ENDPOINT PROTECTOR | by CoSoSys

클라우드 서비스

사용자 매뉴얼

버전: 5.0

날짜: 2022 년 11 월 11 일

목 차

변경 내역

버전	날짜	비고
1.0	2016	문서 만들어짐
2.0	2018	문서 업데이트됨
3.0	2019	문서 업데이트됨
4.0	27.05.2022	Amazon Web Services, Google Cloud Platform, Azure 챕터 업데이트됨
5.0	11.11.2022	Azure 챕터 Create the Storage Account and Container 섹션 업데이트됨

1. 개요

이 사용자 매뉴얼은 Amazon Web Services 또는 Google Cloud Platform 에서 Endpoint Protector 서버 사용 시 빠른 가이드를 제공하는 목적으로 만들었습니다.

중요: 이 문서는 AWS 또는 GCP 계정을 만드는 자세한 가이드를 제공하지 않습니다. 계정은 이미 준비되어 있어야 하고 이러한 제 3 업체 서비스는 각 관리자의 책임 아래에 있다는 것 이해하고 있어야 합니다.

- **Amazon Web Services** - Endpoint Protector AMI 는 Amazon EC2 인스턴스로 제공됩니다.
- **Google Clout Platform** - Endpoint Protector 이미지는 *.tar.gz 으로 제공됩니다.
- **Azure** - Endpoint Protector 이미지는 여러분의 계정에 업로드 될 것입니다.

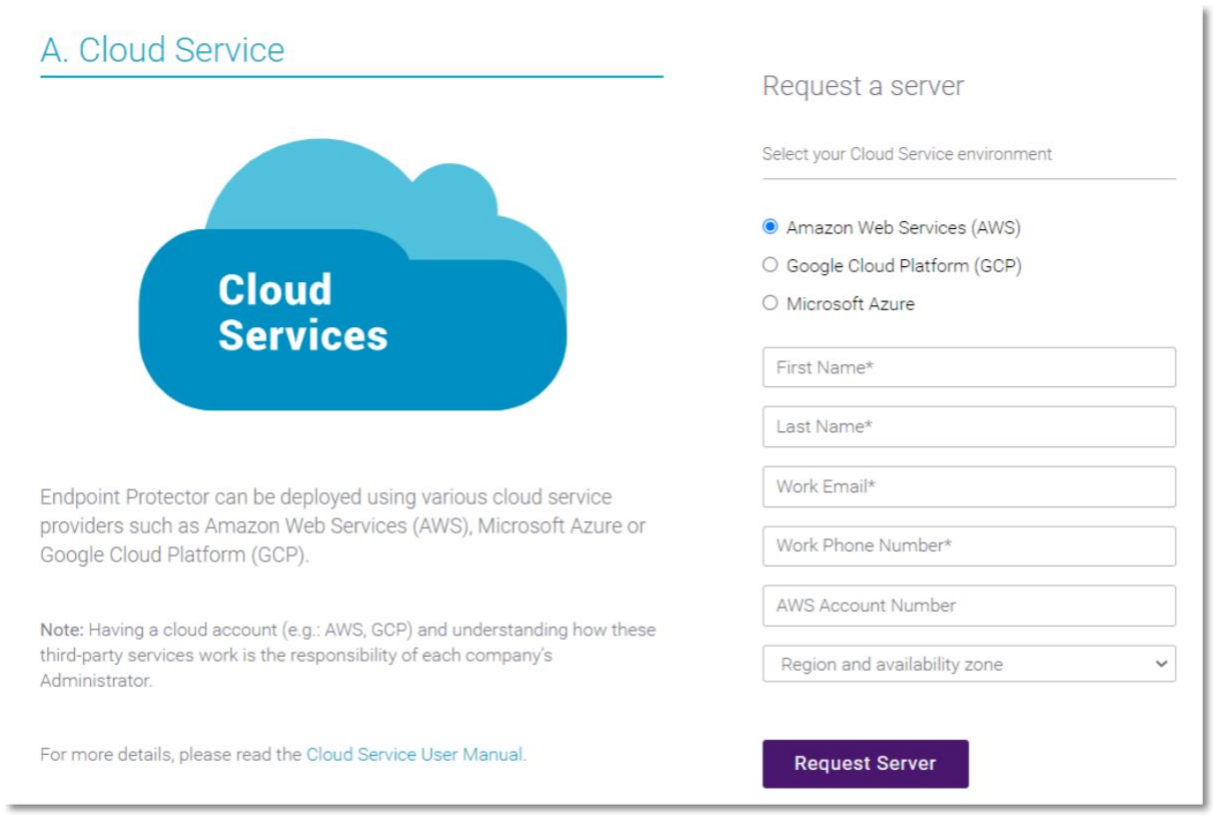
참고: Endpoint Protector 사용에 관련된 자세한 정보는 Endpoint Protector 사용자 매뉴얼을 참조하시기 바랍니다.

2. Amazon Web Services

2.1. Endpoint Protector AMI 가져오기

Endpoint Protector 는 일반적으로 AWS 마켓 플레이스에서 받을 수 없습니다. AMI (Amazon Machine Image)를 받기 위해서는 Endpoint Protector 담당자에게 직접 연락하거나 AWS Account no., Region and availability zone 같은 정보를 웹 사이트에 제공해야 합니다.

Endpoint Protector AMI (Amazon Machine Image)가 공유되면 담당자에게 연락을 받게 될 것입니다.

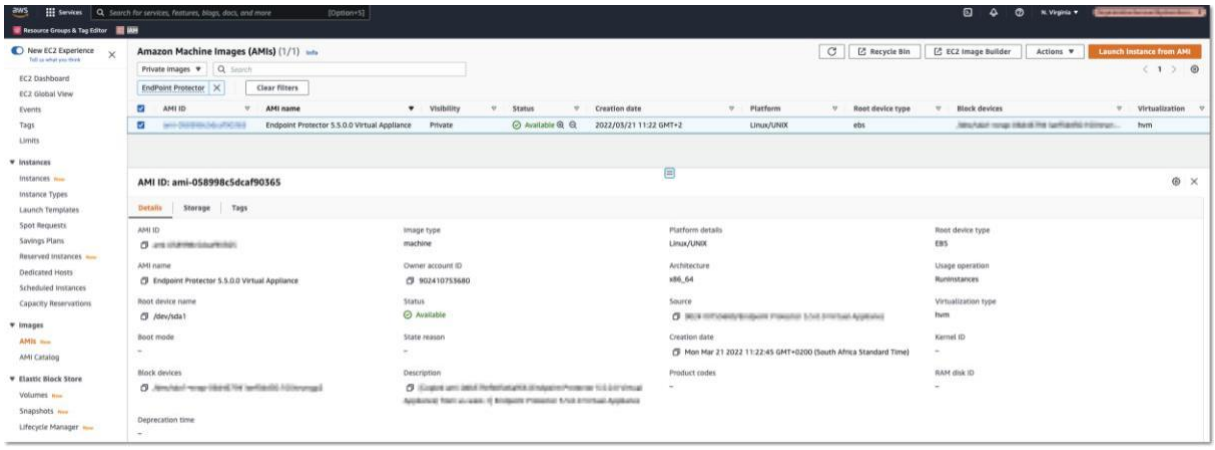


2.2. EC2 이미지 런칭

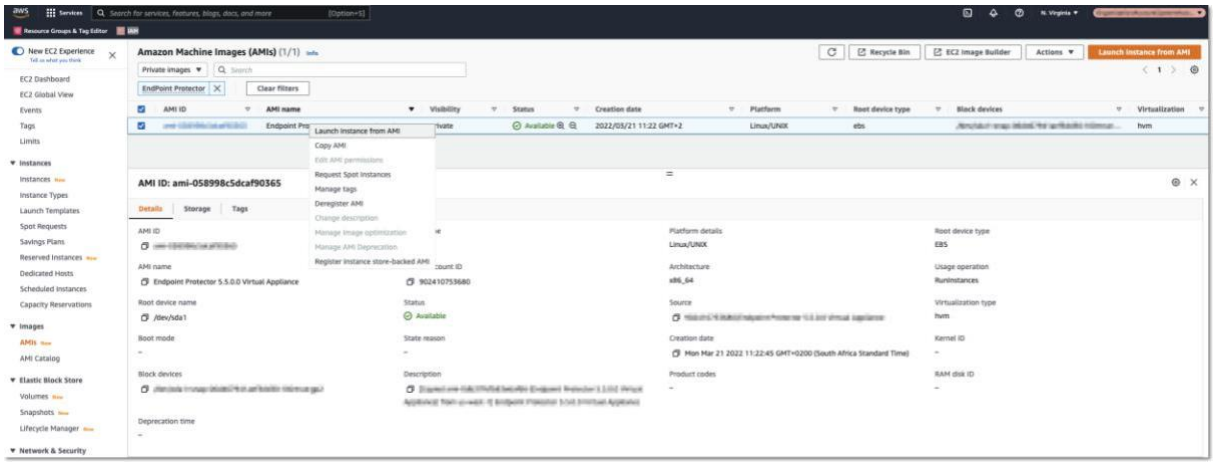
Endpoint Protector 이미지가 이미 공유되었다면 이 과정은 모든 EC2 런칭과 비슷합니다.

EC2 이미지 런칭하려면 아래 단계를 따르시기 바랍니다:

1. **Services: EC2** 이동 후 **region** 을 선택합니다;
2. **Images: AMIs** 이동 후 프라이빗 이미지 유형을 선택하고 **Endpoint Protector** 를 검색합니다;



3. 오른쪽 클릭 후 **Launch Instance** 를 선택합니다;

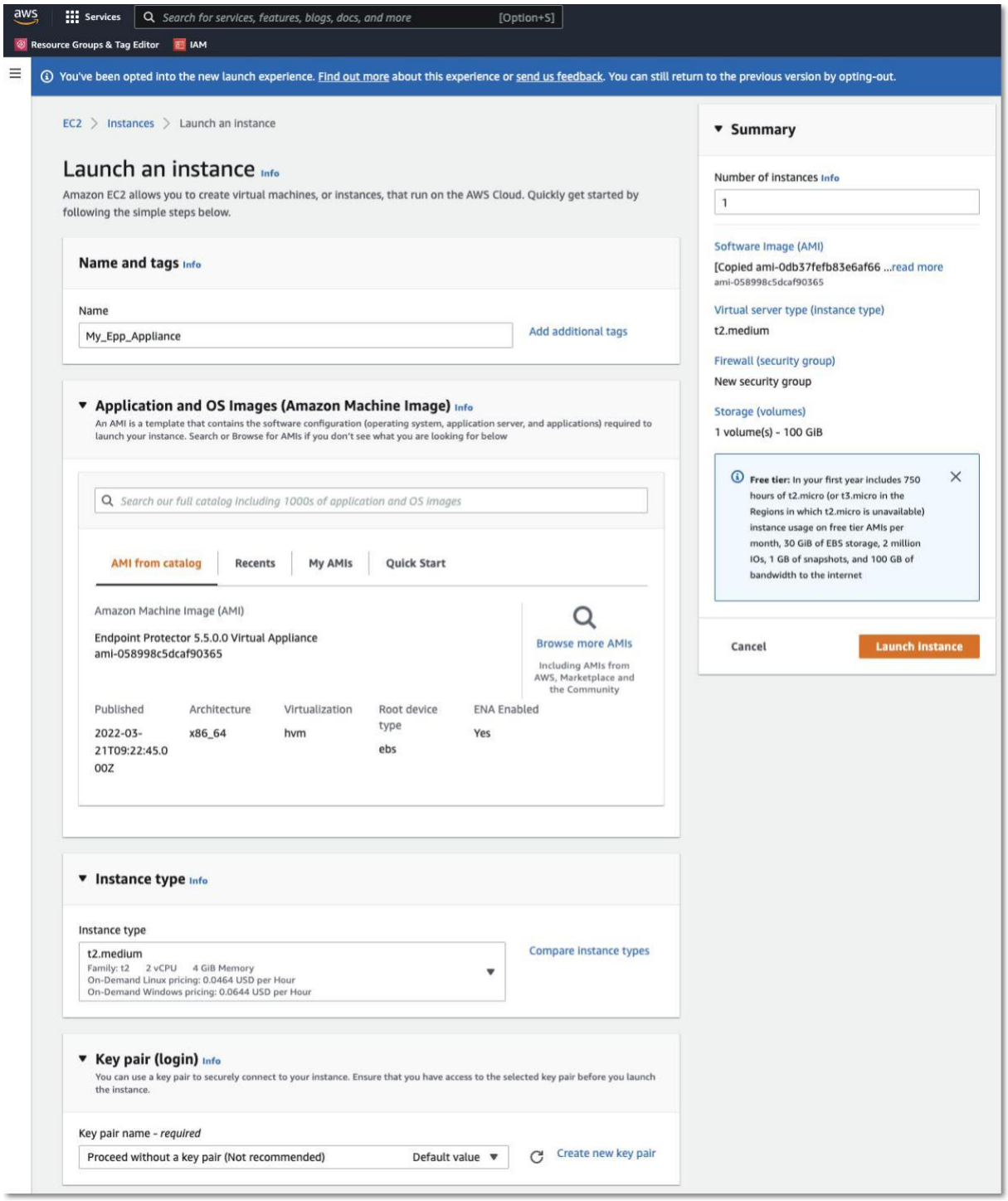


4. 정책에 따라 **Name** 을 입력하고 **Create tags** 합니다;
5. **Instance Type** 을 선택합니다.

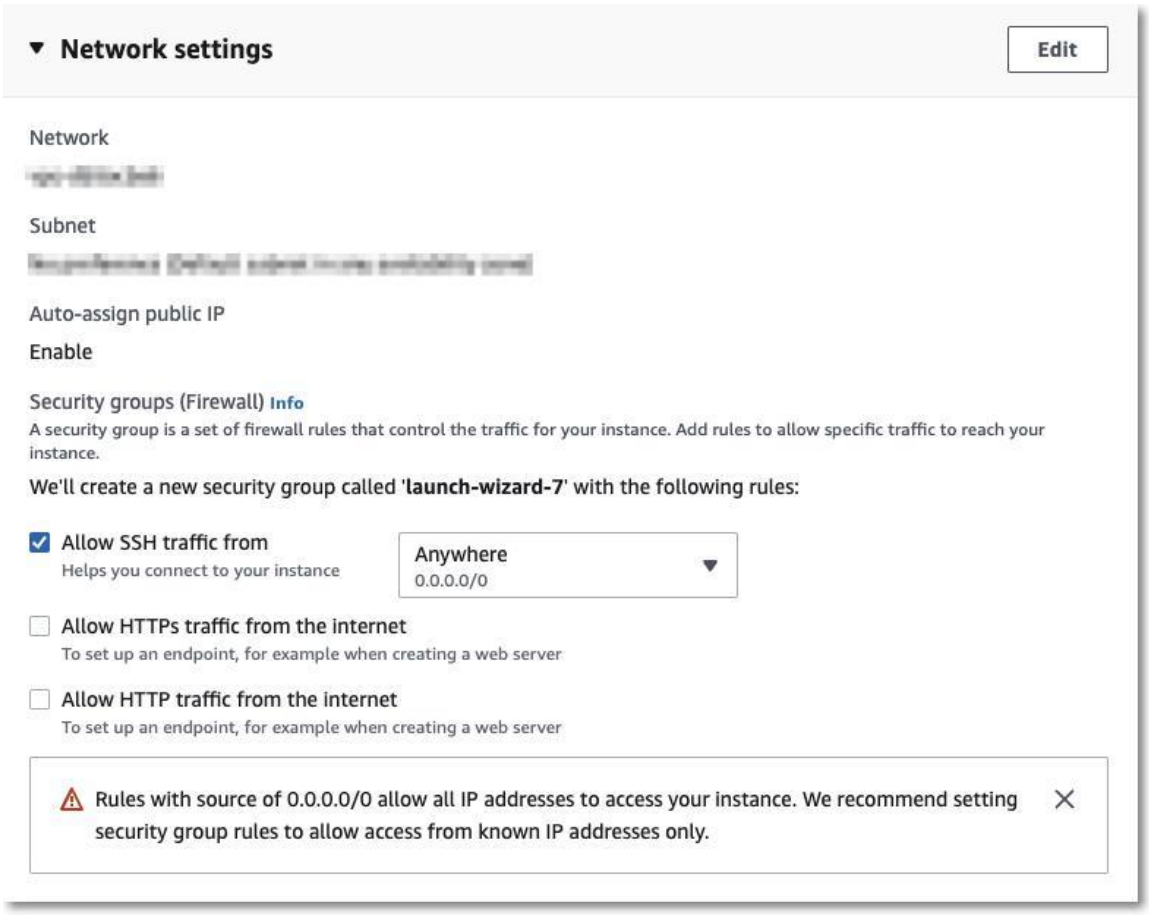
참고: 최적화된 Instance Type 선택에 도움이 필요하시면 담당자에게 연락 주시기 바랍니다.

6. 사용 가능한 **key pair** 선택하거나 **new key pair** 를 만듭니다;

만약 key pair 사용을 선택했다면 지원팀 요청으로 지원팀과 공유해야 할지도 모릅니다. 이 경우 해당 인스턴스만 사용하는지 확인하시기 바랍니다. **Proceed without a Key Pair** 옵션을 선택하고 **Launch Instances** 를 클릭하는 것을 권장할 수도 있습니다.

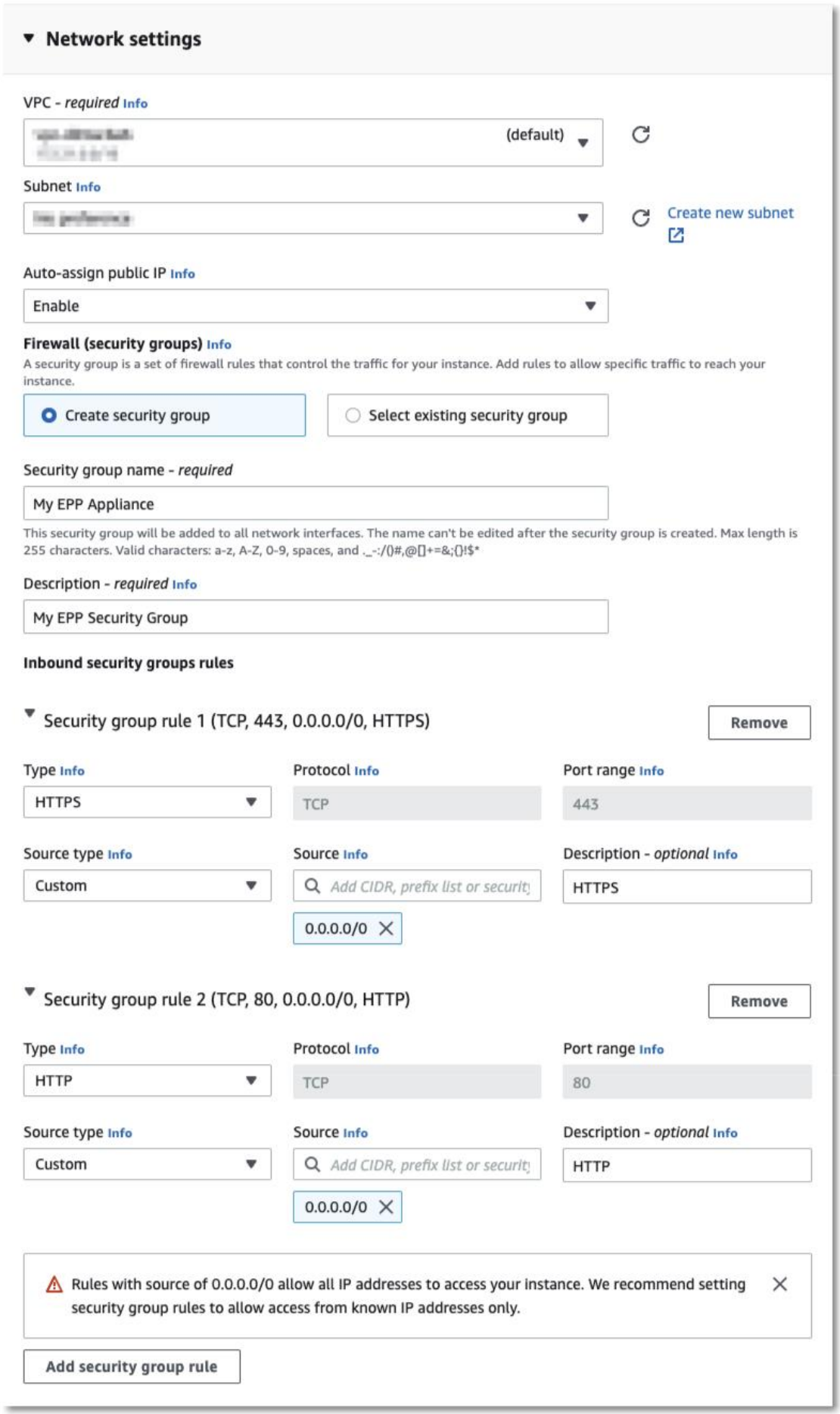


7. **Network** 섹션을 구성합니다:

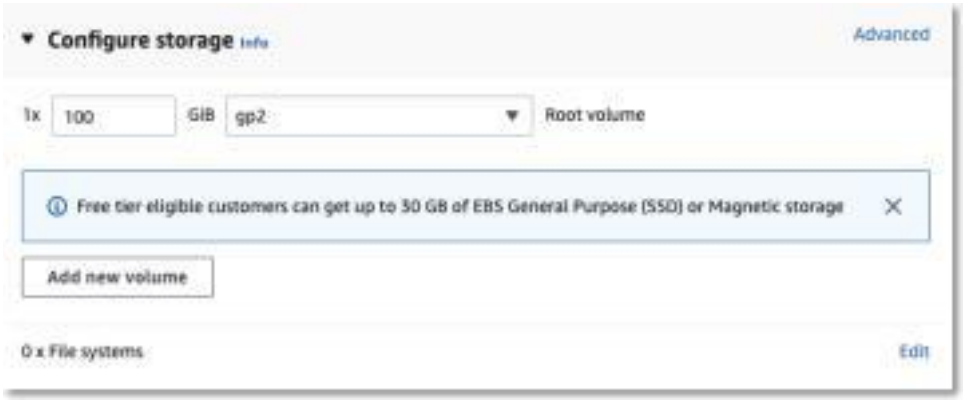


8. 네트워크 섹션을 편집하고 아래 정보를 제공합니다:

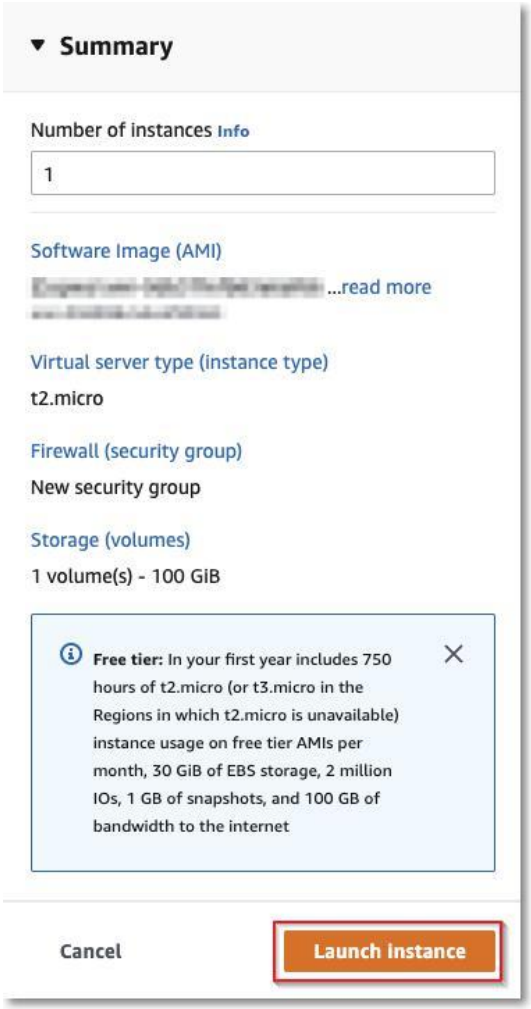
- **VPC** 와 **Subnet** 선택
- **Auto-assign public IP** 사용
- **Create security group** 선택한 후 **name** 과 **description** 제공
- 기존 인바운드 규칙 **Remove** (삭제)
- **Add two new Inbound security group rules** (두 가지 새로운 인바운드 보안 그룹 규칙 추가):
  - **HTTPS** 유형, **TCP** 프로토콜, **443** 포트 범위, **Custom** 소스 유형, 소스 0.0.0.0/0 (**필수**)
  - **HTTP** 유형, **TCP** 프로토콜, **80** 포트 범위, **Custom** 소스 유형, 소스 0.0.0.0/0 (**선택**)



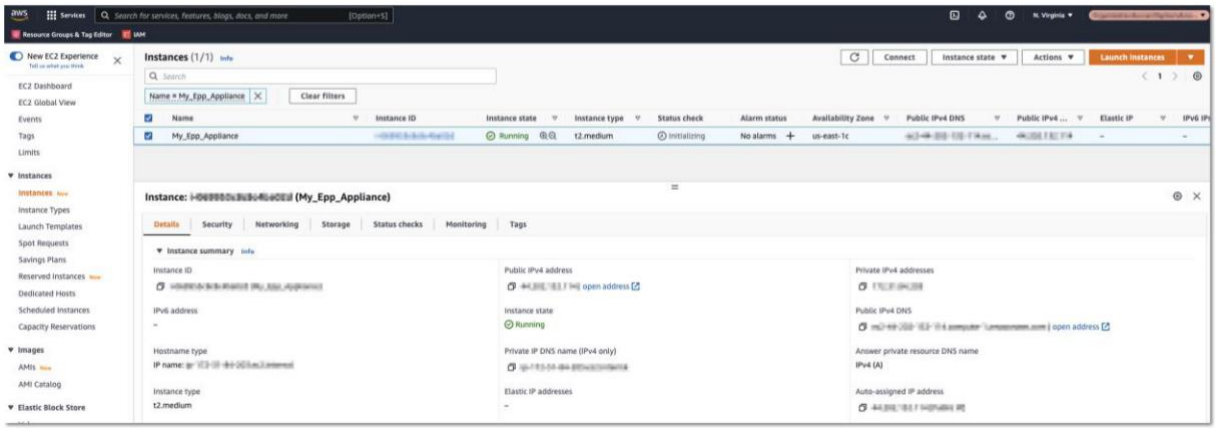
9. **Storage** 섹션은 변경이 필요 없습니다;



10. **Summary** 섹션에서 **Launch Instance** 를 클릭합니다;



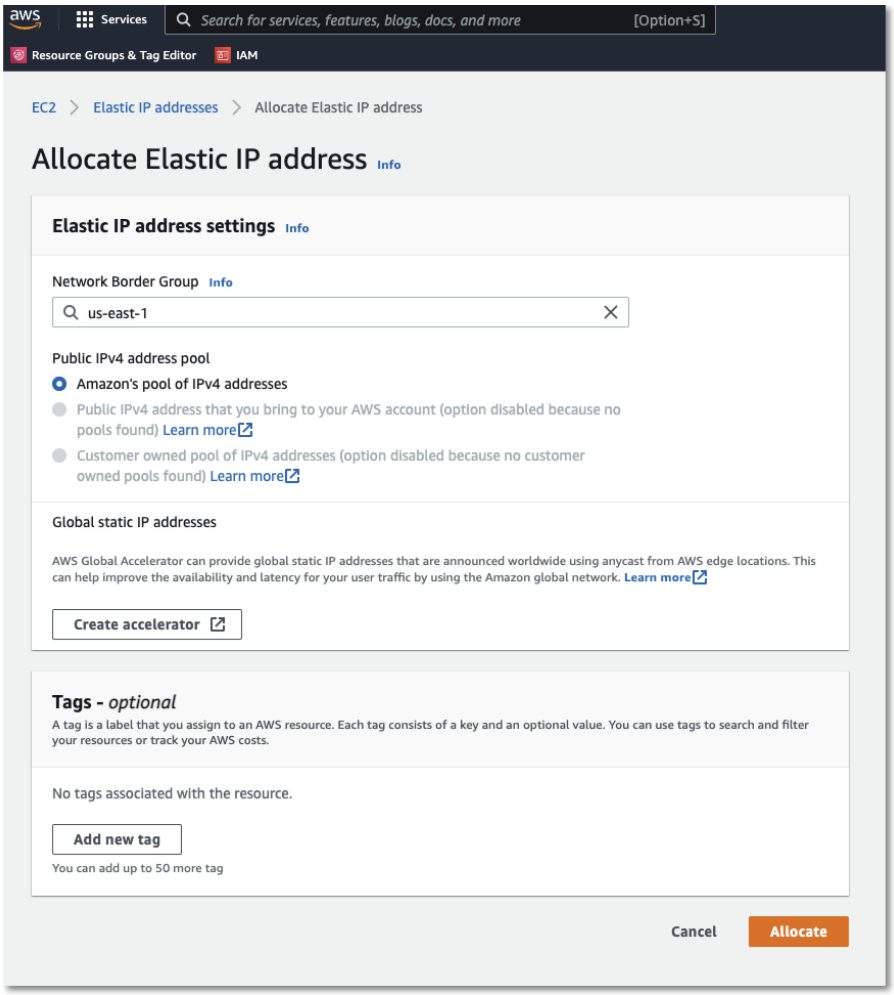
11. 인스턴스 시작을 기다립니다 - **Status Checks** 와 **Initializing** 이 진행되는 동안 몇 분이 걸릴 있습니다.



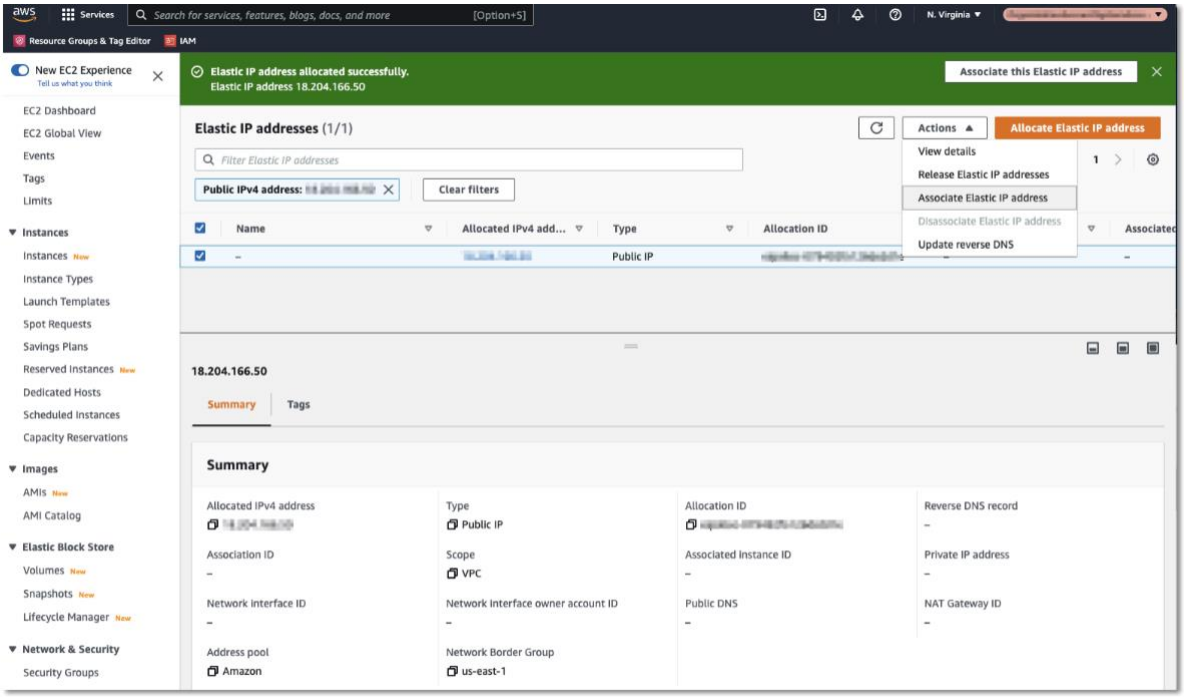
2.2.1. Elastic IP 요청하기

이 단계는 Endpoint Protector 클라이언트가 인스턴스를 재시작하는 경우에 같은 IP 주소로 통신하기 위해서 필요합니다. Elastic IP (Static IP) 없이는 재시작 할 때마다 새로운 IP 를 할당 받아서 Endpoint Protector 클라이언트는 그 때마다 재설치 되어야 합니다.

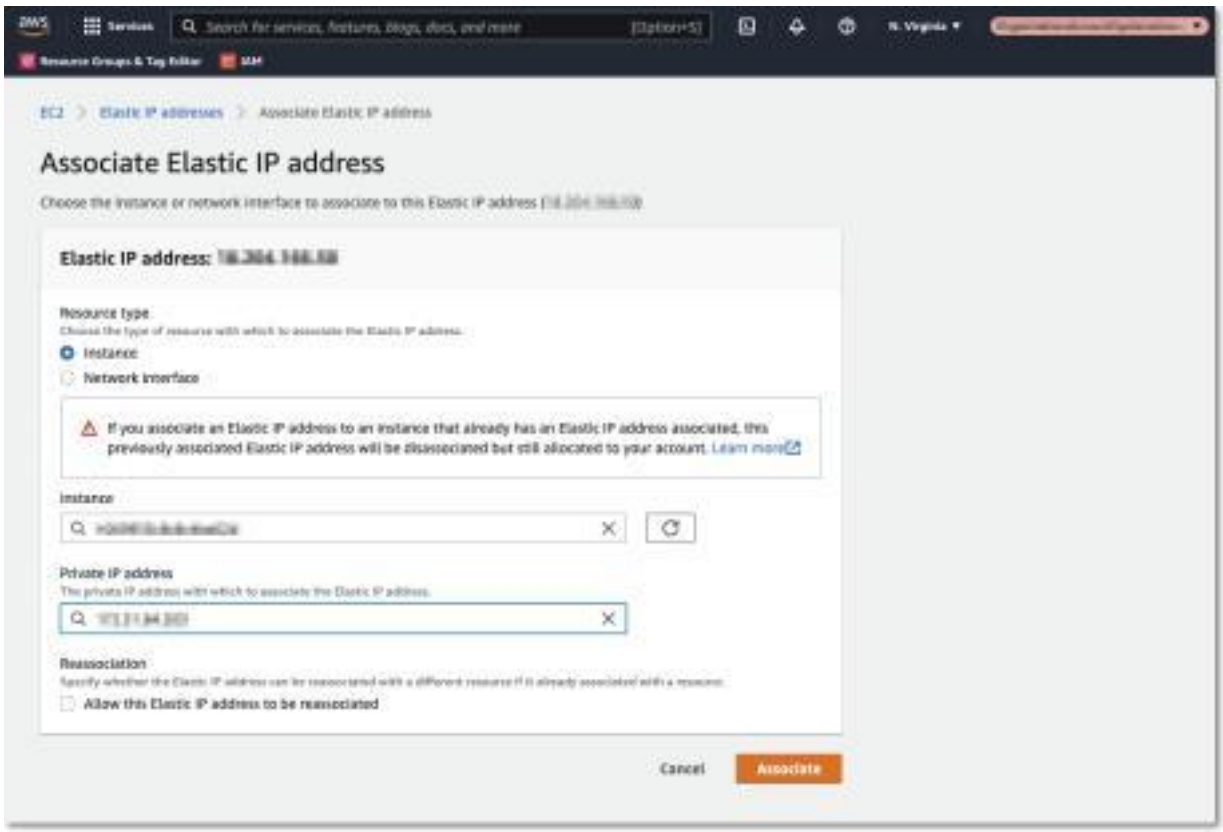
Elastic IP 를 요청하려면 AWS 관리 콘솔의 **Network & Security, Elastic IPs** 로 이동 후 **Allocate New Address** 를 클릭합니다.



1. Endpoint Protector 인스턴스에 **Associate Elastic IP** 합니다;



2. 드롭다운 목록에서 **Endpoint Protector Instance** 의 **Private IP address,** 선택하고 **Associate** 을 클릭합니다;



Endpoint Protector 인스턴스에 Elastic IP 가 이제 연결되었습니다. 몇 분 후에 Endpoint Protector 인스턴스는 연결된 Elastic IP 로 구동될 것입니다.

2.2.2. Secure your Instance

Security Groups 옵션 아래에서 AWS 인터페이스에서 가능한 모든 설정을 만들어서 인스턴스를 더 보호하는 것을 권장합니다.

3. Google Cloud Platform

3.1. Endpoint Protector GCP 이미지 받기

Endpoint Protector 는 Google Cloud Platform 의 기본 이미지를 사용할 수 없습니다.

이미지를 받으려면 아래 설명을 참조하시기 바랍니다.

참고: 이 과정은 콘솔에서 사용자 이미지 업로드와 비슷합니다.

3.2. 이미지 다운로드

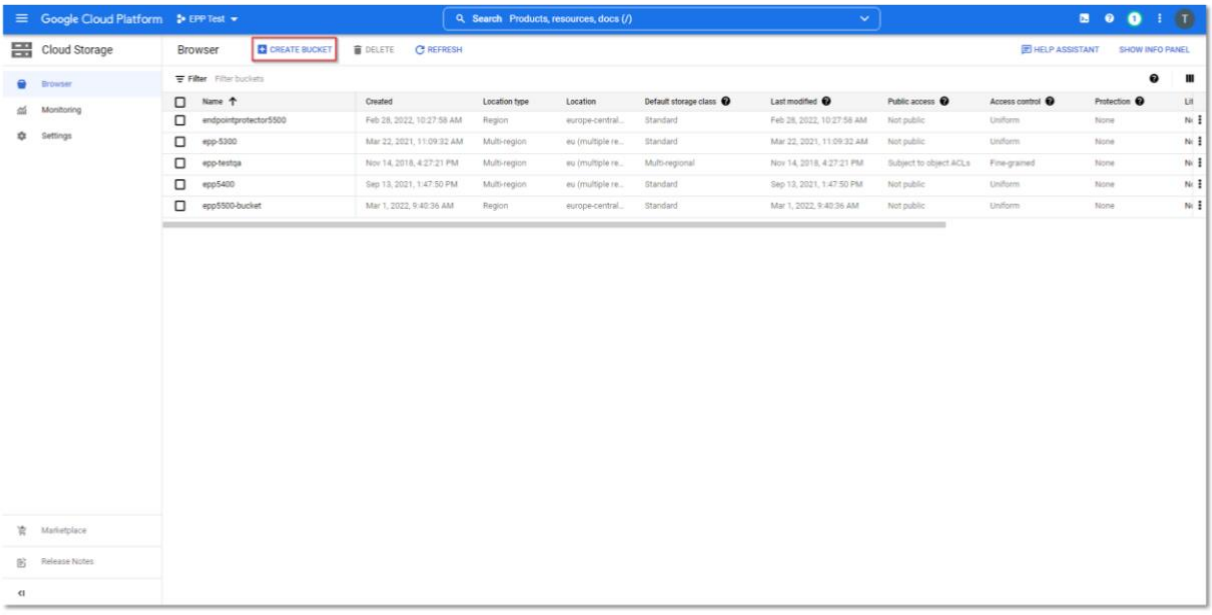
Endpoint Protector 이미지는 담당자가 제공한 링크를 통해서 다운로드 받을 수 있습니다.

만약 이미지를 가지고 있다면 이 단계는 건너뛰기 바랍니다.

3.3. 버킷 만들기

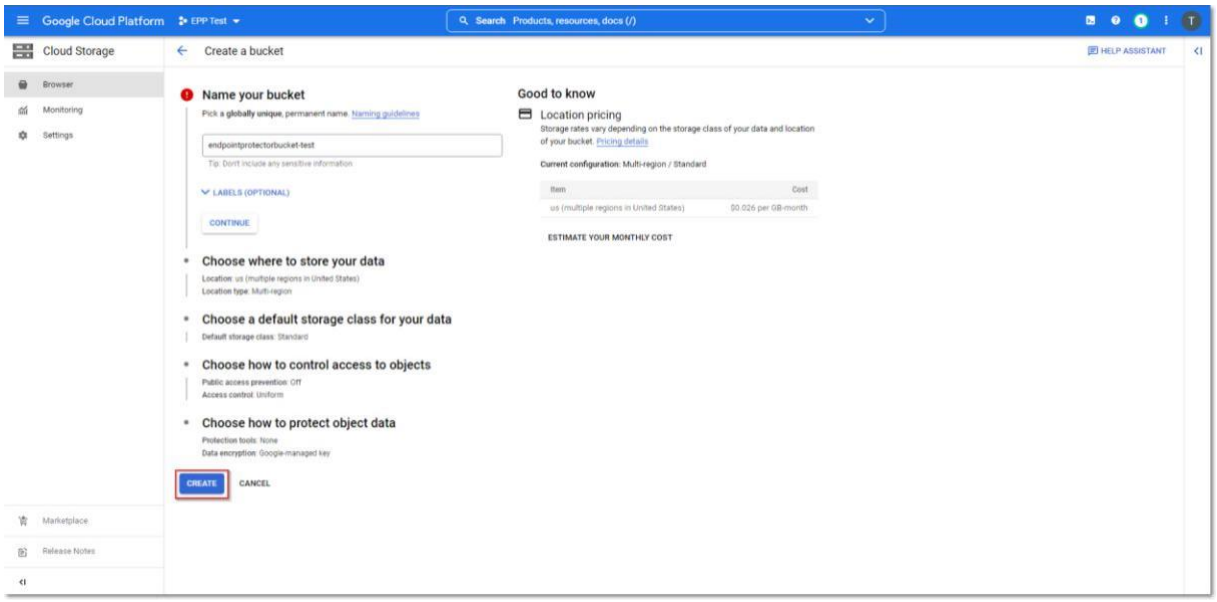
Google Cloud Platform 에 Endpoint Protector 이미지를 업로드하기 위해서 버킷을 만들어야 합니다:

1. Google Cloud Platform Console 에서 **Cloud Storage Browser page** 이동 후 **Create bucket** 을 클릭;



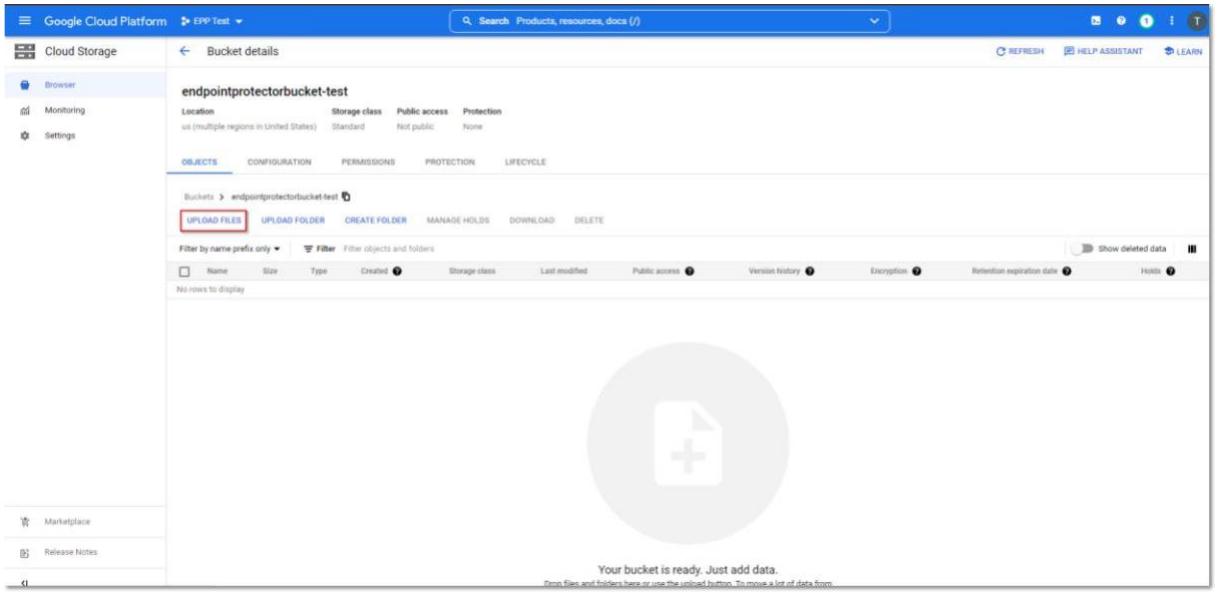
2. 버킷을 만들려면 아래 정보를 입력하고 **Create** 클릭:
   - **Name** – 버킷 이름을 추가

- **Storage** – **standard** 스토리지 클래스 선택
- **Location** – 이미지 저장 위치 선택



3. 새롭게 만들어진 **Bucket details** 페이지에서 **Upload files** 을 클릭하고 전달 받은 Endpoint Protector 이미지 파일을 선택합니다.

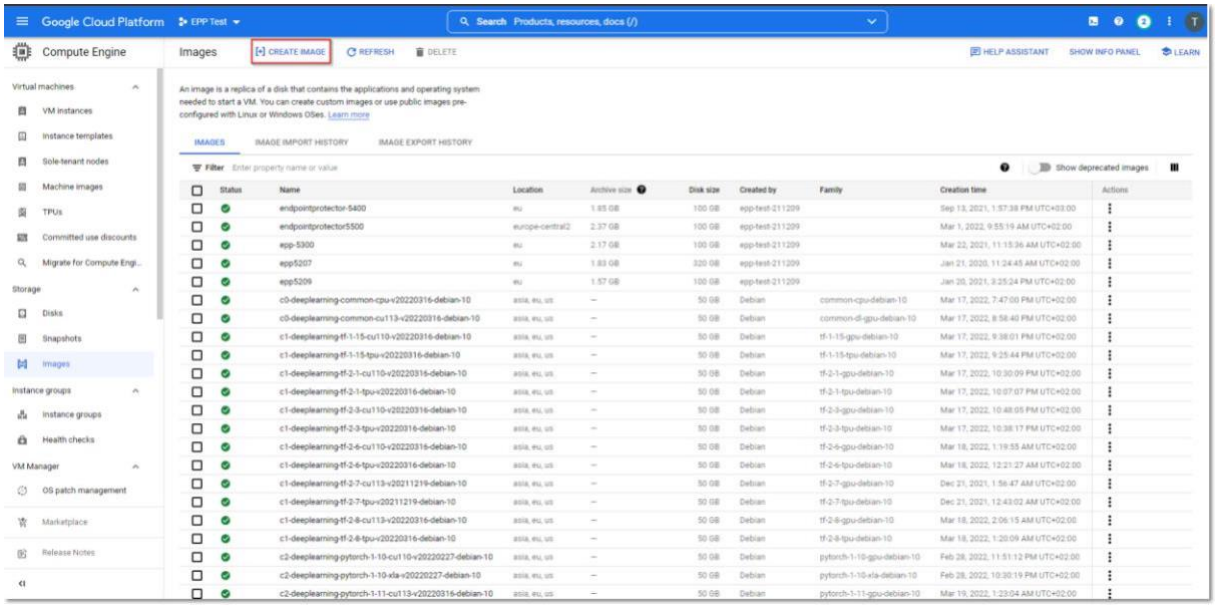
참고: 압축 이미지 크기와 네트워크 연결에 따라서 업로드는 몇 시간이 소요될 수도 있습니다.



3.4. 커스텀 이미지 목록에서 이미지 가져오기

Google Cloud Storage 에 Endpoint Protector 이미지를 업로드 한 후 커스텀 이미지 목록을 가져오시기 바랍니다.

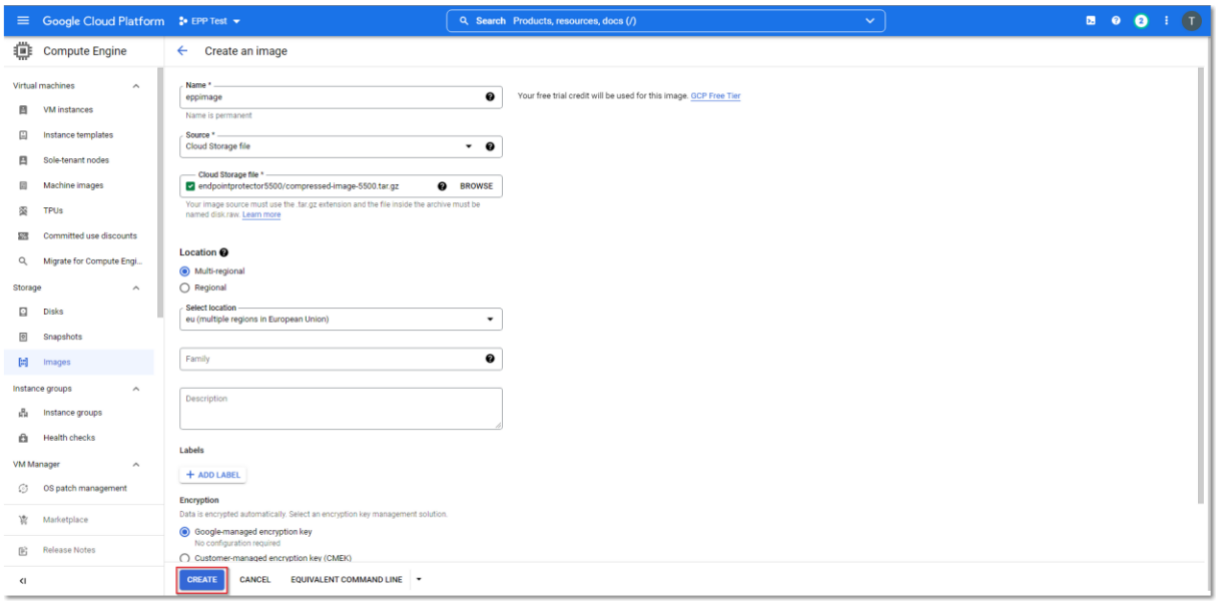
1. Google Cloud Platform 콘솔의 **Image** 페이지 이동 후 **Create image** 를 클릭합니다;



2. 이미지를 만들기 위해서 아래 정보를 입력하고 **Create** 을 클릭합니다:

   - **Name** – 이미지 이름 추가
   - **Source** – **Cloud Storage file** 선택
   - **Cloud Storage file –** Endpoint Protector 이미지 파일 업로드
   - **Location** – **Multi-regional** 선택
   - **Encryption – Google-managed encryption key** 선택

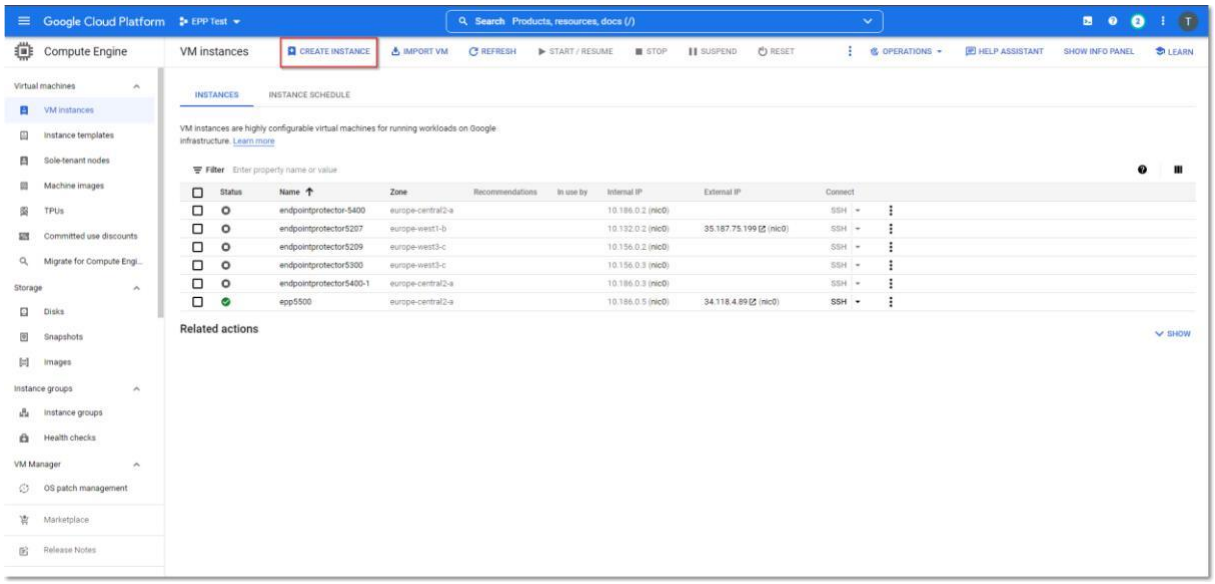
참고: 이 과정은 부트 디스크 이미지 크기에 따라 몇 분이 소요될 수 있습니다.



3.5. Endpoint Protector VM 인스턴스 만들기

Endpoint Protector 이미지는 Google Cloud Platform 이미지 목록에서 사용한 후에 VM(Virtual Machine) 인스턴스를 만듭니다.

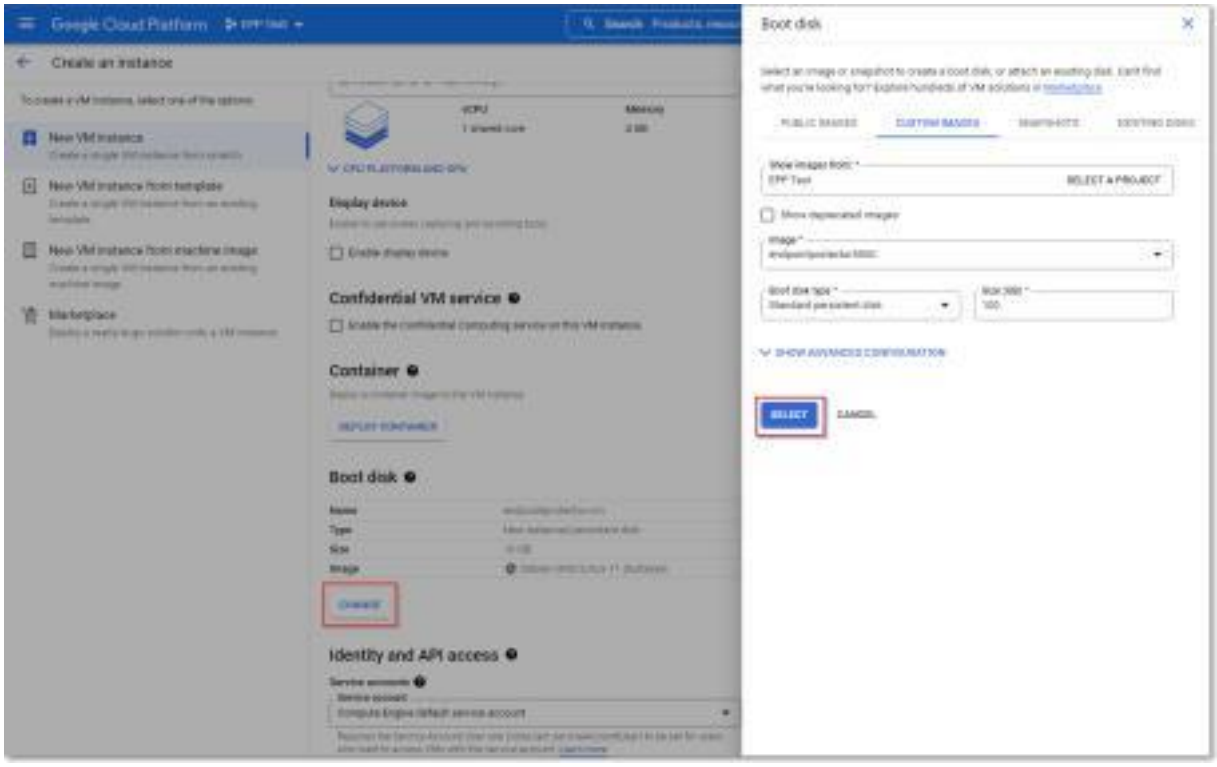
1. **Google Cloud Platform Console** 에서 **VM Instances** 페이지 이동 후 **Create instance** 를 클릭합니다;



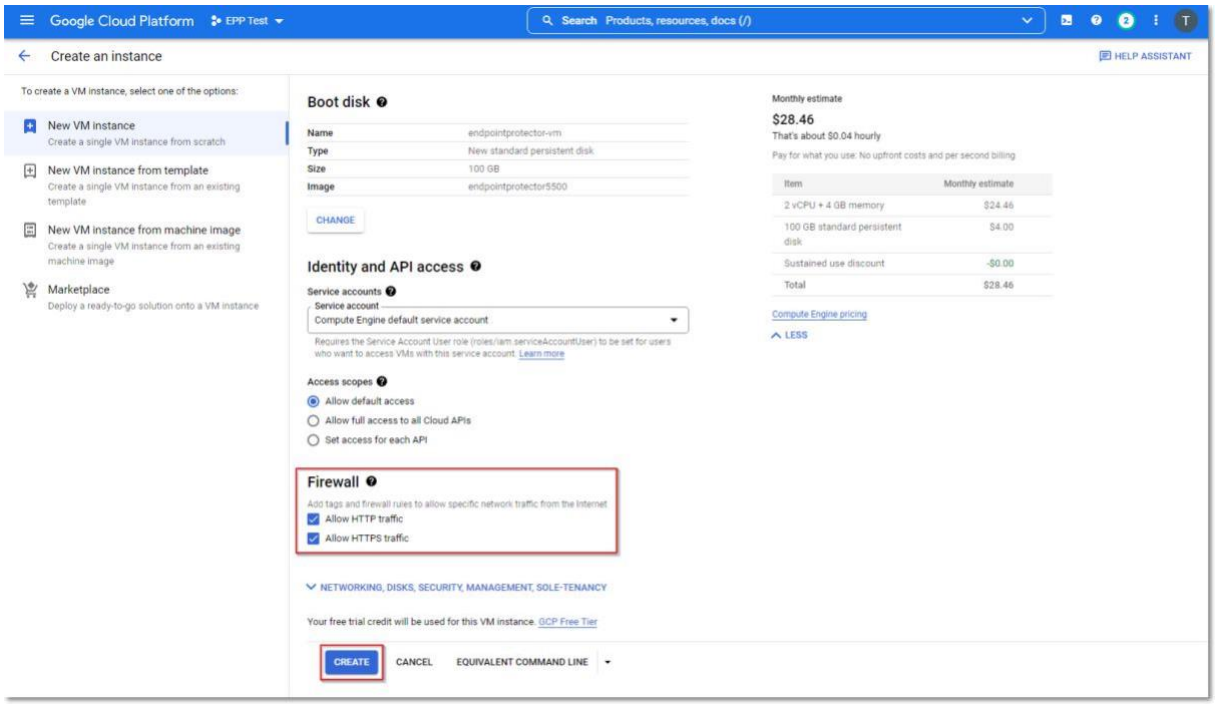
2. **Boot disk** 섹션에서 부트 디스크 구성 시작을 위한 **Change** 클릭 후 **Custom Images** 탭에서 아래 정보를 입력합니다:

   - **Image** – 가져온 이미지 선택
   - **Boot disk type** - **Standard persistent disk** 선택
   - **Size** – 전달 받은 Endpoint Protector 이미지보다 더 크게 추가

부트 디스크 구성 확인을 위해서 **Select** 클릭



3. **Firewall** 섹션에서 **Allow HTTP traffic** 과 **Allow HTTPS traffic** 선택 후 **Create** 클릭합니다.

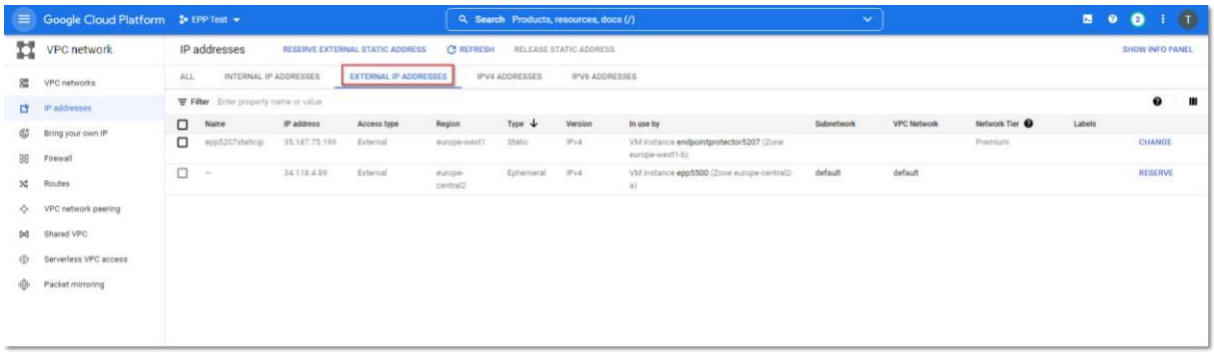


3.6. Request a Static IP

Static IP 를 요청해야 인스턴스 재시작 경우에 Endpoint Protector 클라이언트가 같은 IP 주소로 통신할 수 있습니다.

Static IP (Elastic IP) 없으면 인스턴스는 재시작 할 때마다 새로운 IP 주소를 할당 받을 것이고 매 번 Endpoint Protector 클라이언트를 재설치해야 합니다.

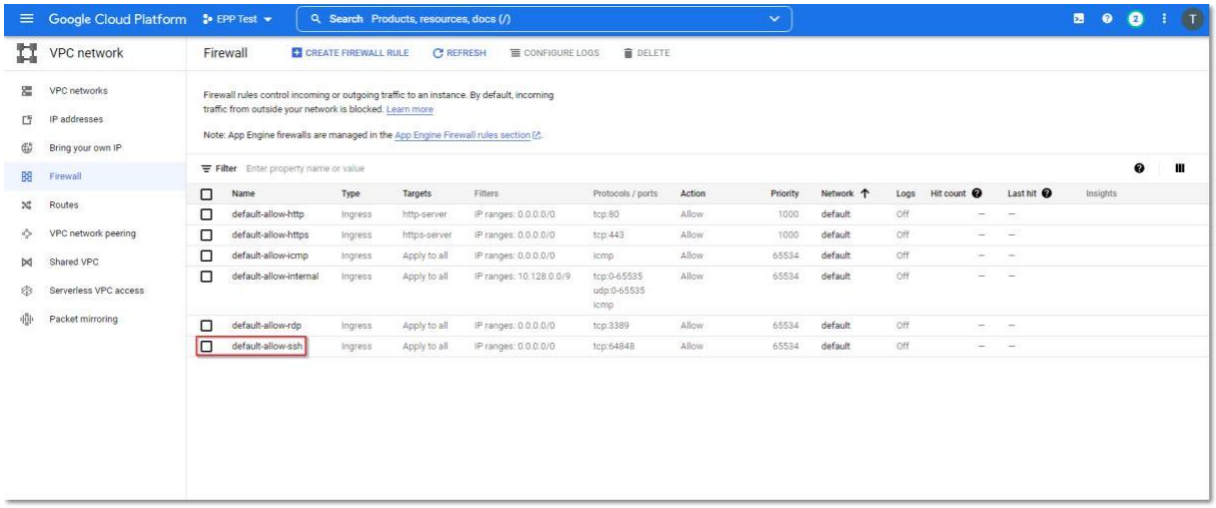
Static IP 를 요청하려면 **IP addresses** 이동 후 **External IP addresses** 탭을 선택합니다.



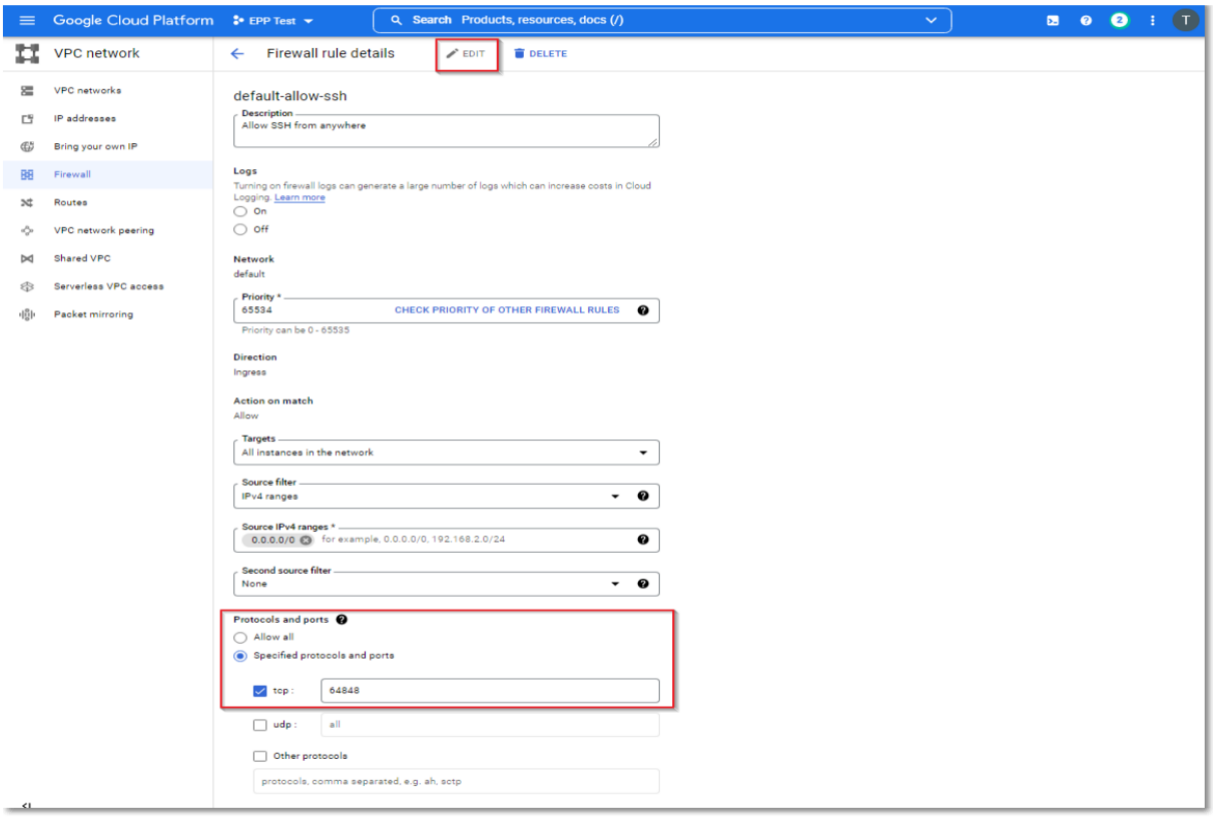
3.7. 방화벽 규칙 만들기

방화벽 규칙을 만들려면 Google Cloud Platform 콘솔에서 다음 단계를 따르시기 바랍니다:

1. **Firewall** 페이지 이동 후 **default-allow-ssh** 을 선택합니다;



2. **Edit** 클릭 후 **Protocols and ports** 섹션에 아래 정보를 입력합니다:
   - **Specified protocols and ports** 선택
   - **tcp** 박스 체크 후 **64848** 입력



4. Azure

4.1. Endpoint Protector Azure VM 받기

Endpoint Protector 는 일반적으로 Azure 마켓 플레이스에서 사용할 수 없습니다. VM (Virtual Machine)을 받기 위해서는 담당자에게 연락하고 Endpoint Protector VM 을 만드는 특정 컨테이너 접근 키와 같은 정보를 제공 받아야 합니다.

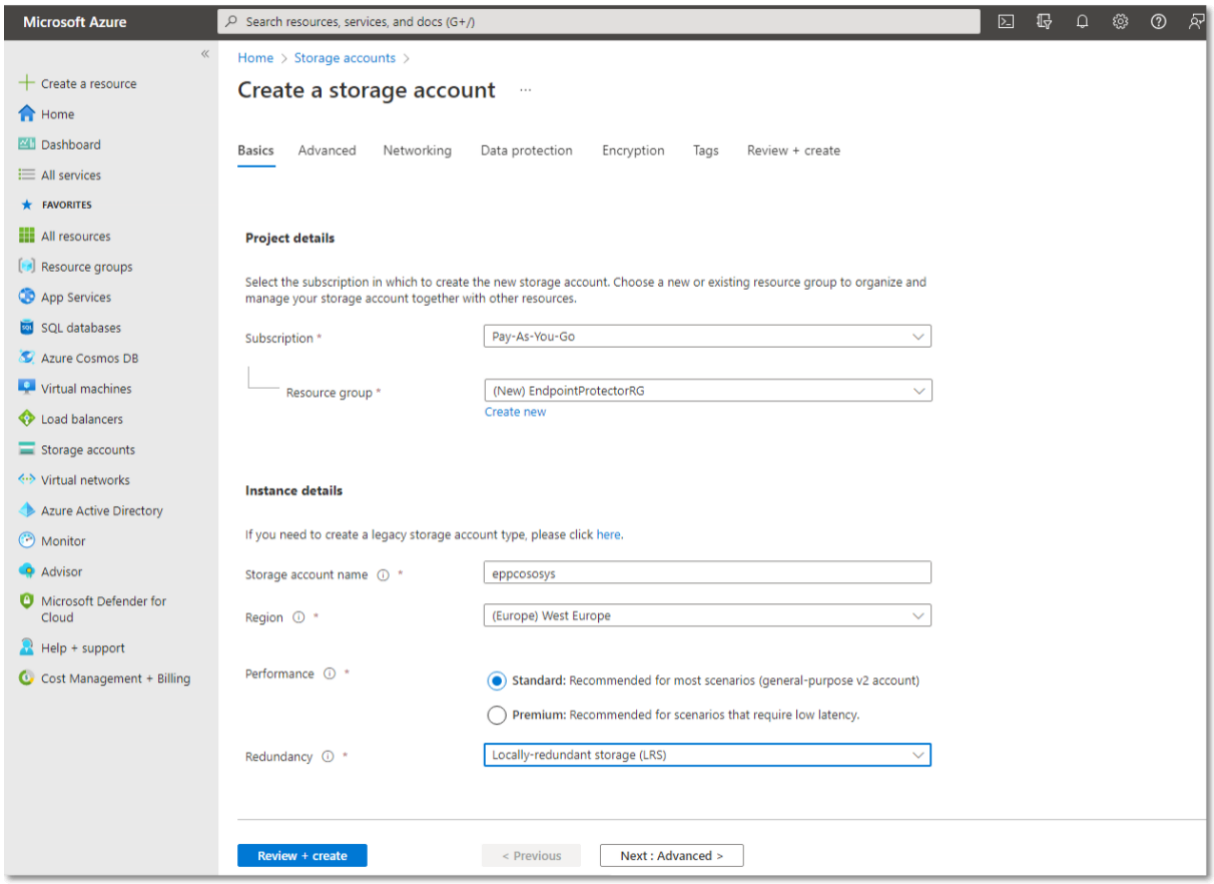
참고: 최대한 빠르게 컨테이너에 Endpoint Protector VM 을 업로드 할 것입니다. 이 단계가 마무리되면 접근 키를 다시 생성하시기 바랍니다.

4.2. 스토리지 계정 및 컨테이너 만들기

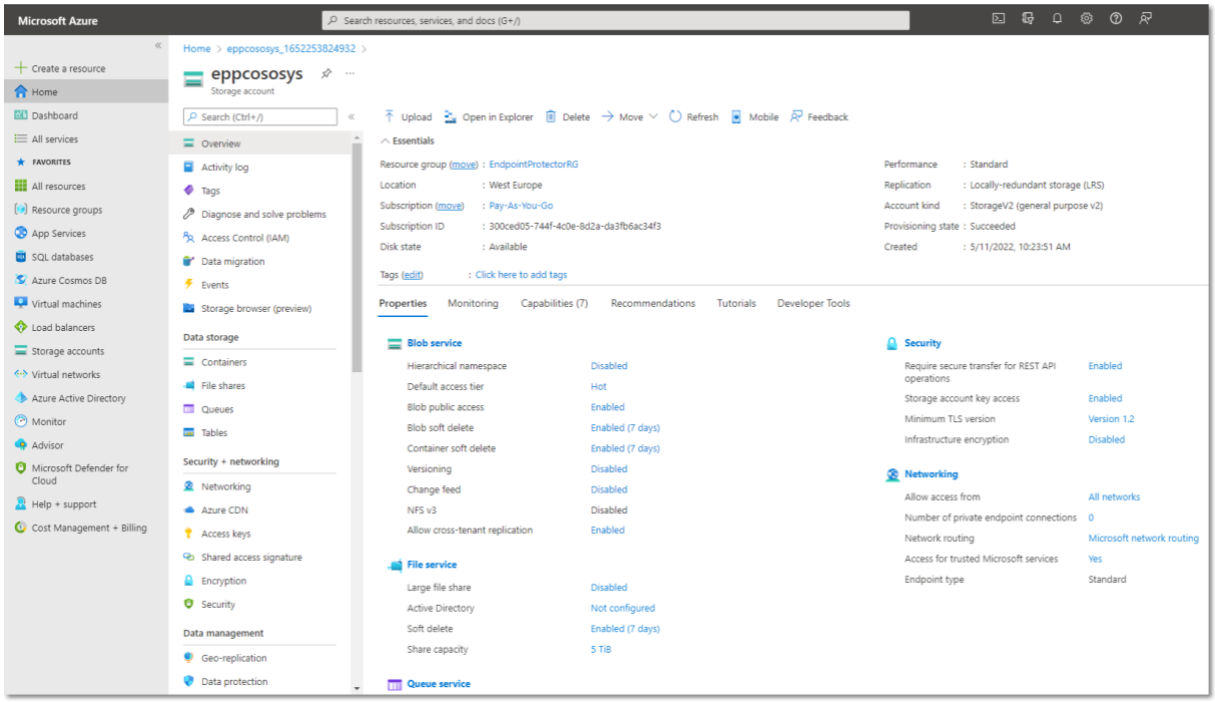
이 과정은 Azure 의 모든 다른 스토리지 계정 및 컨테이너를 만드는 것과 비슷합니다.
이와 비슷하게 준비가 되어 있거나 이미 전용 컨테이너가 만들어져 있다면 다음 단계를 진행하시기 바랍니다.
Azure Endpoint Protector VM 을 받으려면 전용 스토리지 계정 / 컨테이너를 만들어야 합니다. 아래 단계를 따르시기 바랍니다:

1. **Azure portal** 열기;
2. **Storage accounts** 이동 후 **+Create** 클릭;
3. **Storage account** 만들려면 아래 정보를 입력:
   - **Subscription** – **Pay-As-You-Go** 선택
   - **Resource group** – 사용 가능한 목록에서 그룹을 선택하거나 새로운 그룹 만들기

     Storage account name – 스토리지 계정 이름 추가
   - **Region** – Endpoint Protector 로 보호되는 가장 가까운 컴퓨터 위치
   - **Performance – Standard** 성능 선택
   - **Redundancy** – **Locally-redundant storage (LRS)** 선택
4. **Review + create** 클릭;



4. **Storage accounts** 이동 후 새롭게 만든 계정을 클릭합니다.;
5. **Containers** 이동 후 **+Container** 클릭;
6. 컨테이너에 스토리지 계정과 동일한 이름을 지정하고 **Public access level** 에 대해서 **Container (anonymous read access for containers and blobs)**를 선택합니다;



7. 만들어진 컨테이너를 선택하고 **Shared access tokens** 를 클릭합니다;

중요: 스토리지 계정이 아닌 컨테이너 레벨에서 토큰을 만들었는지 확인해야 합니다!

8. CoSoSys 팀이 이미지를 복사할 수 있도록 **5 일**간 창에서 **Create, Write and Add Permissions** 를 사용하여 **SAS token** 을 구성합니다;

9. **Blob SAS URL** 을 복사하고 CoSoSys 에 보냅니다.

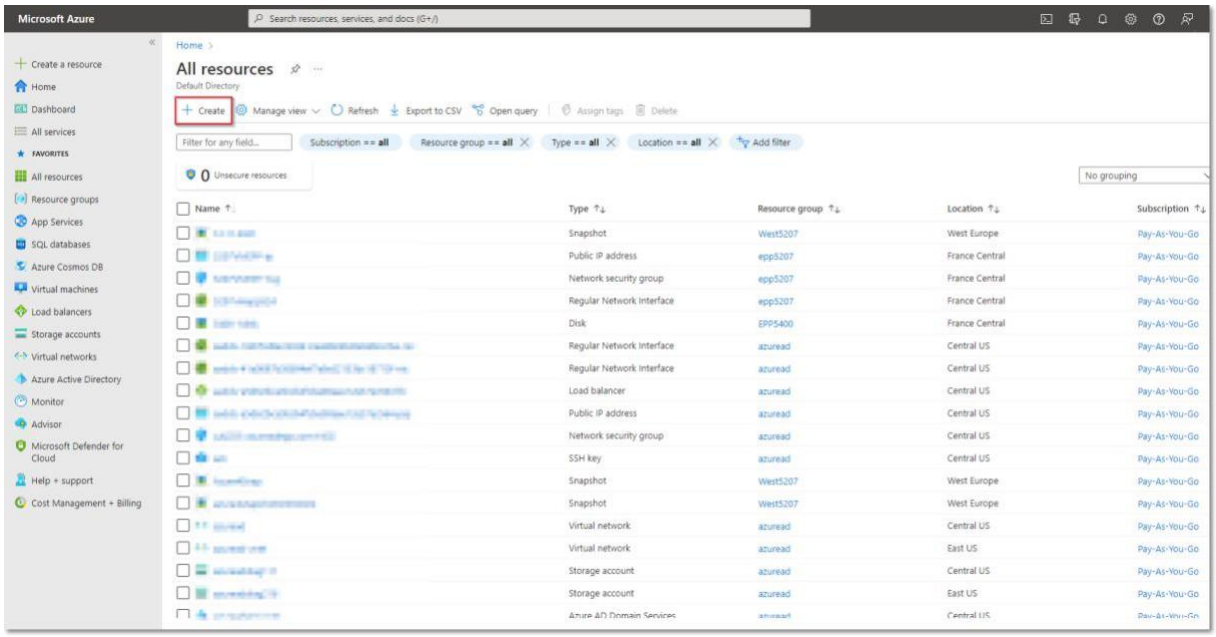
참고: CoSoSys 는 스토리지에 Endpoint Protector VM 을 복사하고 과정이 마무리되면 알려드립니다.

4.3. 디스크 만들기

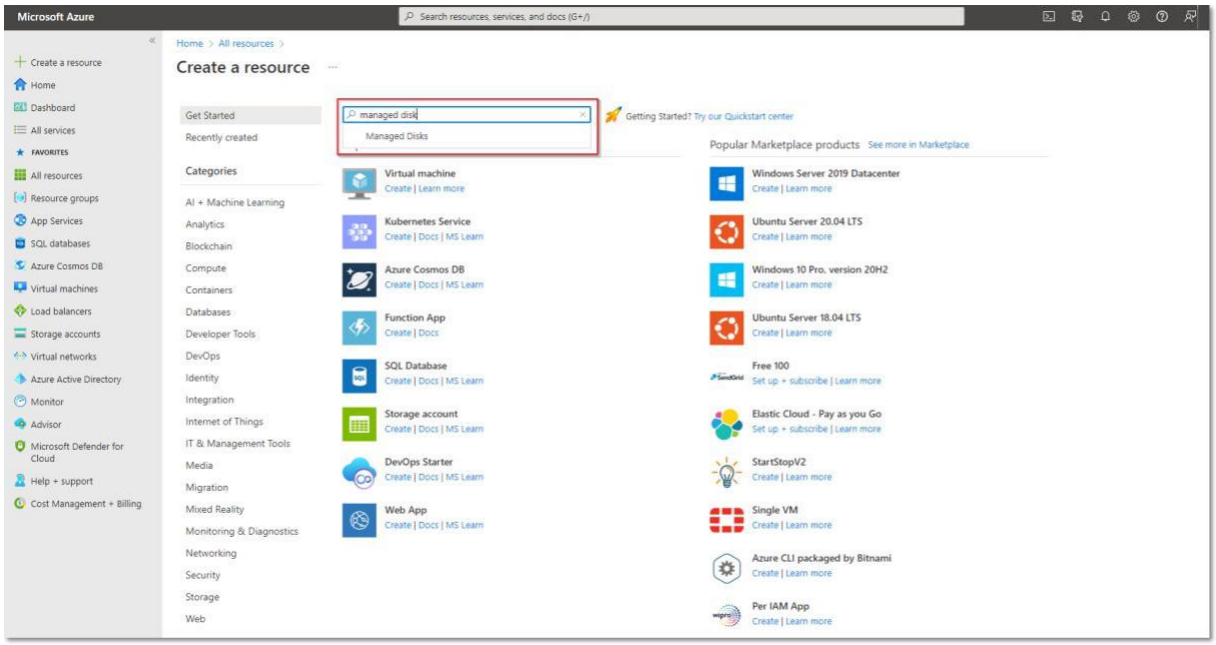
Endpoint Protector VM 을 시작하기 전에 디스크와 VM 을 준비해야 합니다.

디스크를 만들려면 아래 단계를 따르시기 바랍니다.

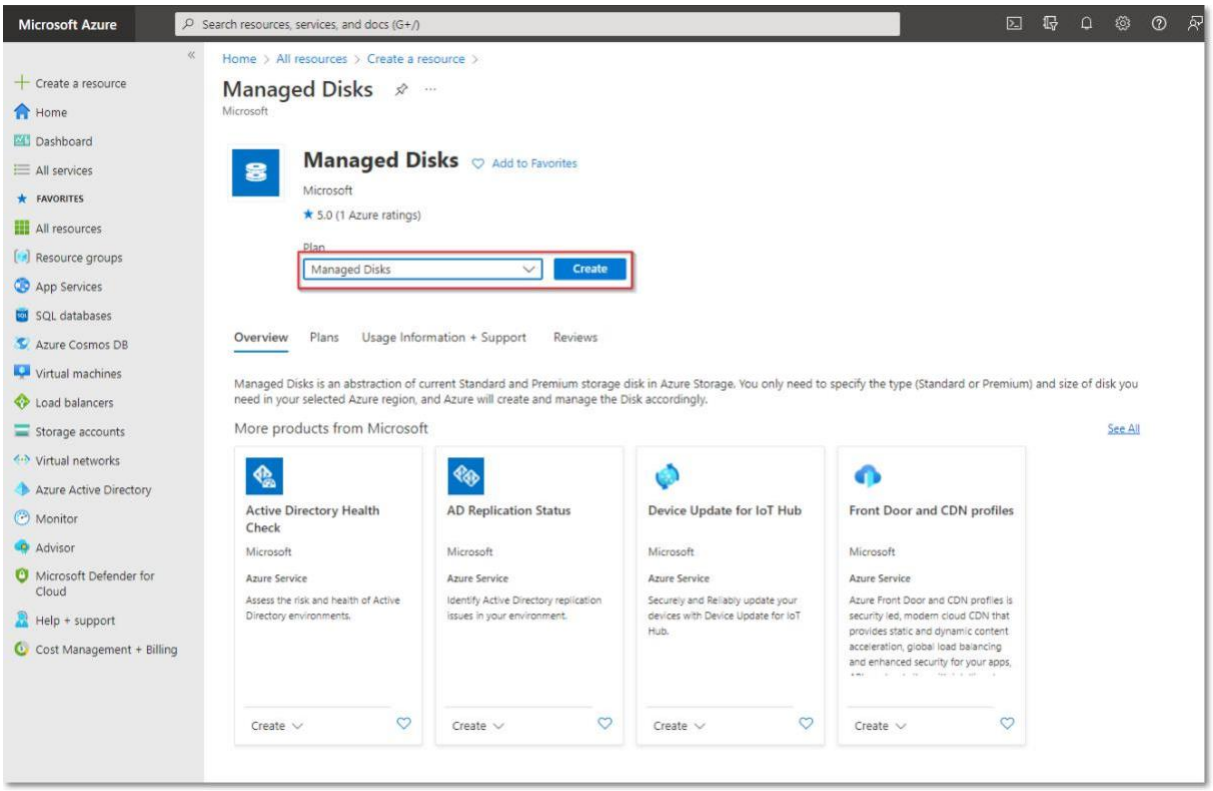
1. 페이지 우측 상단의 **All resources** 이동 후 **+Create** 을 클릭합니다;



2. 마켓 플레이스에서 **Managed Disks** 를 검색합니다;



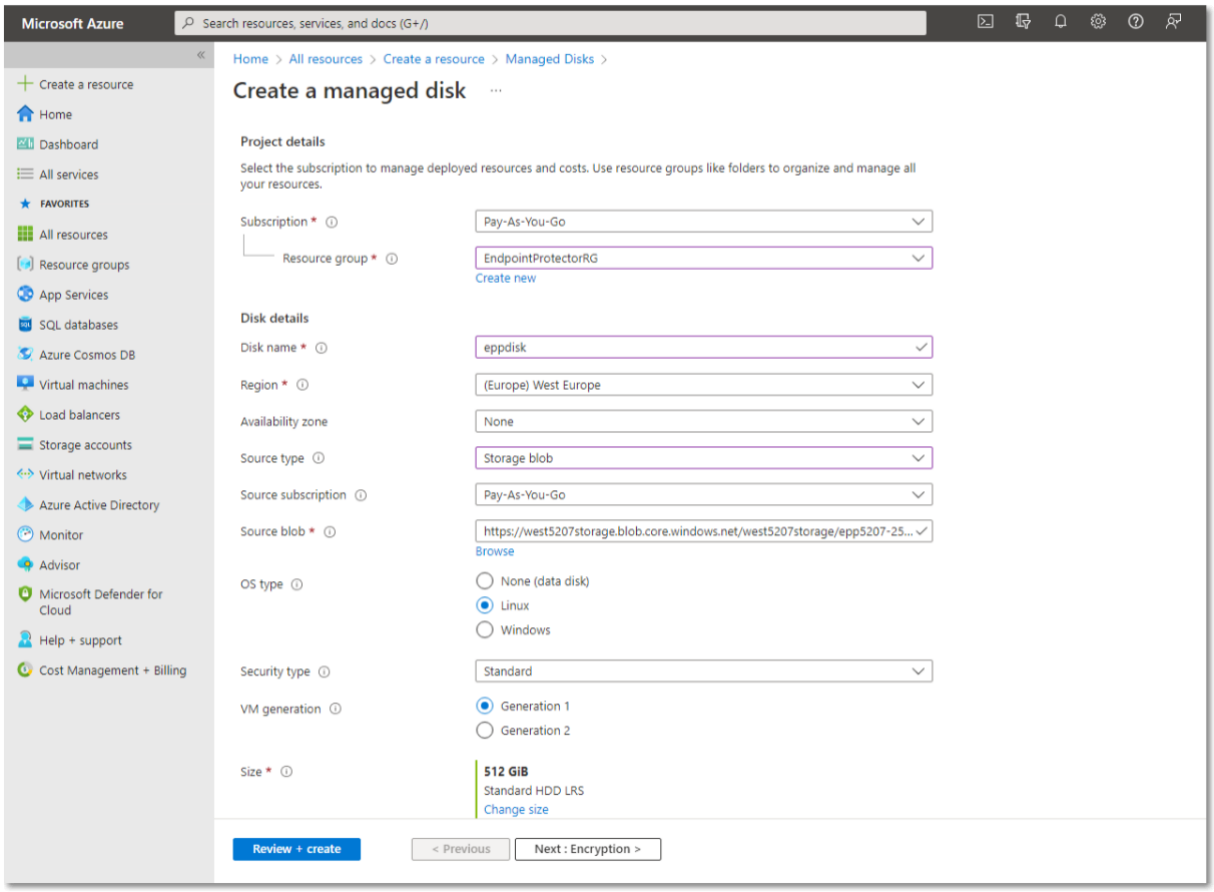
3. **Managed Disks** 이동 후 **Create** 를 선택합니다;



4. 관리 디스크를 만들려면 아래 정보를 입력합니다:

   - **Subscription - Pay-As-You-Go** 선택
   - **Resource group** – 이전에 만든 리소스 그룹 선택
   - **Disk name** – 스토리지 계정 이름 추가
   - **Region** – Endpoint Protector 로 보호되는 가장 가까운 컴퓨터의 위치 선택
   - **Availability Zone**
   - **Source type - Storage Blob** 선택
   - **Source subscription - Pay-As-You-Go** 선택
   - **Source blob** – 위에서 언급한 키와 URL 제공 후 CoSoSys 에서 받은 URL 입력
   - **OS type** - select **Linux**
   - **Security type** – **Standard** 선택
   - **VM generation** – **Generation 1** 선택
   - **Size - 128 GB** 선택

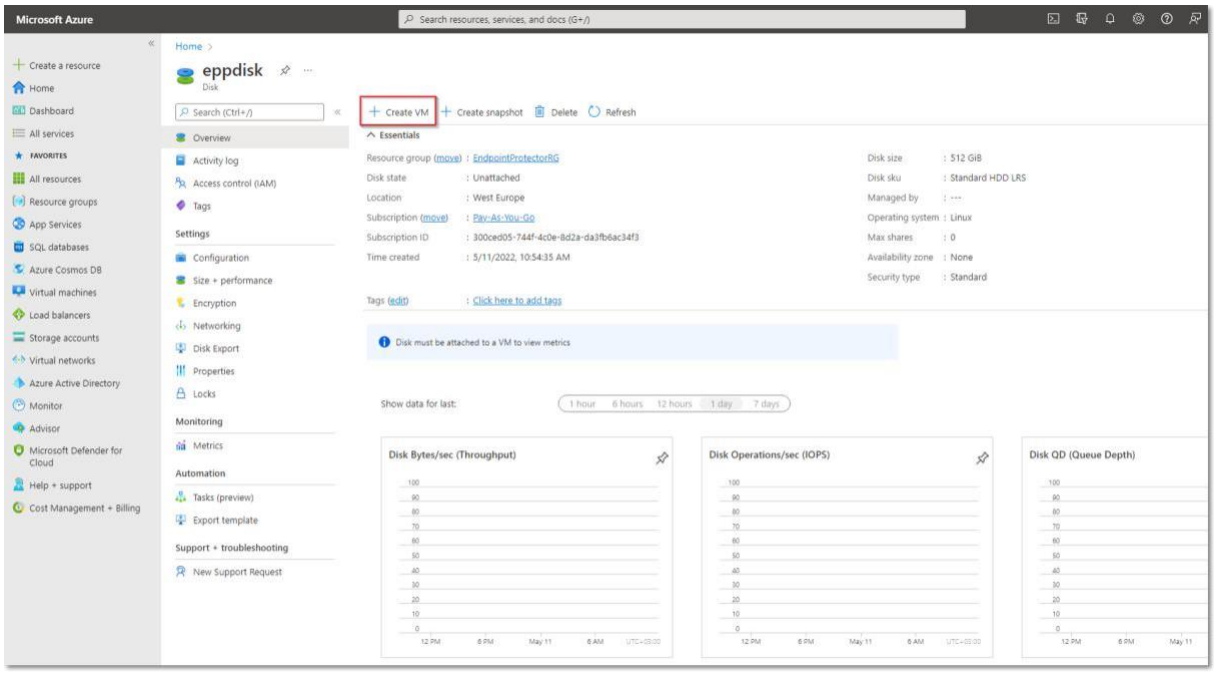
5. **Review + Create** 클리기 후 **Successfully created disk** 메시지가 표시될 때까지 기다립니다.



4.4. 가상 머신 만들기

Azure 에서 Endpoint Protector VM 을 만들려면 아래 단계를 따르시기 바랍니다:

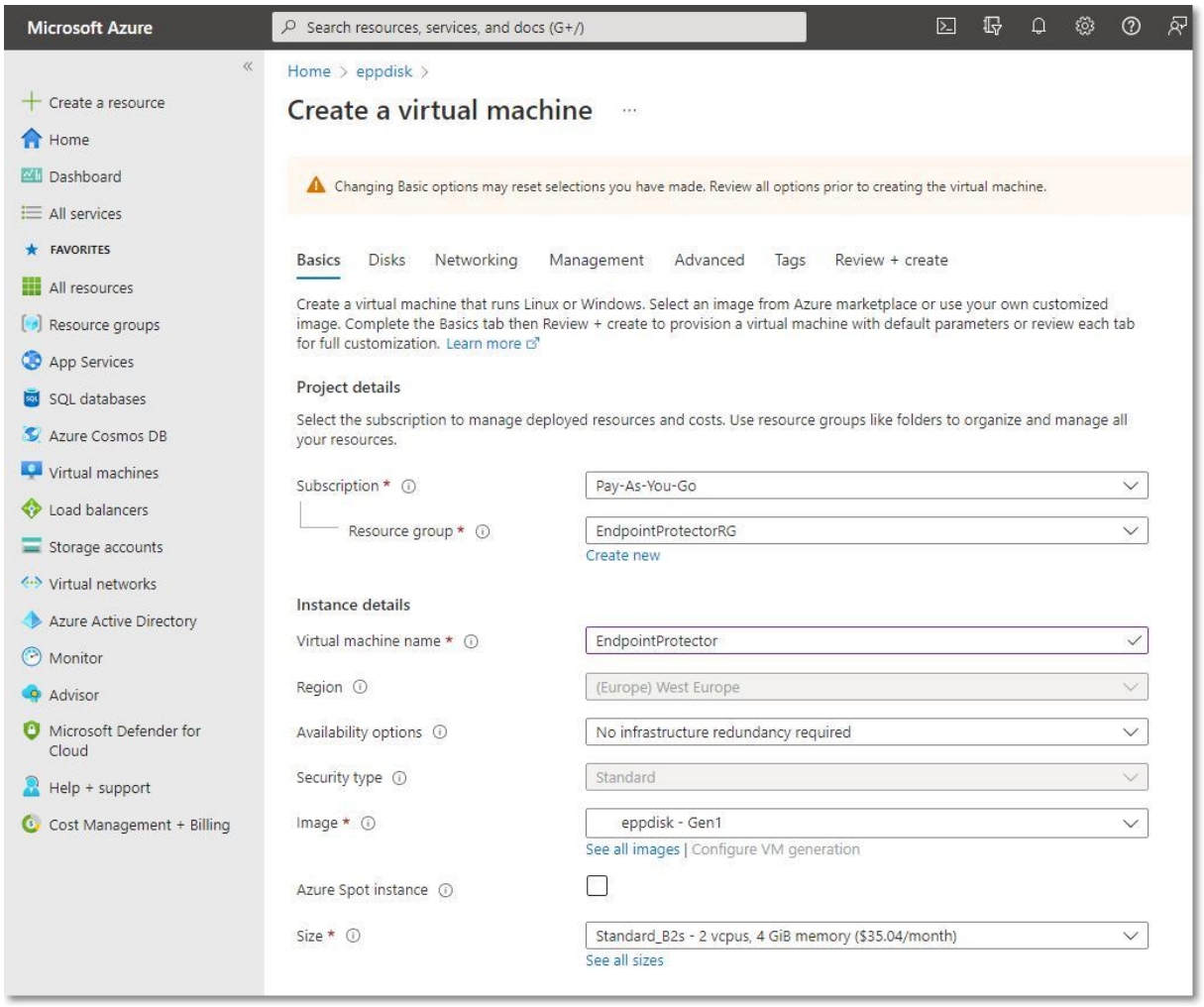
1. **All resources** 페이지 이동 후 새롭게 만든 디스크 선택 후 **Create VM** 클릭



2. VM 을 만들려면 아래 정보를 입력합니다:

Basics 탭에서 아래 내용 제공:

- **Subscription** – **Pay-As-You-Go** 선택
- **Resource group** – 디스크 만들 때 사용된 그룹 선택
- **Virtual Machine Name** – VM 이름 입력
- **Size** – 사용된 디스크 파일의 권장 요구 사항과 가장 가까운 VM 프로파일 기반으로 선택

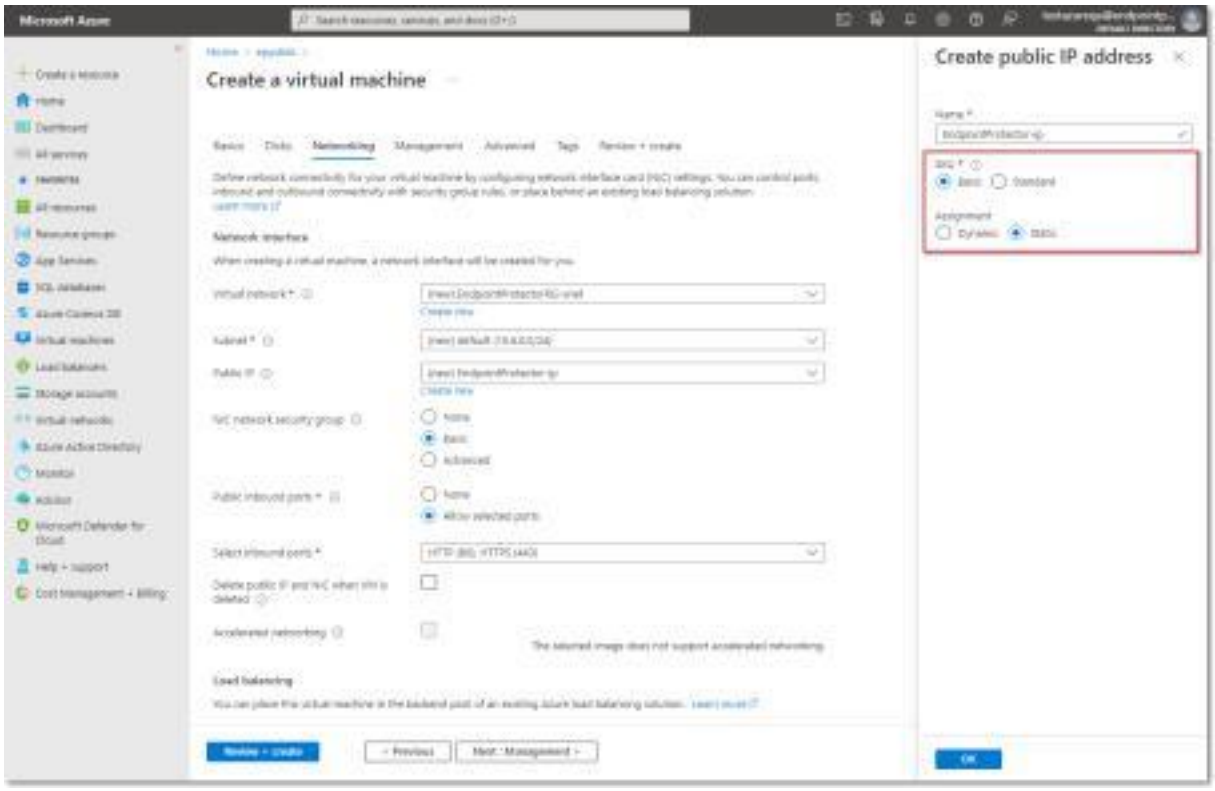


Networking 탭에서 아래 내용 제공:

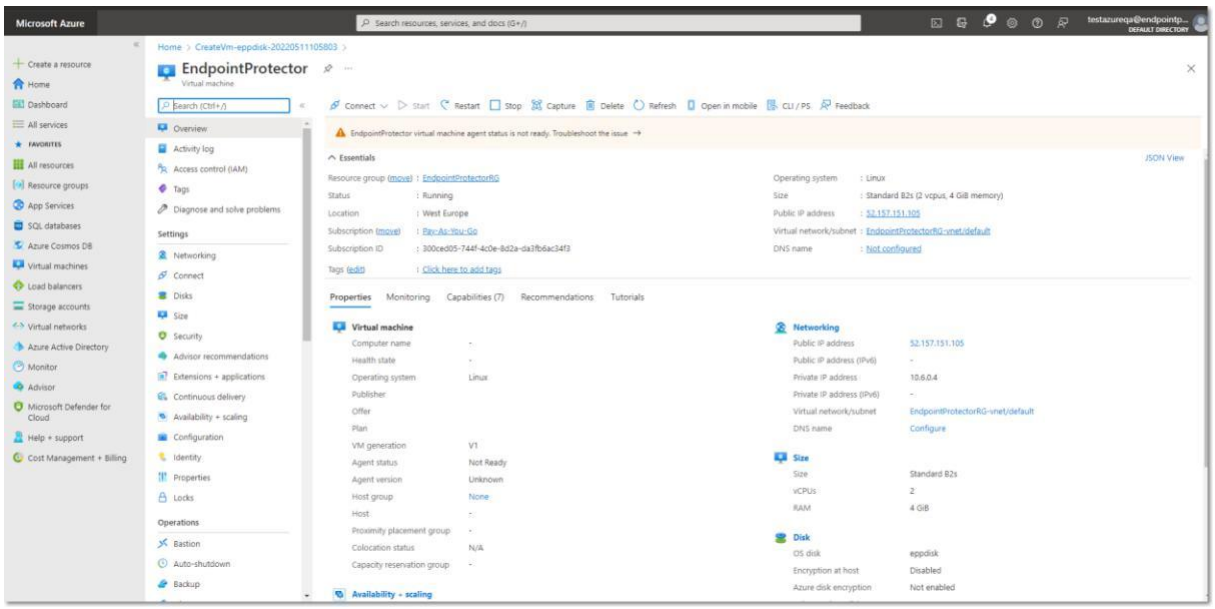
- **Public IP** - **Create new** 클릭 후 **Basic SKU** 와 **Static Assignment** 선택
- **Select inbound ports** – **HTTP (80)**와 **HTTPS (443)** 추가

Review + create 클릭 후 **Create** 합니다.

참고: 추가 기능과 관련하여 VM 에 부착된 사용하지 않는 SSD 의 불필요한 요금 지불을 피하기 위해서 SSD 대신 HDD 선택을 권장합니다.



3. 배포가 끝나면 우측의 **Virtual Machines** 이동 후 Endpoint Protector 이미지를 선택합니다;



4. 웹 브라우저를 열고 할당된 Endpoint Protector 이미지에 Public IP 주소를 연결합니다.

5. Endpoint Protector 라이선스

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.

6. 면책

Endpoint Protector Appliance does not communicate outside of your network except with liveupdate.endpointprotector.com and cloud.endpointprotector.com.

Endpoint Protector does not contain malware software and does not send at any time any of your private information (if Automatic Live Update Reporting is DISABLED).

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.

EndpointProtector.com