



**ENDPOINT  
PROTECTOR**

| by CoSoSys

# Cloud Services

## User Manual



Version 5.0

Date 11.11.2022

## Table of Contents

Document Changelog	1
1. Introduction	2
2. Amazon Web Services	3
2.1. Obtain the Endpoint Protector AMI	3
2.2. Launch the EC2 image	4
2.2.1. Request an Elastic IP	9
2.2.2. Secure your Instance	11
3. Google Cloud Platform	12
3.1. Obtain the Endpoint Protector GCP image	12
3.2. Download the image	12
3.3. Create a bucket	12
3.4. Import the image to the custom image list	14
3.5. Create an Endpoint Protector VM Instance	15
3.6. Request a Static IP	16
3.7. Create Firewall rules	17
4. Azure	19
4.1. Obtain the Endpoint Protector Azure VM	19
4.2. Create the Storage Account and Container	19
4.3. Create the disk	22
4.4. Create the Virtual Machine	24
5. Endpoint Protector Licensing	27
6. Disclaimer	28

# Document Changelog

Version	Date	Notes
1.0	2016	The document was created
2.0	2018	The document was updated
3.0	2019	The document was updated
4.0	27.05.2022	Chapters Amazon Web Services, Google Cloud Platform, and Azure were updated.
5.0	11.11.2022	The Azure chapter, Create the Storage Account and Container section were updated.

# 1. Introduction

This User Manual is intended to provide short guidance when using the Endpoint Protector Server in Amazon Web Services or Google Cloud Platform.

**Important:** This document is not intended as a step-by-step guide to creating an AWS or GCP account. The precondition to already having such accounts in place and understanding the bases of how these 3rd party services are the responsibility of each Administrator.

- **Amazon Web Services** - the Endpoint Protector AMI is provided as an Amazon EC2 instance
- **Google Cloud Platform** - the Endpoint Protector image is provided as a \*.tar.gz.
- **Azure** - the Endpoint Protector image will be uploaded into your account.

**Note:** For information related to the use of Endpoint Protector – main components, features, and functionality, please refer to the [Endpoint Protector User Manual](#).

# 2. Amazon Web Services

## 2.1. Obtain the Endpoint Protector AMI

Endpoint Protector is not generally available in the AWS Marketplace. To have access to the Amazon Machine Image (AMI), you need to contact your Endpoint Protector Representative directly or submit a request on our [website](#) by providing information such as the AWS Account no. and Region and Availability Zone.

You will receive a reply from an Endpoint Protector Representative, notifying you when the Endpoint Protector Amazon Machine Image has been shared with your account.

### A. Cloud Service



Endpoint Protector can be deployed using various cloud service providers such as Amazon Web Services (AWS), Microsoft Azure or Google Cloud Platform (GCP).

Note: Having a cloud account (e.g.: AWS, GCP) and understanding how these third-party services work is the responsibility of each company's Administrator.

For more details, please read the [Cloud Service User Manual](#).

### Request a server

Select your Cloud Service environment

- Amazon Web Services (AWS)
- Google Cloud Platform (GCP)
- Microsoft Azure

First Name\*

Last Name\*

Work Email\*

Work Phone Number\*

AWS Account Number

Region and availability zone

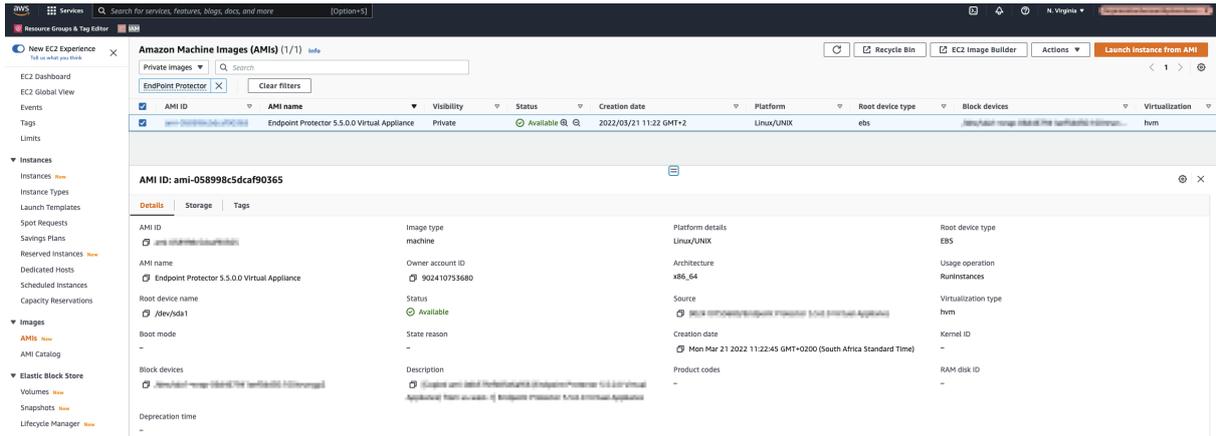
Request Server

## 2.2. Launch the EC2 image

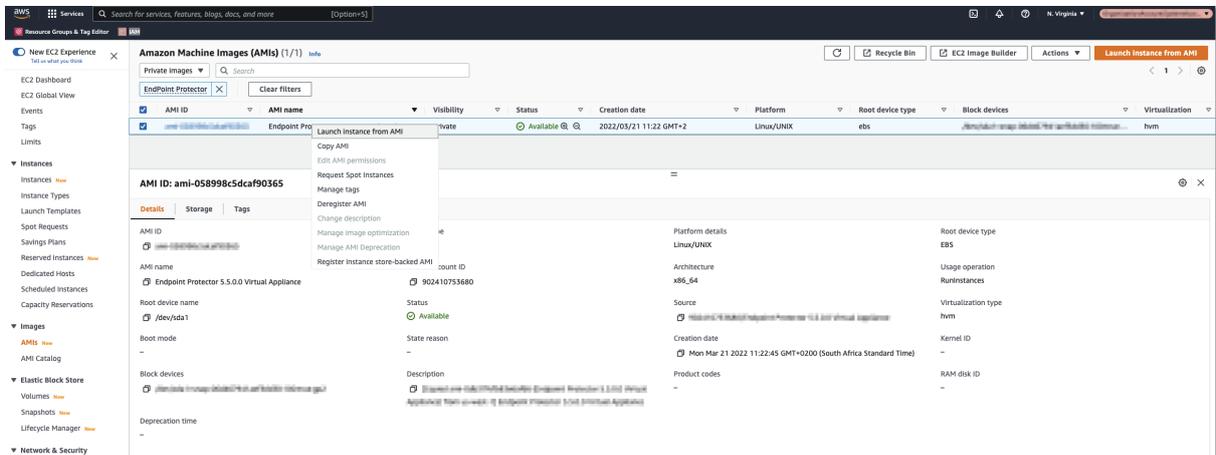
As the Endpoint Protector image has already been shared with you, this process is similar to any other EC2 launch.

To launch the EC2 image, follow these steps:

1. Go to **Services: EC2** and select your **region**
2. Go to **Images: AMIs** and select the type of the Private image and search for **Endpoint Protector**



### 3. Right-click and select **Launch Instance**



4. Enter the **Name** and **Create tags** as per your policies;

5. Select an **Instance Type**;

**Note:** For help in selecting the instance type that best fits your needs, contact [support@endpointprotector.com](mailto:support@endpointprotector.com).

6. Select an available **key pair** or create a **new key pair**;

If you select to use a key pair you might have to share it with our Support Team for support requests. In this case, ensure it is used only for this instance. We would recommend selecting the option **Proceed without a Key Pair** and then click **Launch Instances**.

**Launch an instance** [Info](#)

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

**Name and tags** [Info](#)

Name:  [Add additional tags](#)

**Application and OS Images (Amazon Machine Image)** [Info](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search our full catalog including 1000s of application and OS images

AMI from catalog | Recents | My AMIs | Quick Start

Amazon Machine Image (AMI)

Endpoint Protector 5.5.0.0 Virtual Appliance  
ami-058998c5dca90365

[Browse more AMIs](#)  
Including AMIs from AWS, Marketplace and the Community

Published	Architecture	Virtualization	Root device type	ENA Enabled
2022-03-21T09:22:45.000Z	x86_64	hvm	ebs	Yes

**Instance type** [Info](#)

Instance type:  [Compare instance types](#)

Family: t2 2 vCPU 4 GiB Memory  
On-Demand Linux pricing: 0.0464 USD per Hour  
On-Demand Windows pricing: 0.0644 USD per Hour

**Key pair (login)** [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

[Default value](#) [Create new key pair](#)

**Summary**

Number of Instances [Info](#):

Software Image (AMI): [Copied ami-0db37fefb83e6af66 ...read more] ami-058998c5dca90365

Virtual server type (instance type): t2.medium

Firewall (security group): New security group

Storage (volumes): 1 volume(s) - 100 GiB

**Free tier:** In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet

[Cancel](#) [Launch Instance](#)

7. Configure the **Network** section:

**▼ Network settings** Edit

Network  
vpc-01234567

Subnet  
subnet-01234567 (Default subnet in the availability zone)

Auto-assign public IP  
Enable

Security groups (Firewall) [Info](#)  
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

We'll create a new security group called 'launch-wizard-7' with the following rules:

- Allow SSH traffic from**  
Helps you connect to your instance Anywhere  
0.0.0.0/0
- Allow HTTPS traffic from the internet**  
To set up an endpoint, for example when creating a web server
- Allow HTTP traffic from the internet**  
To set up an endpoint, for example when creating a web server

**⚠ Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.** ✕

8. Edit Network Section and provide the following information:

- Select a **VPC** and a **Subnet**
- Enable the **Auto-assign public IP**
- Select **Create security group** and then provide a **name** and **description**
- **Remove** the existing Inbound rules
- **Add two new Inbound security group rules:**
  - Type **HTTPS**, Protocol **TCP**, Port range **443**, Source type **Custom**, Source 0.0.0.0/0 (**mandatory**)
  - Type **HTTP**, Protocol **TCP**, Port range **80**, Source type **Custom**, Source 0.0.0.0/0 (**optional**)

### ▼ Network settings

**VPC - required** [Info](#)

us-east-1
(default) ▼
↻

**Subnet** [Info](#)

us-east-1a
▼
↻
Create new subnet [↗](#)

**Auto-assign public IP** [Info](#)

Enable
▼

**Firewall (security groups)** [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group

Select existing security group

**Security group name - required**

My EPP Appliance

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and .\_-:/()#,@[]+=&;{}!\$\*

**Description - required** [Info](#)

My EPP Security Group

**Inbound security groups rules**

▼ Security group rule 1 (TCP, 443, 0.0.0.0/0, HTTPS)
Remove

<b>Type</b> <a href="#">Info</a>	<b>Protocol</b> <a href="#">Info</a>	<b>Port range</b> <a href="#">Info</a>
HTTPS ▼	TCP	443
<b>Source type</b> <a href="#">Info</a>	<b>Source</b> <a href="#">Info</a>	<b>Description - optional</b> <a href="#">Info</a>
Custom ▼	<input type="text" value="Add CIDR, prefix list or security group"/>	HTTPS
	<span style="border: 1px solid #0070c0; padding: 2px 5px;">0.0.0.0/0</span> <span style="color: #0070c0; font-size: 0.8em;">✕</span>	

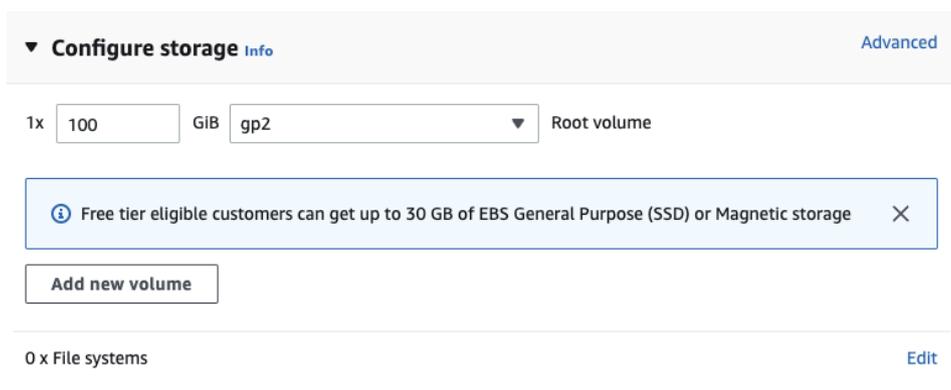
▼ Security group rule 2 (TCP, 80, 0.0.0.0/0, HTTP)
Remove

<b>Type</b> <a href="#">Info</a>	<b>Protocol</b> <a href="#">Info</a>	<b>Port range</b> <a href="#">Info</a>
HTTP ▼	TCP	80
<b>Source type</b> <a href="#">Info</a>	<b>Source</b> <a href="#">Info</a>	<b>Description - optional</b> <a href="#">Info</a>
Custom ▼	<input type="text" value="Add CIDR, prefix list or security group"/>	HTTP
	<span style="border: 1px solid #0070c0; padding: 2px 5px;">0.0.0.0/0</span> <span style="color: #0070c0; font-size: 0.8em;">✕</span>	

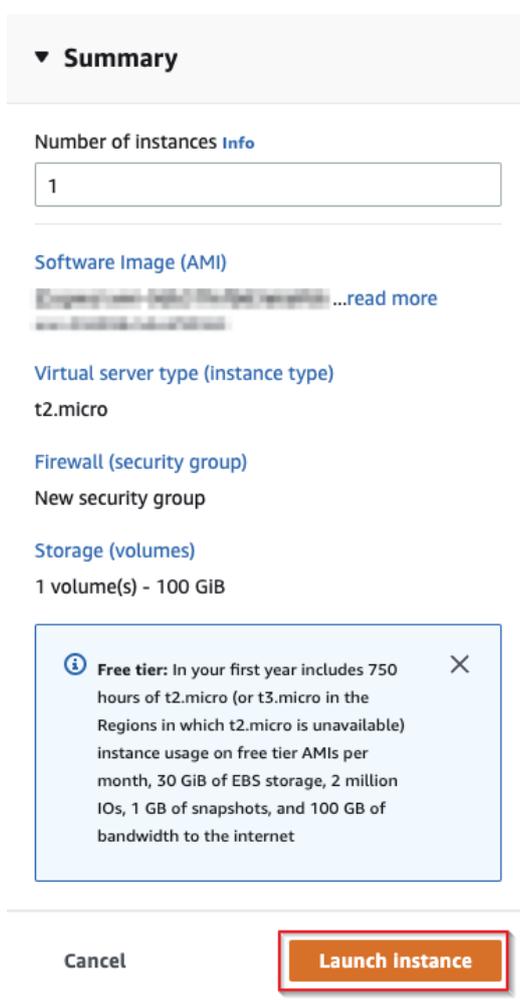
⚠
Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.
✕

Add security group rule

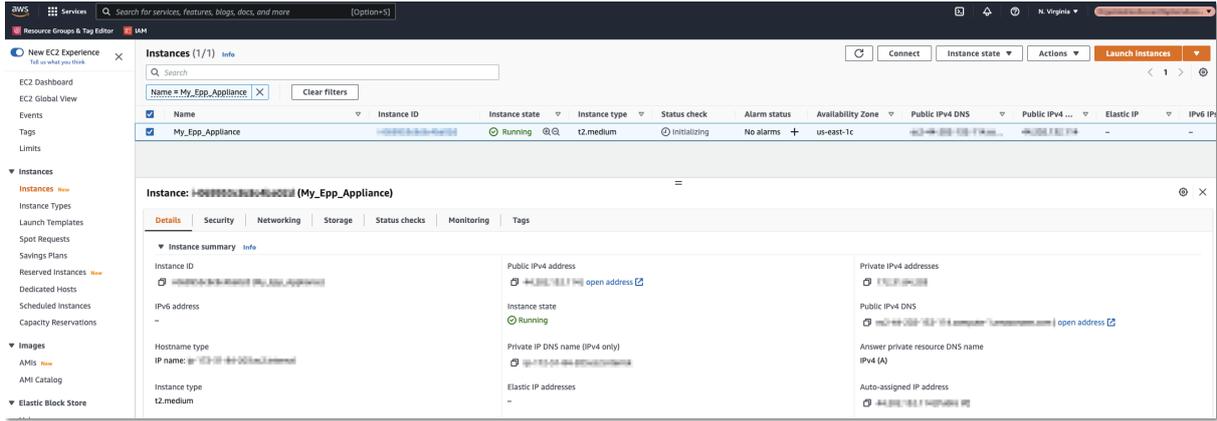
9. The **Storage** section does not require any changes;



10. On the **Summary** section click **Launch Instance**;



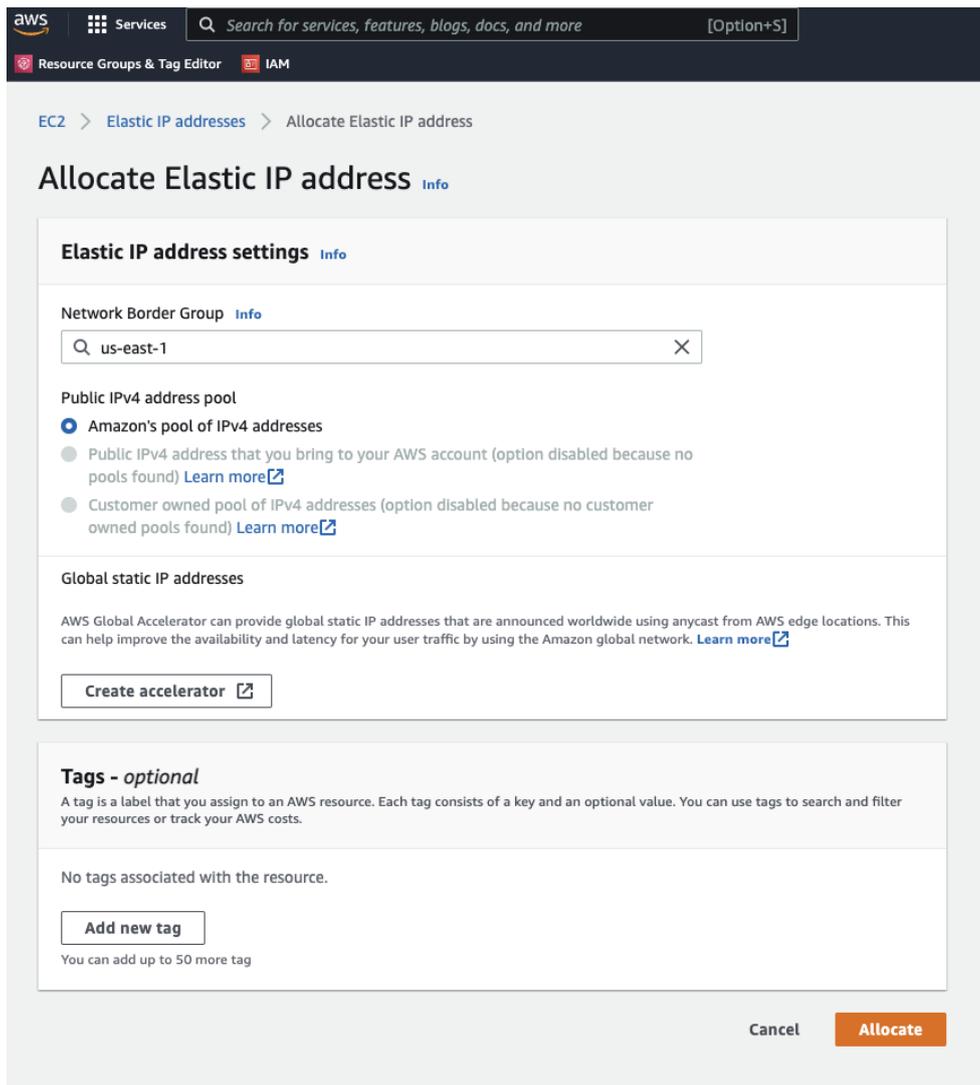
11. Wait for the instance to start - this might take a few minutes while the **Status Checks** appear as **Initializing**.



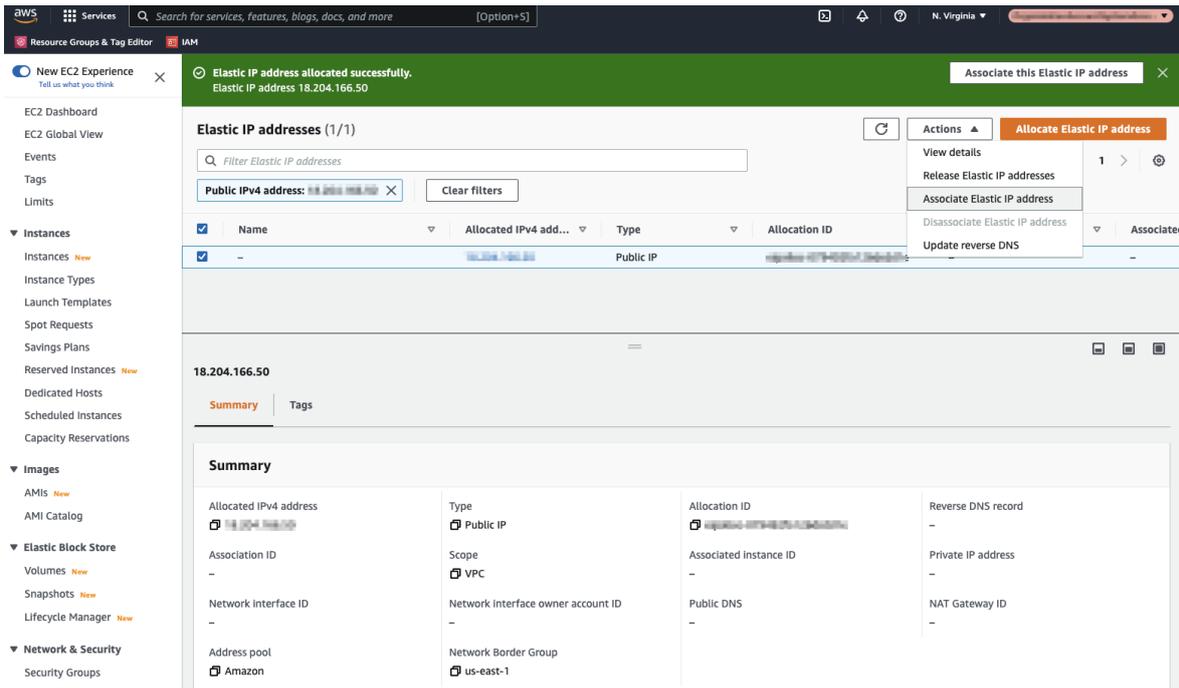
### 2.2.1. Request an Elastic IP

This step is required so the Endpoint Protector Clients can communicate with the same IP Address in case of an instance restart. Without an Elastic IP (Static IP) the instance will assign a new IP address every time it is restarted and the Endpoint Protector Clients have to be reinstalled.

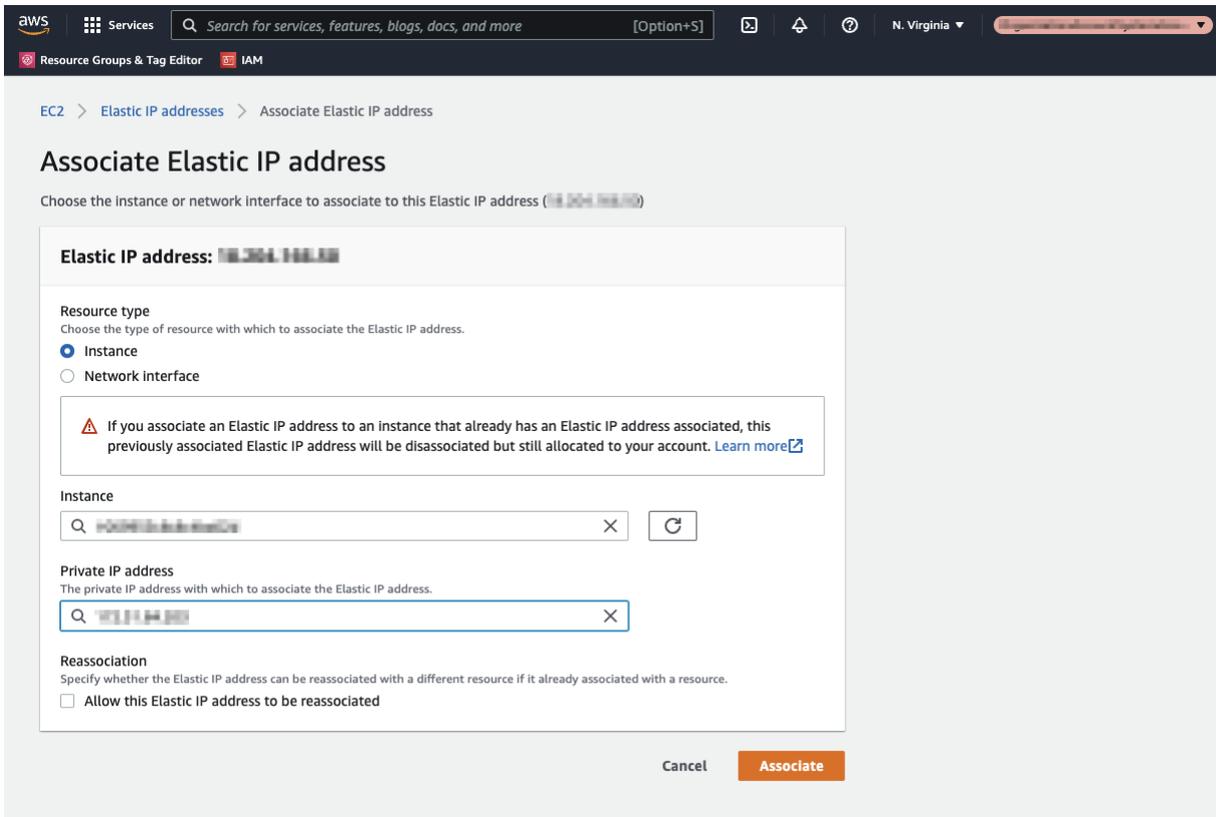
To request an Elastic IP, go in the AWS Management Console to the option **Network & Security**, **Elastic IPs**, and click **Allocate New Address**.



## 1. Associate the **Elastic IP** with your Endpoint Protector Instance.



## 2. Select the **Endpoint Protector Instance** from the dropdown list, the **Private IP address**, and then click **Associate**;



The Elastic IP is now associated with your Endpoint Protector Instance. After a few minutes, the Endpoint Protector Instance will be running associated with the Elastic IP.

### 2.2.2. Secure your Instance

We recommend further securing your Instance by making all possible settings in the AWS Interface under the option **Security Groups**.

# 3. Google Cloud Platform

## 3.1. Obtain the Endpoint Protector GCP image

Endpoint Protector is not available from the default images on the Google Cloud Platform. To obtain it, you will need to follow the process hereby described.

**Note:** This part of the process is similar to uploading any other custom image in the Console.

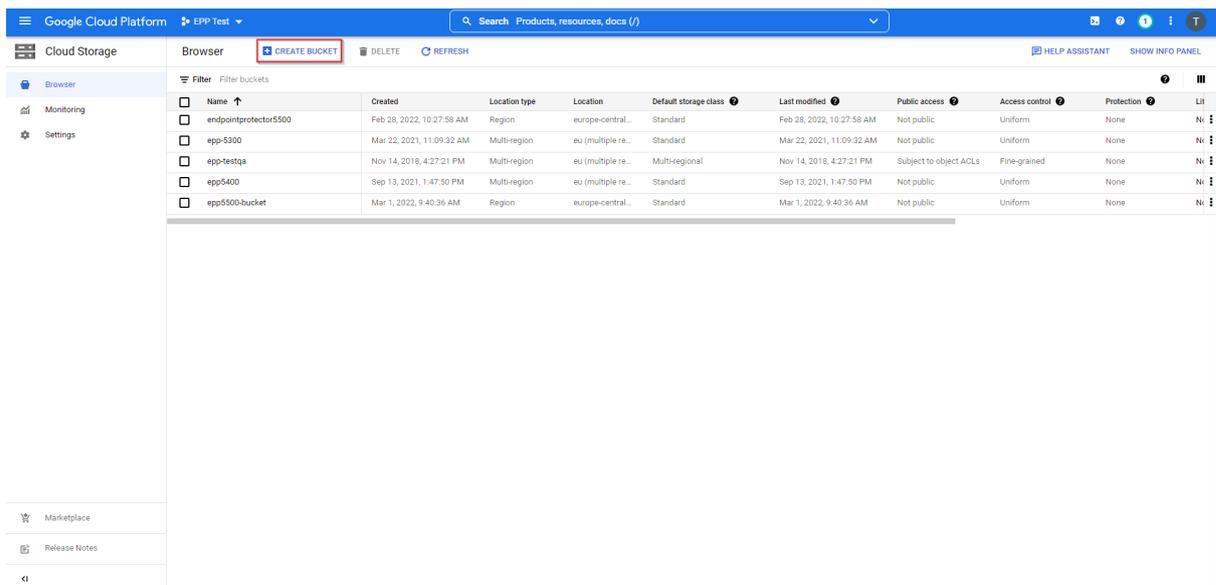
## 3.2. Download the image

The Endpoint Protector image can be downloaded from the link provided by your Endpoint Protector Representative. If this image has already been obtained, you can skip this step.

## 3.3. Create a bucket

To upload the Endpoint Protector image to the Google Cloud Platform, create a bucket:

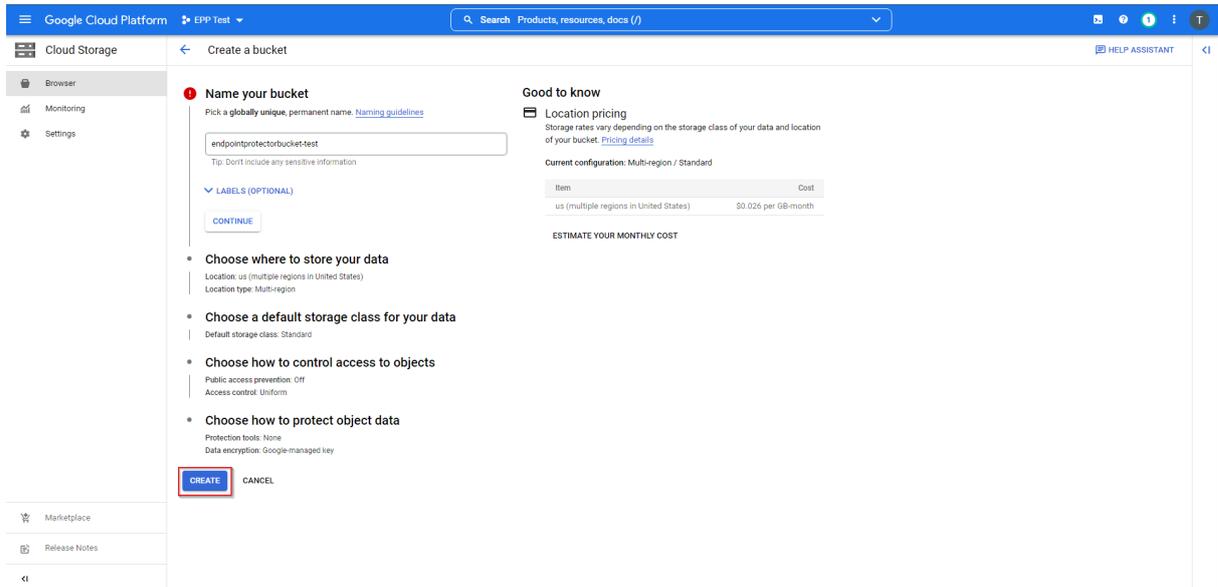
1. On the Google Cloud Platform Console, go to the [Cloud Storage Browser page](#) and click **Create bucket**;



2. To create a bucket, provide the following information and then click **Create**:

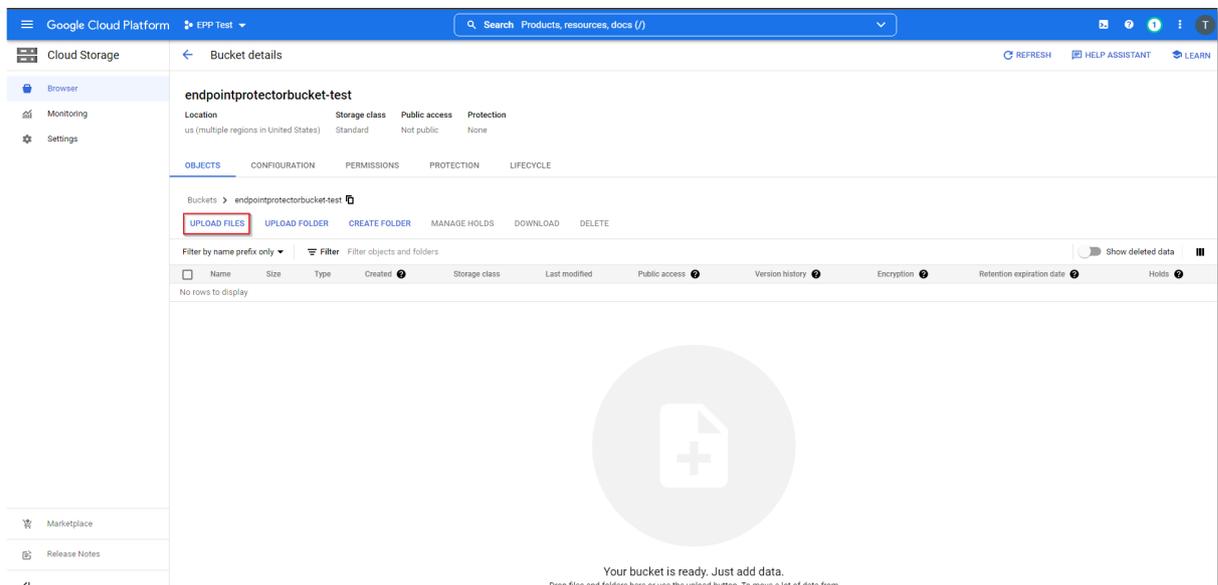
- **Name** – add a name for the bucket

- **Storage** – select the **standard** storage class
- **Location** – select a location to store the image



3. On the newly created **Bucket details** page, click **Upload files** and select the Endpoint Protector image file [received from Endpoint Protector](#).

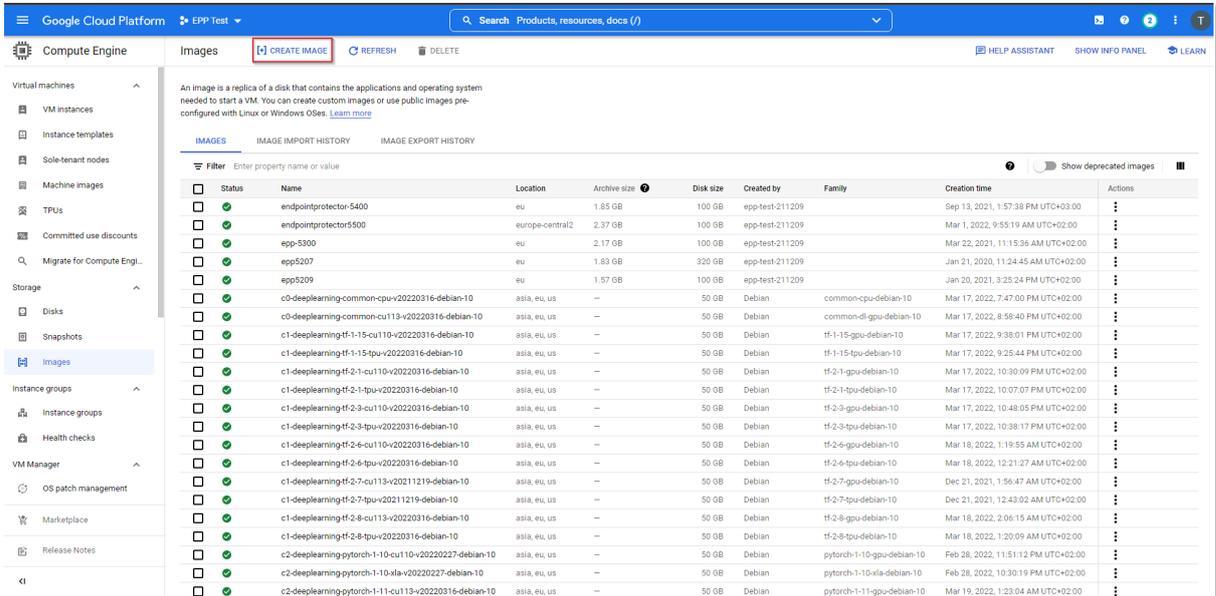
**Note:** Depending on the size of the compressed image and the speed of the network connection, the upload can take several hours.



### 3.4. Import the image to the custom image list

After the Endpoint Protector image has been uploaded to Google Cloud Storage, import the custom image list.

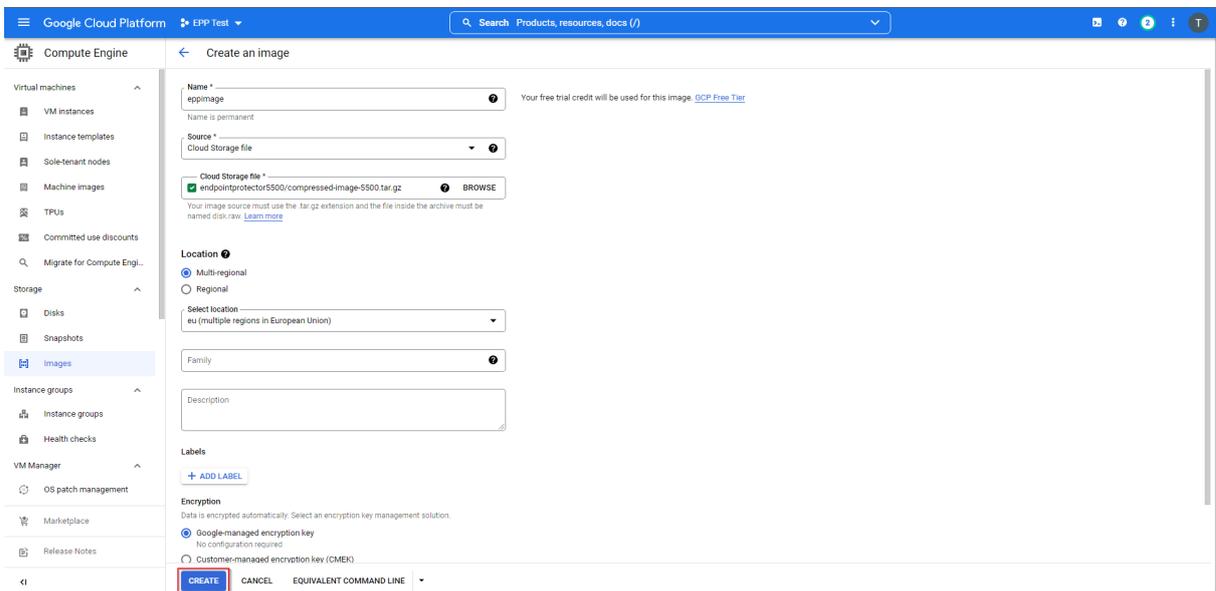
1. On the Google Cloud Platform Console, go to the **Image** page and click **Create image**;



2. To create the image, provide the following information and then click **Create**:

- **Name** – add a name for the image
- **Source** – select **Cloud Storage file**
- **Cloud Storage file** – upload the Endpoint Protector image file
- **Location** – select **Multi-regional**
- **Encryption** – select **Google-managed encryption key**

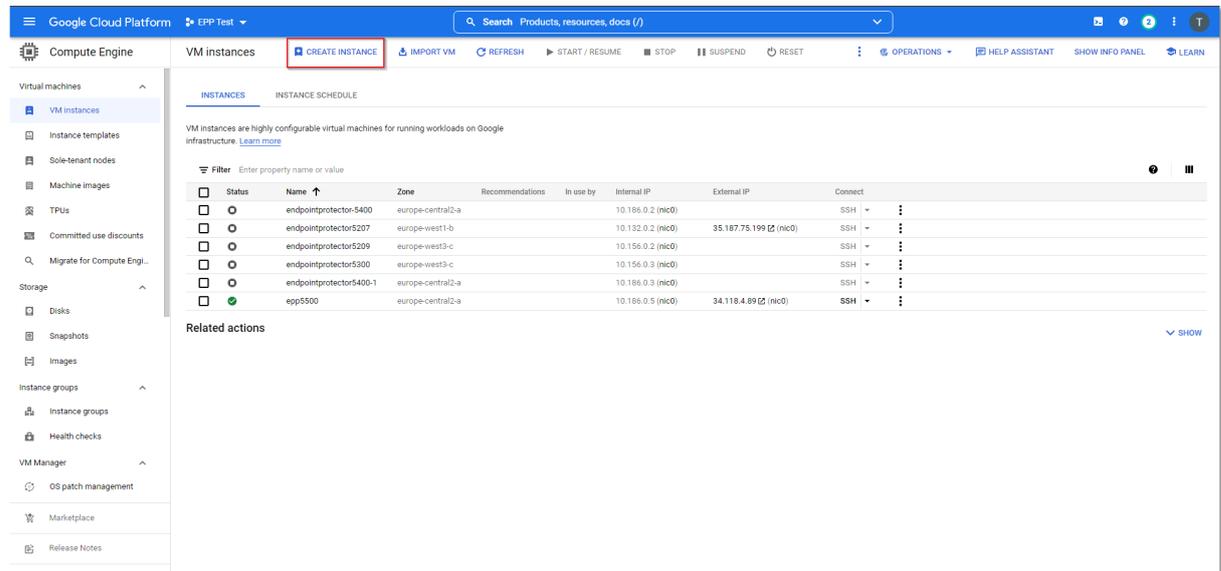
**Note:** The process can take several minutes depending on the size of the boot disk image.



## 3.5. Create an Endpoint Protector VM Instance

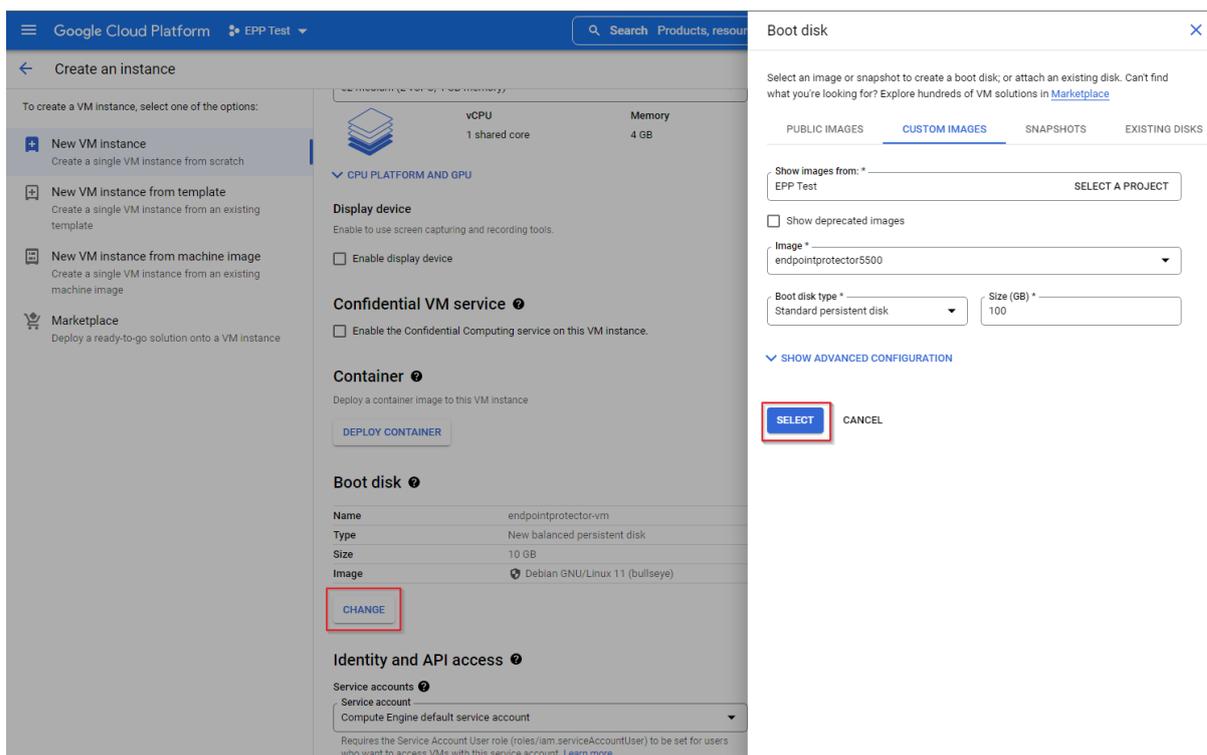
After the Endpoint Protector Image is available in the Google Cloud Platform images list, create a Virtual Machine Instance:

1. In the **Google Cloud Platform Console**, go to the **VM Instances** page and click **Create instance**;

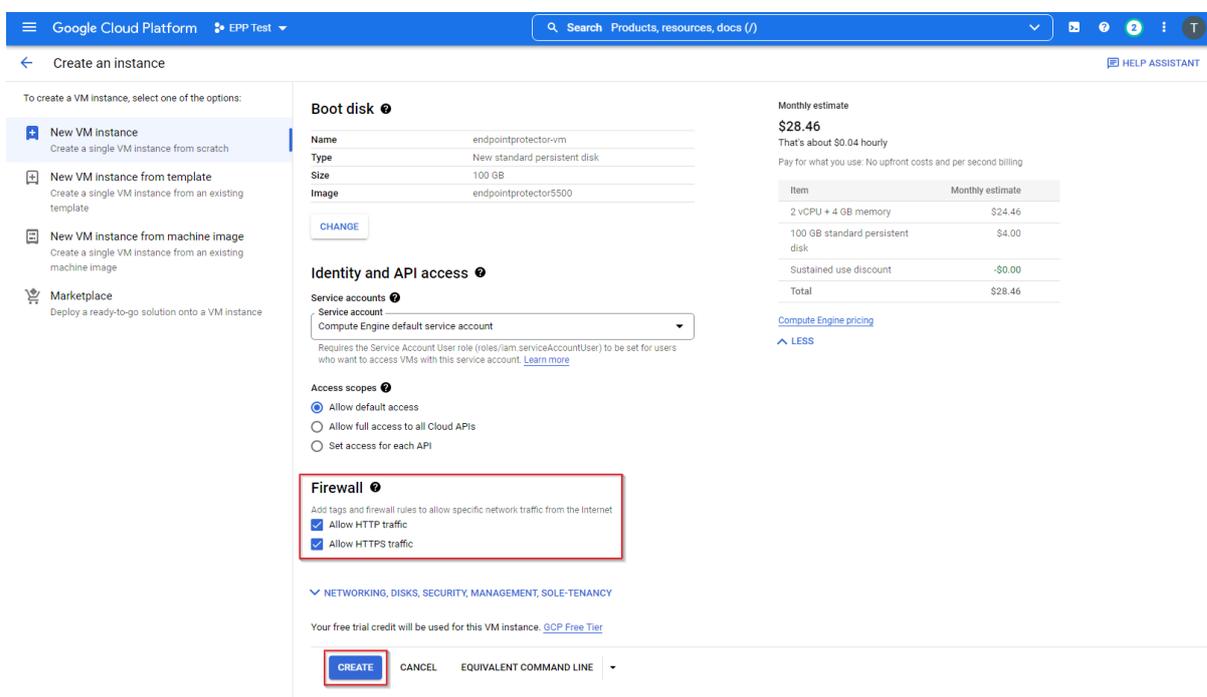


2. In the **Boot disk** section, click **Change** to begin configuring your boot disk and on the **Custom Images** tab, fill in the following:
  - **Image** - select the image you imported
  - **Boot disk type** - select **Standard persistent disk**
  - **Size** – add a size larger than the Endpoint Protector image size received

Click **Select** to confirm the boot disk configuration.



3. On the **Firewall** section, select **Allow HTTP traffic** and **Allow HTTPS traffic**, and then click **Create**.

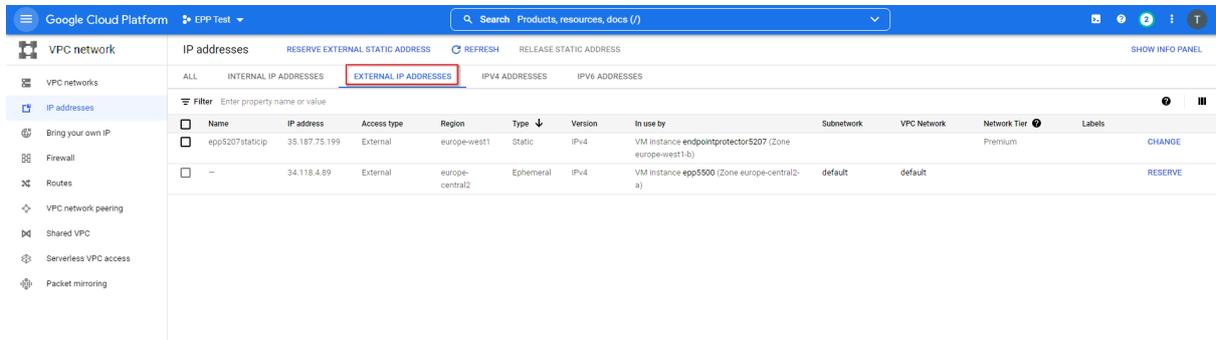


### 3.6. Request a Static IP

You will need to request a static IP so the Endpoint Protector Clients can communicate with the same IP Address in case of an instance restart.

Without a Static IP (Elastic IP) the instance will assign a new IP address every time it is restarted and the Endpoint Protector Clients have to be reinstalled.

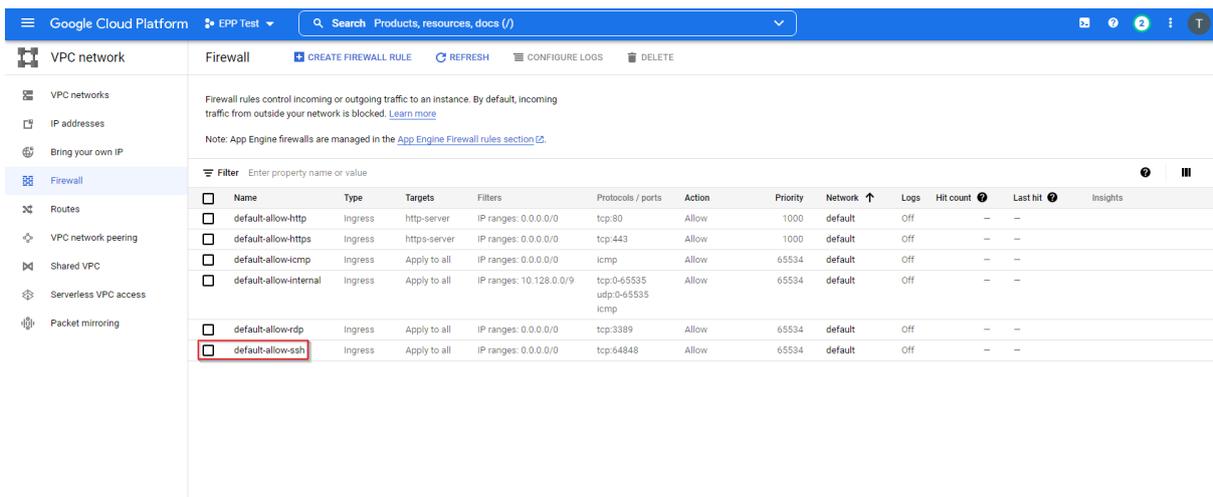
To request a Static IP, go to **IP addresses** and select the **External IP addresses** tab.



### 3.7. Create Firewall rules

To create a Firewall rule, on the Google Cloud Platform Console, follow these steps:

1. Go to the **Firewall** page and select **default-allow-ssh**;



2. Click **Edit** and on the **Protocols and ports** section provide the following information:

- select **Specified protocols and ports**
- check the **tcp** box and enter **64848**

The screenshot shows the Google Cloud Platform interface for editing a firewall rule named 'default-allow-ssh'. The 'EDIT' button is highlighted with a red box. The rule's description is 'Allow SSH from anywhere'. The priority is set to 65534. The direction is 'Ingress' and the action on match is 'Allow'. The target is 'All instances in the network'. The source filter is 'IPv4 ranges' with a source IP range of '0.0.0.0/0'. The protocols and ports section is also highlighted with a red box, showing 'Specified protocols and ports' selected, with 'tcp' checked and port '64848' specified. Other protocols like 'udp' and 'Other protocols' are not selected.

Google Cloud Platform EPP Test Search Products, resources, docs (/)

VPC network Firewall rule details EDIT DELETE

default-allow-ssh

Description  
Allow SSH from anywhere

Logs  
Turning on firewall logs can generate a large number of logs which can increase costs in Cloud Logging. [Learn more](#)  
 On  
 Off

Network  
default  
Priority \* 65534 CHECK PRIORITY OF OTHER FIREWALL RULES ⓘ  
Priority can be 0 - 65535

Direction  
Ingress

Action on match  
Allow

Targets  
All instances in the network

Source filter  
IPv4 ranges ⓘ

Source IPv4 ranges \*  
0.0.0.0/0 ⓘ for example, 0.0.0.0/0, 192.168.2.0/24 ⓘ

Second source filter  
None ⓘ

Protocols and ports ⓘ

Allow all  
 Specified protocols and ports

tcp: 64848

udp: all

Other protocols  
protocols, comma separated, e.g. ah, sctp

# 4. Azure

## 4.1. Obtain the Endpoint Protector Azure VM

Endpoint Protector is not generally available in the Azure Marketplace. To have access to the Virtual Machine, contact your Endpoint Protector Representative and provide information such as the access keys to a Container specifically created for the Endpoint Protector Virtual Machine.

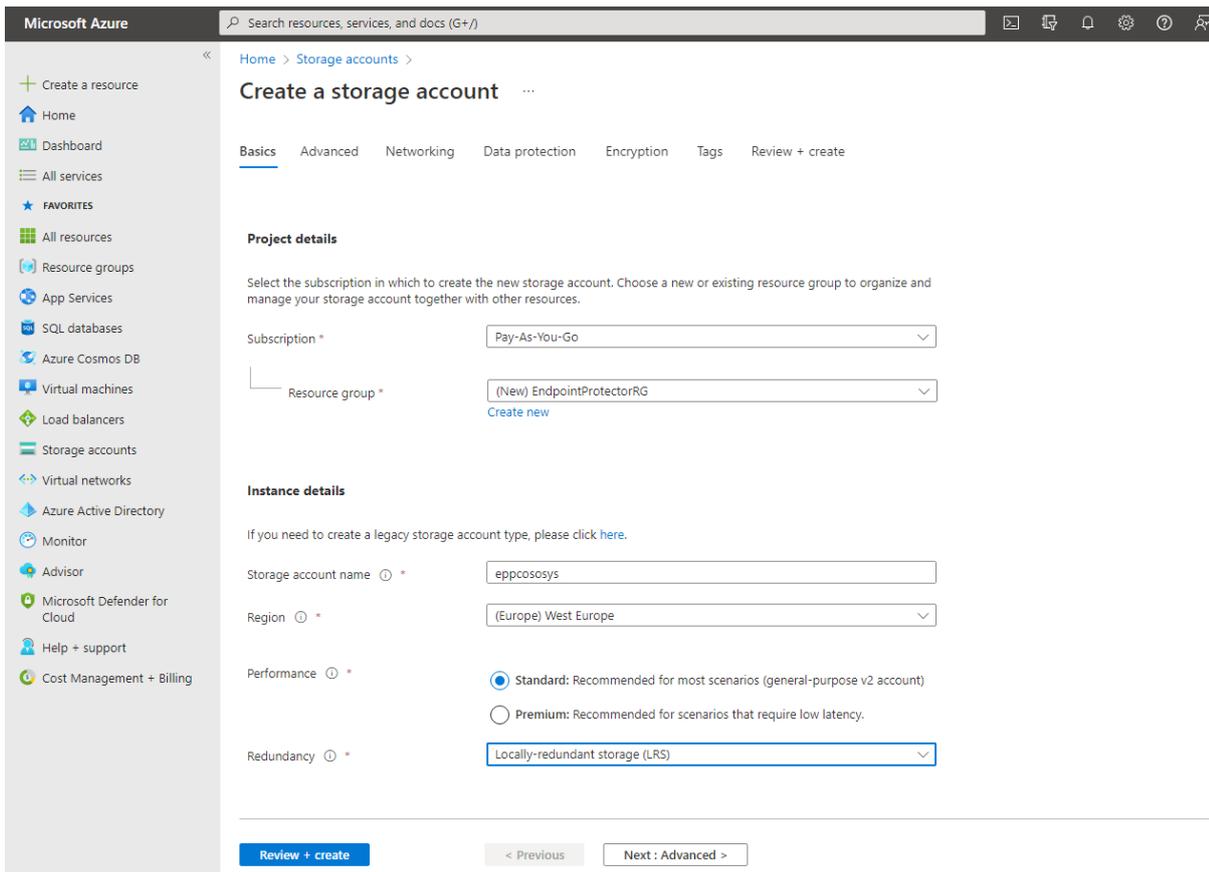
**Note:** We will upload the Endpoint Protector Virtual Machine to your Container as soon as possible. Once this step is done, we advise regenerating the access key.

## 4.2. Create the Storage Account and Container

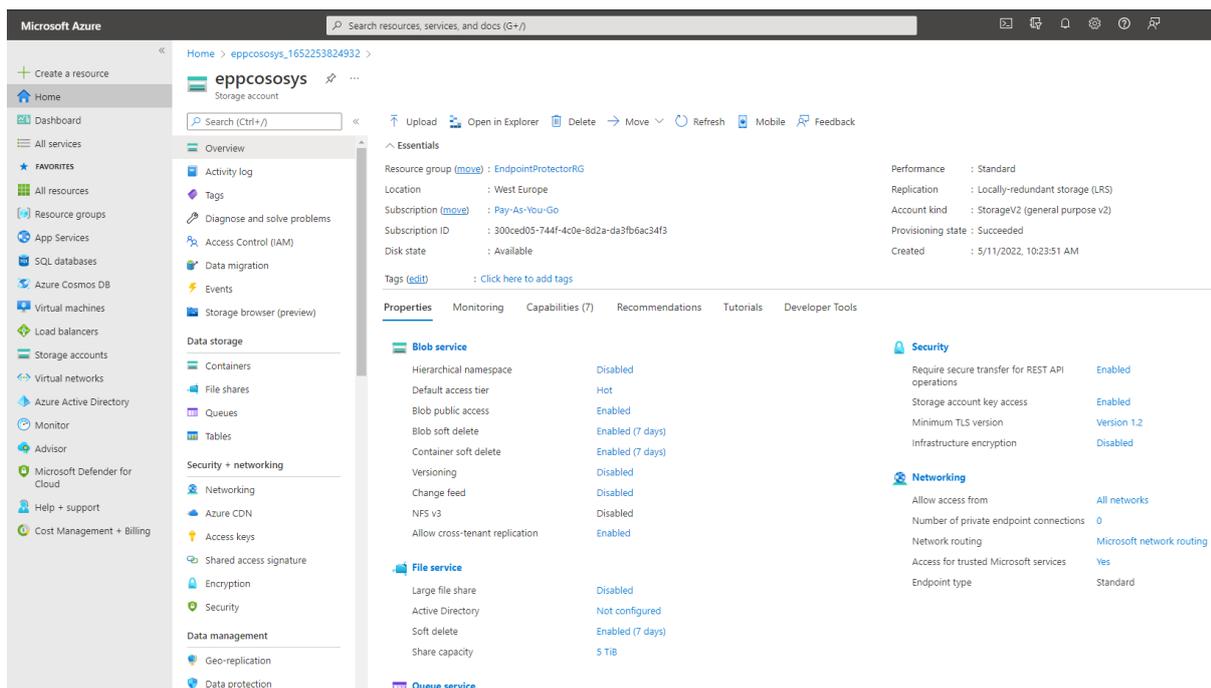
This part of the process is similar to creating any other Storage Account and Container on Azure. If you are already familiar with it or have created a dedicated Container already, proceed to the next step.

To obtain the Azure Endpoint Protector Virtual Machine, you need to create a dedicated Storage account / Container, following these steps:

1. Open the [Azure portal](#);
2. Go to **Storage accounts** and click **+Create**;
3. To **create a storage account**, provide the following information:
  - **Subscription** – select **Pay-As-You-Go**
  - **Resource group** – select a group from the available list or create a new one
  - **Storage account name** – add a name for the storage account
  - **Region** – select the nearest the location of the computers that will be protected by Endpoint Protector
  - **Performance** – select **Standard** performance
  - **Redundancy** – select **Locally-redundant storage (LRS)**
4. Click **Review + create**;



4. Go to **Storage accounts** and click the newly created account;
5. Go to **Containers** and click **+Container**;
6. Give the container the same name as you did to the storage account and for the **Public access level** select **Container (anonymous read access for containers and blobs)**;



7. Select the container you created, and then click **Shared access tokens**.

**Important: Make sure you are creating a token on the container level, not the storage account!**

8. Configure the **SAS token** with **Create, Write and Add Permissions** with a **5-day** window to allow the CoSoSys team to copy the image;



9. Copy the **Blob SAS URL** and send it to CoSoSys.

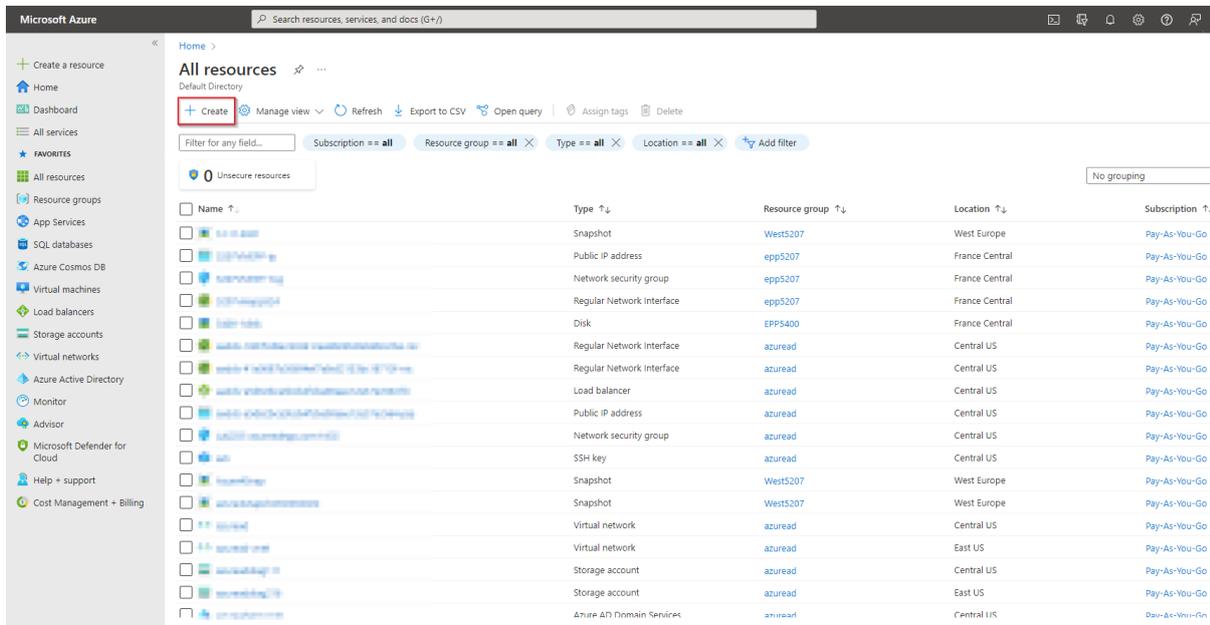
**Note:** CoSoSys will copy the Endpoint Protector Virtual Machine to your storage account and notify you when the process is over.

## 4.3. Create the disk

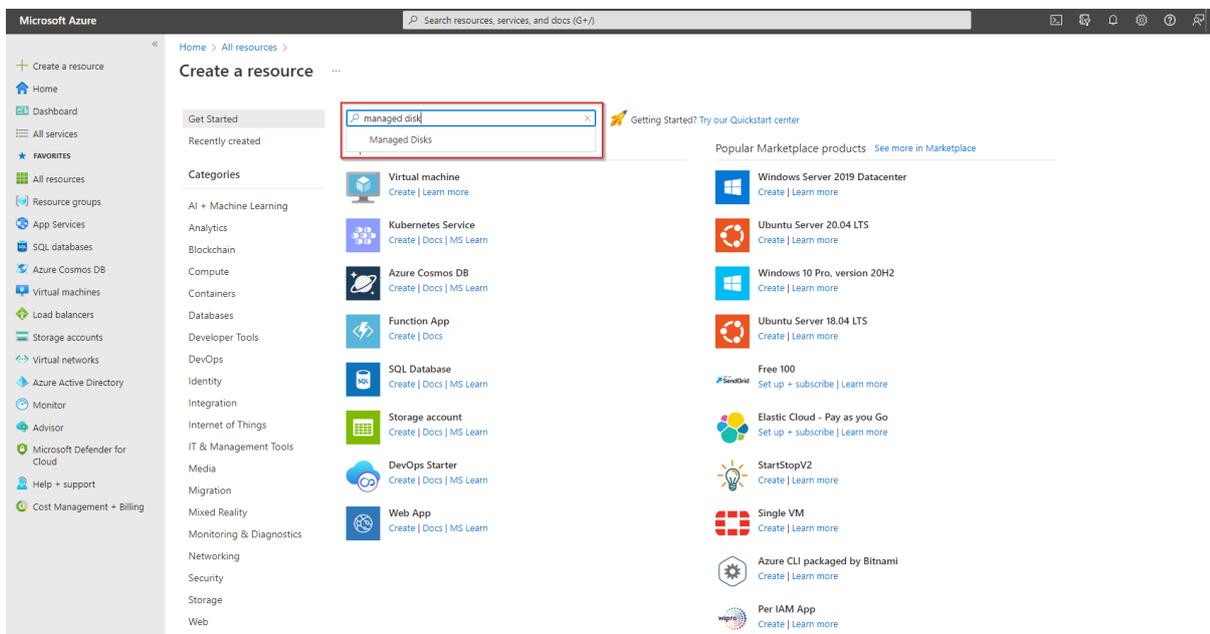
Before starting the Endpoint Protector Virtual Machine, you have to prepare a disk and a Virtual Machine.

To create a disk, follow these steps.

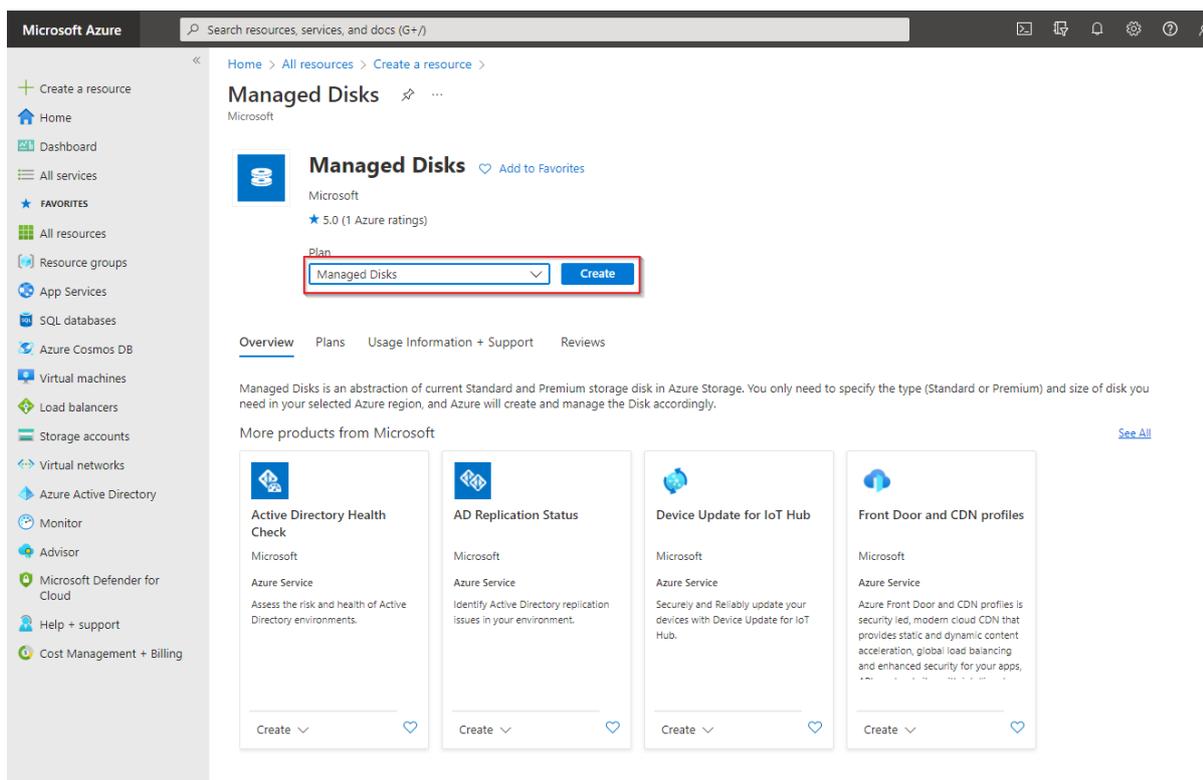
1. From the top right side of the page, go to **All resources** and click **+Create**;



2. Search the marketplace for **Managed Disks**;



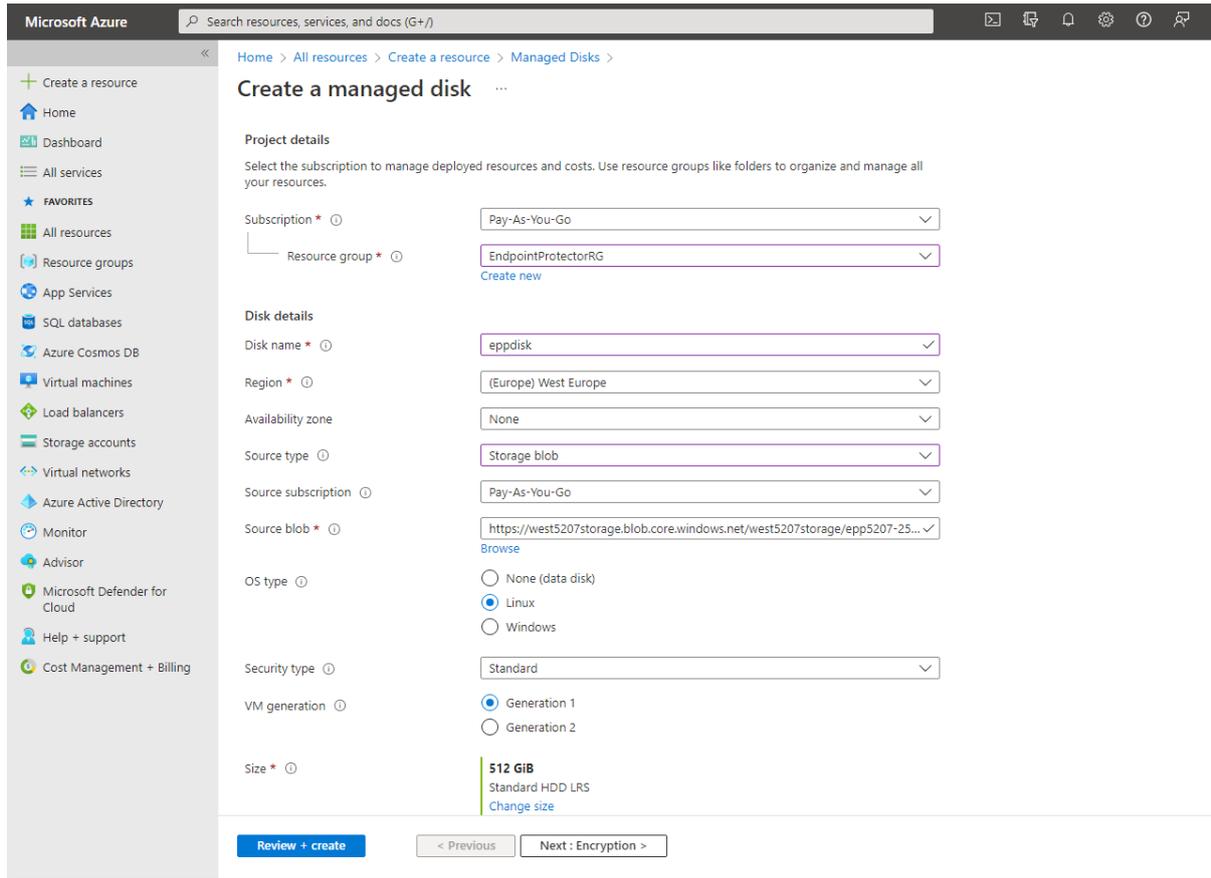
3. Go to **Managed Disks** and select **Create**;



4. To create a managed disk, provide the following information

- **Subscription** - select **Pay-As-You-Go**
- **Resource group** – select the previously created one
- **Disk name** – add a name for the storage account
- **Region** – select the nearest the location of the computers that will be protected by Endpoint Protector
- **Availability Zone**
- **Source type** - select **Storage Blob**
- **Source subscription** - select **Pay-As-You-Go**
- **Source blob** – enter the URL received from CoSoSys after providing the key and URL mentioned above.
- **OS type** - select **Linux**
- **Security type** – select **Standard**
- **VM generation** – select **Generation 1**
- **Size** - select **128 GB**

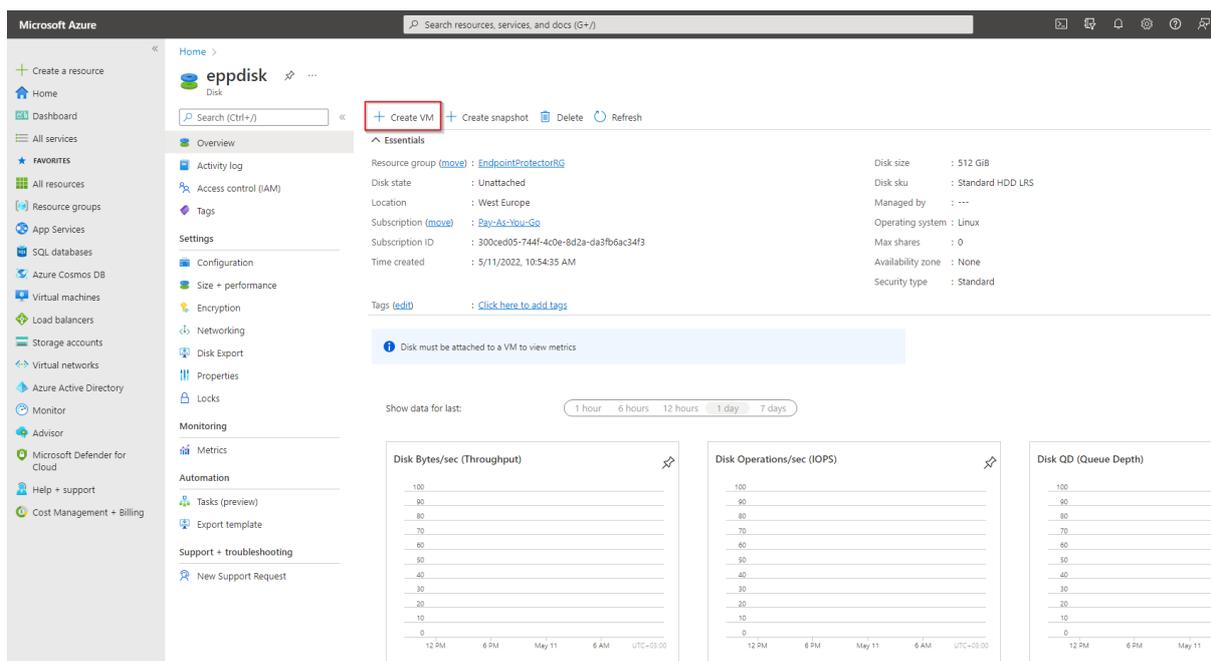
5. Click **Review + Create** and wait for the **Successfully created disk** message to be displayed.



## 4.4. Create the Virtual Machine

To start the Endpoint Protector Virtual Machine in Azure, follow these steps:

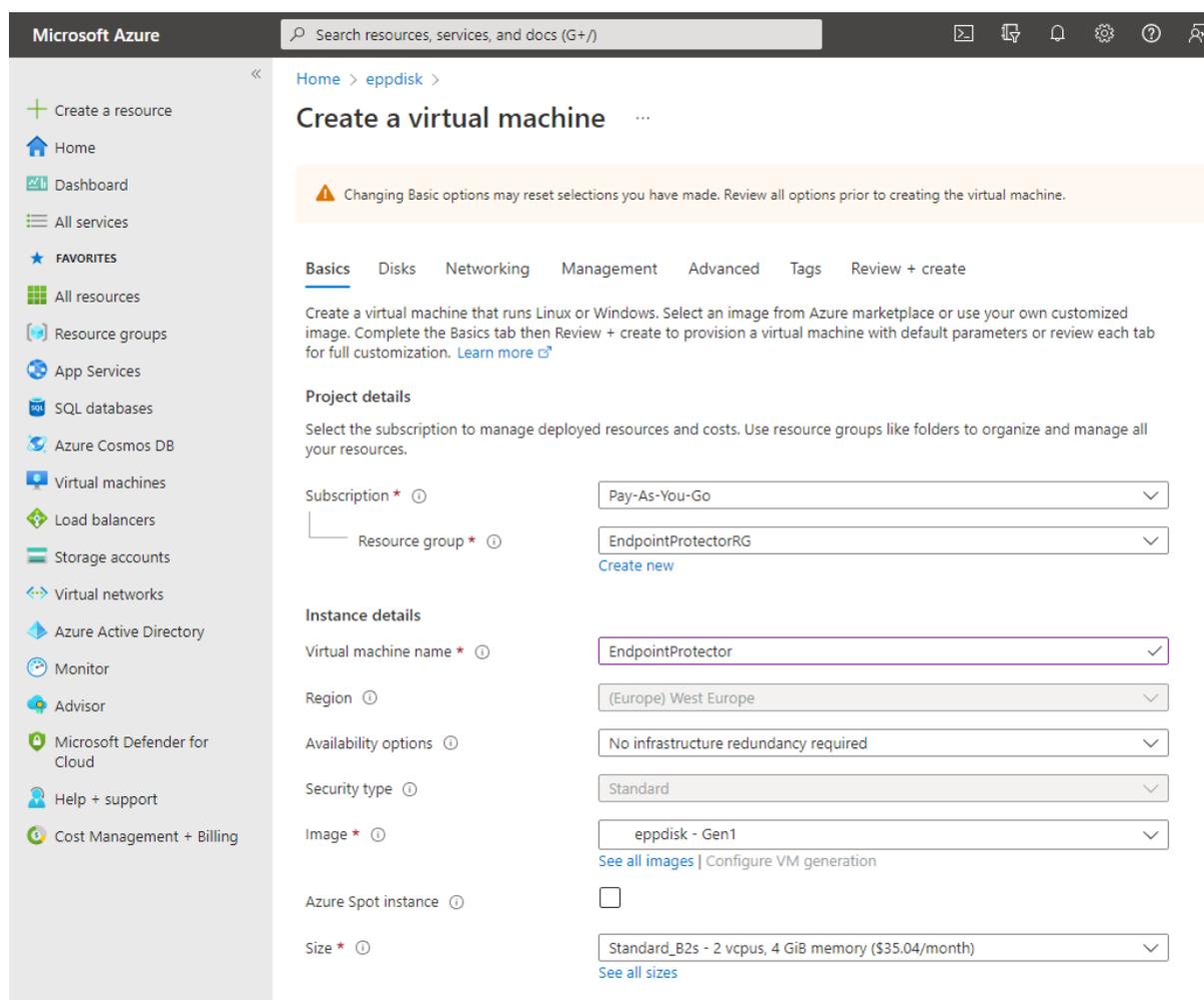
1. Go to the **All resources** page, select the newly created disks and then click **Create VM**



2. To create the Virtual Machine, provide the following information:

On the **Basics** tab, fill in the following:

- **Subscription** – select **Pay-As-You-Go**
- **Resource group** – select the group used when creating the disk
- **Virtual Machine Name** – enter a name for the Virtual Machine
- **Size** - select a virtual machine profile based closest to the recommended requirements for the disk file used

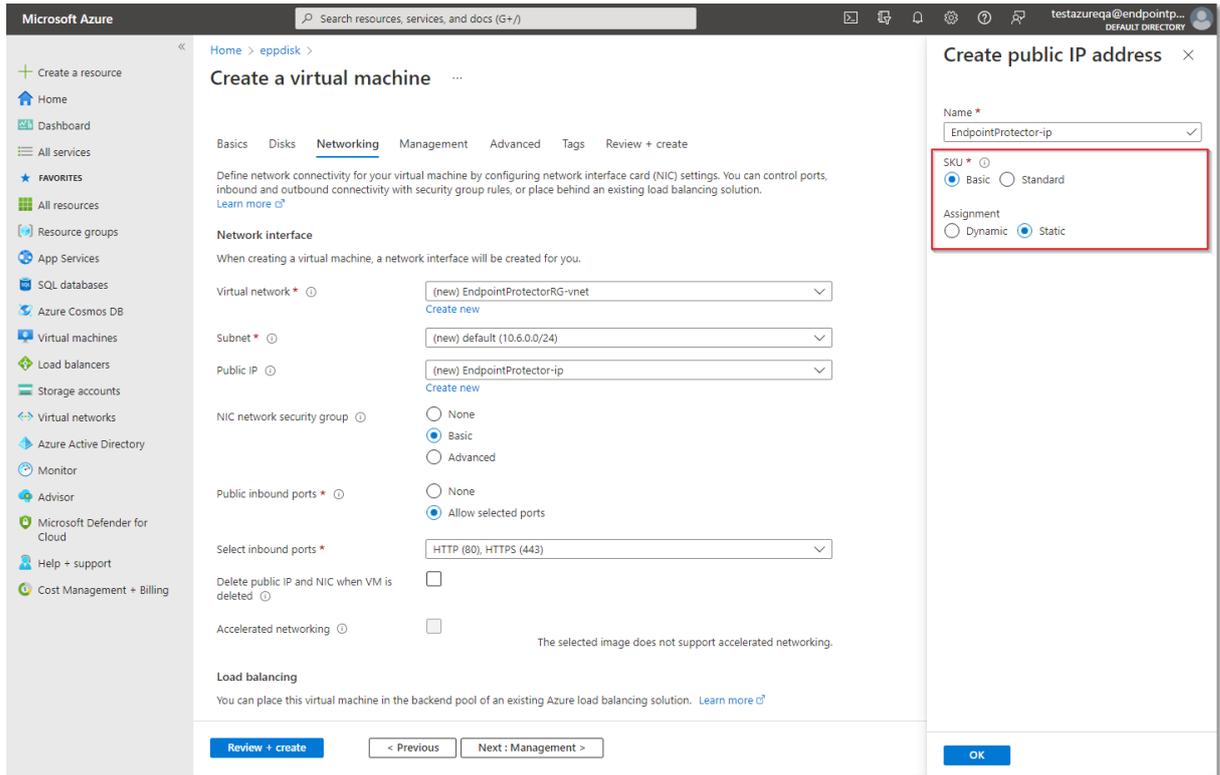


On the **Networking** tab, fill in the following:

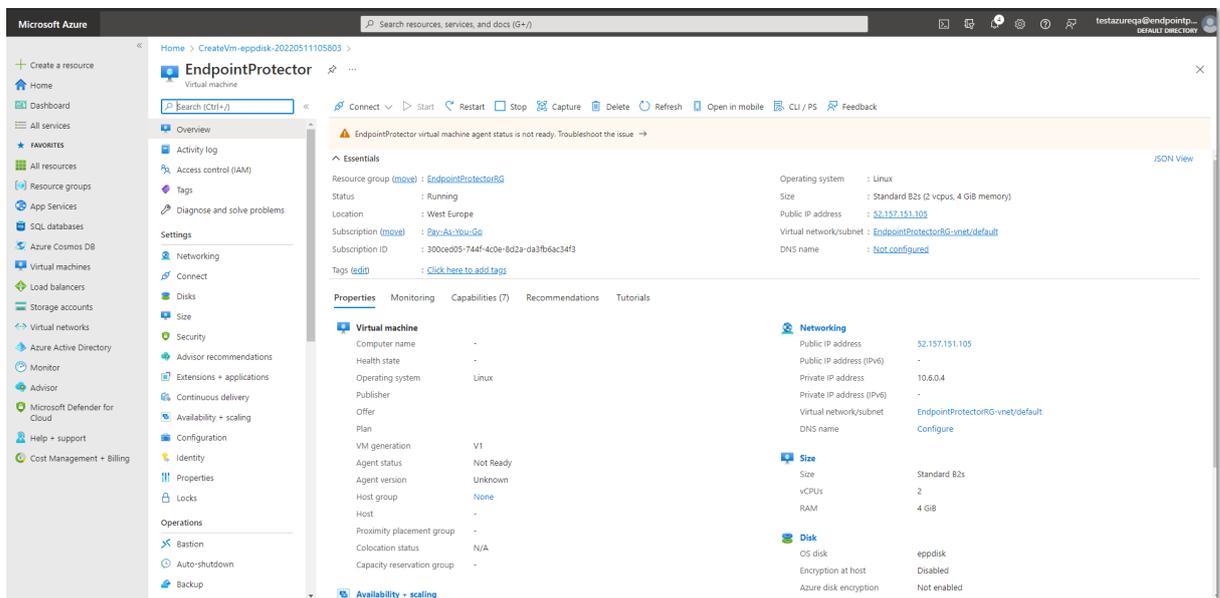
- **Public IP** - click **Create new** and select **Basic SKU** and **Static Assignment**.
- **Select inbound ports** – add **HTTP (80)** and **HTTPS (443)**

Click **Review + create** and then **Create**.

**Note:** For Additional Features, we recommend selecting HDD instead of SSD to avoid unnecessary payments for an unused SSD attached to the Virtual Machine.



- Once the deployment has finished, go to **Virtual Machines** on the right side and select the Endpoint Protector image.



- Open a web browser and connect to the Public IP address assigned to the Endpoint Protector image.

# 5. Endpoint Protector Licensing

Endpoint Protector is a Bring Your License (BYOL) Instance. This means that you are paying Amazon (AWS) / Google (GCP) / Microsoft (Azure) for running the instance and then importing the license previously purchased from CoSoSys or any Endpoint Protector Partner.

The price of the Endpoint Protector Licenses with AWS, GCP, or Azure is the same as licensing the Endpoint Protector Virtual Appliance. To purchase a license please contact your Endpoint Protector Representative or [sales@cososys.com](mailto:sales@cososys.com).

# 6. Disclaimer

The information in this document is provided on an “AS IS” basis. To the maximum extent permitted by law, CoSoSys disclaims all liability, as well as any and all representations and warranties, whether express or implied, including but not limited to fitness for a particular purpose, title, non-infringement, merchantability, interoperability, and performance, in relation to this document. Nothing herein shall be deemed to constitute any warranty, representation, or commitment in addition to those expressly provided in the terms and conditions that apply to the customer’s use of Endpoint Protector.

Each Endpoint Protector Server has the default SSH Protocol (22) open for Support Interventions, and there is one (1) System Account enabled (epproot) protected with a password. The SSH Service can be disabled at customers’ request.

Security safeguards, by their nature, are capable of circumvention. CoSoSys cannot, and does not, guarantee that data or devices will not be accessed by unauthorized persons, and CoSoSys disclaims any warranties to that effect to the fullest extent permitted by law.

© 2004 – 2022 CoSoSys Ltd.; Endpoint Protector, My Endpoint Protector, Endpoint Protector Basic and EasyLock are trademarks of CoSoSys Ltd. All rights reserved. Windows and Azure are registered trademarks of Microsoft Corporation. Macintosh, Mac OS X, and macOS are trademarks of Apple Corporation. AWS and Amazon Web Services are a trademark of Amazon. GCM and Google Cloud Platform is a trademark of Google. All other names and trademarks are the property of their respective owners.

[EndpointProtector.com](https://EndpointProtector.com)