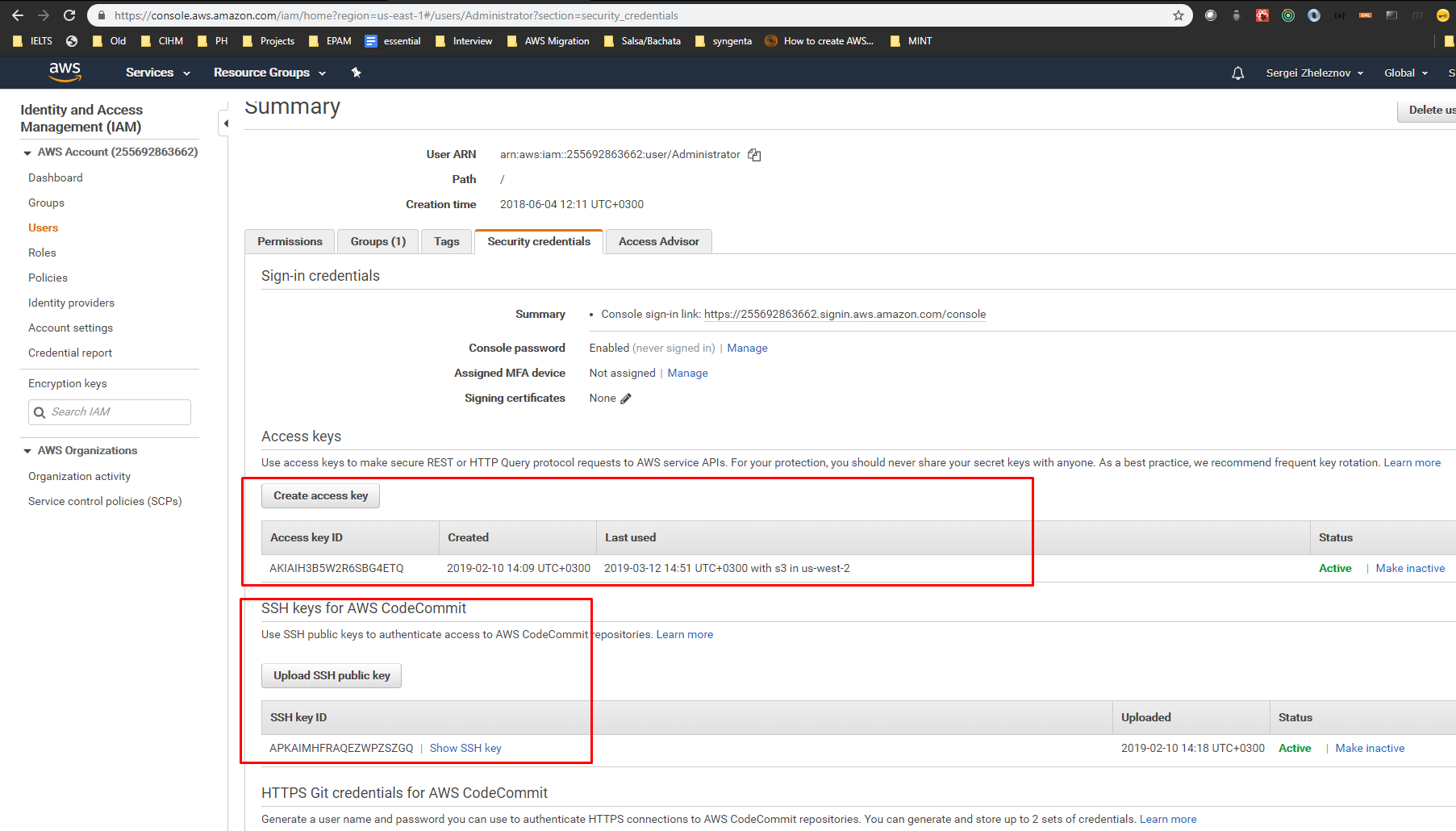
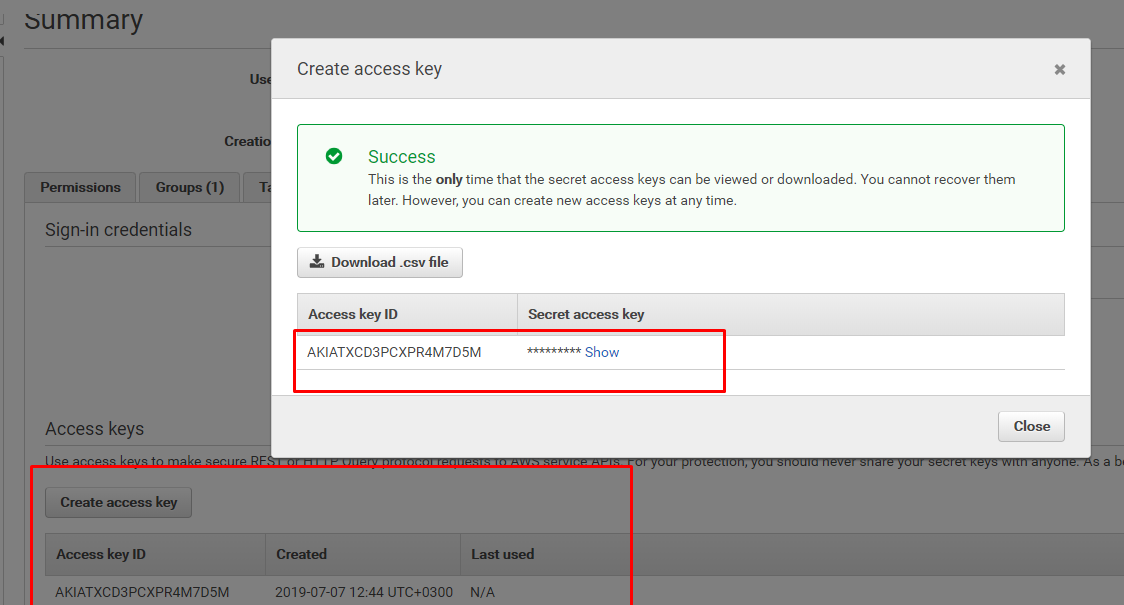
# SSH KEY/AWS Profile/AWS CLI Console/IAM/EC2

## USERS, ACCESS KEY (aws configure), SSH rsa ‘pub’ and ‘private’ keys

1. Create User (do not use roles, groups for this sample). Add the Administrator or another role to it.
   1. Generate Access Keys
   2. Generate SSH key (generate it locally and upload or download from remote and install locally)
2. Recrate key if necessary



1. Remotely create a new key (save Access key ID and key value):
   1. 
      1. Key Id: AKIATXCD3PCXPR4M7D5M
      2. Value: 4UM00FDPOY9izXSldo51tCe64TYYqdj5Eeap4P+J
2. Choose an active profile. The profile is associated with a user.
3. Locally set up a new key:

>aws configure help

*Configure AWS CLI options. If this command is run with no arguments,*

*you will be prompted for configuration values such as your AWS Access*

*Key Id and you AWS Secret Access Key. You can configure a named*

*profile using the "--profile" argument. If your config file does not*

*exist (the default location is "~/.aws/config"), the AWS CLI will*

*create it for you. To keep an existing value, hit enter when prompted*

*for the value. When you are prompted for information, the current*

*value will be displayed in "[brackets]". If the config item has no*

*value, it be displayed as "[None]". Note that the "configure" command*

*only work with values from the config file. It does not use any*

*configuration values from environment variables or the IAM role.*

*Note: the values you provide for the AWS Access Key ID and the AWS*

*Secret Access Key will be written to the shared credentials file*

*("~/.aws/credentials").*

\* \*\*aws\_access\_key\_id\*\* - The AWS access key part of your credentials

\* \*\*aws\_secret\_access\_key\*\* - The AWS secret access key part of your

credentials

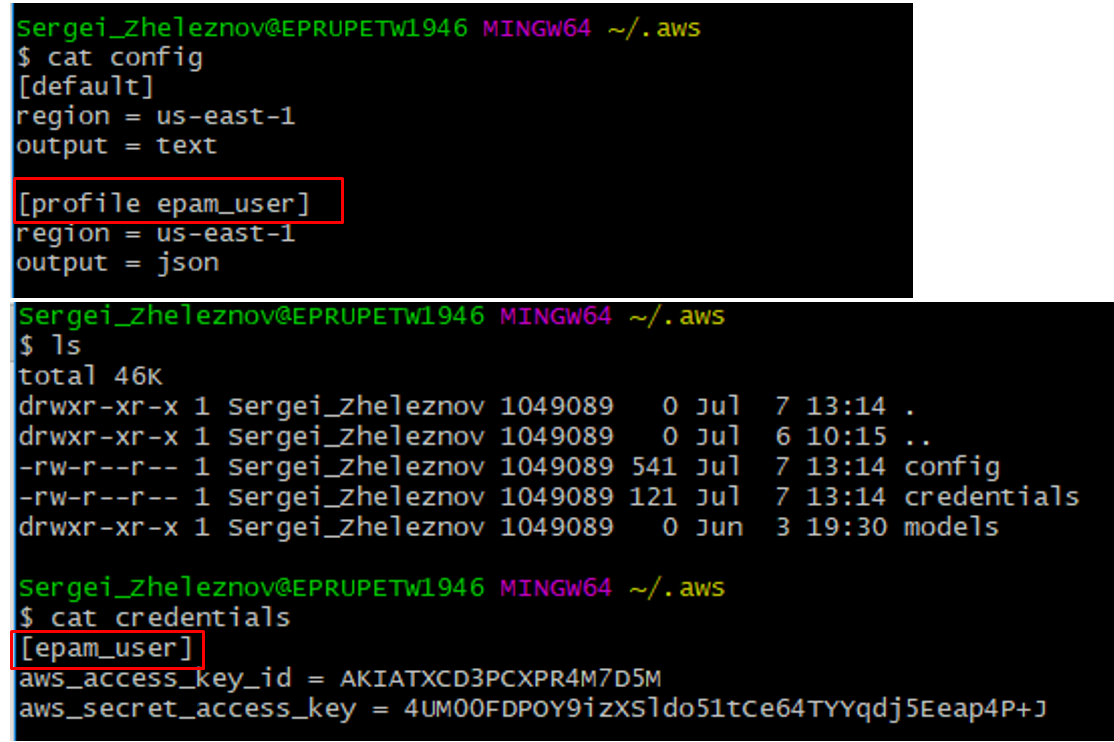
\* \*\*aws\_session\_token\*\* - The session token part of your credentials

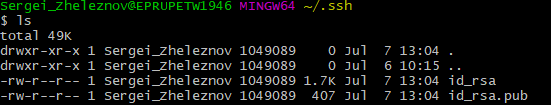
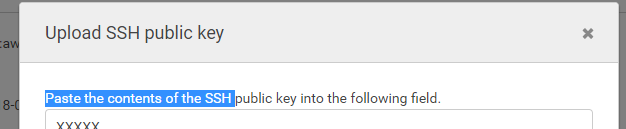
(session tokens only)

1. Copy the data of Access Key and configure the profile (create a new custom one with ‘--profile’ option). Alternatively, keep default profile (miss the ‘--profile' option)

**>aws configure --profile ‘epam\_user’**

$ cat ~/.aws/config

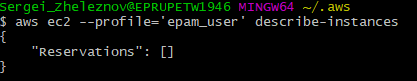


1. Use ssh putty generator if necessary to generate SSH pub and ppk keys.
   1. **$ ssh-keygen -t rsa -C** [**sergei\_zheleznov@epam.com**](mailto:sergei_zheleznov@epam.com)
   2. **Public and private keys will be generated:**
      1. 
   3. Upload public key content ‘**id\_rsa.pub**’ to a server (it will be used to decrype the SSH): 
2. SSH channel will be leveraged when instance is started. For ‘ssh’ connection it is possible to use existing generated ‘id\_rsa’ and ‘id\_rsa.pub’ keys or use downloaded authentic ‘.pem’ file.
   1. ssh -i /path\_to\_key/my\_key.pem user\_name@public\_dns\_name

**The original ‘*id\_rsa’* private key and uploaded public ‘*id\_rsa.pub’* is better!**

## SSH Key Pairs

1. See the currently available EC2 instances on AWS cloud:



1. Create a new instance using image id:
2. Play with key pairs:

$ **aws ec2 describe-key-pairs --profile=epam\_user**

{

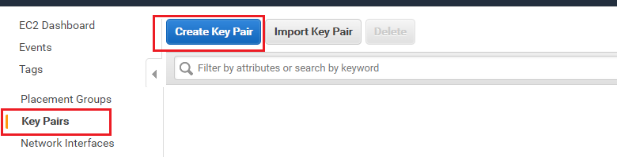
"KeyPairs": []

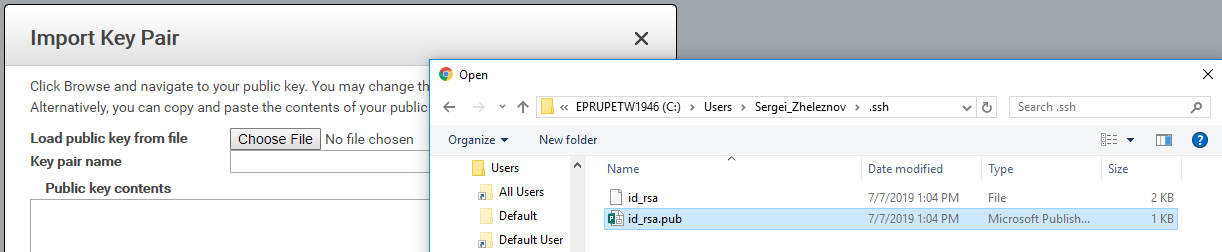
}

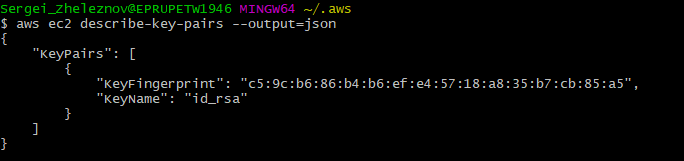
Put default profile name:

**$ export AWS\_DEFAULT\_PROFILE=”epam\_user”**

1. Create and run new EC2 instances from AWS CLI:







Key pair (already third) can be created preliminary. This is the same as before. But SSH key is associated with its ‘name’.

Example CLI:

* **key\_name=devops\_ed\_aws; aws ec2 create-key-pair --key-name $key\_name --query 'KeyMaterial' --output text > $key\_name.pem**
* **aws ec2 run-instances --image-id ami-08842d60 --key-name devops\_ed\_aws --instance-type t2.micro**

**Note: It is better to point out the keys manually**

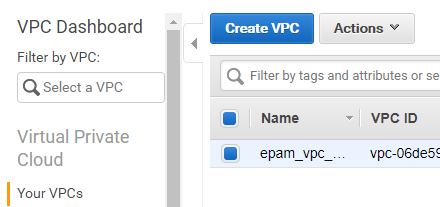
The key pair will be the same for the user and the all instances. It will help to connect to the EC2 instance from CLI (user) or with any SSH client.

## AWS instances

1. Instances cannot be started unless VPC is created (default is always there!):

>**aws ec2 run-instances --image-id ami-035b3c7efe6d061d5 --key-name id\_rsa --instance-type t2.micro**

>An error occurred (VPCIdNotSpecified) when calling the RunInstances operation: No default VPC for this user



Useful commands:

>    aws ec2 describe-key-pairs --output table (example)

>    aws ec2 describe-instances

>    aws ec2 stop-instances --instance-ids XXXXXXX

--user-data file://../aws-crash-course/compute-resources/scripts/instance\_bootstrap.sh