

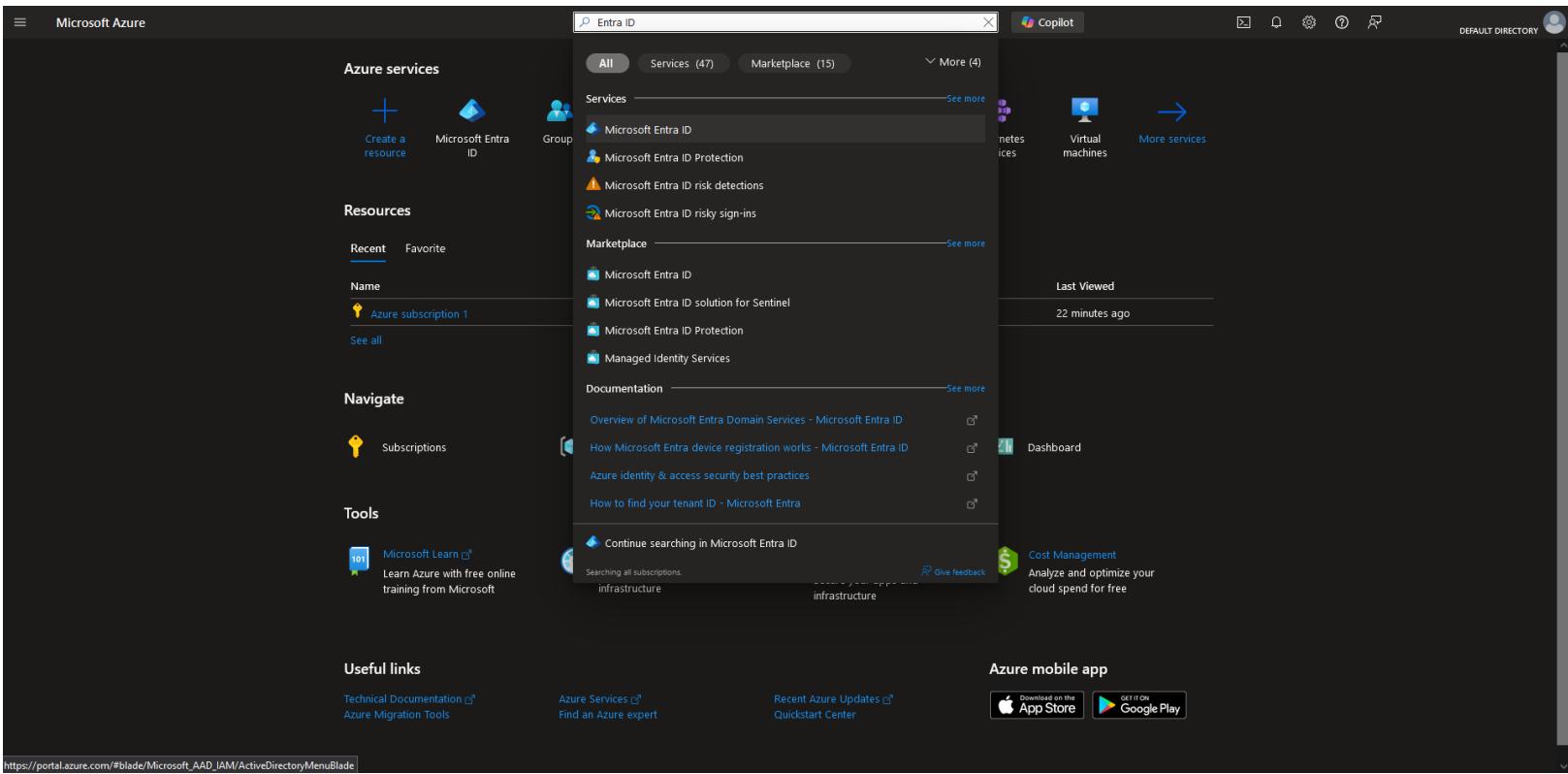
# Azure Security Capstone Project

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
<p><b>Activity 1:</b> Creating three users in Azure Active Directory (Azure AD).</p>	<p>1. After signing in to the Azure Portal, we type in “Microsoft Entra ID” (formerly, Azure Active Directory) into the search box.</p>  <p>The screenshot shows the Microsoft Azure portal interface with a dark theme. In the top right corner, there is a search bar containing the text "Entra ID". Below the search bar, there are three tabs: "All", "Services (47)", and "Marketplace (15)". The "Services" tab is selected. Under the "Services" section, "Microsoft Entra ID" is listed first. Other items include "Microsoft Entra ID Protection", "Microsoft Entra ID risk detections", and "Microsoft Entra ID risky sign-ins". To the right of the search results, there are links for "Virtual machines" and "More services". The left sidebar contains sections for "Azure services", "Resources", "Navigate", "Tools", and "Useful links". The "Resources" section shows a recent item: "Azure subscription 1". The "Tools" section includes "Microsoft Learn". The "Useful links" section has links to "Technical Documentation", "Azure Migration Tools", "Azure Services", "Find an Azure expert", "Recent Azure Updates", and "Quickstart Center". At the bottom of the page, there is a link to the URL "https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade".</p> <p>2. On the Default Directory page, select Users under the Manage blade.</p>

The screenshot shows the Microsoft Azure portal's 'Default Directory | Overview' page. The left sidebar has 'Users' selected. The main area displays basic information about the tenant, including its name, tenant ID, primary domain, license, and device counts. It also features two warning cards: one about service changes to Microsoft Entra Connect and another about migrating authentication methods. A 'My feed' section includes links to the Microsoft Entra admin center and a global administrator profile. A 'Secure Score for Identity' card shows an N/A score.

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

A screenshot of the Microsoft Azure portal interface. The top navigation bar shows 'Microsoft Azure' and a search bar. Below it, the 'Default Directory | Users' section is visible. On the left, a sidebar menu includes 'All users', 'Audit logs', 'Sign-in logs', 'Diagnose and solve problems', 'Deleted users', 'Password reset', 'User settings', 'Bulk operation results', and 'New support request'. The main area shows a table with one row of data: User principal name (t1), User type (Member), On-premises s... (No), Identities (MicrosoftAccount), Company name (empty), and Creation type (empty). A context menu is open over the first row, with the 'Create new user' option highlighted by a green box. The URL in the address bar is 'https://portal.azure.com/#blade/Microsoft\_AAD\_IAM/UsersBlade/CreateNewUser'.

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, <b>AlexSmith1</b> , and select a domain from the dropdown list beside the @ symbol.
Mail nickname	Tick the <b>Derive from user principal name</b> checkbox.
Display name	Enter the user's name, <b>AlexSmith</b> .
Password	Tick the <b>Auto-generate password</b> checkbox.
Account enabled	Tick the <b>Account enabled</b> checkbox.

Microsoft Azure

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

Copilot

DEFAULT DIRECTORY

Create new user ...

Create a new internal user in your organization. This user will have a user name like alice@contoso.com. Learn more

Basics Properties Assignments Review + create

User principal name \* AlexSmith1 @ outlook.onmicrosoft.com

Mail nickname \* AlexSmith1

Display name \* AlexSmith

Password \* ······

Account enabled

Derive from user principal name

Auto-generate password

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**

The screenshot shows the Microsoft Azure portal interface for creating a new user. The top navigation bar includes 'Microsoft Azure', 'Search resources, services, and docs (G+)', 'Copilot', and account settings. The main title is 'Create new user' with a subtitle 'Create a new internal user in your organization'. Below the title are four tabs: 'Basics', 'Properties', 'Assignments', and 'Review + create' (which is underlined, indicating it's the active step). The 'Basics' section contains the following fields:

User principal name	AlexSmith1@
Display name	AlexSmith
Mail nickname	AlexSmith1
Password	[REDACTED]
Account enabled	Yes

The 'Properties' section shows 'User type' as 'Member'. The 'Assignments' section lists 'Administrative units', 'Groups', and 'Roles', all of which are currently empty. At the bottom of the page are three buttons: 'Create' (highlighted in green), '< Previous', and 'Next >'. A 'Give feedback' link is also present.

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

Azure Active Directory is now Microsoft Entra ID.

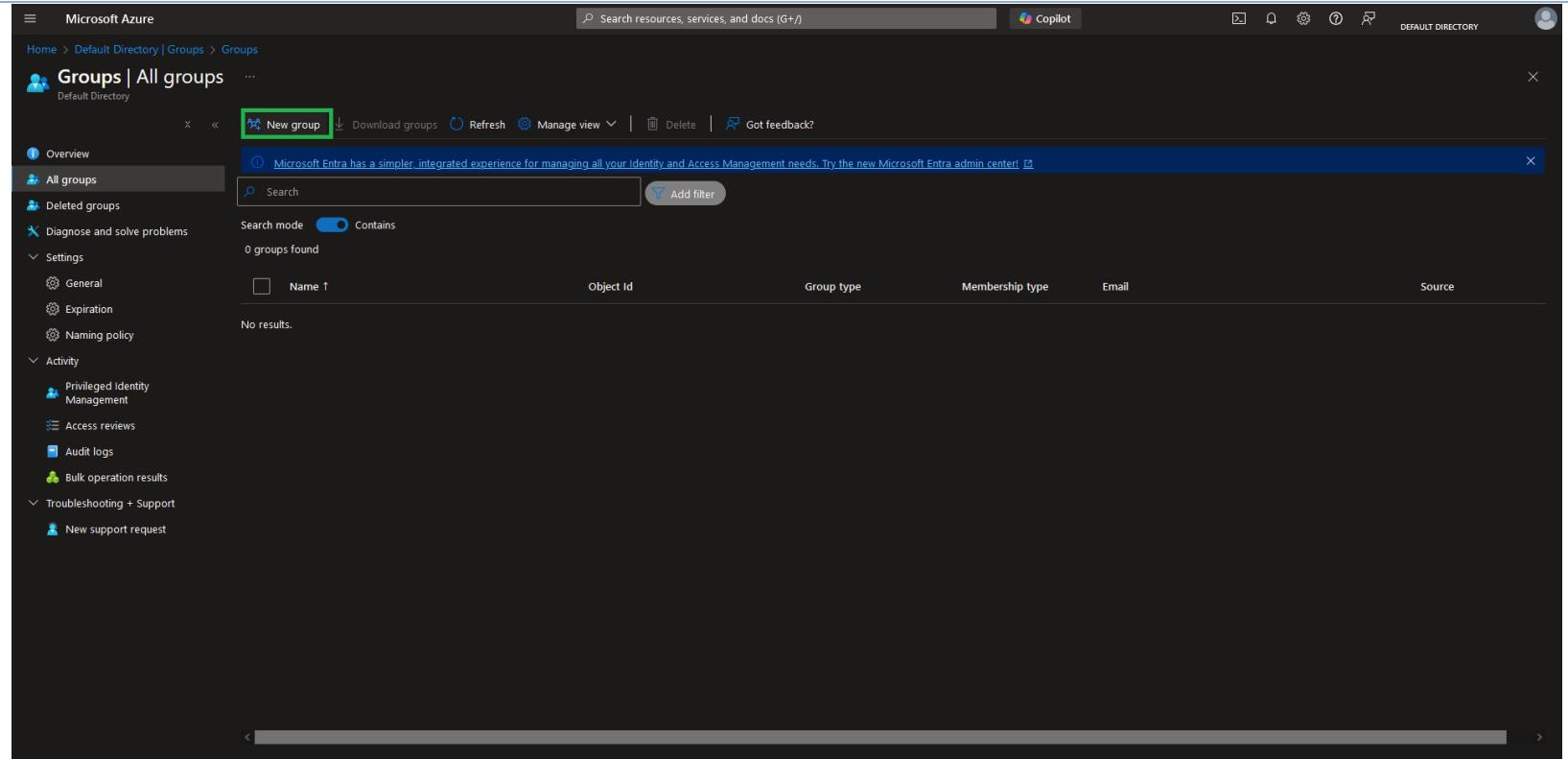
Display name	User principal name	User type	On-premises s...	Identities	Company name	Creation type
AlexSmith	AlexSmith1@...	Member	No			
NishaPatel	NishaPatel3@...	Member	No			
SH		Member	No	MicrosoftAccount		
SofiaLee2	SofiaLee2@...	Member	No			

**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.

The screenshot shows the Microsoft Azure portal's 'Default Directory | Overview' page. The left sidebar has a 'Groups' item highlighted with a green border. The main content area displays basic information about the tenant, including its name ('Default Directory'), users ('4'), and groups ('0'). It also shows the primary domain ('Microsoft.com'), applications ('0'), and devices ('0'). Two warning cards are present: one about service changes to Microsoft Entra Connect and another about migrating to converged authentication methods. The 'My feed' section includes links to the Microsoft Entra admin center, user profile management, and secure score details.

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

A screenshot of the Microsoft Azure portal showing the 'Groups | All groups' page. The 'New group' button is highlighted with a green box. The page includes a sidebar with options like Overview, All groups (which is selected), Deleted groups, Diagnose and solve problems, Settings (General, Expiration, Naming policy), Activity (Privileged Identity Management, Access reviews, Audit logs, Bulk operation results), and Troubleshooting + Support (New support request). The main area shows a search bar, a 'Search mode' toggle set to 'Contains', and a table with columns: Object ID, Group type, Membership type, Email, and Source. A message at the top right says 'Microsoft Entra has a simpler, integrated experience for managing all your Identity and Access Management needs. Try the new Microsoft Entra admin center.'

New group

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

Search resources, services, and docs (G+)

Copilot

DEFAULT DIRECTORY

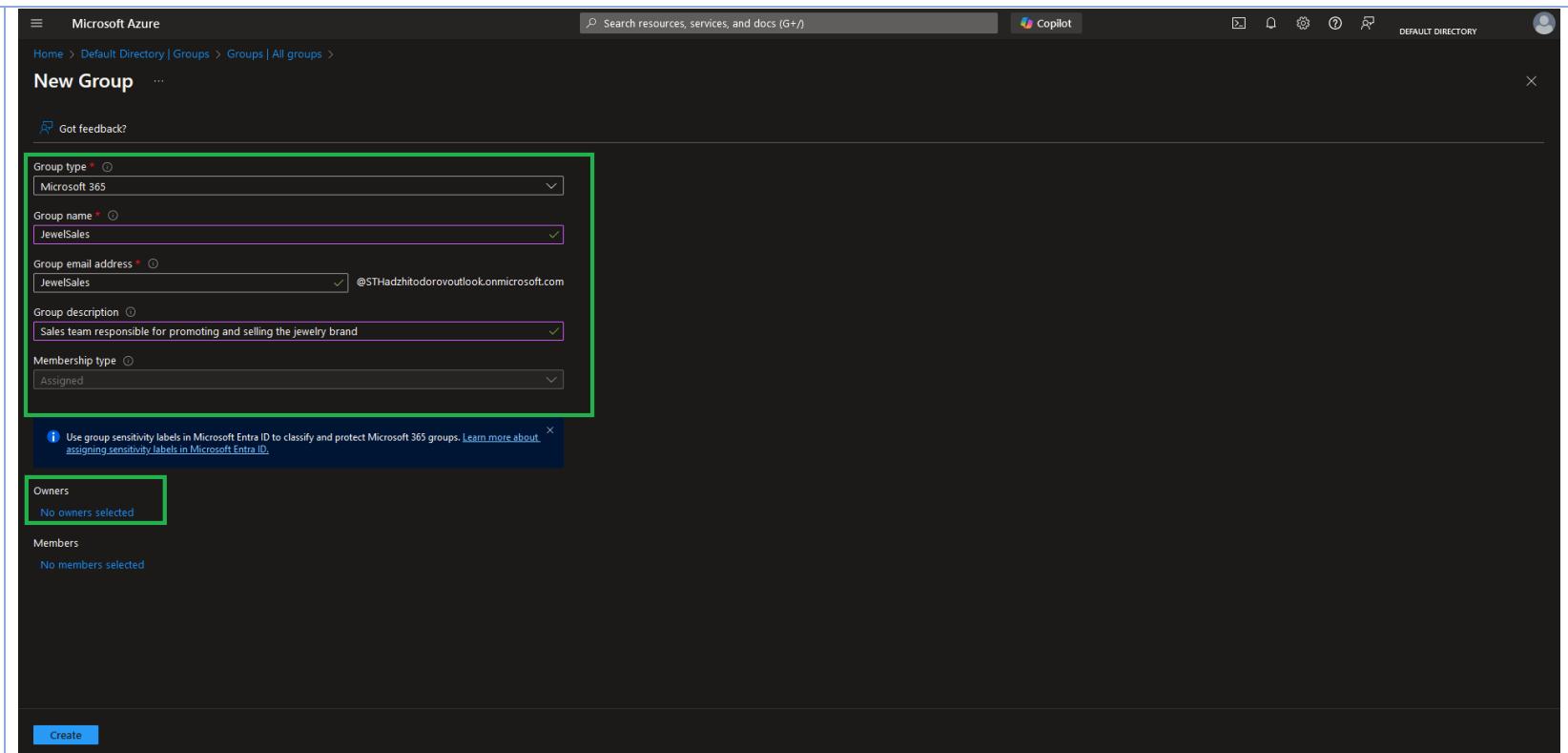
Microsoft Entra has a simpler, integrated experience for managing all your Identity and Access Management needs. Try the new Microsoft Entra admin center.

No results.

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

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

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



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

## Add owners

X

ⓘ Try changing or adding filters if you don't see what you're looking for.

Search ⓘ



4 results found

All Users

	Name	Type	Details
<input type="checkbox"/>	AlexSmith	User	AlexSmith1@
<input type="checkbox"/>	NishaPatel	User	NishaPatel3@
<input checked="" type="checkbox"/>	User		
<input type="checkbox"/>	SofiaLee	User	SofiaLee2@

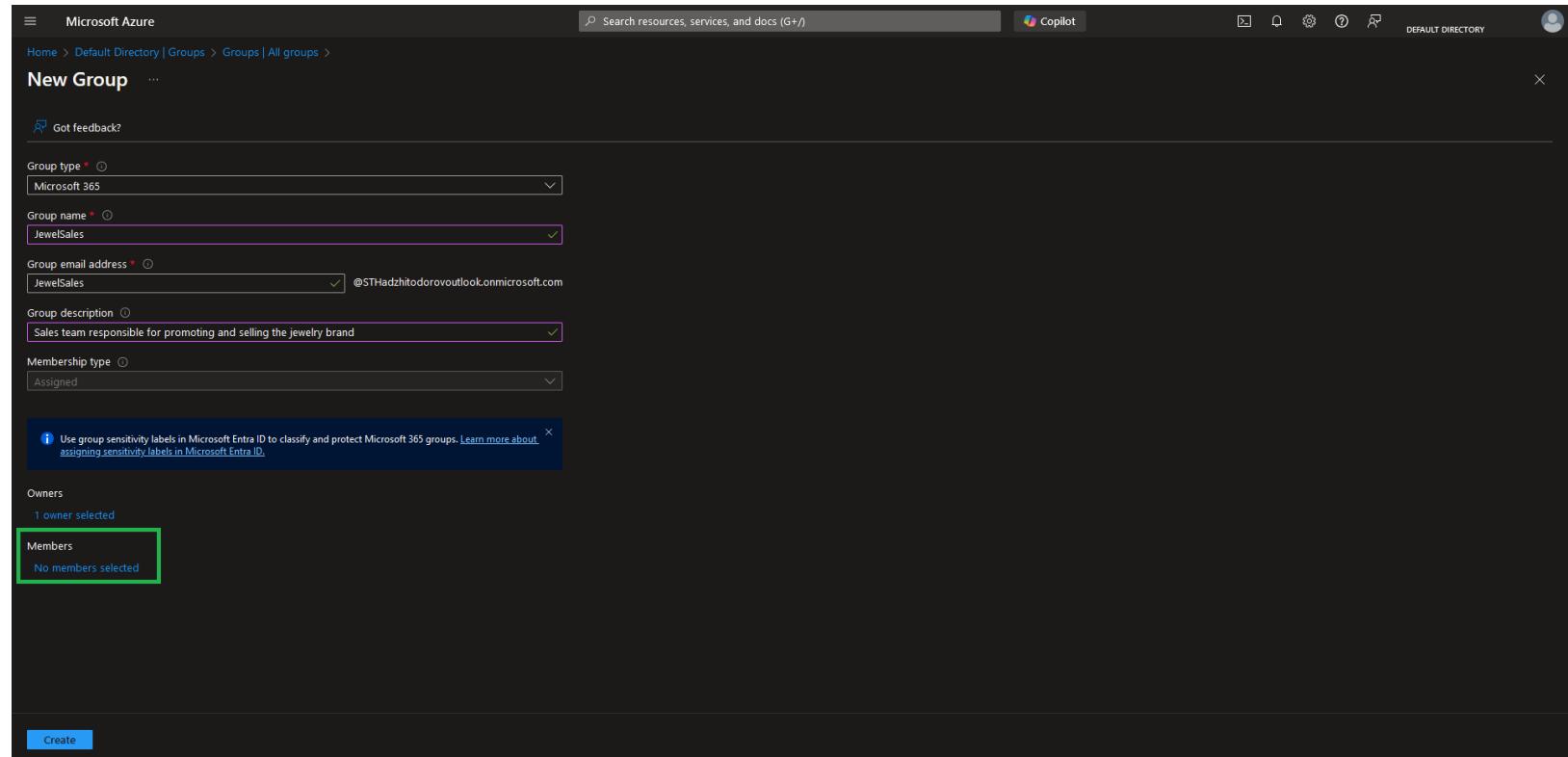
Owners (1)

⟲ Reset



Select

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



The screenshot shows the 'New Group' page in Microsoft Azure. The 'Group type' is set to 'Microsoft 365'. The 'Group name' is 'JewelSales'. The 'Group email address' is 'JewelSales' followed by a placeholder '@STHadzhitodorovoutlook.onmicrosoft.com'. The 'Group description' is 'Sales team responsible for promoting and selling the jewelry brand'. The 'Membership type' is 'Assigned'. A tooltip at the bottom left of the page says: '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.' In the 'Members' section, it says 'No members selected'. The 'Create' button is at the bottom.

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

## Add members

X

Try changing or adding filters if you don't see what you're looking for.

Search ⓘ



4 results found

All Users

	Name	Type	Details
<input checked="" type="checkbox"/>	AlexSmith	User	AlexSmith1@
<input checked="" type="checkbox"/>	NishaPatel	User	NishaPatel3@
<input type="checkbox"/>		User	
<input checked="" type="checkbox"/>	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

Home > Default Directory | Groups > Groups

Groups | All groups

New group Download groups Refresh Manage view Delete Got feedback?

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

Search mode Contains

Search Add filter

1 group found

	Name ↑	Object Id	Group type	Membership type	Email	Source
<input type="checkbox"/>	JewelSales	7651f958-a91e-489c-b6cb-52170893d78d	Microsoft 365	Assigned	JewelSales@	Cloud

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

The screenshot shows the Microsoft Azure portal interface. The user is navigating through the 'Groups' section under the 'Default Directory'. The left sidebar contains navigation links for Overview, All groups (which is selected and highlighted in grey), Deleted groups, Diagnose and solve problems, Settings (General, Expiration, Naming policy), Activity (Privileged Identity Management, Access reviews, Audit logs, Bulk operation results), and Troubleshooting + Support (New support request). The main content area displays a table of groups. A single group, 'JewelSales', is listed. The table columns include Name, Object Id, Group type, Membership type, Email, and Source. The 'Name' column is sorted in ascending order. The 'JewelSales' row is highlighted with a green border around the 'Name' cell. A tooltip message at the top right encourages switching to the Microsoft Entra admin center. The bottom of the page features a navigation bar with icons for Home, Groups, Subscriptions, Storage, Functions, and more, along with a search bar and a Copilot button.

The screenshot shows the Microsoft Azure portal interface. At the top, there is a navigation bar with the text "Microsoft Azure" and "Upgrade". A search bar is located next to it with the placeholder "Search resources, services, and docs (G+)" and a Copilot icon. On the far right of the top bar are icons for a profile picture, DEFAULT DIRECTORY, and other account settings.

The main content area is titled "Azure services" and features a grid of service icons. The "Subscriptions" icon, which is a key inside a square, is highlighted with a green border. Other visible icons include "Create a resource", "Microsoft Entra ID", "Cost Management ...", "Groups", "Quickstart Center", "Azure AI services", "Kubernetes services", and "Virtual machines". There is also a "More services" button.

Below the service icons is a section titled "Resources" with tabs for "Recent" and "Favorite". Under "Recent", there is a table with one item: "Azure subscription 1" (Subscription type) last viewed 6 minutes ago. A "See all" link is also present.

The central part of the screen is a detailed view of the "Subscriptions" blade. It has a title "Subscriptions" with a "View" button. Below the title is a "Description" section stating: "Subscriptions serve as the foundational access and billing mechanism for Azure, offering flexibility and control over cloud resources." It also includes links for "Free training from Microsoft" (Learn Azure with free online training from Microsoft), "Create an Azure account" (7 units · 39 min), and "Useful links" (Overview, Get started, Pricing).

On the right side of the blade, there are links to "All resources", "Dashboard", "Microsoft Defender for Cloud", "Cost Management" (with a "Secure your apps and infrastructure" sub-link), and "Azure mobile app". There are also download links for the "Azure mobile app" on the App Store and Google Play.

At the bottom left of the blade, the URL "https://portal.azure.com/#blade/Microsoft\_Azure\_Billing/SubscriptionsBlade" is displayed. The entire "Subscriptions" blade is also highlighted with a green border.

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

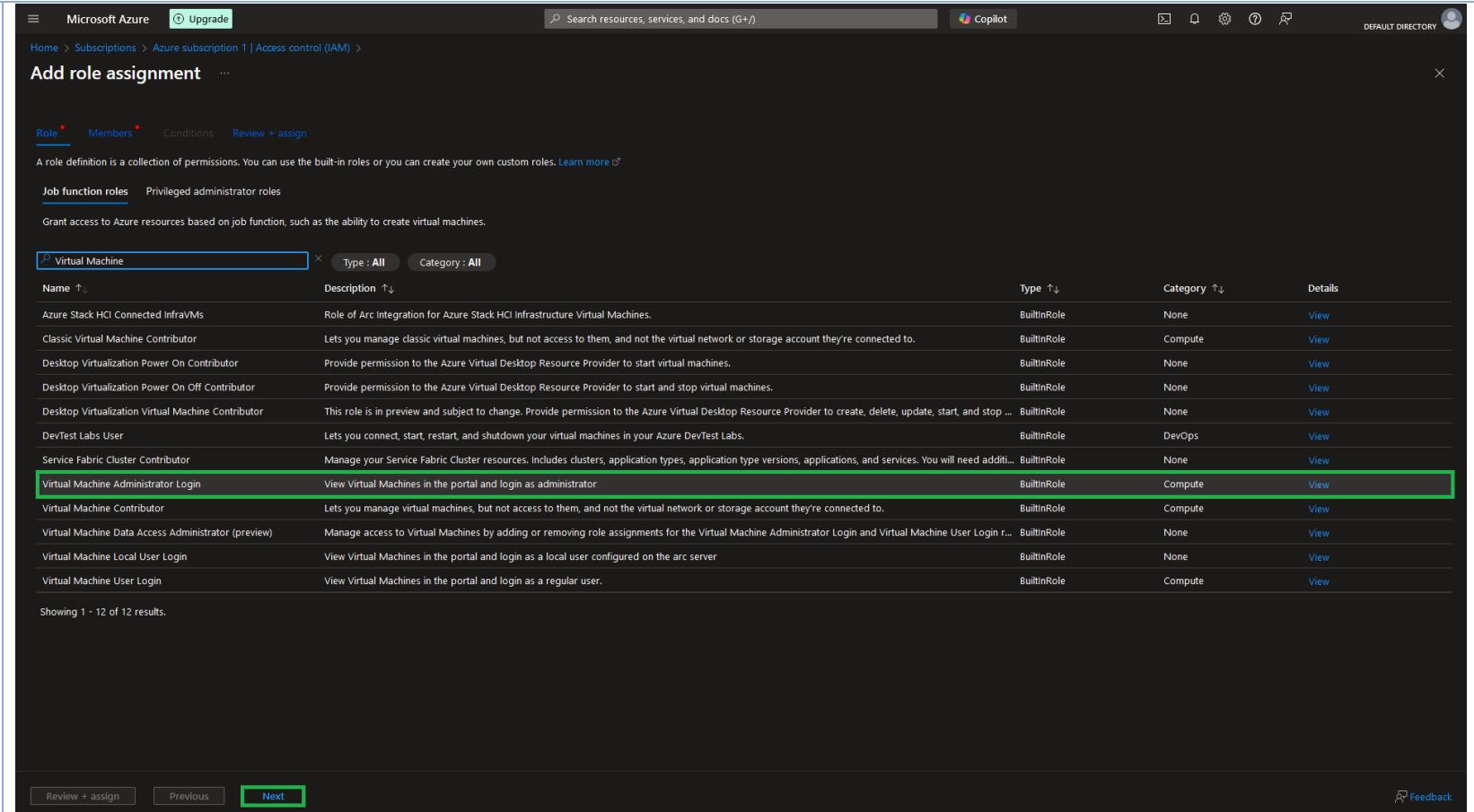
The screenshot shows the Microsoft Azure Subscriptions page. At the top, there is a navigation bar with 'Microsoft Azure' and 'Upgrade' buttons, a search bar 'Search resources, services, and docs (G+)', a Copilot button, and account settings. Below the navigation is a breadcrumb trail 'Home > Subscriptions >'. The main title is 'Subscriptions' with a 'Default Directory' link. Below the title are several buttons: '+ Add', 'Manage Policies', 'View Requests', 'View eligible subscriptions', and 'Export to CSV'. A note says 'Global administrators can manage all subscriptions in this list by updating their policy setting [here](#)'. Another note says '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](#)'. A link 'Switch directories' is also present. Below these are filter buttons: 'Search for any field...', 'Subscriptions : Filtered (1 of 1)', 'My role == all', 'Status == all', and 'Add filter'. The main table has columns: 'Subscription name ↑↓', 'Subscription ID ↑↓', 'My role ↑↓', 'Current cost', 'Secure Score ↑↓', 'Parent management group ↑↓', and 'Status ↑↓'. There is one row in the table: 'Azure subscription 1' (highlighted with a green border), '1c231d77-b506-4287-925c-aba83bfaf6fb', 'Owner', '0', '-', 'Tenant Root Group', and 'Active'. A '...' button is at the end of the table.

Subscription name ↑↓	Subscription ID ↑↓	My role ↑↓	Current cost	Secure Score ↑↓	Parent management group ↑↓	Status ↑↓
Azure subscription 1	1c231d77-b506-4287-925c-aba83bfaf6fb	Owner	0	-	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.

The screenshot shows the Azure Access control (IAM) interface for 'Azure subscription 1'. The left sidebar lists various subscription management options like Overview, Activity log, and Access control (IAM). The main content area is titled 'Azure subscription 1 | Access control (IAM)' and contains sections for 'Check access', 'Role assignments', 'Roles', 'Deny assignments', and 'Classic administrators'. A prominent 'Add role assignment' button is at the top. Below it, a note about retired Co-administrator roles is displayed. The 'My access' section allows viewing access levels. Several cards provide links to 'Grant access to this resource', 'View access to this resource', 'View deny assignments', and 'Create a custom role'. A 'New! Permissions Management' section is also present.

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**.



The screenshot shows the Microsoft Azure 'Add role assignment' interface. At the top, there are tabs for 'Role', 'Members', 'Conditions', and 'Review + assign'. The 'Role' tab is selected. Below the tabs, a search bar says 'Search resources, services, and docs (G+/' and a Copilot button is present. On the right, there are icons for notifications, help, and user profile.

The main content area is titled 'Add role assignment' and shows the 'Job function roles' section. A sub-section titled 'Privileged administrator roles' is shown. A note states: 'Grant access to Azure resources based on job function, such as the ability to create virtual machines.' Below this, a search bar contains 'Virtual Machine' and filters for 'Type : All' and 'Category : All'. A table lists 12 results:

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 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
<b>Virtual Machine Administrator Login</b>	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

At the bottom, it says 'Showing 1 - 12 of 12 results.' and has buttons for 'Review + assign', 'Previous', 'Next', and 'Feedback'.

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

The screenshot shows the Microsoft Azure portal interface for adding a role assignment. The main page displays the 'Add role assignment' wizard with the 'Members' tab selected. The 'Selected role' is set to 'Virtual Machine Administrator Login'. The 'Assign access to' section has 'User, group, or service principal' selected. Below this, a 'Members' section contains a button to 'Select members'. A modal window titled 'Select members' is overlaid, showing a search bar and a list of users and groups. The group 'JewelSales' is listed with a detailed description: 'Sales team responsible for promoting and selling the jewelry brand'. This group is highlighted with a green border, indicating it is selected. Other listed items include AlexSmith, NishaPatel, and SofiaLee. At the bottom of the modal, there is a 'Selected members:' section showing the same 'JewelSales' entry with its description, also highlighted with a green border. The overall interface is dark-themed.

Microsoft Azure Upgrade

Search resources, services, and docs (G+)

Copilot

DEFAULT DIRECTORY

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

No members selected

Description Optional

Review + assign Previous Next

Select Close

Search by name or email address

AlexSmith AlexSmith1@

JewelSales Sales team responsible for promoting and selling the jewelry brand

NishaPatel NishaPatel3@

SofiaLee SofiaLee2@

JewelSales Sales team responsible for promoting and selling the jewelry brand

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

The screenshot shows the Microsoft Azure 'Add role assignment' interface. At the top, there are navigation links for 'Home', 'Azure subscription 1 | Access control (IAM)', and a search bar. On the right, there are icons for Copilot, notifications, and user profile.

The main area is titled 'Add role assignment' with tabs for 'Role', 'Members', 'Conditions', and 'Review + assign'. The 'Members' tab is selected, showing a table with one row:

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

Below the table, there is a 'Description' field labeled 'Optional' and a 'Next' button at the bottom.

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

The screenshot shows the Microsoft Azure portal interface. At the top, there is a navigation bar with the Microsoft Azure logo, an 'Upgrade' button, a search bar containing 'Search resources, services, and docs (G+)', a Copilot icon, and various account and settings icons. The main content area is titled 'Add role assignment' and shows a step-by-step process:

- Role:** Virtual Machine Administrator Login
- Scope:** /subscriptions/1c231d77-b506-4287-925c-aba83bffa6fb
- Members:** A table showing one member: JewelSales (Object ID: 7651f958-a91e-489c-b6cb-52170893d78d, Type: Group).
- Description:** No description.

At the bottom of the page, there are buttons for 'Review + assign' (highlighted in blue), 'Previous', and 'Next'. On the far right, there is a 'Feedback' link.

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

The screenshot shows the Microsoft Azure Access control (IAM) interface for 'Azure subscription 1'. The left sidebar includes links for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Security, Events, Cost Management, Billing, Settings, and various resource-related sections. The main content area displays a summary of role assignments: 'Number of role assignments for this subscription' (7 total, 3 privileged), a search bar, and a table of assignments. The table has columns for Name, Type, Role, Scope, and Condition. One row is highlighted with a green border, showing 'JewelSales' as a Group assigned the 'Virtual Machine Administrator Login' role with 'This resource' scope and 'None' condition.

**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.

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes 'Microsoft Azure', 'Upgrade', 'Search resources, services, and docs (G+)', 'Copilot', and various account and settings icons. The main content area is titled 'Default Directory | Overview'. On the left, a sidebar titled 'Manage' is expanded, showing options like 'Users', 'Groups', 'External Identities', and 'Security' (which is highlighted with a green box). The main content area displays 'Basic information' for the tenant, including:

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

Below this are two service change notifications:

- 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](#)

The 'My feed' section contains three items:

- Try Microsoft Entra admin center**: Secure your identity environment with Microsoft Entra ID, permissions management and more. [Go to Microsoft Entra](#)
- Sibil Hadzhitodorov**: 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](#)

At the bottom of the page, the URL is shown: [https://portal.azure.com/#view/Microsoft\\_AAD\\_IAM/ActiveDirectoryMenuBlade#/Security](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.

The screenshot shows the Microsoft Azure portal's "Security | Getting started" page. The left sidebar has a green box highlighting the "Multifactor authentication" link under the "Manage" section. The main content area has a green box highlighting the "Multifactor authentication" section under "Security guidance".

[https://portal.azure.com/#view/Microsoft\\_AAD\\_IAM/SecurityMenuBlade/~/MultifactorAuthentication](https://portal.azure.com/#view/Microsoft_AAD_IAM/SecurityMenuBlade/~/MultifactorAuthentication)

**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**.

The screenshot shows the 'Multifactor authentication | Getting started' page in the Azure portal. The left sidebar has a red box around the 'Getting started' link under 'Diagnose and solve problems'. The main content area has a red box around the 'Configure Additional cloud-based multifactor authentication settings' section. The URL in the browser is: Home > Default Directory | Security > Security | Multifactor authentication > Multifactor authentication | Getting started

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:

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**.

The screenshot shows the Azure Active Directory Users page. On the left, there's a sidebar with links like 'Audit logs', 'Sign-in logs', 'Diagnose and solve problems', 'Deleted users', 'Password reset', 'User settings', and 'Bulk operation results'. The 'All users' link is highlighted with a red box. At the top right, there's a 'Per-user MFA' button, also highlighted with a red box. A message at the top says 'Azure Active Directory is becoming Microsoft Entra ID.' The main area displays a table with five users:

	Display name	User principal name	User type	On-premises sync	Identities	Company name	Creation type
<input type="checkbox"/>	AD	AlexSmith@	Member	No			
<input type="checkbox"/>	AL	AlexSmith	Member	No			
<input type="checkbox"/>	AZ		Member	No			
<input type="checkbox"/>	Ni	NishaPatel@	Member	No			
<input type="checkbox"/>	SO	SofiaLee@	Member	No			

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.

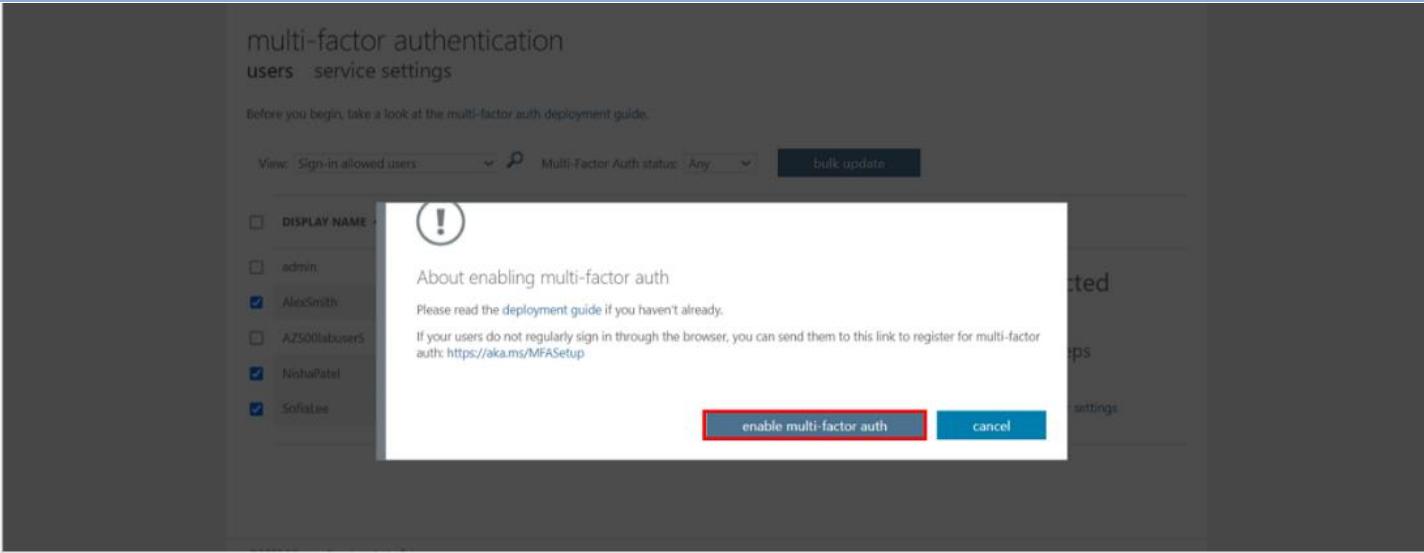
## multi-factor authentication

users service settings

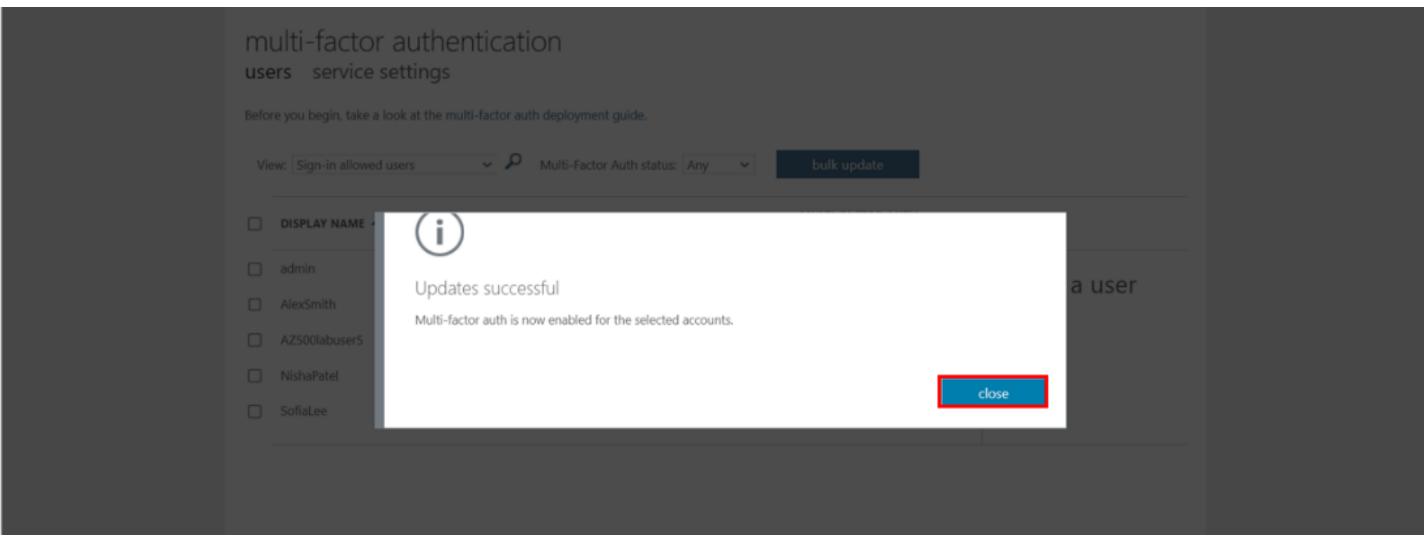
Before you begin, take a look at the [multi-factor auth deployment guide](#).

View:	Sign-in allowed users	Multi-Factor Auth status:	Any	bulk update
<input type="checkbox"/>	DISPLAY NAME	USER NAME	MULTI-FACTOR AUTH STATUS	
<input type="checkbox"/>			Disabled	
<input checked="" type="checkbox"/>	AlexSmith	AlexSmith1@	Disabled	3 selected
<input type="checkbox"/>			Disabled	
<input checked="" type="checkbox"/>	NishaPatel	NishaPatel3@	Disabled	quick steps
<input checked="" type="checkbox"/>	SofiaLee	SofiaLee2@	Disabled	<a href="#">Enable</a>

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

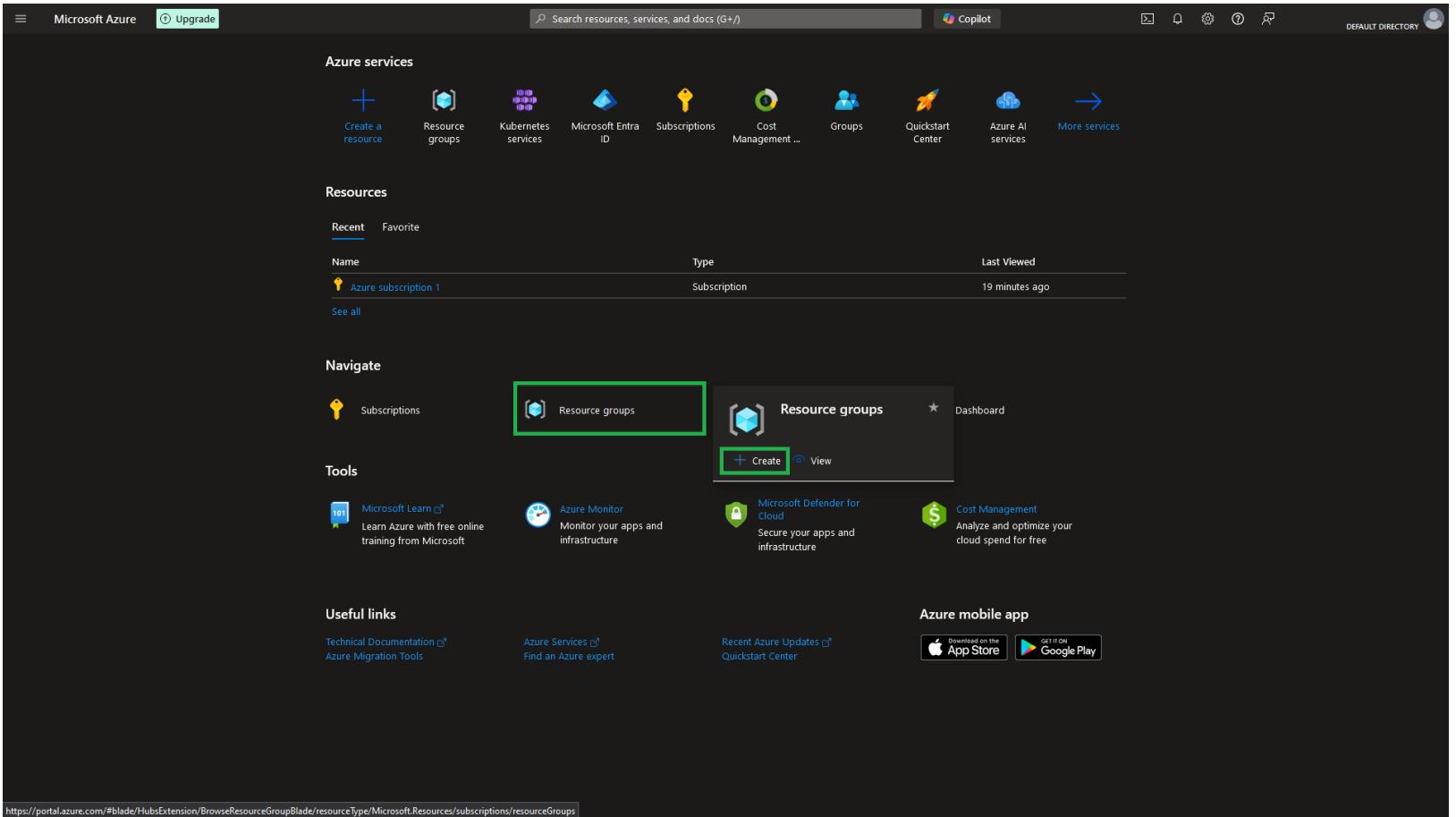
## multi-factor authentication

users service settings

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

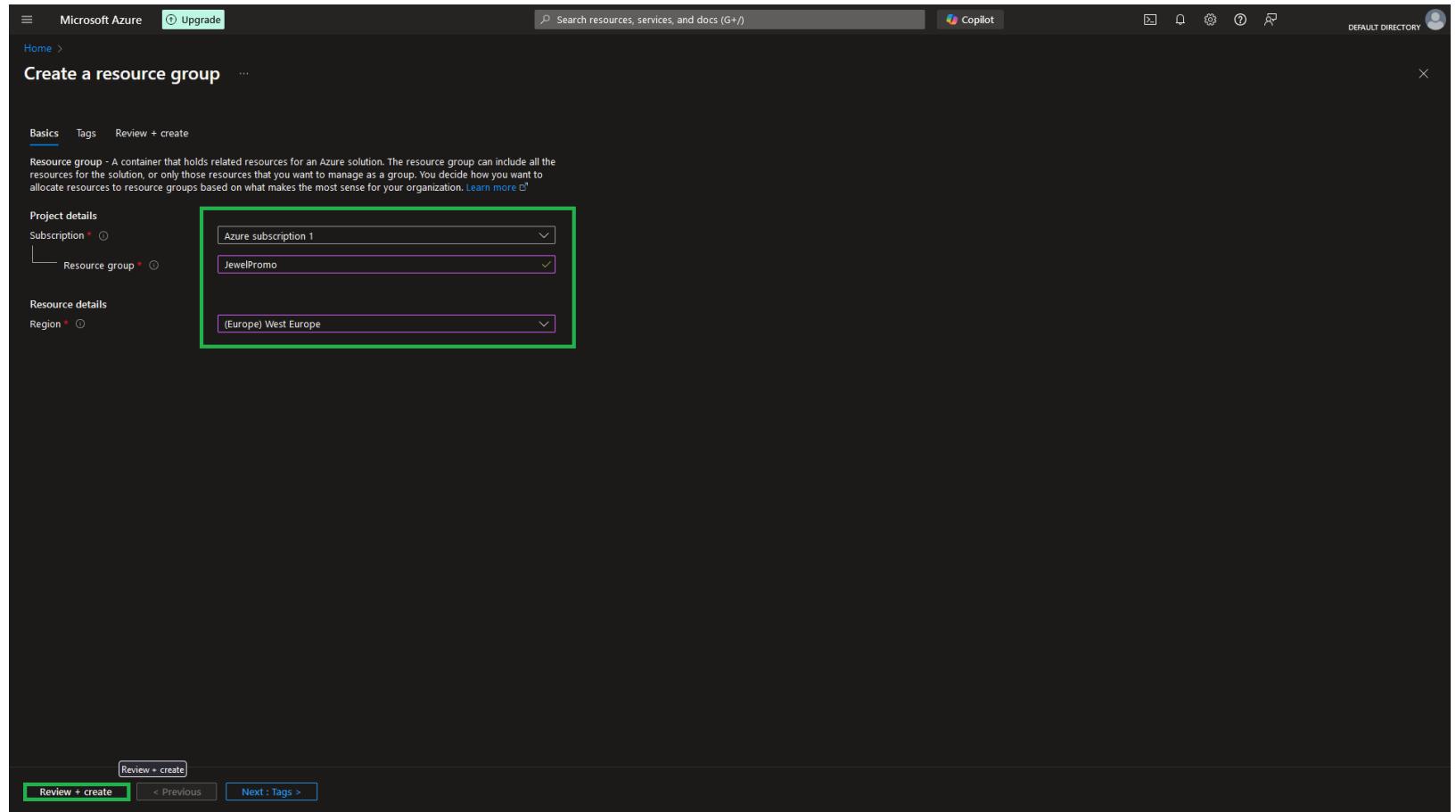
	DISPLAY NAME ▾	USER NAME	MULTI-FACTOR AUTH STATUS	Select a user
<input type="checkbox"/>			Disabled	
<input type="checkbox"/>	AlexSmith	AlexSmith1@	Enabled	
<input type="checkbox"/>			Disabled	
<input type="checkbox"/>	NishaPatel	NishaPatel3@	Enabled	
<input type="checkbox"/>	SofiaLee	SofiaLee2@	Enabled	

## 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.

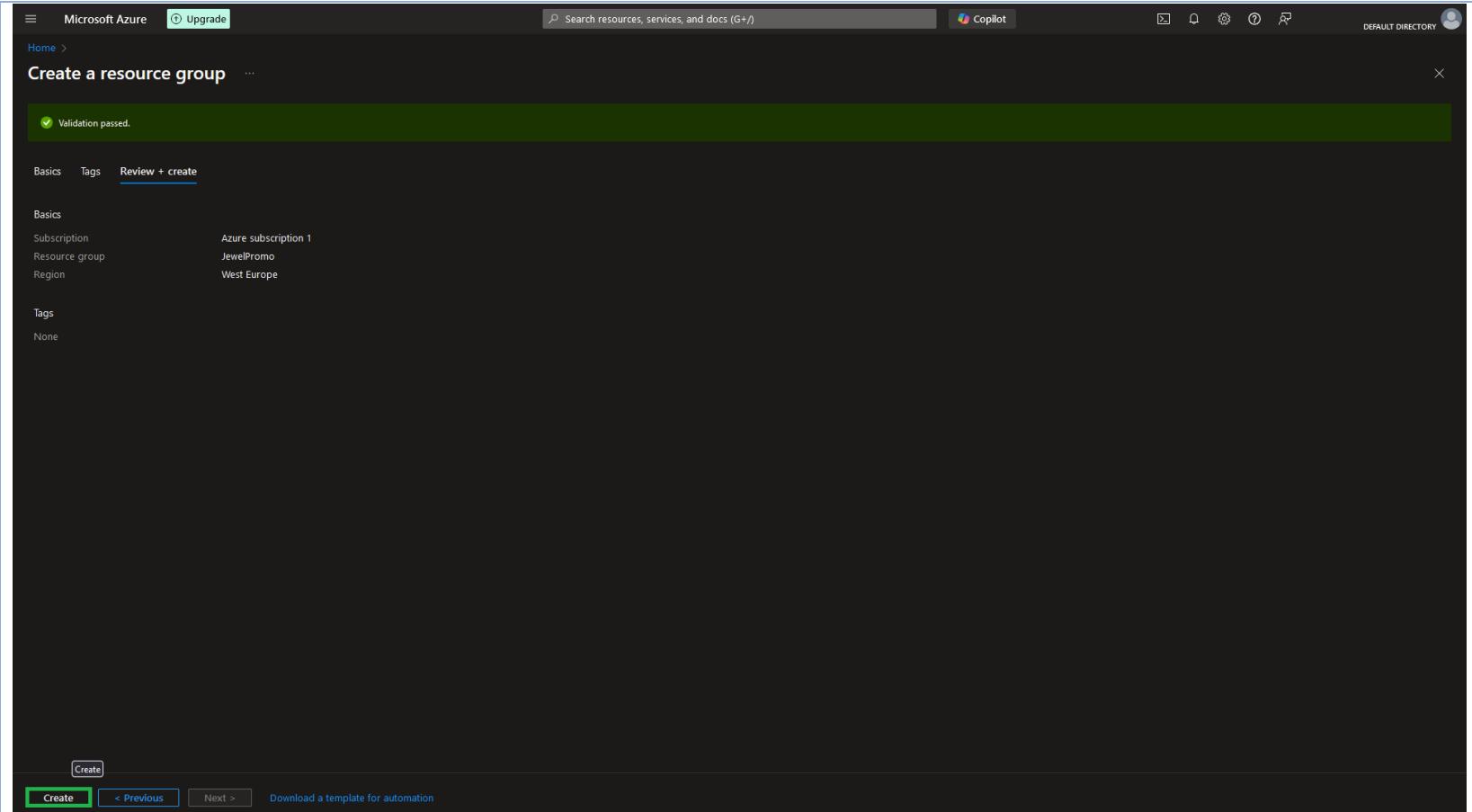
Activity	Key evidence
<p><b>Activity 1:</b> Create a resource group, a Storage account, and a container.</p>	<ol style="list-style-type: none"><li>After signing in to the Azure Portal, we hover over <b>Resource groups</b> and click on <b>Create</b>. <b>Note:</b> This can also be achieved by selecting <b>Create a resource</b> and using the <i>Search services and marketplace</i> search box to search for “resource group”.</li></ol>  <p>2. On the <b>Create a resource group</b> page, on the <b>Basics</b> tab, we then input the following information:</p>

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

3. Click on **Review + create**



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



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

The screenshot shows the Microsoft Azure Resource Groups page. At the top, there are navigation links for 'Home', 'Resource groups', and 'Default Directory'. Below the header are buttons for '+ Create', 'Manage view', 'Refresh', 'Export to CSV', 'Open query', and 'Assign tags'. A message indicates that the user is viewing a new version of the Browse experience and provides a link to access the old experience. The main area displays a table with one row, where the 'Name' column contains 'JewelPromo' (highlighted with a green border), the 'Subscription' column shows 'Azure subscription 1', and the 'Location' column shows 'West Europe'. At the bottom of the table, there is a filter bar with 'Subscription equals all' and 'Location equals all' options, along with a '+ Add filter' button. The footer includes a 'Display count' dropdown set to 20 and a 'Give feedback' link.

Name	Subscription	Location
JewelPromo	Azure subscription 1	West Europe

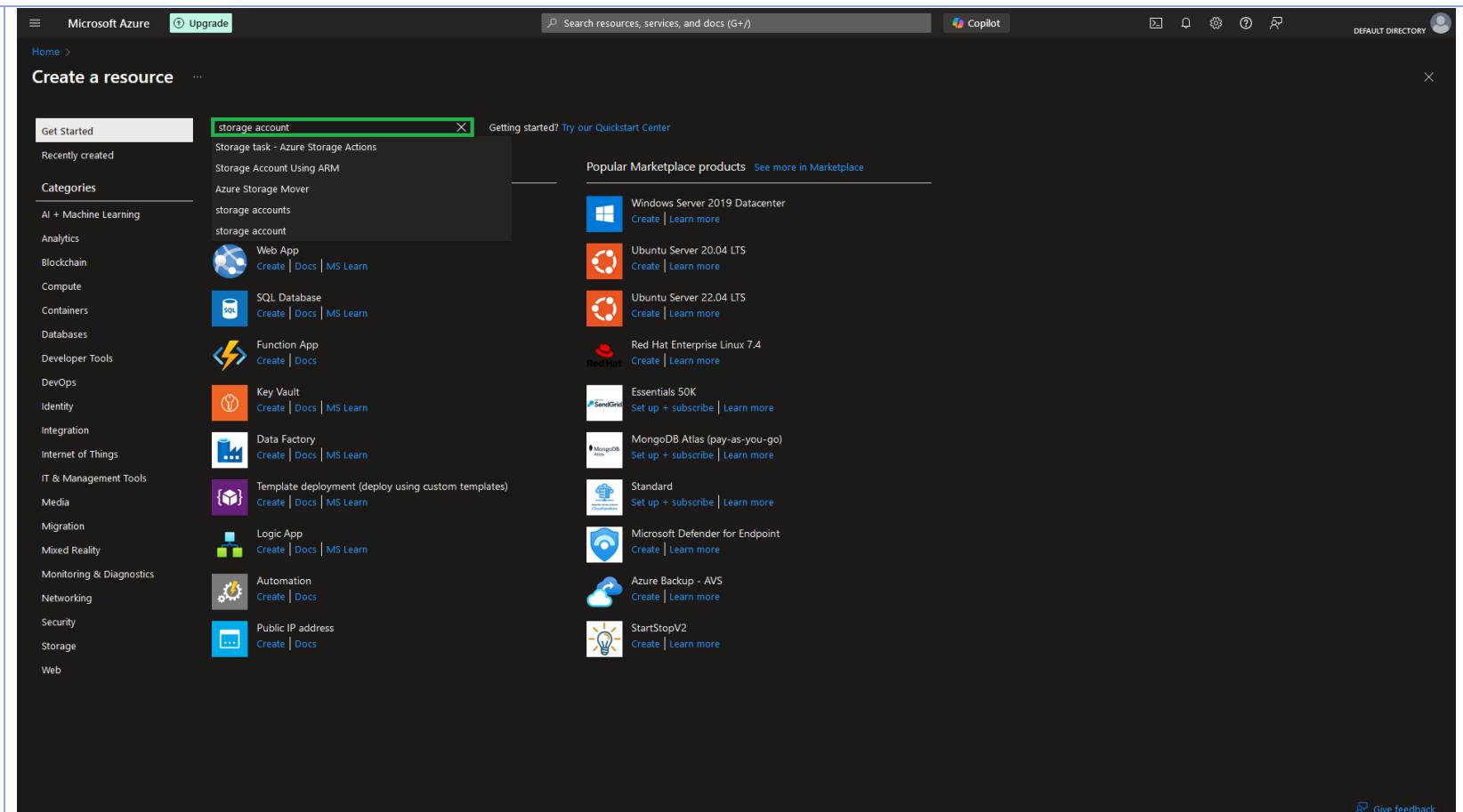
6. To create a storage account, we can either go to the **Storage accounts** page and click on **Create**, or use the **Marketplace** page. Let's go to the **Marketplace** page by clicking on **Create a resource**.

The screenshot shows the Microsoft Azure portal interface. At the top, there's a navigation bar with 'Microsoft Azure' and an 'Upgrade' button. A search bar is followed by a 'Copilot' button and several icons for account management. On the far right, it says 'DEFAULT DIRECTORY' with a user profile icon.

The main content area is titled 'Azure services' and features a large green button labeled 'Create a resource'. Below this are sections for 'Resources' (Recent and Favorite), 'Navigate' (Subscriptions, Resource groups, All resources, Dashboard), 'Tools' (Microsoft Learn, Azure Monitor, Microsoft Defender for Cloud, Cost Management), 'Useful links' (Technical Documentation, Azure Services, Recent Azure Updates), and 'Azure mobile app' (links to App Store and Google Play).

A red box highlights the 'Create a resource' button. The URL 'https://portal.azure.com/#create/hub' is visible at the bottom left of the screenshot.

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+/)

Marketplace ...

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

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

Azure services only

Showing 1 to 20 of 207 results for 'storage account'. [Clear search](#)

Tile view

Storage Account Using ARM	Storage account	Storage Account Using ARM Template	Storage Account Using ARM Template	Storage task - Azure Storage Actions	Azure Storage Mover
DIGISTORM LTD. Azure Application storage account arm	Microsoft Azure Service Use Blobs, Tables, Queues, Files, and Data Lake Gen 2 for reliable, economical cloud storage.	FortuneCloud LLC Azure Application storage account arm template	VIRTUCLLOUD LTD. Azure Application storage account arm	CloudGate LLC Azure Application storage account arm template	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	Price varies	Price varies	Price varies	Create
Blob Storage Digests Backed by Confidential Ledger	Azure Storage solution for Sentinel	RamSoft Image Storage	MDACA Cloud Storage Explorer	S3 API for Azure Blob Storage (Flexify.IO)	Dell APEX Protection Storage for Microsoft Azure (DDVE)
Azure Confidential Ledger Azure Application An application that securely creates and stores blob storage digests in a tamper-proof ledger	Microsoft Sentinel, Microsoft Co... Azure Application Azure Storage solution for Sentinel	RamSoft Inc. Azure Application Azure Storage solution for Sentinel	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.	Flexify Inc. Virtual Machine Allows S3-compatible applications store data in Azure Blob Storage via the standard S3 API	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 Free	Price varies	Price varies	Starts at £0.083/3 years	Starts at £0.225/3 years	Starts at €0.225/3 years
Create	Create	Create	Create	Create	Create

Is Marketplace helpful? X

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

The screenshot shows the Microsoft Azure Marketplace page for creating a storage account. At the top, there's a navigation bar with 'Microsoft Azure' and an 'Upgrade' button. Below it, a breadcrumb trail shows 'Home > Create a resource > Marketplace > Storage account'. The main title is 'Storage account' with a 'Create' button highlighted with a green border. Below the title, there's a summary card for 'Storage account' from 'Microsoft | Azure Service' with a 4.2 rating. A dropdown menu 'Plan' is set to 'Storage account' with a 'Create' button next to it. Below this, there are tabs for 'Overview', 'Plans', 'Usage Information + Support', and 'Ratings + Reviews'. The 'Overview' tab is selected. A descriptive text block explains that Azure provides scalable, durable cloud storage for any data, big or small, working with existing infrastructure and supporting various applications. Below this, there's a section titled 'More products from Microsoft' with four items: 'Active Directory Health Check', 'AD Replication Status', 'Device Update for IoT Hub', and 'Front Door and CDN profiles', each with a 'Create' button.

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 <b>JewelPromo</b> .
Storage account name	Enter the storage account name, <b>advtstorage</b> . <b>Note:</b> Storage account name must be globally unique
Region	Select the same region as the resource group we created earlier.
Performance	Select <b>Standard: Recommended for most scenarios (general-purpose v2 account)</b> .
Redundancy	Select <b>Geo-redundant storage (GRS)</b> .

**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.

The screenshot shows the 'Create a storage account' wizard in the Microsoft Azure portal. The 'Basics' tab is selected. In the 'Project details' section, the 'Subscription' dropdown is set to 'Azure subscription 1' and the 'Resource group' dropdown is set to 'JewelPromo'. The 'Storage account name' field contains 'admaterials'. The 'Region' dropdown is set to '(Europe) West Europe'. Under 'Primary service', the 'Standard: Recommended for most scenarios (general-purpose v2 account)' radio button is selected. Under 'Performance', the 'Geo-redundant storage (GRS)' option is chosen. A note at the top right of the page reads: 'Note: Selecting this option replicates the data to a datacenter in a different region. Ensure that the **Make read access to data available in the event of regional unavailability** checkbox is selected.'

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

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

Home > Create a resource > Marketplace > Storage account > Create a storage account ...

Basics Advanced Networking Data protection Encryption Tags Review + 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**

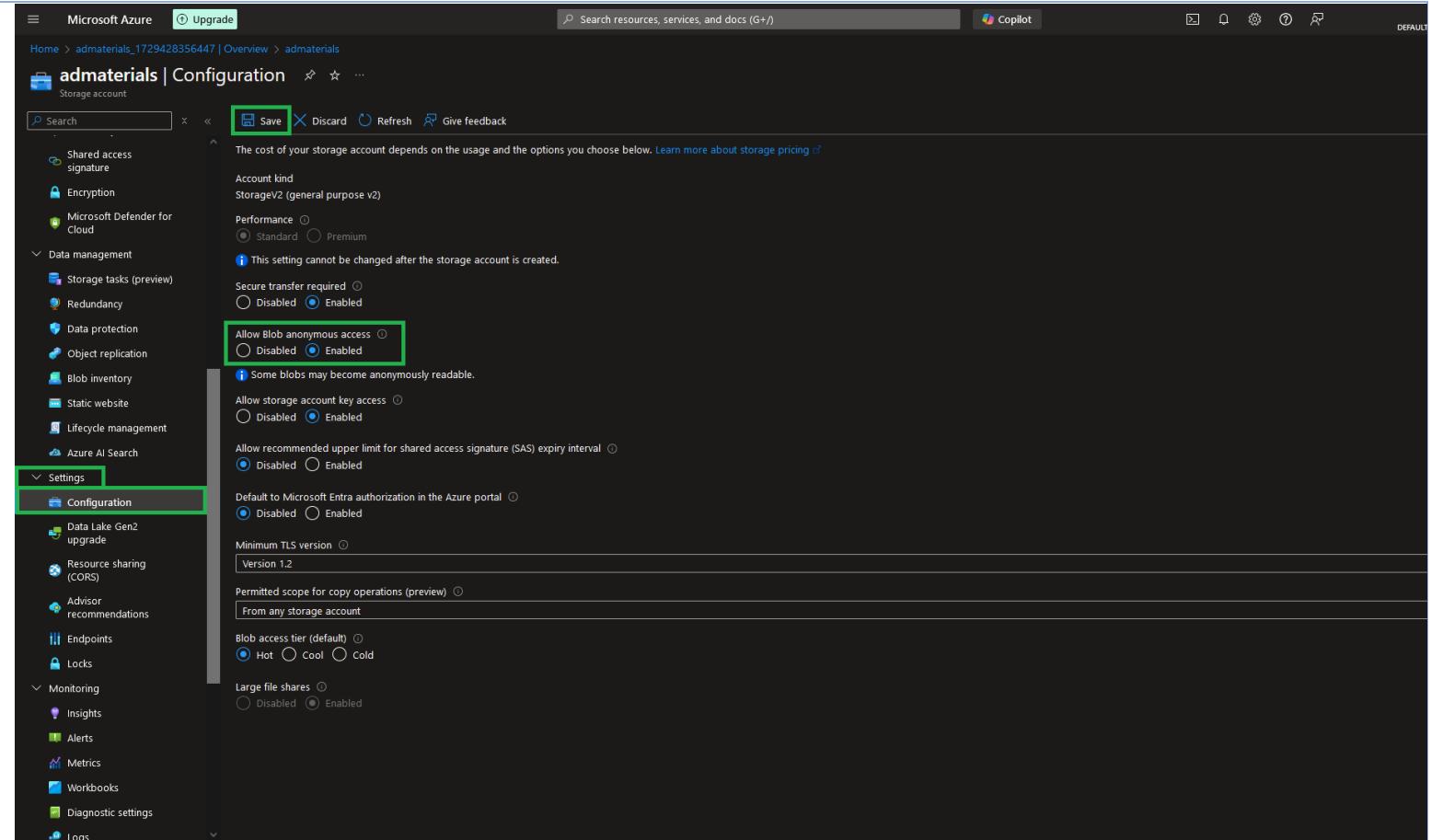
Network connectivity	Public endpoint (all networks)
Default routing tier	Microsoft network routing

Previous Next Create Give feedback

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

The screenshot shows the Microsoft Azure Deployment Overview page for a deployment named "admaterials\_1729428356447". The main message is "Your deployment is complete". Deployment details include: Deployment name: admaterials\_1729428356447, Subscription: Azure subscription 1, Resource group: JewelPromo. The deployment started at 20/10/2024, 15:47:31. A "Go to resource" button is highlighted in green. To the right, there are links for Cost Management, Microsoft Defender for Cloud, and Work with an expert.

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.

The screenshot shows the Microsoft Azure Storage account interface. On the left, the navigation menu is expanded, showing categories like Data storage, Security + networking, and Data management. Under Data storage, the 'Containers' option is selected and highlighted with a green box. The main content area displays a list of existing containers, including 'Slogs'. A modal window titled 'New container' is open on the right, also highlighted with a green box. In the 'Name' field, 'campaignimages' is typed. Below it, the 'Anonymous access level' dropdown is set to 'Blob (anonymous read access for blobs only)'. A warning message at the bottom of the modal states: '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.' At the bottom right of the modal are 'Create' and 'Give feedback' buttons.

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

The screenshot shows the Microsoft Azure Storage account interface for the 'admaterials' container. The left sidebar lists various storage management options like Overview, Activity log, Tags, and Data storage (Containers, File shares, Queues, Tables). The main area displays a table of containers with columns for Name, Last modified, Anonymous access level, and Lease state. Two containers are listed: 'Slogs' (Last modified 20/10/2024, 15:47:56, Private, Available) and 'campaignimages' (Last modified 20/10/2024, 16:21:40, Blob, Available). A green box highlights the 'campaignimages' row.

Name	Last modified	Anonymous access level	Lease state
Slogs	20/10/2024, 15:47:56	Private	Available
campaignimages	20/10/2024, 16:21:40	Blob	Available

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

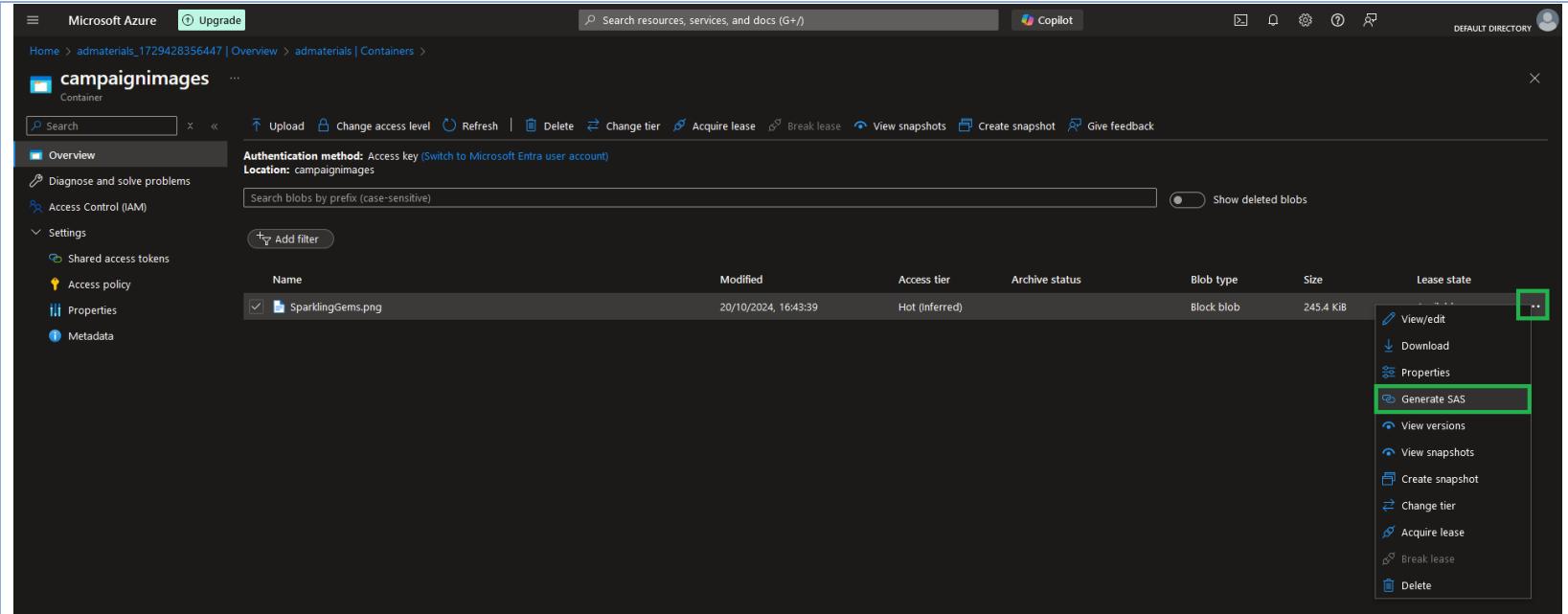
1. We now click on the newly created container called **campaignimages**, select the **Upload** button to open the **Upload blob** wizard, and add the SparklingGems.png to the container.

The screenshot shows the Microsoft Azure Storage Explorer interface. On the left, there's a sidebar with options like Overview, Diagnose and solve problems, Access Control (IAM), Settings, Shared access tokens, Access policy, Properties, and Metadata. The main area shows a table with columns: Name, Modified, Access tier, and Archive status. A search bar at the top says 'Search blobs by prefix (case-sensitive)'. To the right, a large window titled 'Upload blob' contains a central area with a cloud icon and the text 'Drag and drop files here or Browse for files'. Below this are checkboxes for 'Overwrite if files already exist' and 'Advanced', and a 'Upload' button.

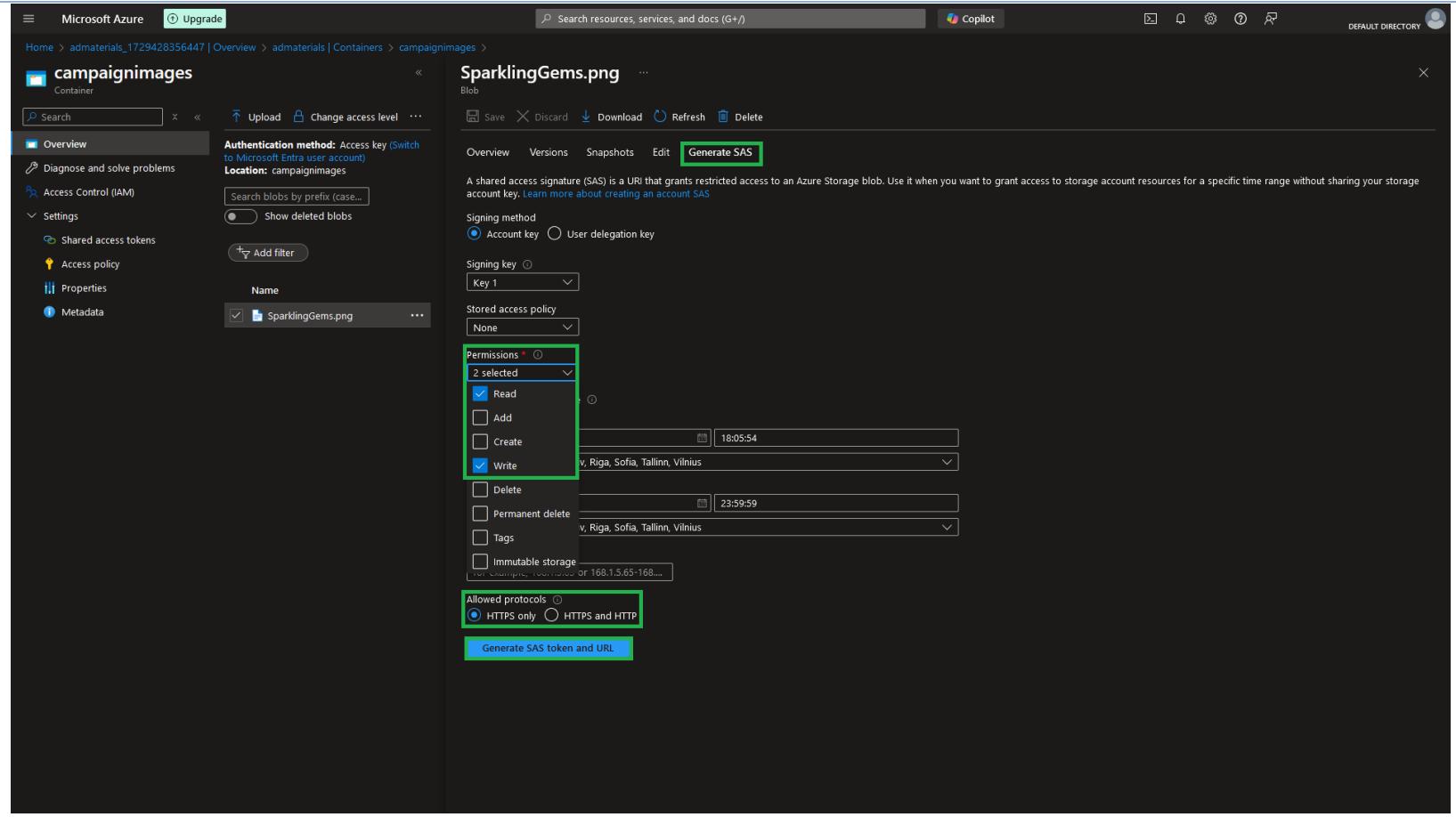
2. After adding the image, we click on **Upload** and it should successfully appear within the container.

The screenshot shows the Microsoft Azure Storage Explorer interface after a file has been uploaded. The left sidebar remains the same. The main area now displays a table with a single row for the uploaded file. The columns are: Name, Modified, Access tier, Archive status, Blob type, Size, and Lease state. The file listed is 'SparklingGems.png' with the details: Modified: 20/10/2024, 16:43:39, Access tier: Hot (Inferred), Archive status: Not yet used, Blob type: Block blob, Size: 245.4 KiB, Lease state: Available. A success message at the top right of the interface says 'Successfully uploaded blob(s)'.

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



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



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

The screenshot shows the Azure Storage Blob SAS configuration interface. On the left, the 'Overview' tab is selected in the campaignimages container. In the center, a blob named 'SparklingGems.png' is highlighted. The right pane displays the 'Generate SAS' settings. Key fields include:

- Authentication method:** Access key (Switch to Microsoft Entra user account)
- Location:** campaignimages
- Signing method:** Account key (selected)
- Key 1:** Selected
- Permissions:** 2 selected (checkboxes are visible but not explicitly labeled)
- Start:** 20/10/2024 at 18:05:54 (UTC+02:00 Helsinki, Kyiv, Riga, Sofia, Tallinn, Vilnius)
- Expiry:** 20/10/2024 at 23:59:59 (UTC+02:00 Helsinki, Kyiv, Riga, Sofia, Tallinn, Vilnius)
- Allowed IP addresses:** [Input field for example: 168.1.5.65 or 168.1.5.65-168...]
- Allowed protocols:** HTTPS only (radio button selected)

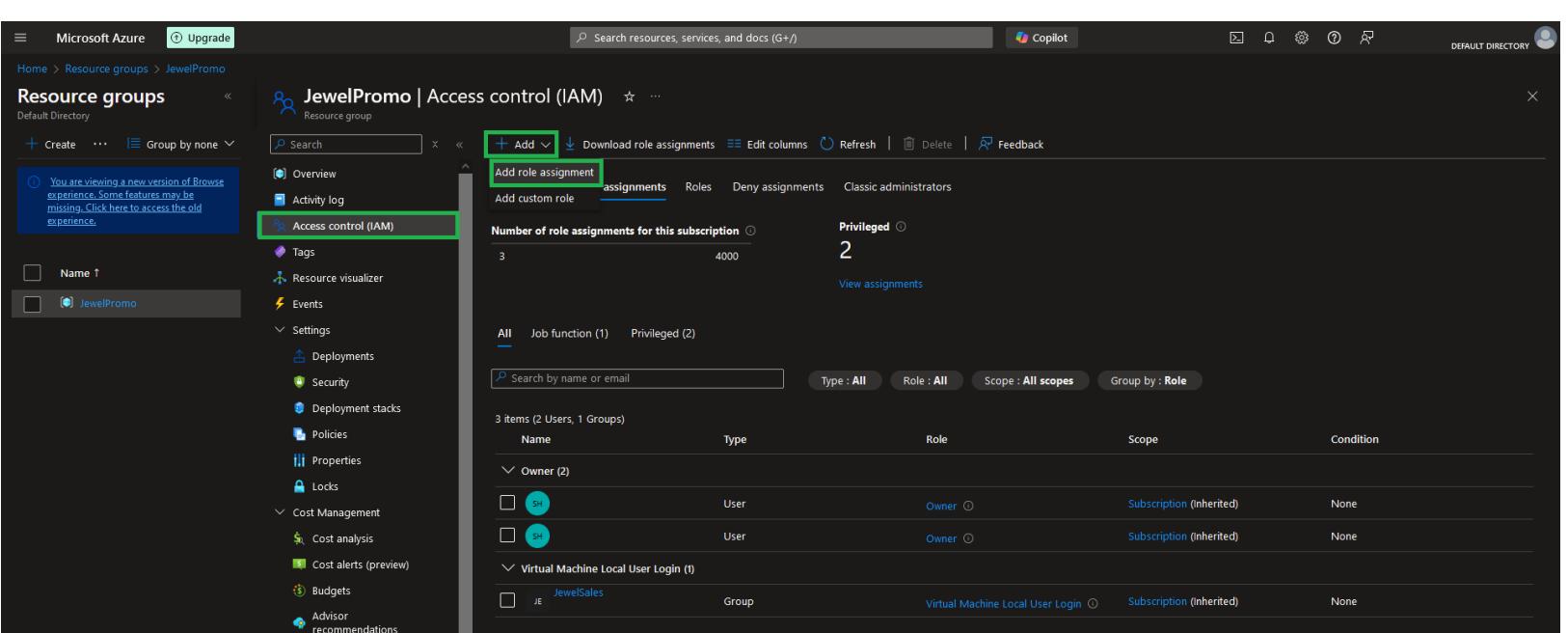
At the bottom, two output fields are shown:

- Blob SAS token:** A long URL starting with `sp=rw&t=2024-10-20T15:05:54Z&se=2024-10-20T20:59:59Z&spr=https&sv=2022-11-02&sr=b&sig=%2Fz%2BXGfvQk0p%2Fi6xcr%2BG4c7y4PgI99%2Bqx%2BqroluRo%3D`
- Blob SAS URL:** <https://admaterials.blob.core.windows.net/campaignimages/SparklingGems.png?sp=rw&t=2024-10-20T15:05:54Z&se=2024-10-20T20:59:59Z&spr=https&sv=2022-11-02&sr=b&sig=%2Fz%2BXGfvQk0p%2Fi6xcr%2BG4c7y4PgI99%2Bqx%2BqroluRo%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**.



The screenshot shows the Microsoft Azure Resource groups interface for the 'JewelPromo' resource group. The left sidebar lists various options like Overview, Activity log, and Access control (IAM). The main area displays the 'Access control (IAM)' section, which includes a summary of role assignments (Number of role assignments for this subscription: 3 / 4000, Privileged: 2), a search bar, and a table of assigned users and groups. The 'Add role assignment' button at the top of the table is highlighted with a green box.

Name	Type	Role	Scope	Condition
SH	User	Owner	Subscription (Inherited)	None
SJ	User	Owner	Subscription (Inherited)	None
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**.

The screenshot shows the Microsoft Azure 'Add role assignment' wizard. The 'Role' tab is selected. In the search bar, 'Blob data' is typed. The results table shows five roles:

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 Dfender CSPM.	BuiltinRole	None	<a href="#">View</a>
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	<a href="#">View</a>
Storage Blob Data Contributor	Allows for read, write and delete access to Azure Storage blob containers and data	BuiltinRole	Storage	<a href="#">View</a>
Storage Blob Data Owner	Allows for full access to Azure Storage blob containers and data, including assigning POSIX access control.	BuiltinRole	Storage	<a href="#">View</a>
Storage Blob Data Reader	Allows for read access to Azure Storage blob containers and data	BuiltinRole	Storage	<a href="#">View</a>

Showing 1 - 5 of 5 results.

Navigation buttons at the bottom: Review + assign, Previous, Next.

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

The screenshot shows the Microsoft Azure 'Add role assignment' interface. On the left, the 'Members' tab is selected under the 'Role Assignment' section. The 'Selected role' is set to 'Storage Blob Data Contributor'. The 'Assign access to' option is set to 'User, group, or service principal'. Below these, there are fields for 'Members' (with a green border) and 'Description' (with a green border). At the bottom, there are buttons for 'Review + assign', 'Previous', and 'Next'. On the right, a modal window titled 'Select members' is open, showing a list of users and their email addresses. A user named 'AlexSmith' is selected, indicated by a green border around the row. The 'Selected members' list also contains 'NishaPatel' and 'SofiaLee'. At the bottom of the modal are 'Select' and 'Close' buttons.

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

The screenshot shows the Microsoft Azure 'Add role assignment' interface. The 'Review + assign' tab is selected. The 'Role' is set to 'Storage Blob Data Contributor'. The 'Scope' is '/subscriptions/1c231d77-b506-4287-925c-aba83bffa6fb/resourceGroups/JewelPromo'. The 'Members' section lists three users: AlexSmith, NishaPatel, and SofiaLee, each with their Object ID and User type. A green box highlights the 'Members' table. The 'Description' field is empty, and the 'Condition' field is set to 'None'. At the bottom, there are 'Review + assign', 'Previous', and 'Next' buttons, with 'Review + assign' being the active button.

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.

The screenshot shows the Microsoft Azure Resource Groups page for a resource group named 'JewelPromo'. The 'Role assignments' tab is active, displaying 2 privileged role assignments. The table lists three users under the 'Storage Blob Data Contributor' role:

Name	Type	Role	Scope	Condition
AlexSmith	User	Storage Blob Data Contributor	This resource	Add
NishaPatel	User	Storage Blob Data Contributor	This resource	Add
SofiaLee	User	Storage Blob Data Contributor	This resource	Add

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

Activity	Key evidence
<b>Activity 1:</b> Create a Key Vault and a managed identity and assign key permissions to the managed identity.	<ol style="list-style-type: none"> <li>From the Azure Portal, we select <b>Create a resource</b> to go to the <b>Marketplace</b> page where we type “key vault” into the <i>Search services and marketplace</i> search box, and then click on <b>Key Vault</b> from the results.</li> </ol>

- 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 <b>JewelPromo</b> .
Key vault name	Enter a key vault name, <b>EntraKeyVault1</b> .
Region	Select the same region as previous resources
Pricing tier	Select <b>Standard</b> .
Purge protection	Select <b>Enable purge protection (enforce a mandatory retention period for deleted vaults and vault objects)</b> .

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

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.

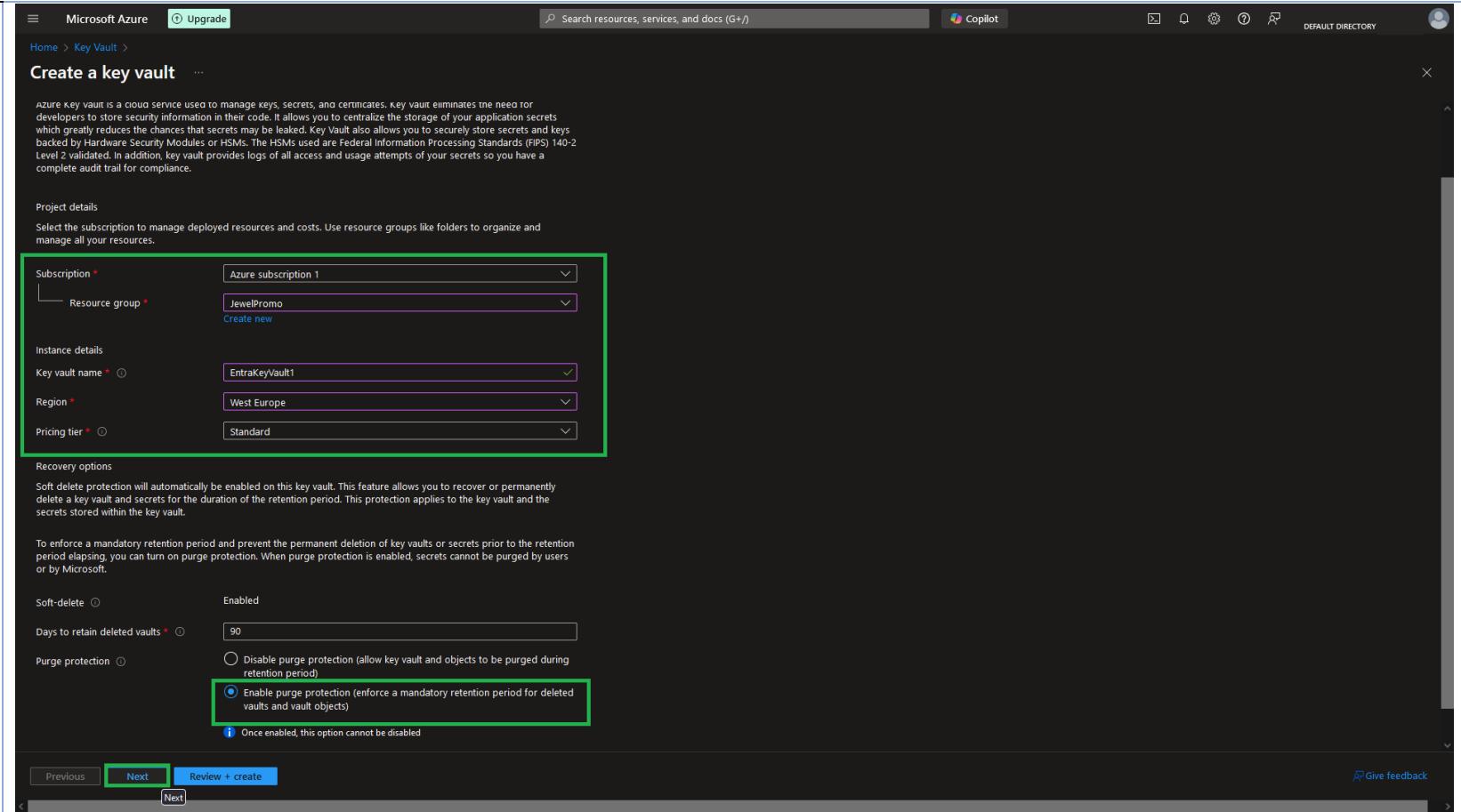
Subscription \* Azure subscription 1  
Resource group \* JewelPromo Create new

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**.

The screenshot shows the Microsoft Azure portal interface for creating a new Key Vault. The top navigation bar includes 'Microsoft Azure', 'Upgrade', a search bar ('Search resources, services, and docs (G+)'), 'Copilot', and various account settings. The main title is 'Create a key vault ...'. Below it, the 'Access configuration' tab is selected, highlighted with a green border. Other tabs include 'Basics', 'Networking', 'Tags', and 'Review + create'. A note at the top states: '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.' A link to 'Learn more' is provided. Under 'Permission model', there are two options: 'Azure role-based access control (recommended)' and 'Vault access policy'. The 'Vault access policy' option is selected and highlighted with a green border. The 'Resource access' section lists three options: 'Azure Virtual Machines for deployment', 'Azure Resource Manager for template deployment', and 'Azure Disk Encryption for volume encryption', all of which are currently unchecked. The 'Access policies' section allows for fine-grained control over vault items. It includes a table with columns for 'Name' (sorted by Email), 'Key Permissions', 'Secret Permissions', and 'Certificate Permissions'. A single row is shown for a user named 'USER', with permissions listed under each column. At the bottom of the page are 'Previous' and 'Next' buttons, and a prominent 'Review + create' button.

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

The screenshot shows the 'Create a key vault' wizard in the Microsoft Azure portal. The 'Review + create' tab is selected, highlighted with a green border. The page displays configuration details across three sections: Basics, Access configuration, and Networking.

**Basics**

Subscription	Azure subscription 1
Resource group	JewelPromo
Key vault name	EntraKeyVault1
Region	West Europe
Pricing tier	Standard
Soft-delete	Enabled
Purge protection during retention period	Enabled
Days to retain deleted vaults	90 days

**Access configuration**

Azure Virtual Machines for deployment	Disabled
Azure Resource Manager for template deployment	Disabled
Azure Disk Encryption for volume encryption	Disabled
Permission model	Vault access policy
Access policies	1

**Networking**

Connectivity method	Public endpoint (all networks)
---------------------	--------------------------------

At the bottom, there are 'Previous' and 'Next' buttons, and a prominent 'Create' button, also highlighted with a green border. A 'Give feedback' link is located in the bottom right corner.

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

The screenshot shows the Microsoft Azure Portal interface. At the top, there's a navigation bar with 'Microsoft Azure' and an 'Upgrade' button. A search bar says 'Search resources, services, and docs (G/)' and a 'Copilot' button is nearby. On the right, there are icons for notifications, security, and help, along with a 'DEFAULT DIRECTORY' dropdown and a user profile icon.

The main content area shows a deployment named 'EntraKeyVault1'. A green box highlights the message 'Your deployment is complete'. Below it, deployment details are listed: Deployment name: EntraKeyVault1, Subscription: Azure subscription 1, Resource group: JewelPromo. To the right, deployment logs show 'Start time : 21/10/2024, 00:45:53' and 'Correlation ID : 6010ca89-8ee3-4575-8315-b25fc3f19bc2'. A blue 'Go to resource' button is at the bottom of this section.

On the right side of the page, there are several promotional cards:

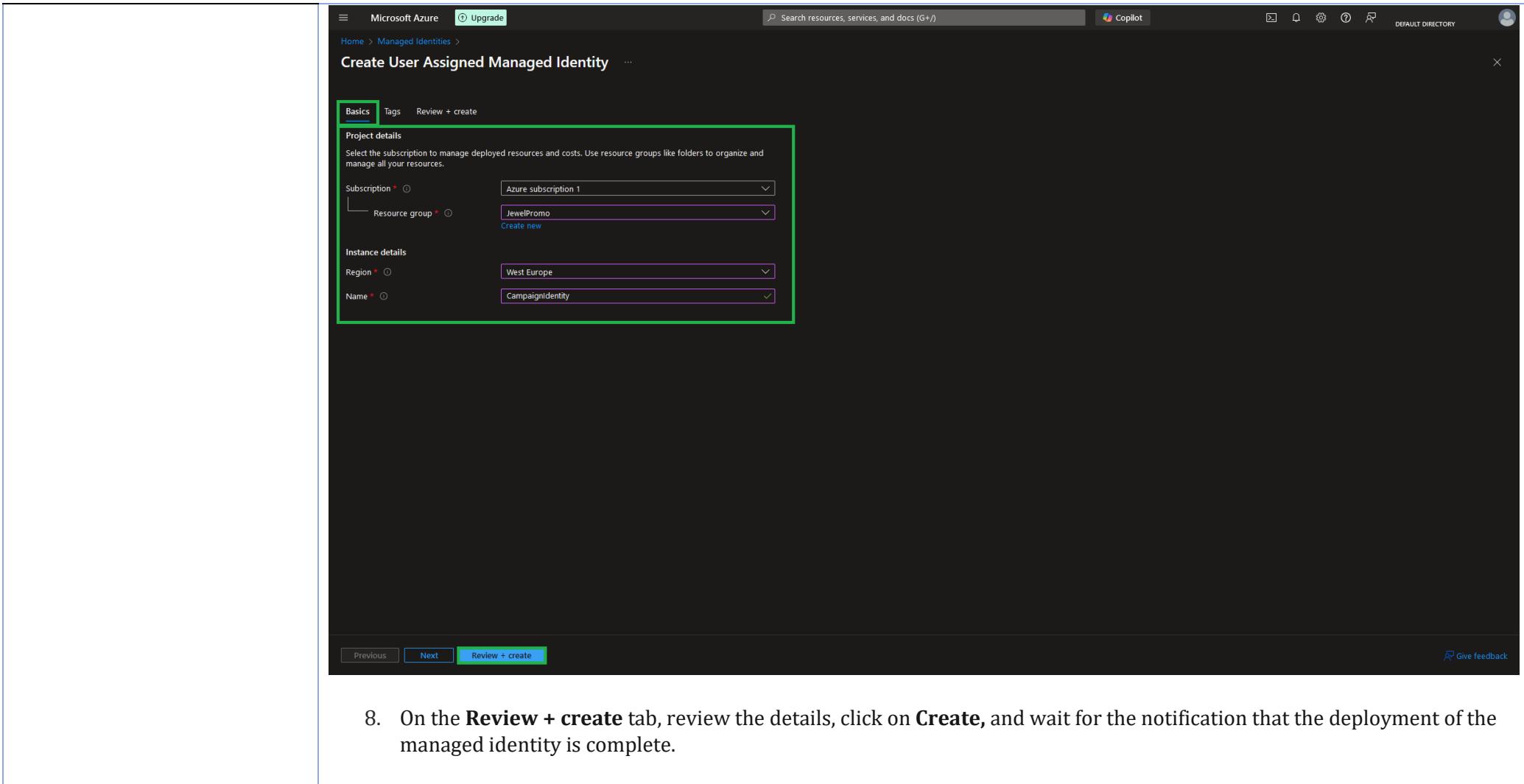
- Cost management**: Get notified to stay within your budget and prevent unexpected charges on your bill. [Set up cost alerts >](#)
- Microsoft Defender for Cloud**: Secure your apps and infrastructure. [Go to Microsoft Defender for Cloud >](#)
- Free Microsoft tutorials**: Start learning today. [Start learning today >](#)
- Work with an expert**: Azure experts are service provider partners who can help manage your assets on Azure and be your first line of support. [Find an Azure expert >](#)

At the bottom left, a numbered step 6 is described: 'We then go back to the Azure Portal home page, and type "managed identities" into the search box.'

The screenshot shows the Microsoft Azure portal homepage. The search bar at the top contains the text "managed identities". Below the search bar, the "Services" section is displayed, with "Managed identities" highlighted in green. Other services listed include "External identities", "Workload identities", and "Microsoft Entra Privileged Identity Management". To the left, the "Azure services" sidebar shows options like "Create a resource", "Microsoft Entra ID", and "Resource groups". The "Resources" sidebar lists recent resources such as "EntraKeyVault1", "JewelPromo", "admaterials", and "Azure subscription 1". The "Documentation" section provides links to various Azure services. At the bottom, there are links to "Continue searching in Microsoft Entra ID" and "Give feedback".

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 <b>JewelPromo</b> .
Region	Select the same region as previous resources.
Name	Enter a unique name, such as <b>CampaignIdentity</b> .



The screenshot shows the Microsoft Azure portal interface for creating a User Assigned Managed Identity. The top navigation bar includes 'Microsoft Azure', 'Upgrade', 'Search resources, services, and docs (G+)', 'Copilot', and account settings. The main title is 'Create User Assigned Managed Identity'. The 'Basics' tab is selected. A green box highlights the 'Project details' section, which contains fields for 'Subscription' (set to 'Azure subscription 1') and 'Resource group' (set to 'JewelPromo'). Below this is the 'Instance details' section with 'Region' (set to 'West Europe') and 'Name' (set to 'CampaignIdentity'). At the bottom of the form are 'Previous', 'Next', and 'Review + create' buttons, with 'Review + create' being the active tab.

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.

The screenshot shows the Microsoft Azure Deployment Overview page for a deployment named 'Microsoft.ManagedIdentity-20241021005219'. The status is 'Deployment succeeded'. The deployment was started at 21/10/2024, 01:02:03 with Correlation ID c9c86f77-f113-4145-a80b-65f56726f3f1. It was deployed to an Azure subscription and a resource group named 'JewelPromo'. A green box highlights the message 'Your deployment is complete'. On the right side, there are promotional links for Cost management, Microsoft Defender for Cloud, Free Microsoft tutorials, and Work with an expert.

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

The screenshot shows the Microsoft Azure Resource Group Overview page for 'JewelPromo'. The 'Essentials' section displays the subscription information (move to Azure subscription 1), deployment status (3 succeeded), and location (West Europe). The 'Resources' section lists three resources: 'admaterials' (Storage account, West Europe), 'Campaignidentity' (Managed identity, East US), and 'EntraKeyVault1' (Key vault, West Europe). A green box highlights 'EntraKeyVault1' in the list.

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

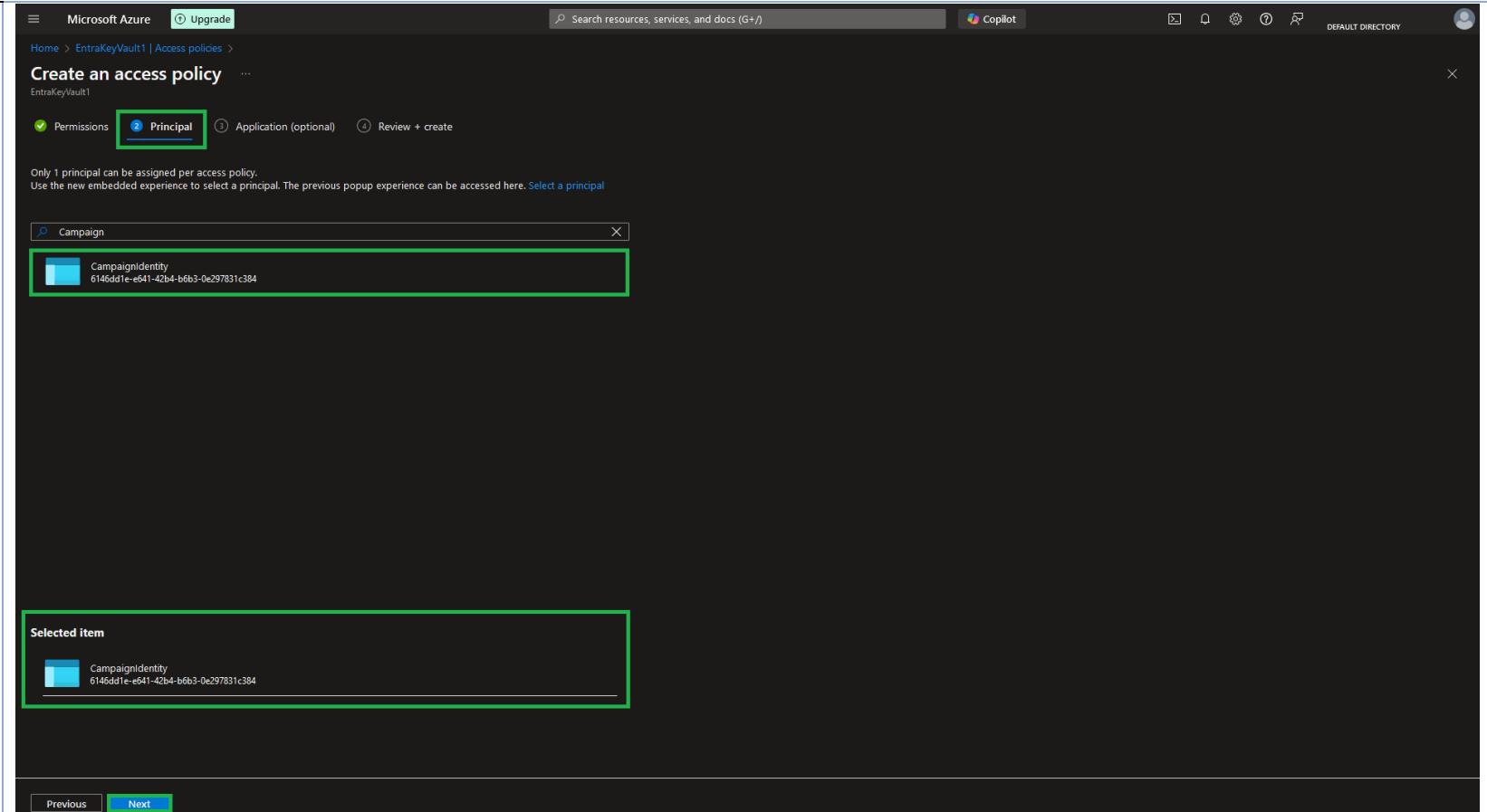
The screenshot shows the Microsoft Azure portal interface for managing access policies in a Key Vault. The left sidebar lists several options: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, **Access policies** (which is selected and highlighted with a green border), Events, Objects (with sub-options Keys, Secrets, and Certificates). The main content area is titled "EntraKeyVault1 | Access policies". It includes a search bar, a "Create" button, and links for Refresh, Delete, and Edit. A sub-header states: "Access policies enable you to have fine grained control over access to vault items. Learn more". Below this is a table header with columns: Name, Email, Key Permissions, Secret Permissions, and Certificate Permissions. A single record is listed: "USER". The "Name" column has a checkbox and the value "USER". The "Email" column has a value "user@contoso.com". The "Key Permissions" column is empty. The "Secret Permissions" column is empty. The "Certificate Permissions" column is empty.

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**.

The screenshot shows the 'Create an access policy' page in the Microsoft Azure portal. The 'Permissions' tab is active. The 'Key permissions' section contains several operations: 'Select all', 'Get' (checked), 'List' (checked), 'Update', 'Create', 'Import', 'Delete', 'Recover', 'Backup', and 'Restore'. The 'Secret permissions' section includes 'Select all', 'Get', 'List', 'Set', 'Delete', 'Recover', 'Backup', 'Restore', 'Manage Contacts', 'Manage Certificate Authorities', 'Get Certificate Authorities', 'List Certificate Authorities', 'Set Certificate Authorities', and 'Delete Certificate Authorities'. The 'Certificate permissions' section lists 'Select all', 'Get', 'List', 'Update', 'Create', 'Import', 'Delete', 'Recover', 'Backup', 'Restore', 'Manage Contacts', 'Manage Certificate Authorities', 'Get Certificate Authorities', 'List Certificate Authorities', 'Set Certificate Authorities', and 'Delete Certificate Authorities'. At the bottom, there are 'Previous' and 'Next' buttons, with 'Next' being highlighted.

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.

The screenshot shows the 'Create an access policy' step in the Microsoft Azure portal. The 'Permissions' tab is selected, showing the following key permissions:

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

The 'Principal' section shows the principal assigned to this policy:

Principal name	Campaignidentity
Object ID	149b0095-93c5-4b3c-9c1a-785e559f9564

The 'Application' section shows no application selected:

Authorized application	None selected
Object ID	None selected

At the bottom, there are 'Previous' and 'Create' buttons, with 'Create' being the active button.

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

Microsoft Azure | Upgrade

Search resources, services, and docs (G/)

Copilot

DEFAULT DIRECTORY

Notifications

More events in the activity log > Dismiss all

Updating the key vault 'EntraKeyVault1'. The key vault 'EntraKeyVault1' has been successfully updated. a minute ago

EntraKeyVault1 | Access policies

Key vault

+ Create | Refresh | Delete | Edit

Access policies enable you to have fine grained control over access to vault items. Learn more

Showing 1 to 2 of 2 records.

Name ↑	Email ↑	Key Permissions	Secret Permissions	Certificate Permissions
CampaignIdentity		Get, List, Unwrap Key, Wrap Key		

APPLICATION

USER

Events

Objects

Keys

Secrets

Certificates

**Activity 2:** Encrypt the Storage account using customer-managed keys.

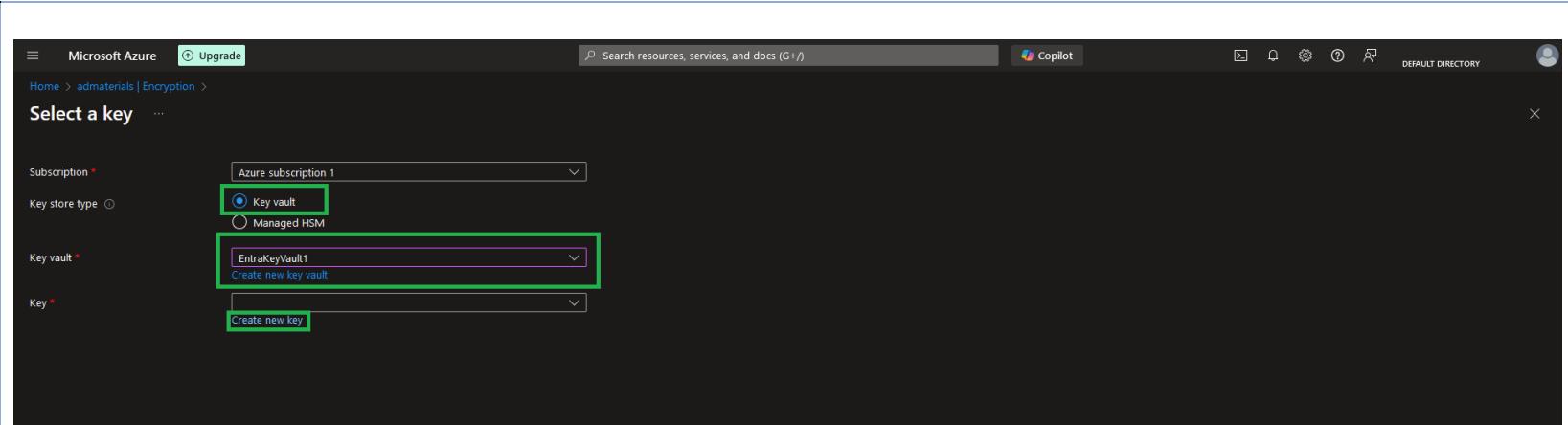
1. We navigate to our storage account, **adstorage**, and select **Encryption** from the storage account's menu, under the *Security + networking* blade.
2. On the **Encryption** page, we go to the **Encryption** tab and select the **Customer-managed keys radio button** in the **Encryption type** field.
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**.

The screenshot shows the Azure Storage account settings for 'admaterials'. The left sidebar is collapsed, and the main area displays the 'Encryption' configuration. Key sections include:

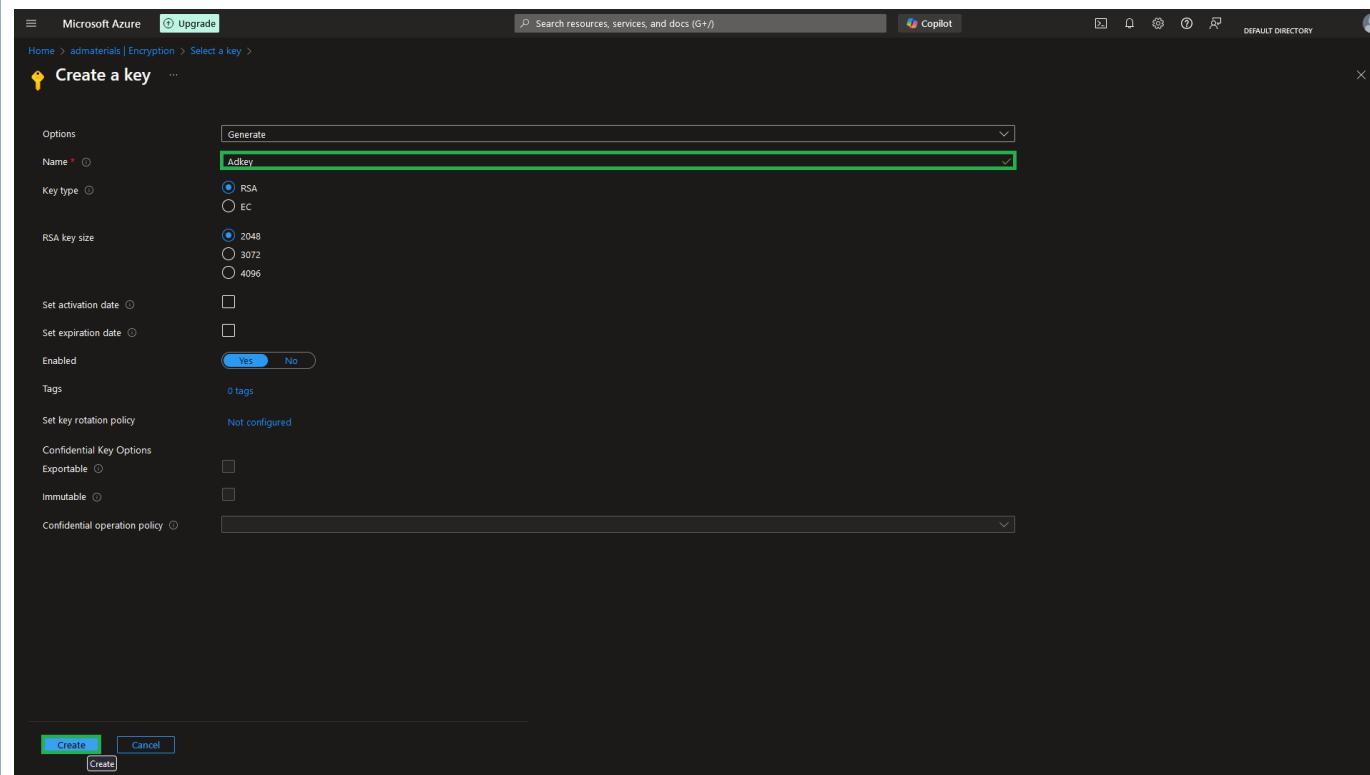
- Encryption selection:** Shows 'Enable support for customer-managed keys' (radio button selected) and 'Blobs and files only'.
- Infrastructure encryption:** Set to 'Disabled'.
- Encryption type:** Set to 'Customer-managed keys' (radio button selected).
- Key selection:** Set to 'Select from key vault' (radio button selected).
- Encryption key:** A dropdown menu is open, showing 'Select a key vault and key'.
- Identity type:** Set to 'System-assigned' (radio button selected).

At the bottom are 'Save' and 'Discard' buttons, and a 'Give feedback' link.

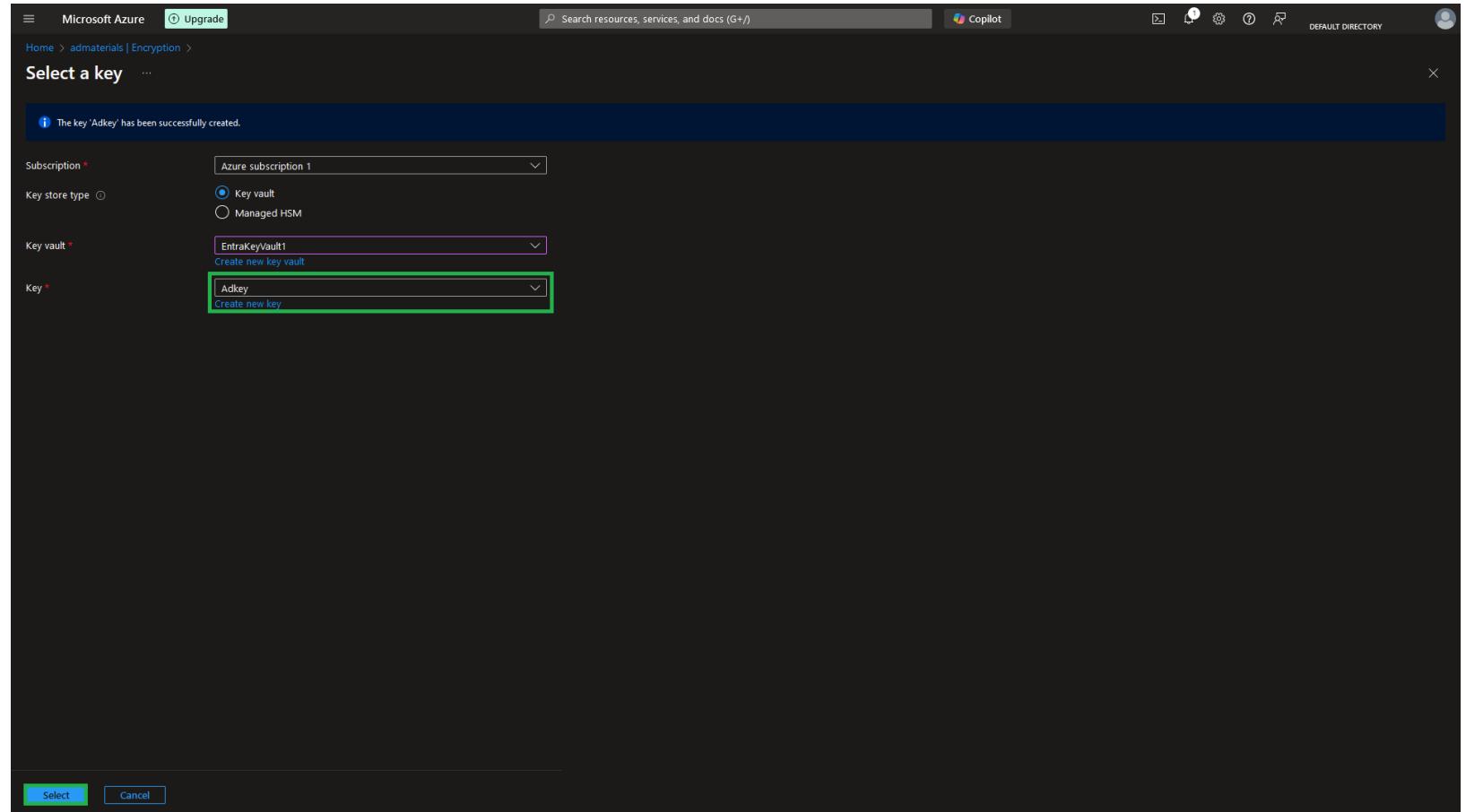
4. On the **Select a key page**, the subscription is automatically populated.  
5. In the **Key store type** field, we select the **Key vault** radio button, and then select **EntraKeyVault1** from the dropdown list in the **Key vault** field.  
6. Next, in the **Key** field, we click on **Create new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



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



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



The screenshot shows the 'Select a key' dialog box from the Microsoft Azure portal. At the top, there's a success message: 'The key 'Adkey' has been successfully created.' Below this, there are four main configuration fields:

- Subscription \***: A dropdown menu showing 'Azure subscription 1'.
- Key store type**: A radio button group where 'Key vault' is selected, while 'Managed HSM' is unselected.
- Key vault \***: A dropdown menu showing 'EntrakVault1' with 'Create new key vault' as an option below it.
- Key \***: A dropdown menu showing 'Adkey' with 'Create new key' as an option below it. This field is highlighted with a green border.

At the bottom of the dialog are two buttons: 'Select' (highlighted in blue) and '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 shows the Microsoft Azure portal interface. On the left, the navigation menu is open, showing various storage account management options like 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 (selected), and Data management (Storage tasks (preview), Redundancy, Data protection, Object replication).

The main content area is titled "Encryption" under "Encryption scopes". It contains sections for "Encryption selection", "Encryption type", "Key selection", "Key vault and key", "Identity type", and "User-assigned identity".

In the "User-assigned identity" section, the "User-assigned" radio button is selected, and a callout box highlights the "Select an identity" button.

A modal window titled "Select user assigned managed..." is displayed on the right. It shows a dropdown for "Subscription" set to "Azure subscription 1". Below it is a search bar with the placeholder "Filter by identity name and/or resource group name". A list item "CampaignIdentity" is selected, with a sub-item "Resource Group: JewelPromo".

The "Selected identity" section shows the chosen identity: "CampaignIdentity" (Resource Group: JewelPromo, Subscription: Azure subscription 1). An "Add" button is located at the bottom right of the modal.

**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.**

The screenshot shows the Microsoft Azure Storage account 'admaterials' Encryption settings page. The 'Encryption' blade is selected. Under 'Encryption selection', 'Customer-managed keys' is selected. In the 'Encryption type' section, 'Customer-managed keys' is also selected. A note states: '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 also enabled on the key vault and cannot be disabled.' The 'Save' button at the bottom left is highlighted with a green box.

## 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 <b>admaterials</b> storage account page, select <b>Microsoft Defender for Cloud</b> under <i>the Security + Networking</i> blade, and click on the <b>Enable on storage account</b> 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

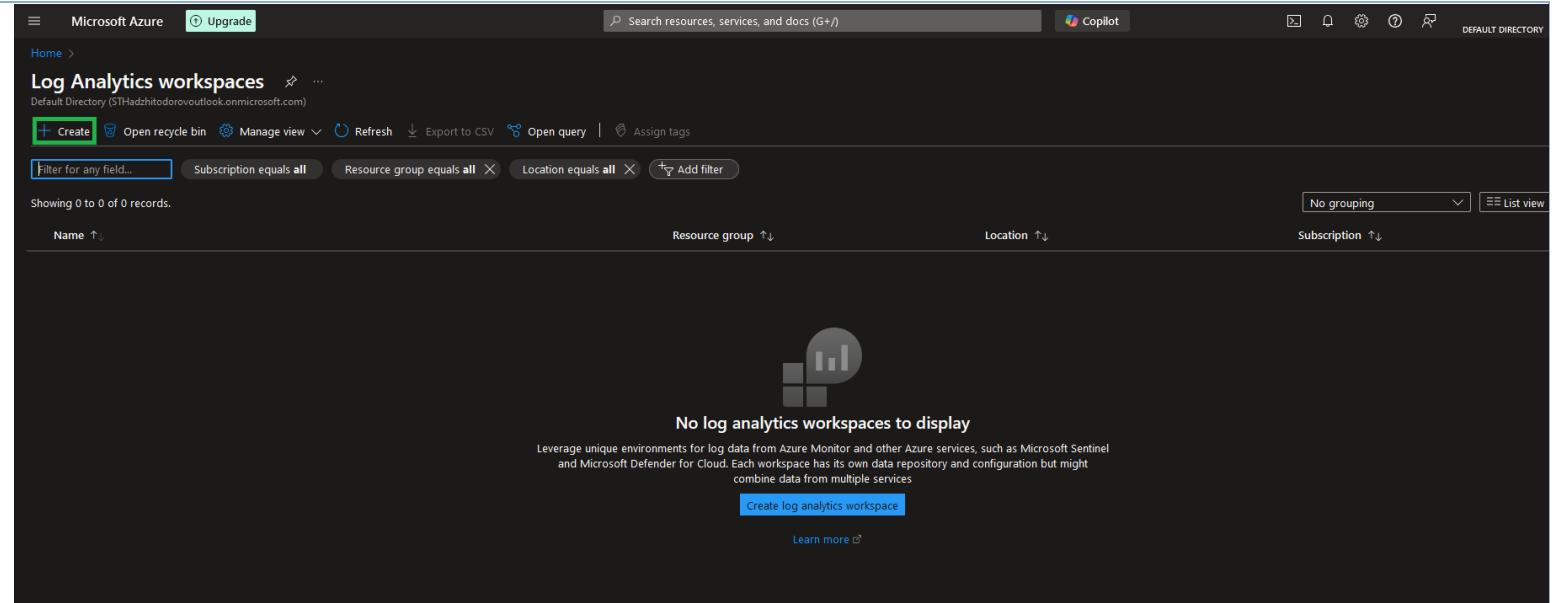
[View all recommendations in Defender for Cloud](#)

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

The screenshot shows the Microsoft Azure portal interface for a storage account named 'admaterials'. The left sidebar lists various services like Overview, Activity log, Tags, and Microsoft Defender for Cloud, which is highlighted. The main content area displays the 'Microsoft Defender for Storage' section. It shows that Defender is 'On' and enabled on the storage account. A green box highlights this status. Below it, there's a list of features: Activity monitoring (log analysis based threat detection), Sensitive data threat detection, and On-upload malware scanning. To the right, there's a call-to-action button 'Enable Defender for Storage on entire subscription' with the note that it protects all existing and newly created storage accounts in the subscription. Under 'Recommendations', it says 'No recommendations to display'. In the 'Security incidents and alerts' section, it states that alerts are from the past 21 days and provides a link to check for alerts.

**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.

A screenshot of the Microsoft Azure 'Create Log Analytics workspace' wizard. The page title is 'Create Log Analytics workspace'. The 'Basics' tab is selected. A callout box at the top left says: '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](#)'.

The 'Project details' section asks to select a subscription and resource group. The 'Subscription' dropdown shows 'Azure subscription 1' and the 'Resource group' dropdown shows 'JewelPromo' with a 'Create new' option below it. Both are highlighted with a green box.

The 'Instance details' section asks for a 'Name' and 'Region'. The 'Name' dropdown shows 'JewelAnalytics' and the 'Region' dropdown shows 'West Europe'. Both are highlighted with a green box.

At the bottom, there are three buttons: 'Review + Create' (highlighted with a green box), '< Previous', and '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

DEFAULT DIRECTORY

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	<input type="radio"/> Disabled
blob	Storage account	JewelPromo	<input type="radio"/> Disabled
queue	Storage account	JewelPromo	<input type="radio"/> Disabled
table	Storage account	JewelPromo	<input type="radio"/> Disabled
file	Storage account	JewelPromo	<input type="radio"/> Disabled

admaterials

Static website

Lifecycle management

Azure AI Search

Settings

- Configuration
- Data Lake Gen2 upgrade
- Resource sharing (CORS)
- Advisor recommendations
- Endpoints
- Locks

Monitoring

- Insights
- Alerts
- Metrics
- Workbooks
- Diagnostic settings
- Logs

Monitoring (classic)

- Metrics (classic)
- Diagnostic settings (classic)
- Usage (classic)

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

The screenshot shows the Microsoft Azure Diagnostic settings page for a Storage account named 'admaterials'. The left sidebar includes options like Azure AI Search, Settings, Configuration, Data Lake Gen2 upgrade, Resource sharing (CORS), Advisor recommendations, Endpoints, Locks, Monitoring (with Insights, Alerts, Metrics, Workbooks, Diagnostic settings selected, and Logs), and Logs. The main area displays filter settings: Subscription (Azure subscription 1), Resource group (JewelPromo), Resource type (Storage accounts), and Resource (admaterials). A table titled 'Diagnostic settings' shows 'No diagnostic settings defined'. A green box highlights the '+ Add diagnostic setting' button. Below the table, instructions say 'Click 'Add Diagnostic setting' above to configure the collection of the following data:' followed by a bullet point '• Transaction'.

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

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

The screenshot shows the Microsoft Azure Diagnostic settings page. At the top, there are navigation links for 'Home', 'admaterials | Diagnostic settings', and a 'Diagnostic setting' card. Below the header, there are buttons for 'Save', 'Discard', 'Delete', and 'Feedback'. A note about platform metrics collection is displayed. The main form has a 'Diagnostic setting name' field set to 'AdStorageMonitor' and a 'Metrics' section containing a checked checkbox for 'Transaction'. On the right, under 'Destination details', a checked checkbox for 'Send to Log Analytics workspace' is highlighted with a green box. Other destination options like 'Subscription', 'Log Analytics workspace', and 'Archive to a storage account' are listed below it.

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.

The screenshot shows the Microsoft Azure Diagnostic settings page for the 'admaterials' storage account. The left sidebar includes options like Configuration, Data Lake Gen2 upgrade, Resource sharing (CORS), Advisor recommendations, Endpoints, Locks, Monitoring (Insights, Alerts, Metrics, Workbooks), Diagnostic settings, and Logs. The main area displays a table of diagnostic settings:

Name	Storage account	Event hub	Log Analytics workspace	Partner solution	Edit setting
AdStorageMonitor	-	-	JewelAnalytics	-	<b>Edit setting</b>

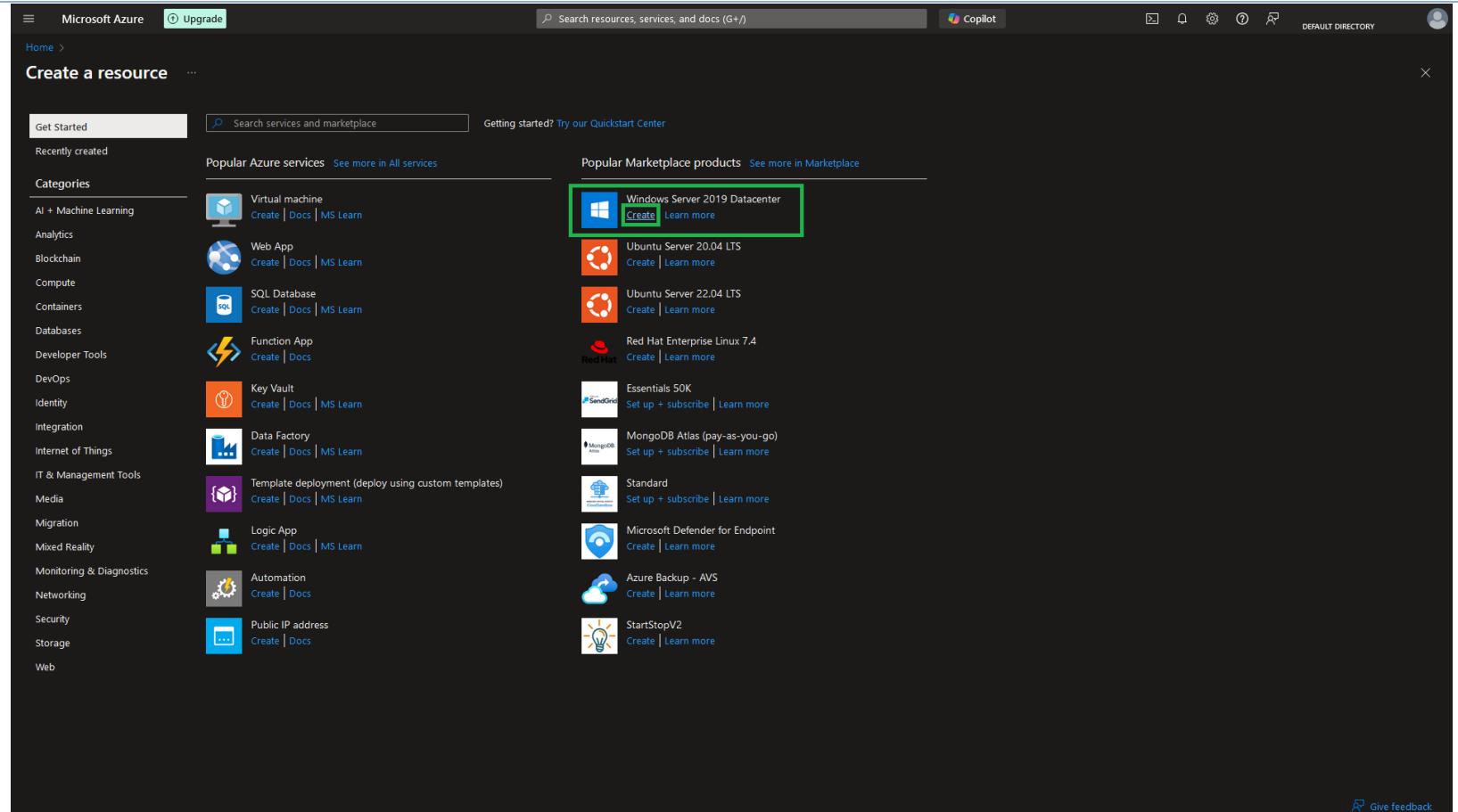
A tooltip for the 'Edit setting' button states: 'Click 'Add Diagnostic setting' above to configure the collection of the following data:

- Transaction

'.

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

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



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 <b>JewelPromo</b> .
Virtual machine name	Enter a unique VM name, such as <b>CampaignVM</b> .
Region	Select the same region as our other resources
Availability options	Select <b>Availability zone</b> .
Availability zone	Select <b>Zones 1</b> .

The screenshot shows the 'Create a virtual machine' wizard in Microsoft Azure, specifically the 'Basics' tab. The interface is dark-themed.

**Project details:**

- Subscription: Azure subscription 1
- Resource group: JewelPromo (selected)
- Virtual machine name: CampaignVM
- Region: (Europe) West Europe
- Availability options:
  - Zone options: Self-selected zone (selected)
  - Availability zone: Zone 1
- Security type: Trusted launch virtual machines
- Image: Windows Server 2019 Datacenter - x64 Gen2

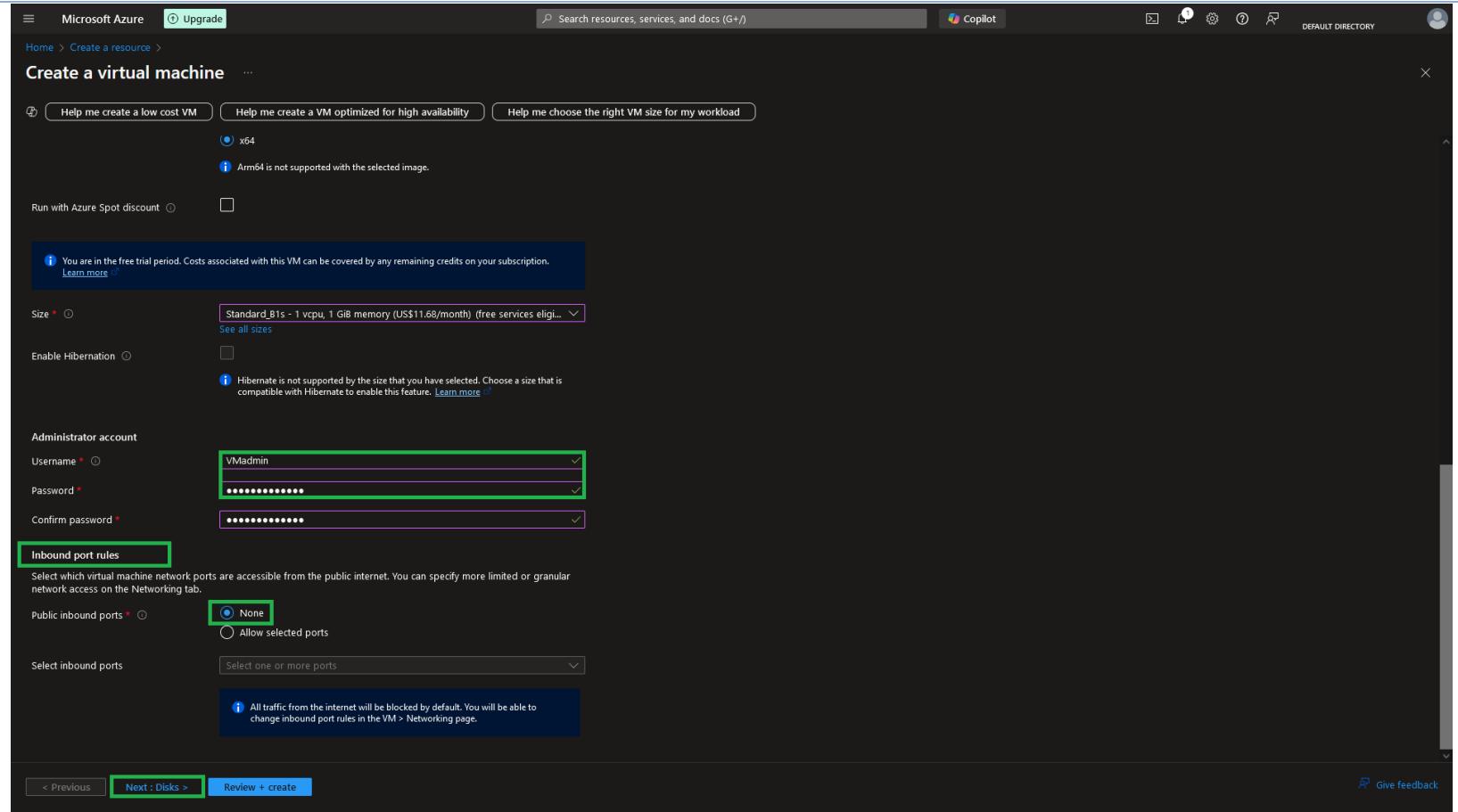
A green box highlights the 'Subscription' and 'Resource group' fields, and a purple box highlights the 'Virtual machine name' field.

**Bottom navigation:**

- < Previous
- Next : Disks >
- Review + create

**Feedback:** 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**.

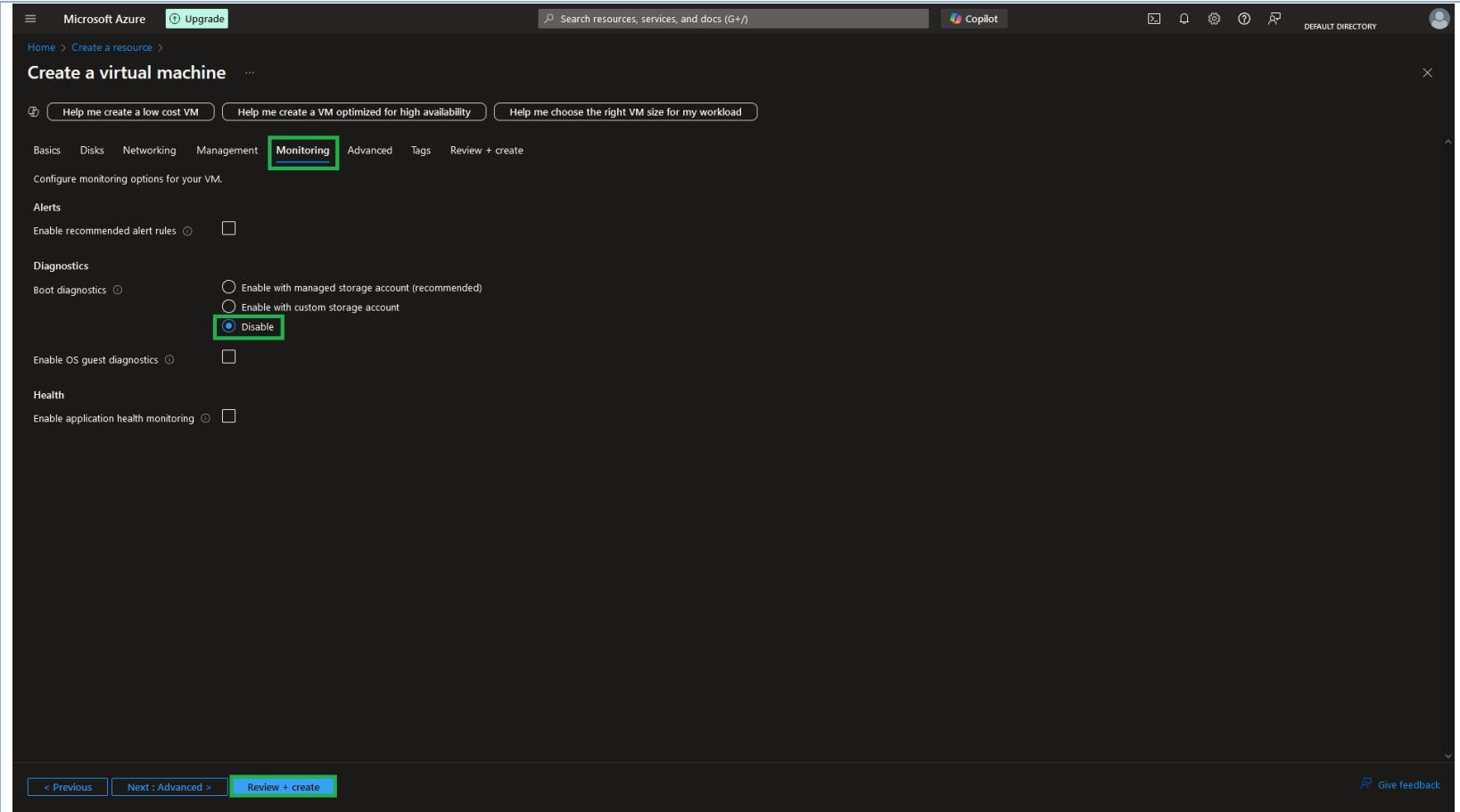


5. On the **Disks** tab, we retain the default settings, and select **Next: Networking**.
6. On the **Networking** tab, under the **Network interface** section, we specify the following information and click on **Next: Management**:

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

The screenshot shows the 'Create a virtual machine' wizard in Microsoft Azure, specifically the 'Networking' tab. A green box highlights the 'Virtual network', 'Subnet', and 'Public IP' fields, which are all set to '(new) CampaignVM-vnet', '(new) default (10.0.0.0/24)', and '(new) CampaignVM-ip' respectively. Below these, under 'NIC network security group', the 'Basic' radio button is selected. Under 'Public inbound ports', the 'None' radio button is selected. A note at the bottom of this section states: 'All traffic from the internet will be blocked by default. You will be able to change inbound port rules in the VM > Networking page.' Other options like 'Delete public IP and NIC when VM is deleted' and 'Enable accelerated networking' are shown with their respective checkboxes.

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



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

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

**CampaignVM** Virtual machine

**Essentials**

- 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
- 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

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

**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 ( <a href="#">edit</a> )	1
--	---

**Networking**

Public IP address	<a href="#">172.201.216.151</a> ( Network interface <a href="#">campaignvm984_z1</a> )
Public IP address (IPv6)	-
Private IP address	10.0.0.4
Private IP address (IPv6)	-
Virtual network/subnet	<a href="#">CampaignVM-vnet/default</a>
DNS name	<a href="#">Configure</a>

**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	<a href="#">CampaignVM_OsDisk_1_c9ba37df9eb34d6fb4cea29203fc1d1</a>
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.

The screenshot shows the Microsoft Azure portal interface for a virtual machine named 'CampaignVM'. The left sidebar contains navigation links for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Connect (highlighted with a green box), Bastion, Windows Admin Center, Networking (highlighted with a yellow box), Network settings, Load balancing, Application security groups, Network manager, Settings, Disks, Extensions + applications, Operating system, Configuration, Advisor recommendations, Properties, Locks, Availability + scale, Size, Availability + scaling, and Security. The main content area displays connection information: Connecting using Public IP address 172.20.0.1, Admin username VMadmin, Port 3389, and Just-in-time policy Unsupported by plan. It also shows a 'Native RDP' section with a 'Select' button and a 'Download RDP file' button. A 'More Options' dropdown menu is open, with 'Add incoming NSG port rule' highlighted with a green box. The top right corner includes a search bar, Copilot, and various account and directory management icons.

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

The screenshot shows the Microsoft Azure portal interface. On the left, the navigation menu includes Home, CampaignVM, Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Connect (selected), Bastion, Windows Admin Center, Networking (selected), Network settings, Load balancing, Application security groups, Network manager, Settings (selected), Disks, Extensions + applications, Operating system, Configuration, Advisor recommendations, Properties, Locks, Availability + scale, Size, Availability + scaling, Security, and Identity.

In the center, the main content area displays the details for the virtual machine "CampaignVM". It shows the connection status: "Connecting using Public IP address | 172.201.216.151". Below this, it lists the Admin username (VMadmin), Port (3389), and Just-in-time policy (Unsupported by plan). Under "Most common", there is a "Native RDP" section with a "Local machine" button and a "Public IP address (172.201.216.151)" link. At the bottom of this section, there are "Select" and "Download RDP file" buttons.

To the right, a modal dialog titled "Add inbound security rule" is open. The configuration is as follows:

- Source:** Any
- Source port ranges:** \*
- Destination:** Any
- Service:** Custom
- Destination port ranges:** 3389
- Protocol:** Any (radio button selected)
- Action:** Allow (radio button selected)
- Priority:** 310
- Name:** AllowAnyCustom3389Inbound
- Description:** (empty)

At the bottom of the dialog are "Add" and "Cancel" buttons.

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

The screenshot shows the Microsoft Azure portal interface for a virtual machine named 'CampaignVM'. The left sidebar has a green highlight over the 'Network settings' option under the 'Networking' section. The main content area displays the 'Network interface / IP configuration' for 'campaignvm984\_z1 (primary) / ipconfig1 (primary)'. It shows basic network details like the network interface, virtual network, and IP addresses. Below this, the 'Rules' section is expanded, showing 'Inbound port rules (4)' and 'Outbound port rules (3)'. A specific rule is highlighted with a green border: '310 AllowAnyCustom3389/inbound' with port 3389, protocol Any, source Any, destination Any, and action Allow.

Priority ↑	Name	Port	Protocol	Source	Destination	Action
310	AllowAnyCustom3389/inbound	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

**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.

# 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

Network settings

Load balancing

Application security groups

Network manager

Settings

Disks

Extensions + applications

Operating system

Configuration

Connecting using

Public IP address | 172.201.216.151

Admin username : VMadmin

Port (change) : 3389 Check access ⓘ

Just-in-time policy : Unsupported by plan ⓘ

## Most common



Local machine

### Native RDP

Connect via native RDP without any additional software needed. Recommended for testing only.

Public IP address (172.201.216.151)

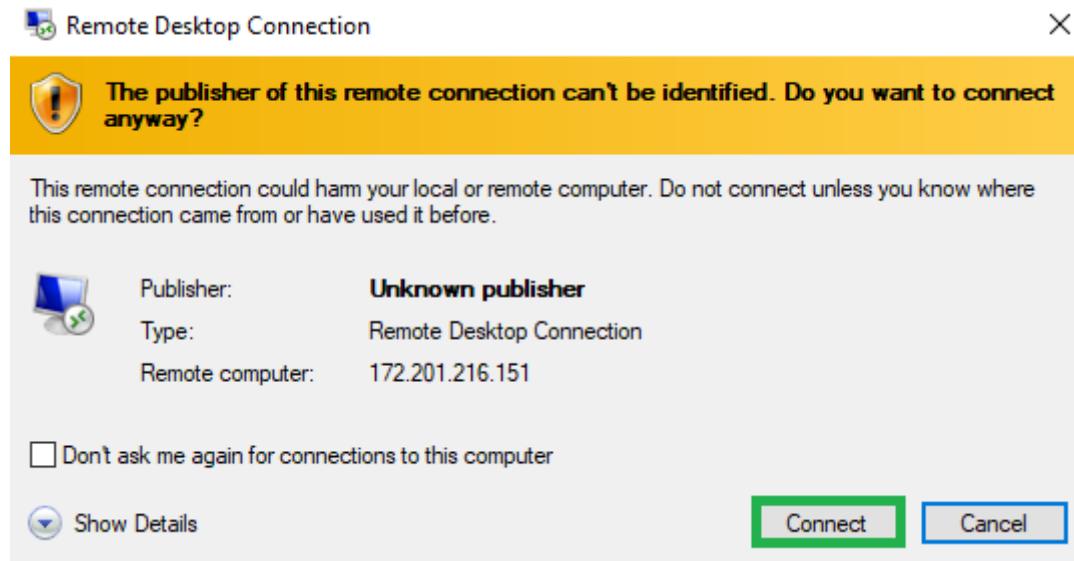
Select

Download RDP file

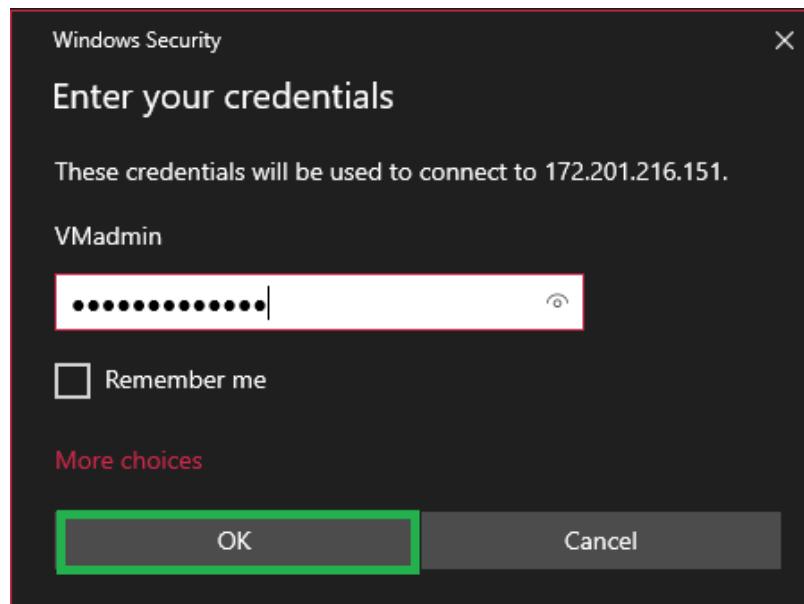


More ways to connect (4)

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



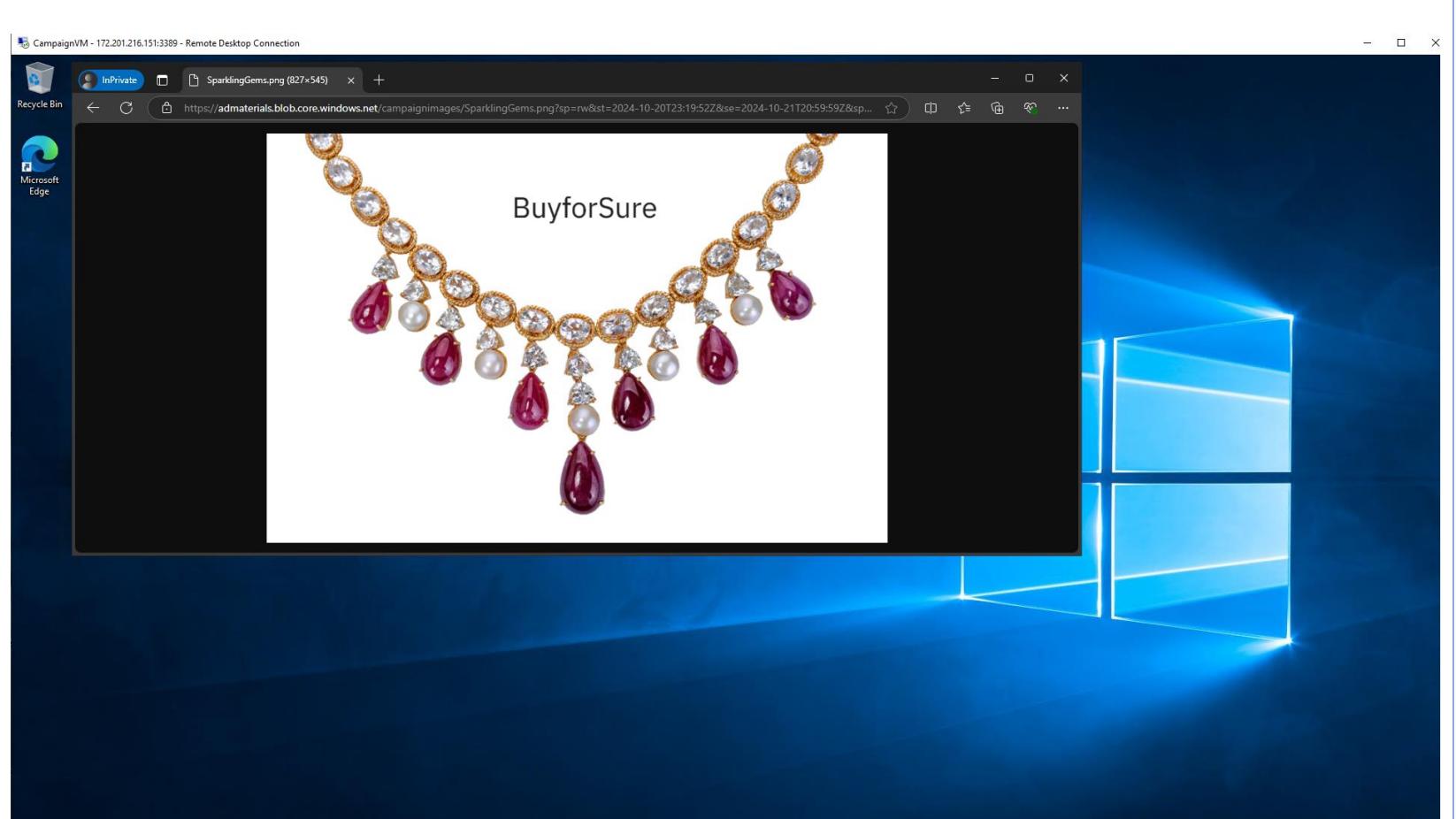
3. Then, on the **Enter your credentials** pop-up window, enter the **Username** and **Password**, and select **OK**.



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



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



**Activity 4:** Access the image as a sales team member using the Blob SAS URL.

1. We first log in using the credentials of one of our three test users, for example, **AlexSmith**, and go to the **Virtual Machines** page.

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the Microsoft Azure logo, a search bar with placeholder text 'Search resources, services, and docs (G+)', a Copilot icon, and user account information for 'AlexSmith1@DEFAULT DIRECTORY'. Below the header, the 'Virtual machines' section is displayed under 'Default Directory'. The page title is 'Virtual machines' with a back arrow and three dots for more options. A toolbar above the table includes buttons for '+ Create', 'Switch to classic', 'Reservations', 'Manage view', 'Refresh', 'Export to CSV', 'Open query', 'Assign tags', 'Start', 'Restart', 'Stop', 'Delete', 'Services', and 'Maintenance'. Filter options at the top of the table allow filtering by 'Subscription equals all', 'Type equals all', 'Resource group equals all', 'Location equals all', and an 'Add filter' button. The table displays one record: 'CampaignVM'. The columns are: Name (with a checkbox), Subscription, Resource group, Location, Status, Operating system, Size, Public IP address, and Disks. The 'Name' column is sorted in ascending order. The 'CampaignVM' row is highlighted with a green background. At the bottom of the table, there are navigation links for '< Previous', 'Page 1 of 1', and 'Next >'. On the far right, there is a 'Give feedback' link.

Name	Subscription	Resource group	Location	Status	Operating system	Size	Public IP address	Disks
CampaignVM	Azure subscription 1	JewelPromo	West Europe	Running	Windows	Standard_B1s	172.0.216.151	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

Virtual machines > CampaignVM

Virtual machines

Default Directory

+ Create Switch to classic ...

Filter for any field...

Name: CampaignVM

Access control (IAM)

Tags

Diagnose and solve problems

> Connect

> Networking

> Settings

> Availability + scale

> Security

> Backup + disaster recovery

> Operations

> Monitoring

> Automation

> Help

Search

Connect

Start

Restart

Stop

Hibernate

Capture

Delete

Refresh

Open in mobile

Feedback

CLI / PS

JSON View

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

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

Tags (edit) : Add tags

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

Networking

Public IP address : 172.201.216.151 (Network interface campaignvm984\_z1)

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\_c9ba37df9eb34d6fb4cea29203fc1d1

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

Home > Virtual machines > CampaignVM

CampaignVM | Connect

Virtual machines

Default Directory

+ Create ⚙ Switch to classic ⚙

Filter for any field...

Name ↑

CampaignVM ...

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Connect

Bastion

Windows Admin Center

Networking

Settings

Availability + scale

Security

Backup + disaster recovery

Operations

Monitoring

Automation

Help

Search resources, services, and docs (G+)

Copilot

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 : 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.

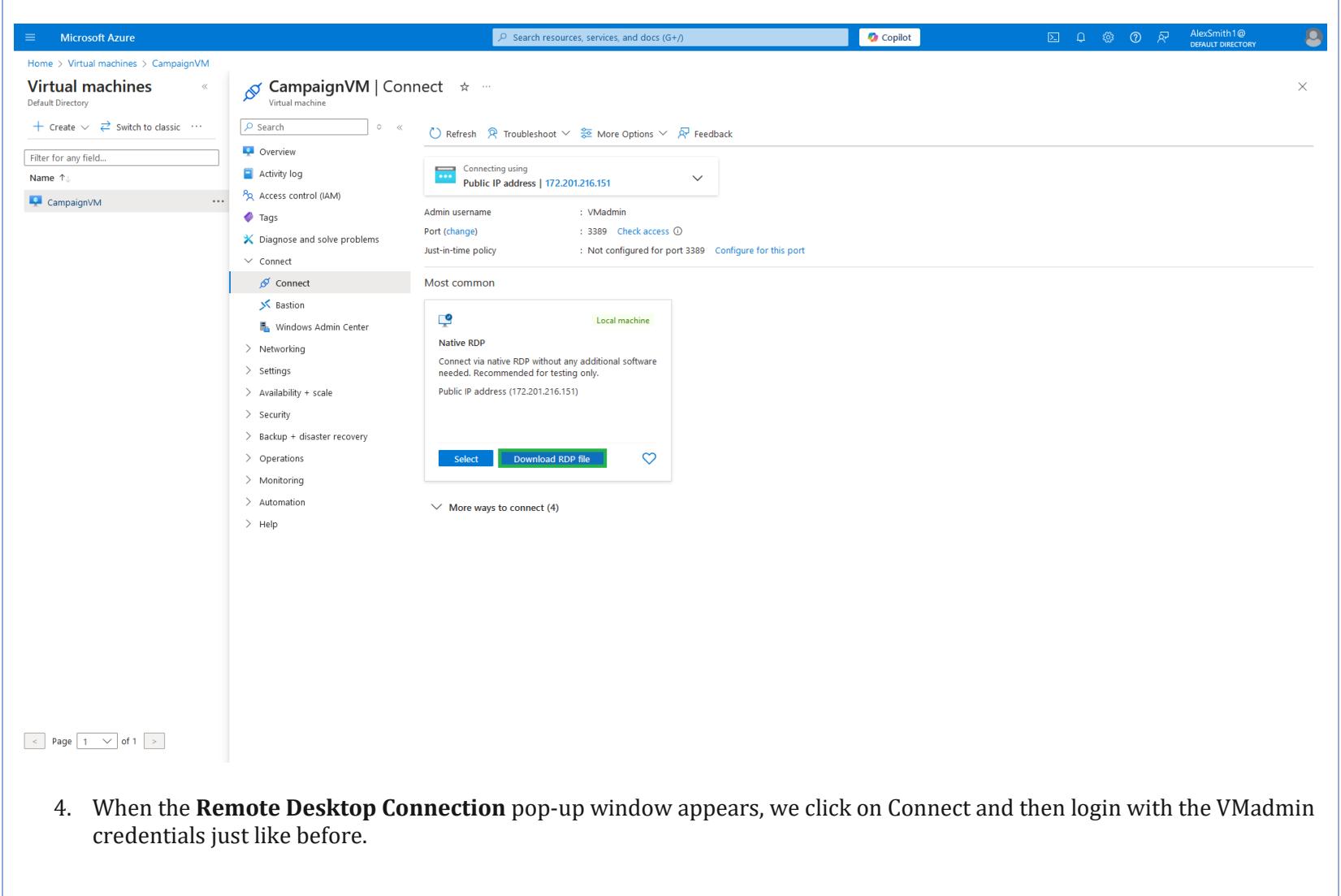
Public IP address (172.201.216.151)

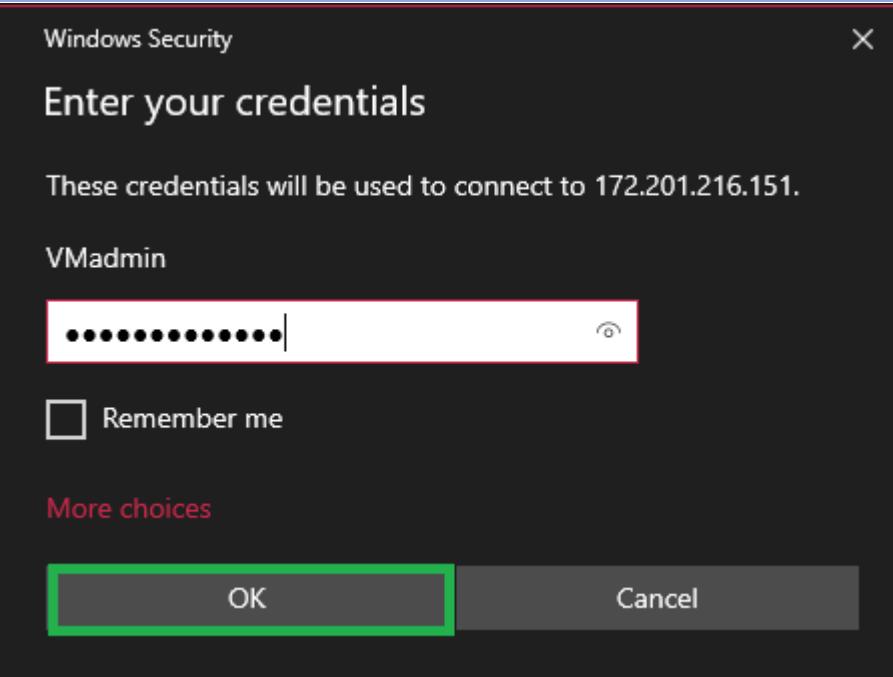
Select Download RDP file

More ways to connect (4)

< Page 1 >

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.

