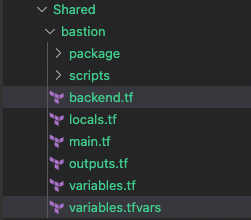
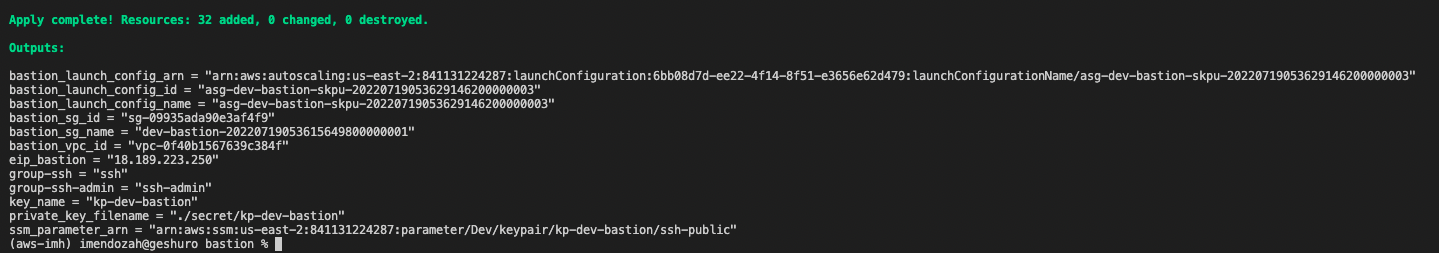
**DESPLIEGUE DE BASTION, IAM-SSH-OPENVPN Y SNS DESDE TERRAFORM**

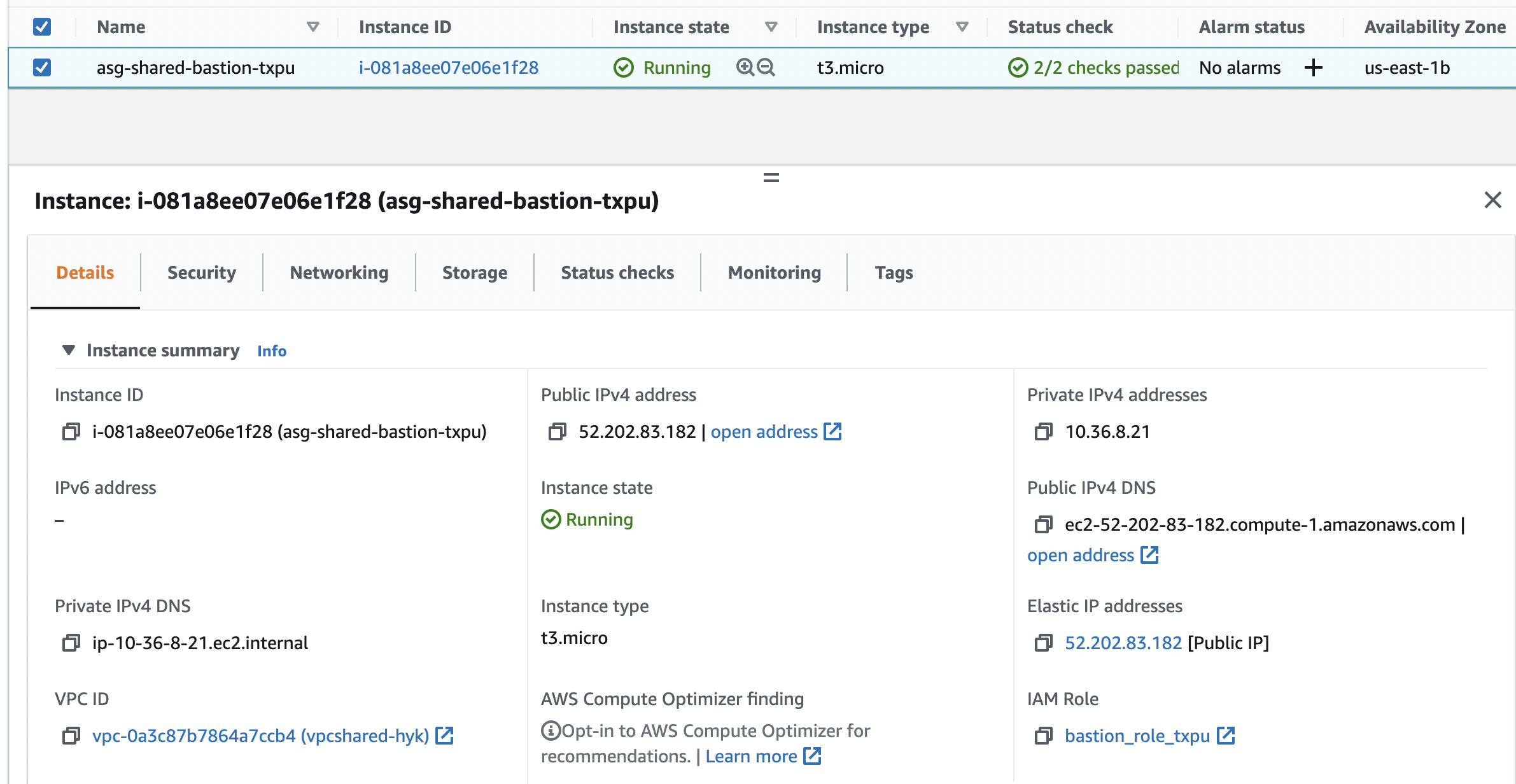
1. **Despliegue de Bastion**
   1. Nos ubicamos en el repositorio **integracam/aws/Shared/bastion**
   2. Es necesario modificar el nombre del recurso S3 y Dynamo que usemos en los archivos



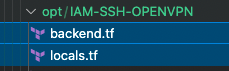
* 1. Ejecutamos el script
     1. Nos ubicamos en el repositorio **integracam/aws** y luego ejecutamos bash 3-project-install-bastion.sh



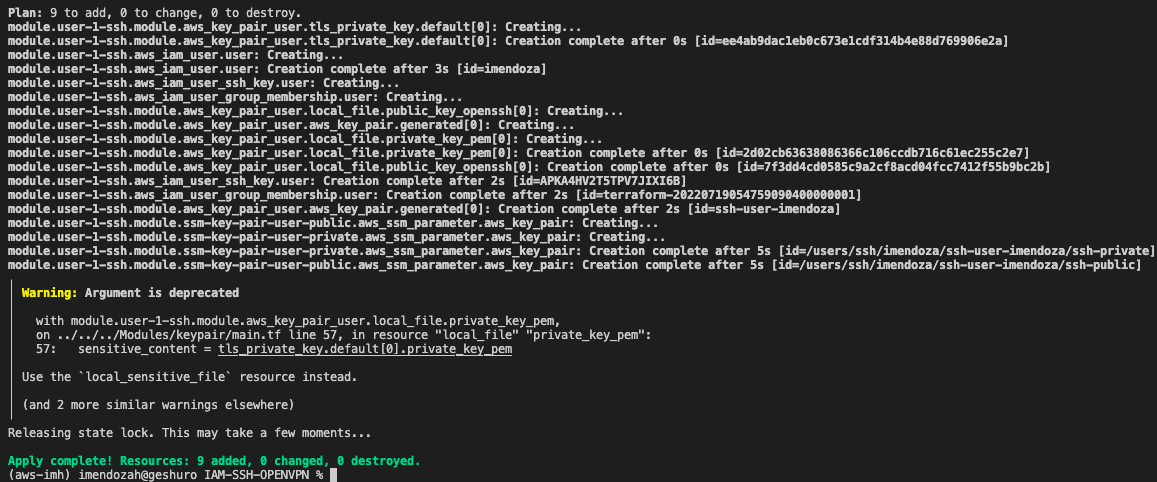
* + 1. Al terminar la ejecución del proceso de creación del bastion , se debe visualizar desde la consola de AWS



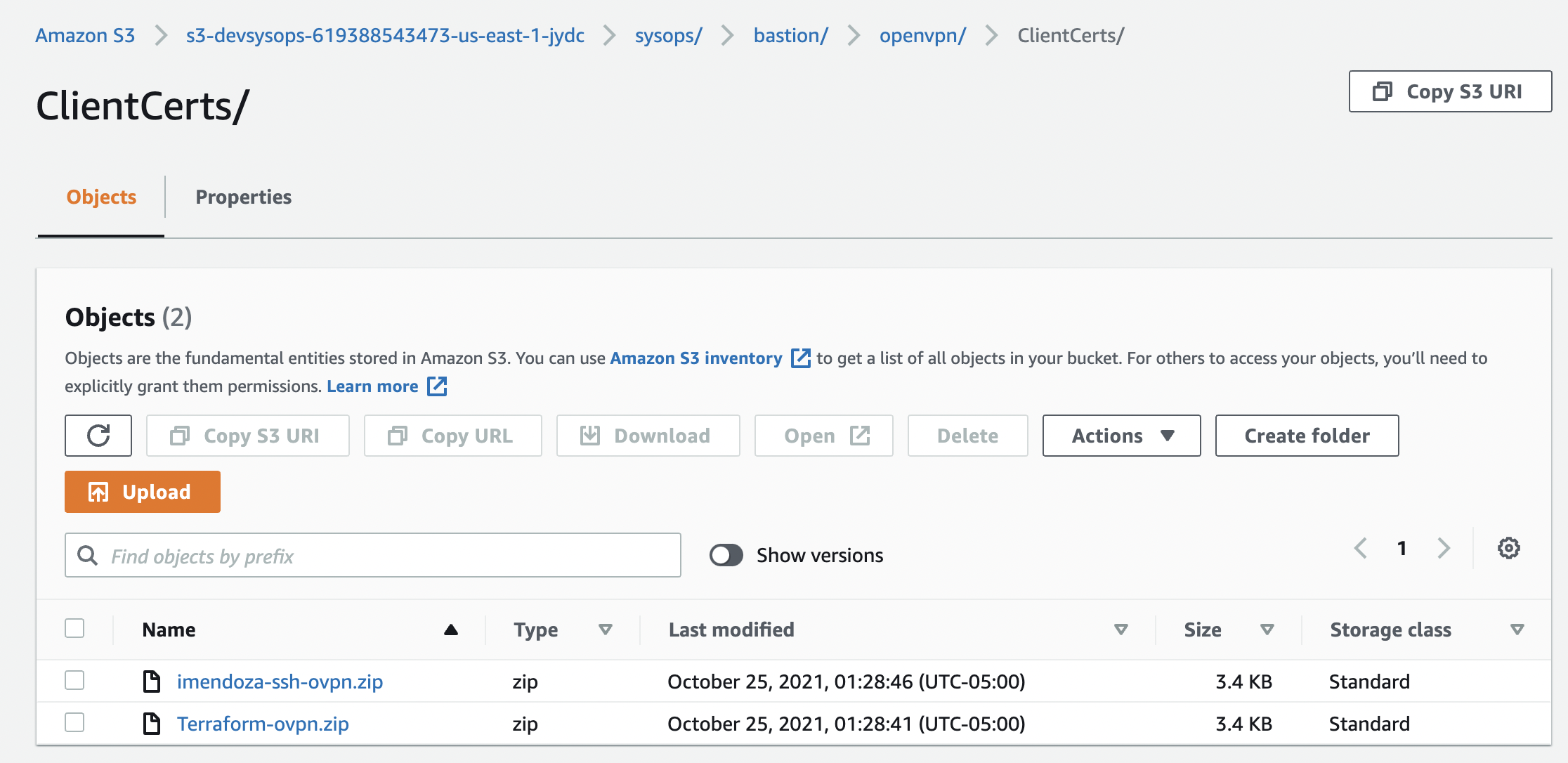
1. **Despliegue de IAM-SSH-OPENVPN**
   1. Nos ubicamos en el repositorio **integracam/aws/Shared/opt/ IAM-SSH-OPENVPN**
   2. Es necesario modificar el nombre del recurso S3, Dynamo, profile de cuenta aws, que usemos en los archivos:

****

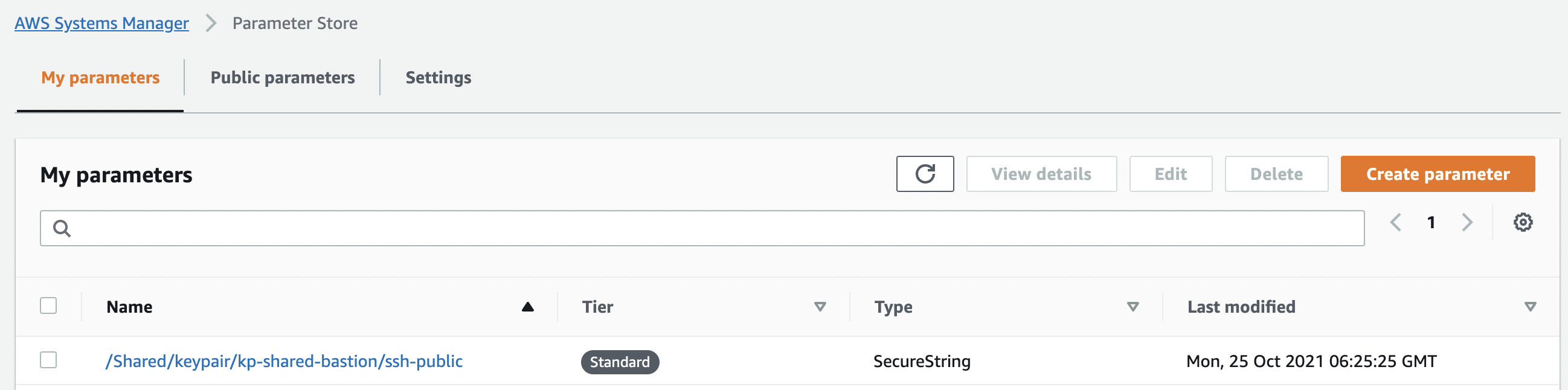
1. Ejecutamos el script
   * 1. Nos ubicamos en el repositorio **skydropx/aws** y luego ejecutamos bash 4-project-install-bastion-openvpn.sh



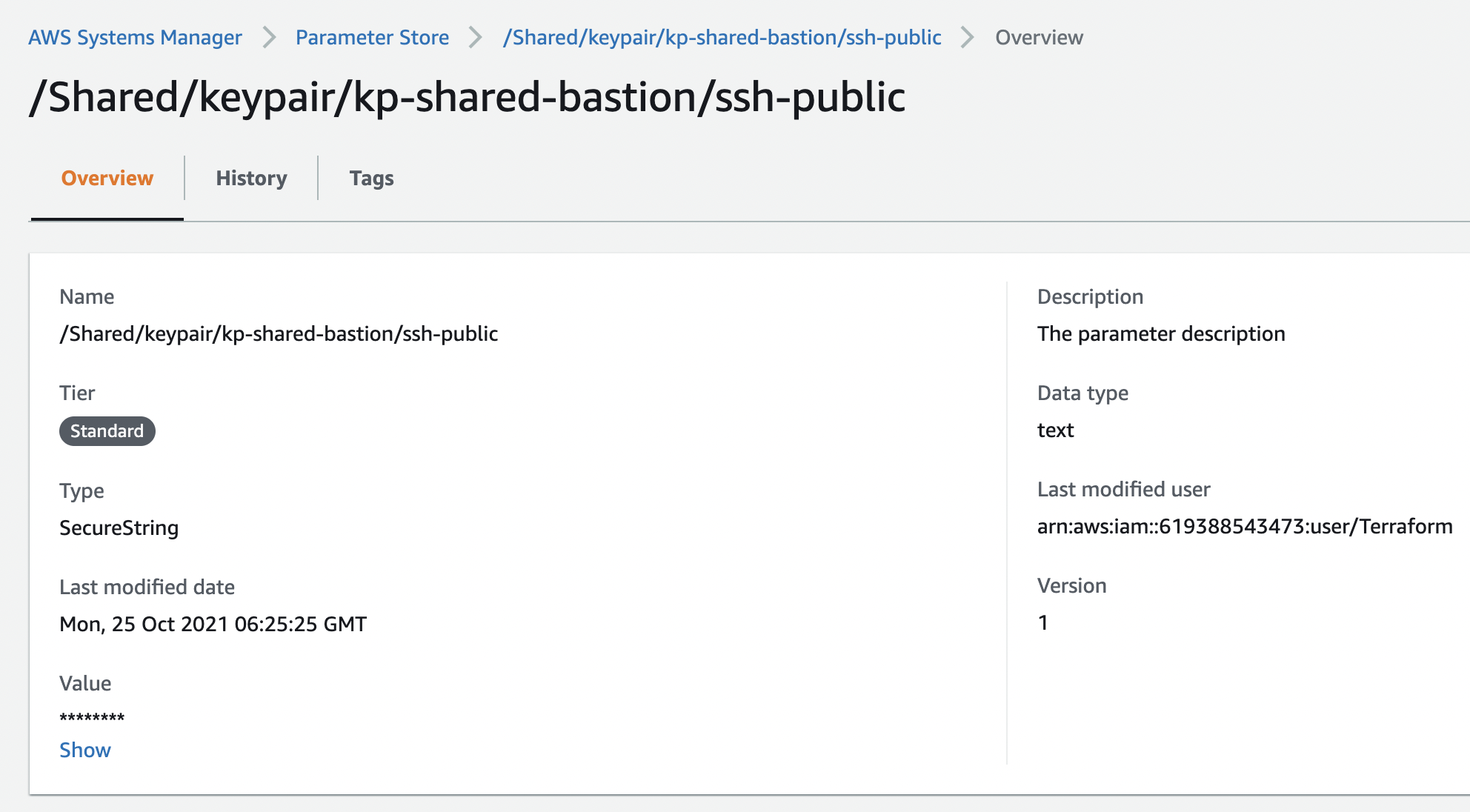
1. **Creación de certificados de clientes para la conexión VPN**
   1. Opción 1: Durante la creación del bastion se copia en la ruta /usr/bin el script import\_users.sh, el cual está configurado para que se ejecute cada 10 minutos y entre sus funciones está la creación de los certificados cliente de los usuarios de la VPN. Por lo que debemos esperar 10 minutos luego de la creación del bastión para ver los certificados en el S3 que tenemos creado en la siguiente ruta (El nombre del recurso cambia, de acuerdo al despliegue realizado):



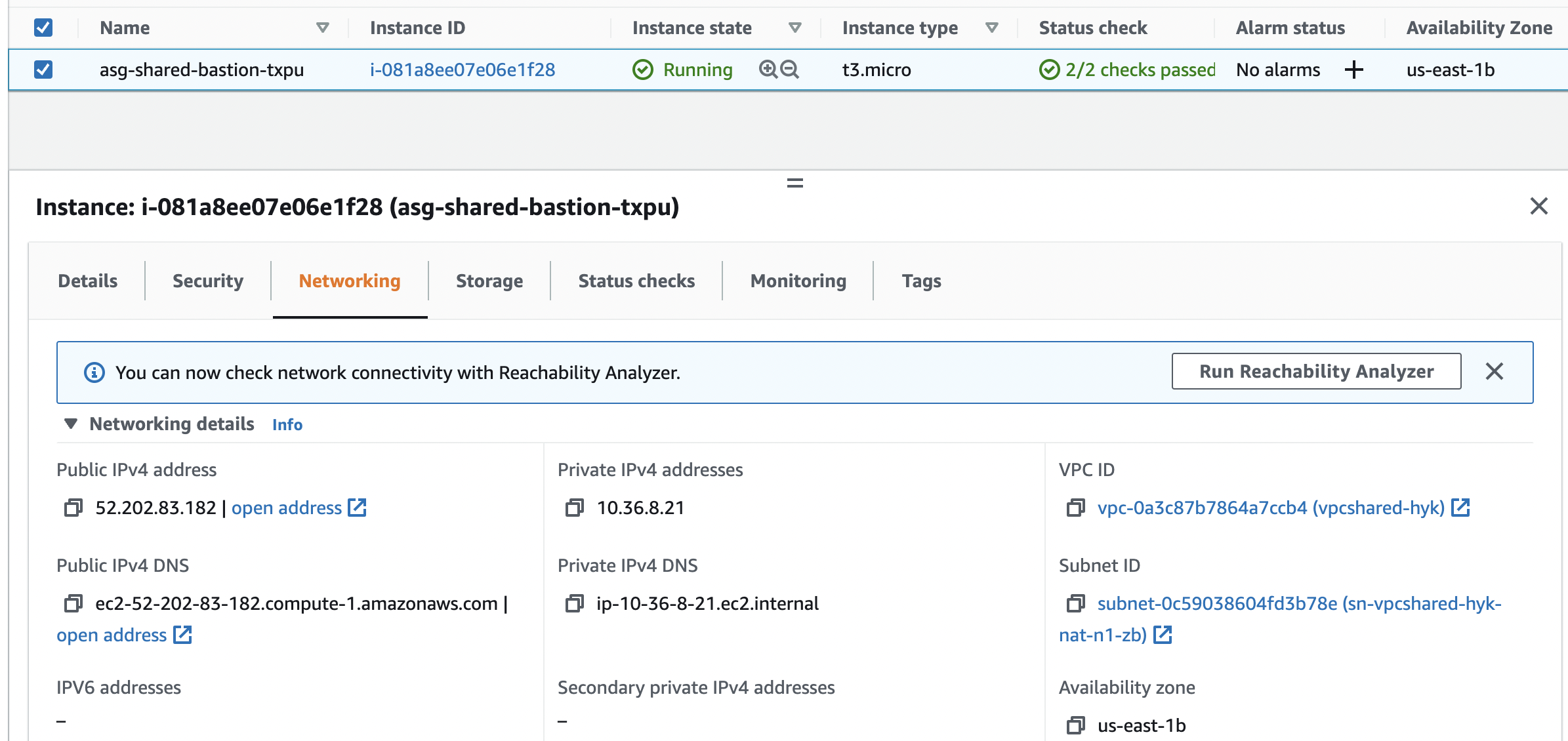
* 1. Opción 2: Si requerimos crear los usuarios antes de pasados los 10 minutos comentados en la opción 1. Procedemos a acceder vía ssh al bastion para ejecutar el script ubicado en /usr/bin/import\_users.sh de forma manual.
     1. Buscamos la Key Pair asociada al bastion: /Shared/keypair/kp-shared-bastion/ssh-public



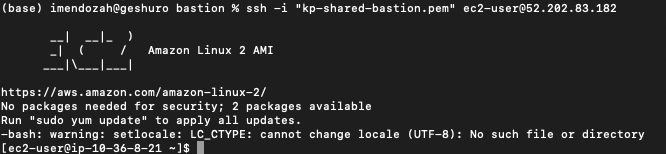
* + 1. La seleccionamos y hacemos clic en Value 🡪 Show



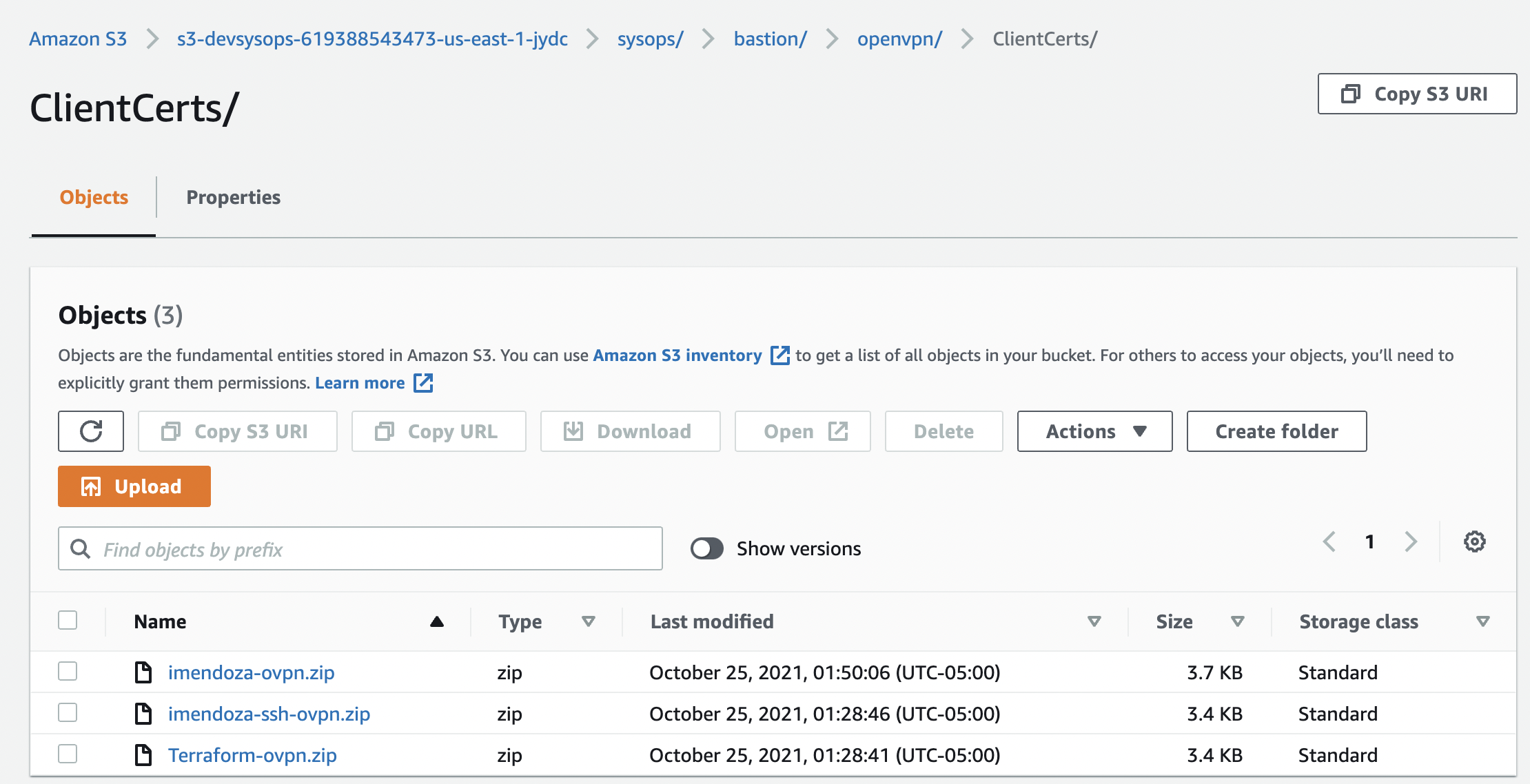
* + 1. Copiamos la key desde “-----BEGIN RSA PRIVATE KEY-----“ hasta “-----END RSA PRIVATE KEY-----“. Lo pegamos en un editor de texto y la guardamos como kp-dev-bastion.pem
    2. Revisamos la ip pública asignada al bastion en el Dashboard de EC2



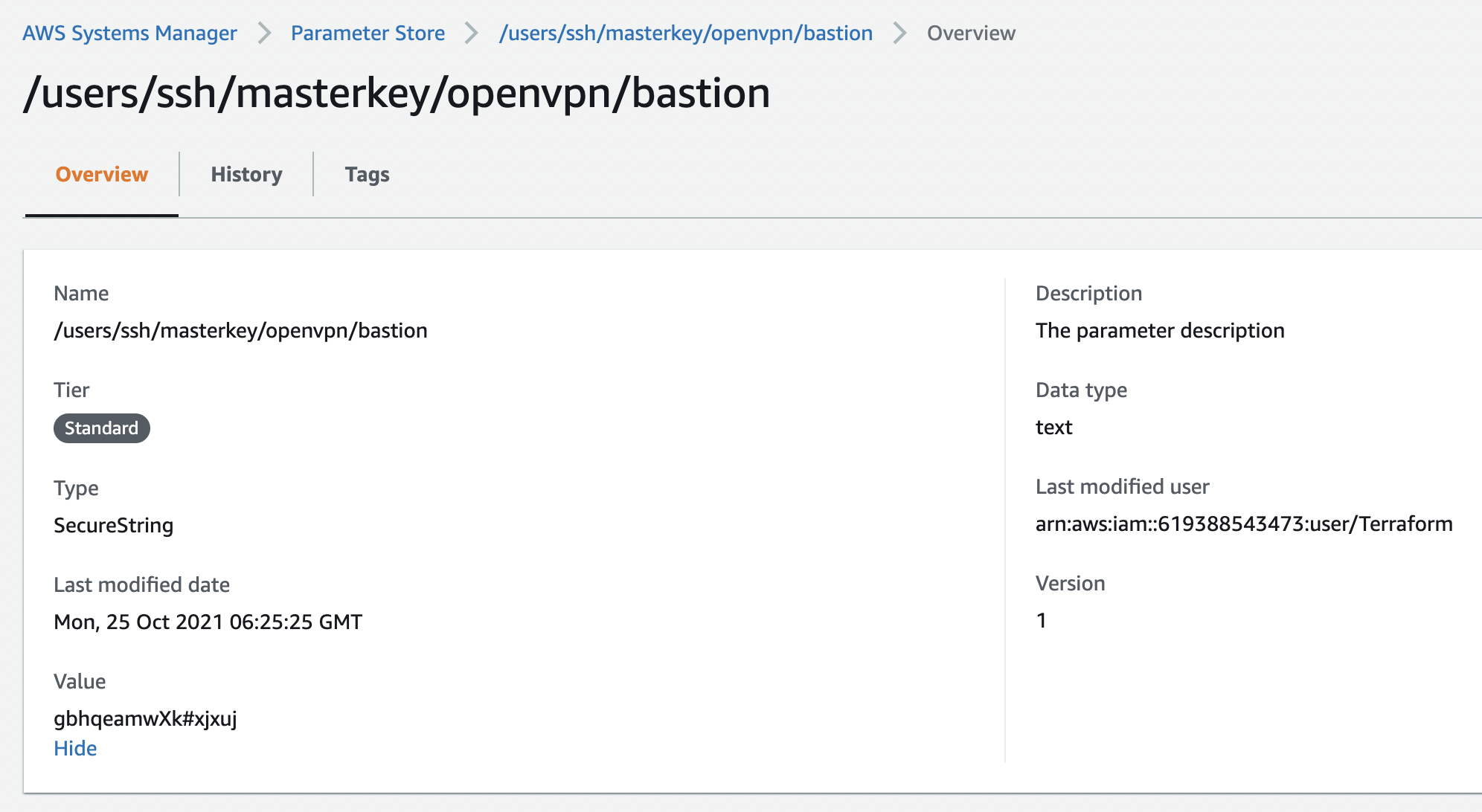
* + 1. Ejecutamos el comando ssh –i “kp-shared-bastion.pem” ec2-user@52.202.83.182 (La ip cambiaría según el caso que despleguemos)



* + 1. Una vez hemos accedido al bastion ejecutamos **sudo /usr/bin/import\_users.sh.** Esta ejecución no muestra salida, sólo debemos verificar que se hayan creado los certificados de los clientes para conexión a la VPN, en el recurso S3, en la siguiente ruta:

****

1. **Pruebas de conexión a la VPN**
   1. Descargar el archivo del usuario, de la ruta descrita en el paso anterior, por se descarga el ejemplo: imendoza-ovpn.zip.
   2. Se descarga y luego para descomprimir es necesario usar una clave maestra, la cual está almacenada en la consola de AWS en System Manager 🡪 Parameter Store



* 1. Una vez que podamos descomprimir el archivo .ovpn.
  2. La conexión a la VPN debe resultar exitosa para comprobar que el servicio está funcionando correctamente.

1. **Conexión a una instancia a través de la conexión VPN establecida**
   1. Crear una instancia.
   2. Visualizar la ip privada asignada a la máquina creada y acceder a través de ssh con la key pair que hayamos asociado a la máquina, con el comando ssh –i “keypair” ubuntu@ipprivadamaquina
   3. Si logramos hacer la conexión de forma exitosa lograremos comprobar el correcto funcionamiento de la VPN.