and docs (G+/) Copilot

Home > Create a resource >

Create a virtual machine

Help me create a low cost VM Help me create a VM optimized for high availability Help me choose the right VM size for my workload

Basics Disks Networking Management Monitoring Advanced Tags Review + create

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. [Learn more](#)

This subscription may not be eligible to deploy VMs of certain sizes in certain regions.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * Azure subscription 1

Resource group * JewelPromo [Create new](#)

Instance details

Virtual machine name * CampaignVM

Region * (Europe) West Europe

Availability options Availability zone

Zone options

☒ Self-selected zone
Choose up to 3 availability zones, one VM per zone

☐ Azure-selected zone (Preview)
Let Azure assign the best zone for your needs

Availability zone * Zone 1

☒ You can now select multiple zones. Selecting multiple zones will create one VM per zone. [Learn more](#)

Security type * Trusted launch virtual machines [Configure security features](#)

Image * Windows Server 2019 Datacenter - x64 Gen2 [See all images](#) [Configure VM generation](#)

< Previous Next : Disks > Review + create

[Give feedback](#)

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**.

Microsoft Azure Upgrade

Home > Create a resource >

Create a virtual machine

Help me create a low cost VM | Help me create a VM optimized for high availability | Help me choose the right VM size for my workload

x64

Arm64 is not supported with the selected image.

Run with Azure Spot discount ☐

You are in the free trial period. Costs associated with this VM can be covered by any remaining credits on your subscription. [Learn more](#)

Size * See all sizes

Enable Hibernation ☐

Hibernate is not supported by the size that you have selected. Choose a size that is compatible with Hibernation to enable this feature. [Learn more](#)

Administrator account

Username * ✓

Password * ✓

Confirm password * ✓

Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports * ☒ None ☐ Allow selected ports

Select inbound ports

All traffic from the internet will be blocked by default. You will be able to change inbound port rules in the VM > Networking page.

< Previous | **Next : Disks >** | Review + create

Give feedback

- On the **Disks** tab, we retain the default settings, and select **Next: Networking**.
- 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 .

Microsoft Azure Upgrade

Home > Create a resource >

Create a virtual machine

Help me create a low cost VM | Help me create a VM optimized for high availability | Help me choose the right VM size for my workload

Basics | Disks | **Networking** | Management | Monitoring | Advanced | Tags | Review + create

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution. [Learn more](#)

Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network * (new) CampaignVM-vnet [Create new](#)

Subnet * (new) default (10.0.0.0/24)

Public IP (new) CampaignVM-ip [Create new](#)

NIC network security group ☐ None ☒ Basic ☐ Advanced

Public inbound ports * ☒ None ☐ Allow selected ports

Select inbound ports Select one or more ports

All traffic from the internet will be blocked by default. You will be able to change inbound port rules in the VM > Networking page.

Delete public IP and NIC when VM is deleted ☐

Enable accelerated networking ☐

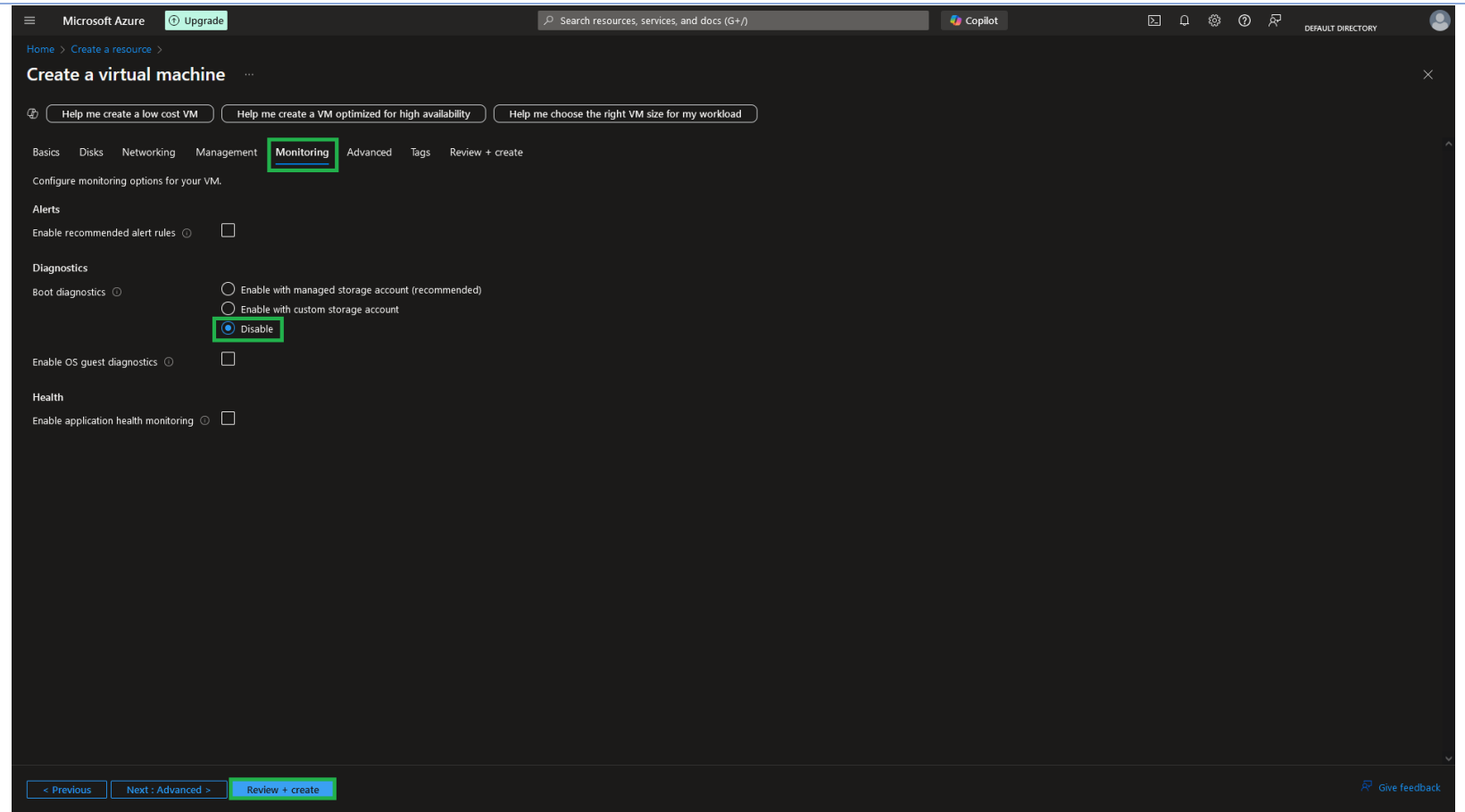
The resource provider "Microsoft.Network" should be registered in order to enable accelerated networking. [Learn more](#)

Next: Management >

< Previous | **Next: Management >** | Review + create

[Give feedback](#)

- On the **Management** tab, we also retain the default settings, and select **Next: Monitoring**.
- 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.

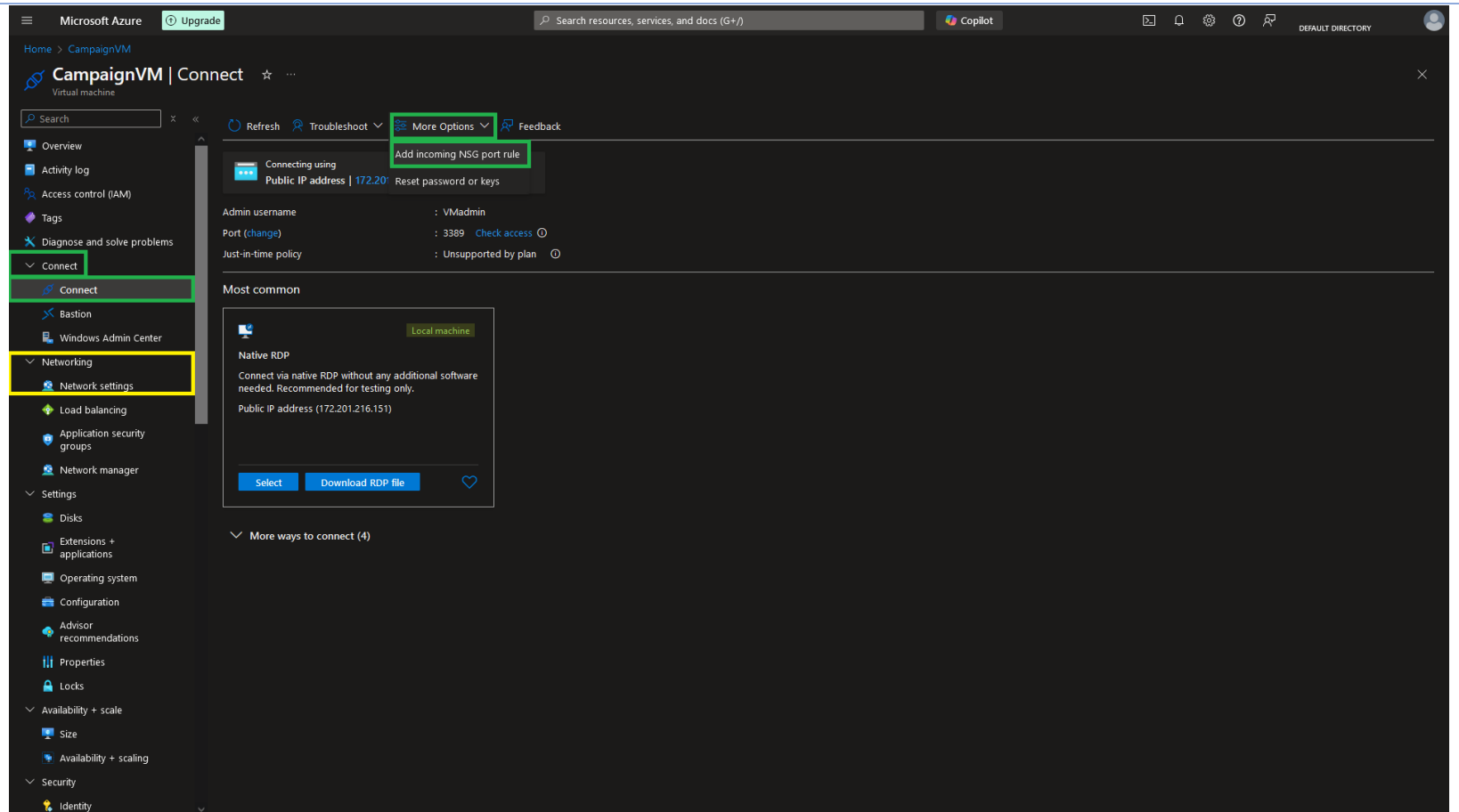
Note: At this point we cannot connect to the VM because the RDP port is blocked. We first need to allow RDP traffic with an **inbound network security group rule for port 3389**.

The screenshot shows the Microsoft Azure portal interface for a virtual machine named 'CampaignVM'. The 'Connect' button in the top toolbar is highlighted with a green box. The left sidebar shows the 'Networking' blade selected. The main content area displays the 'Essentials' and 'Properties' tabs, with the 'Properties' tab showing details for the virtual machine, including its name, operating system, and network settings.

Section	Property	Value	
Essentials	Resource group	JewelPromo	
	Status	Running	
	Location	West Europe (Zone 1)	
	Subscription	Azure subscription 1	
	Subscription ID	1c231d77-b506-4287-925c-aba83bffa6fb	
	Availability zone	1	
	Operating system	Windows (Windows Server 2019 Datacenter)	
	Size	Standard B1s (1 vcpu, 1 GiB memory)	
	Public IP address	172.201.216.151	
	Virtual network/subnet	CampaignVM-vnet/default	
Properties	Computer name	CampaignVM	
	Operating system	Windows (Windows Server 2019 Datacenter)	
	VM generation	V2	
	VM architecture	x64	
	Agent status	Ready	
	Agent version	2.7.41491.1139	
	Hibernation	Disabled	
	Host group	-	
	Host	-	
	Proximity placement group	-	
Networking	Public IP address	172.201.216.151 (Network interface campaignvm984_21)	
	Public IP address (IPv6)	-	
	Private IP address	10.0.0.4	
	Private IP address (IPv6)	-	
	Virtual network/subnet	CampaignVM-vnet/default	
	DNS name	Configure	
	Size	Size	Standard B1s
		vCPUs	1
		RAM	1 GiB
	Source image details	Source image publisher	MicrosoftWindowsServer
Source image offer		WindowsServer	
Source image plan		2019-datacenter-gensecond	
Disk	OS disk	CampaignVM_OsDisk_1_c9ba37df9eb34d6fb4cea29203fcd1	
	Encryption at host	Disabled	

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.

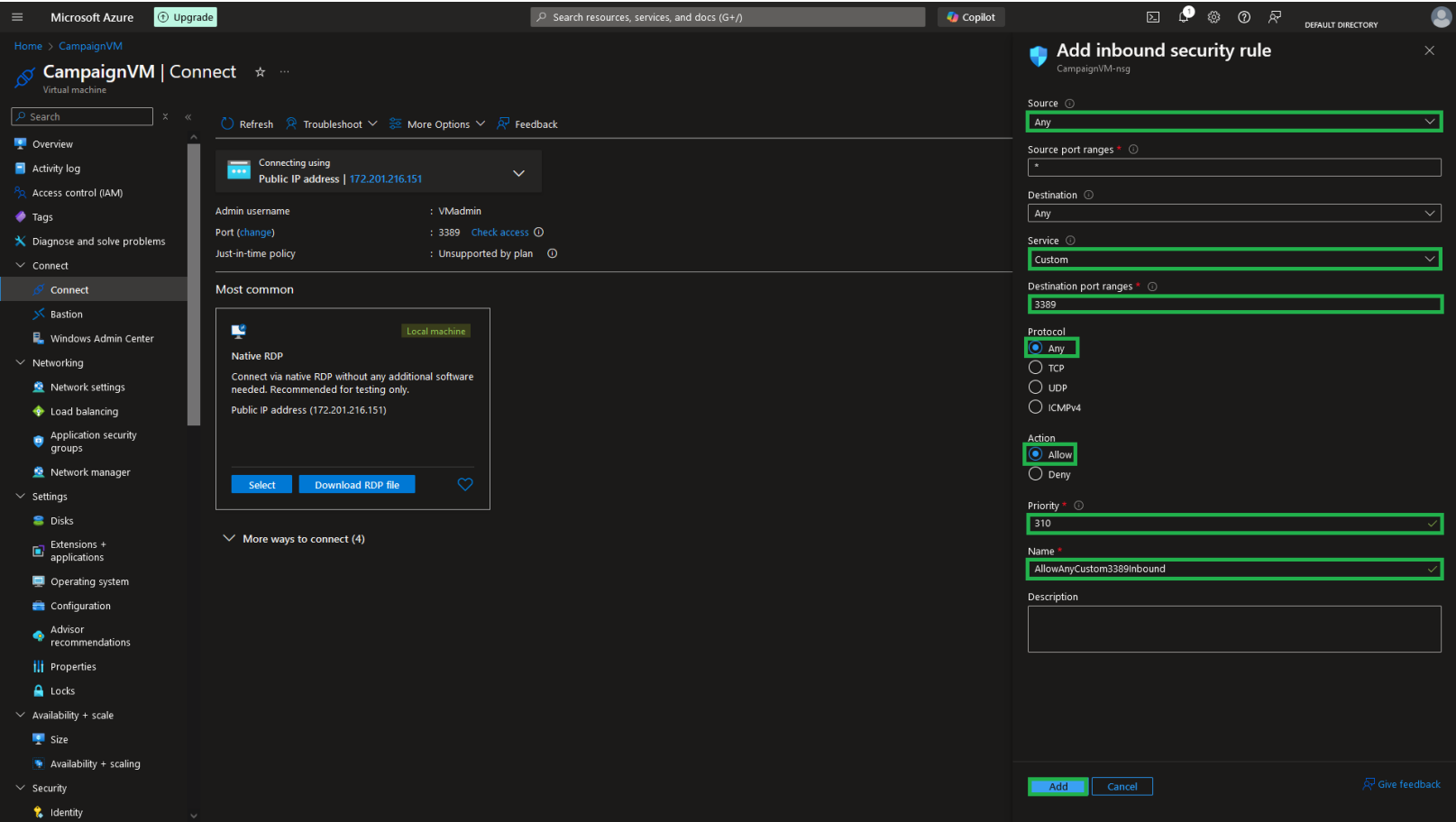


2. In the **Add inbound security rule** wizard, specify the following information and click on **Add**:

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.

Microsoft Azure Upgrade

Search resources, services, and docs (G+)

Copilot

Home > CampaignVM

CampaignVM | Network settings

Virtual machine

Search

This is a new experience. [Please provide feedback](#)

Attach network interface Detach network interface View topology Troubleshoot Refresh Give feedback

Network interface / IP configuration
campaignvm984_z1 (primary) / ipconfig1 (primary)

Essentials

Network interface	: campaignvm984_z1	Load balancers	: 0 (Configure)
Virtual network / subnet	: CampaignVM-vnet / default	Application security groups	: 0 (Configure)
Public IP address	: 172.201.216.151	Network security group	: CampaignVM-nsg
Private IP address	: 10.0.0.4	Accelerated networking	: Disabled
Admin security rules	: 0 (Configure)	Effective security rules	: 0

Rules Collapse all

Network security group CampaignVM-nsg (attached to networkInterface: campaignvm984_z1)
Impacts 0 subnets, 1 network interfaces

Create port rule

Search rules Source == all Destination == all Protocol == all Action == all

Priority ↑	Name	Port	Protocol	Source	Destination	Action
Inbound port rules (4)						
310	AllowAnyCustom3389Inbound	3389	Any	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny
Outbound port rules (3)						

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)

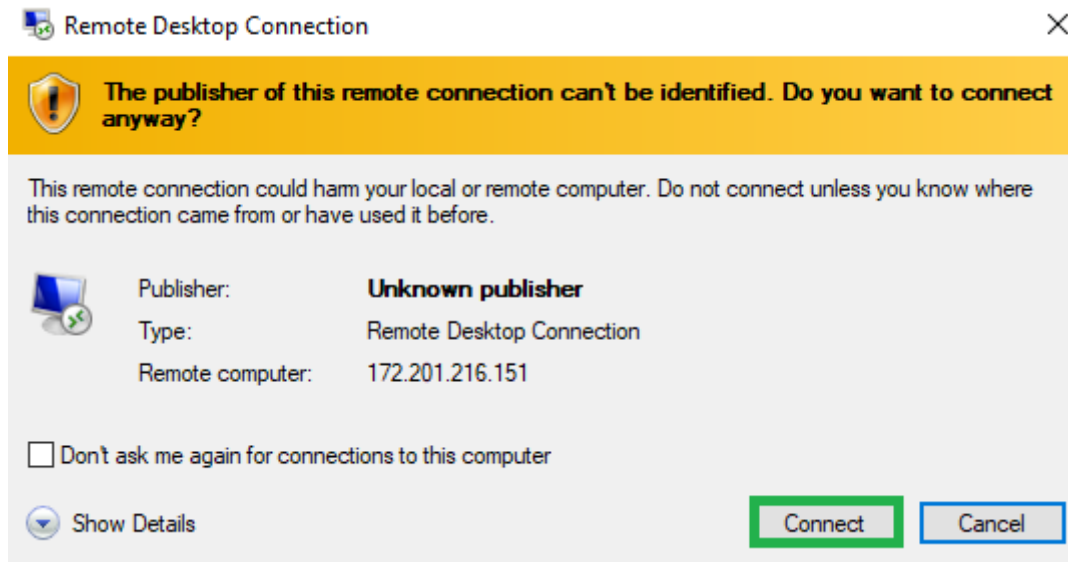
Select

Download RDP file

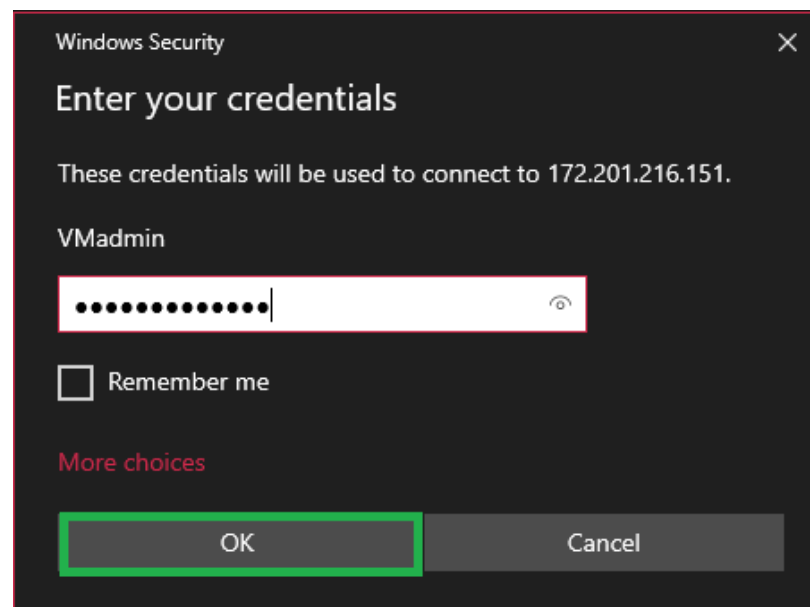


More ways to connect (4)

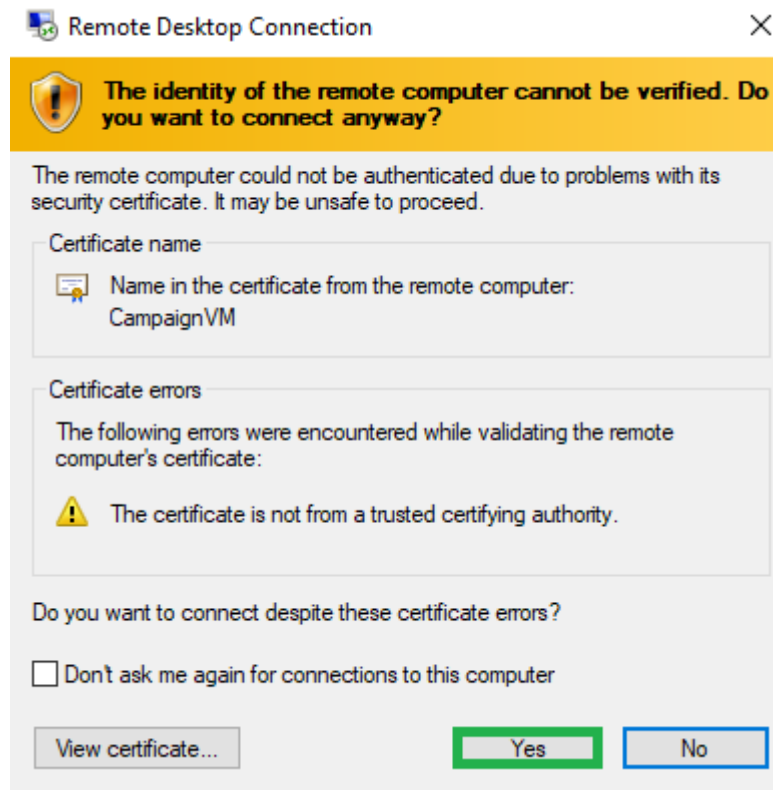
2. When we open the file a **Remote Desktop Connection** pop-up window will appear where we will click on **Connect**.



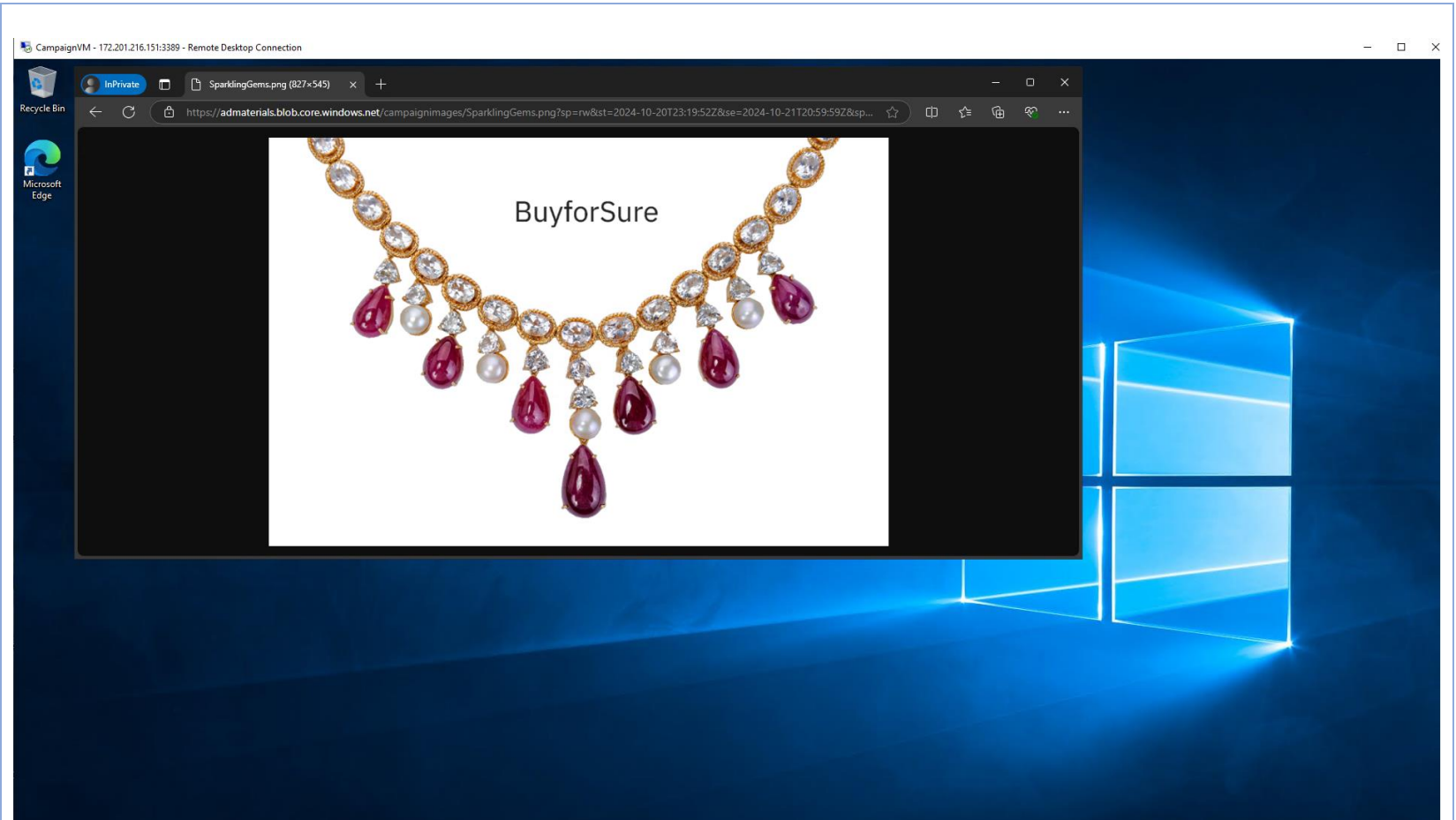
3. Then, on the **Enter your credentials** pop-up window, enter the **Username** and **Password**, and select **OK**.



- 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.



- The virtual machine screen will be displayed.
- 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.

Microsoft Azure

Search resources, services, and docs (G+/I)

Copilot

AlexSmith1@
DEFAULT DIRECTORY

Home >

Virtual machines

Default Directory

+ Create

Switch to classic

Reservations

Manage view

Refresh

Export to CSV

Open query

Assign tags

Start

Restart

Stop

Delete

Services

Maintenance

Filter for any field...

Subscription equals all

Type equals all

Resource group equals all

Location equals all

Add filter

Showing 1 to 1 of 1 records.

No grouping

List view

☐ Name	Subscription	Resource group	Location	Status	Operating system	Size	Public IP address	Disks	
☐ CampaignVM	Azure subscription 1	JewelPromo	West Europe	Running	Windows	Standard_B1s	172.201.216.151	1	...

< Previous

Page 1 of 1

Next >

Give feedback

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

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

Home > Virtual machines >

Virtual machines

Default Directory

+ Create Switch to classic

Filter for any field...

Name

CampaignVM

CampaignVM

Virtual machine

Search

Connect

Connect via Bastion

Start Restart Stop Hibernate Capture Delete Refresh Open in mobile Feedback CLI / PS

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Connect

Networking

Settings

Availability + scale

Security

Backup + disaster recovery

Operations

Monitoring

Automation

Help

Resource group (move): [JewelPromo](#)

Status: Running

Location: West Europe (Zone 1)

Subscription (move): [Azure subscription 1](#)

Subscription ID: 1c231d77-b506-4287-925c-aba83bffa6fb

Availability zone: 1

Tags (edit): [Add tags](#)

Operating system: Windows (Windows Server 2019 Datacenter)

Size: Standard B1s (1 vcpu, 1 GiB memory)

Public IP address: [172.201.216.151](#)

Virtual network/subnet: [CampaignVM-vnet/default](#)

DNS name: [Not configured](#)

Health state: -

Time created: 21/10/2024, 14:27 UTC

JSON View

Properties

Monitoring Capabilities (8) Recommendations Tutorials

Virtual machine

Computer name	CampaignVM
Operating system	Windows (Windows Server 2019 Datacenter)
VM generation	V2
VM architecture	x64
Agent status	Ready
Agent version	2.7.41491.1139
Hibernation	Disabled
Host group	-
Host	-
Proximity placement group	-
Colocation status	N/A
Capacity reservation group	-
Disk controller type	SCSI

Azure Spot

Azure Spot	-
Azure Spot eviction policy	-

Availability + scaling

Availability zone (edit)	1
--------------------------	---

Networking

Public IP address	172.201.216.151 (Network interface campaignvm984_x1)
Public IP address (IPv6)	-
Private IP address	10.0.0.4
Private IP address (IPv6)	-
Virtual network/subnet	CampaignVM-vnet/default
DNS name	Configure

Size

Size	Standard B1s
vCPUs	1
RAM	1 GiB

Source image details

Source image publisher	MicrosoftWindowsServer
Source image offer	WindowsServer
Source image plan	2019-datacenter-gensecond

Disk

OS disk	CampaignVM_OsDisk_1_c9ba37df9eb34d6fbb4cea29203fc1d1
Encryption at host	Disabled

Page 1 of 1

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

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

AlexSmith1@
DEFAULT DIRECTORY

Home > Virtual machines > CampaignVM

Virtual machines

Default Directory

+ Create ▾ Switch to classic ⋮

Filter for any field...

Name ↑

CampaignVM ⋮

CampaignVM | Connect

Virtual machine

Search

Refresh Troubleshoot ▾ More Options ▾ Feedback

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Connect
- Connect
- Bastion
- Windows Admin Center
- Networking
- Settings
- Availability + scale
- Security
- Backup + disaster recovery
- Operations
- Monitoring
- Automation
- Help

Connecting using
Public IP address | 172.201.216.151 ▾

Admin username : VMAdmin
Port (change) : 3389 [Check access](#) ⓘ
Just-in-time policy : Not configured for port 3389 [Configure for this port](#)

Most common

Local machine

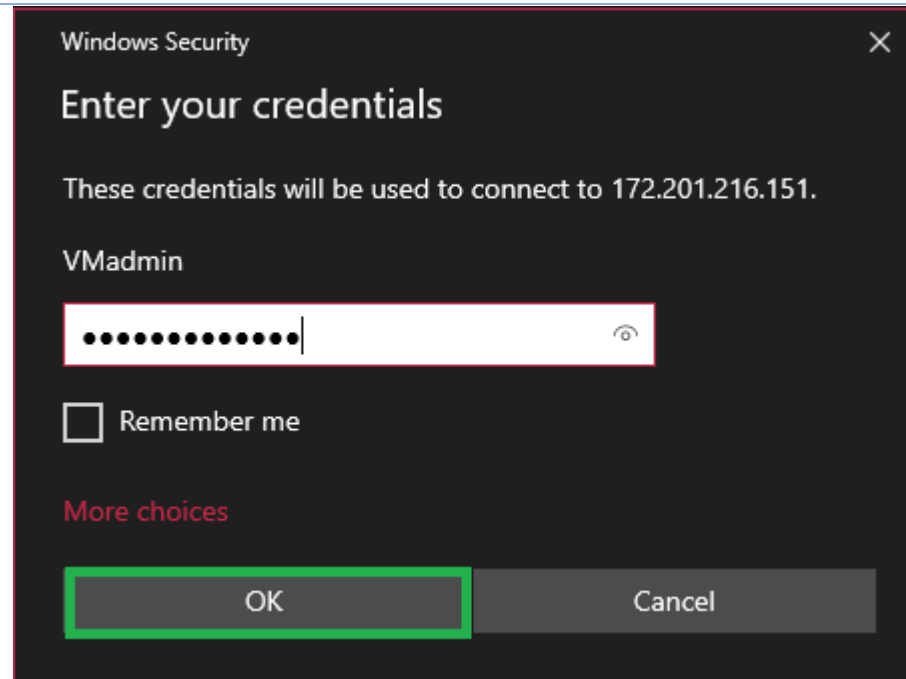
Native RDP
Connect via native RDP without any additional software needed. Recommended for testing only.
Public IP address (172.201.216.151)

Select Download RDP file

More ways to connect (4)

< Page 1 of 1 >

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.

