* Create EC2 instance

→ Sign in to the AWS management console and open the Amazon EC2 console.

→ Choose EC2 dashboard and then choose launch instance.

→ Choose the Amazon Linux 2 AMI

→ Choose the t2 micro type and then choose next configure instance details.

→ On the configure instance details page choose following set these values and keep the other values as their defaults

Network :- Choose the VPC with both public and private subnets that you choose for the DB instance, such as the VPC shatpar tutorial VPN

Subnet :- Choose an existing public subnet, such as us-west-2a auto assign public ip

→ Choose next - add storage

→ On the add storage page, keep the default values and choose next - add tags.

→ On the add page choose add key then enter name for key and enter tutorial, web-services for value.

→ Choose next - configure security group.

→ On the configure security group page choose select an existing security group then choose an existing security group such as the tutorial security group.

→ Choose review & launch

→ On the review instance launch page, verify your setting and then choose launch.

→ On the select an existing key pair or create a new key pair page. Choose a new key pair and set key pair name to tutorial key pair

→ Choose download key pair and then save the key pair file on your local machine. You use this key pair link to connect to your EC2 instance.

→ To launch your EC2 interface choose launch instance. On the launch status page note the identifier for your new EC2 instance.

→ Choose view instances to find your instance

→ Wait until instance status for your instance reads as running before continuing

☆ Connect to windows instance

→ Open the Amazon EC2 console

→ In the navigation page, select instances select the instance and then choose connect

→ In the connect to instance page choose ROP client and then choose get password.

→ Choose browse and navigate to the private key file you created when you launched the instance. Select the file and choose open to copy the entire contents of the file to this page.

→ Choose decrypt password. The console displays the default admin password for the instance in password, replacing the set password link. Save password at safe place. Need to connect the instance.

→ Choose download remote desktop file. Your browser prompts you to either open or save the RDP shortcut file. Check cancel to return to the instance page.

→ Navigate to your downloads directory and open the RDP shortcut file

→ You might get a warning that the publisher of the remote connection is unknown.

→ The administrator account is chosen by default. Copy & paste the password that you saved previously.

→ Due to the nature of self ~~signed~~ signed certificates you might get warning that the security certificate could not be authenticated.

☆ Connect to linux instance

→ In a terminal window, use the ssh command to connect to the instance you specify the path and filename of the private key the username for your instance, and the public DNS name or IPv6 address for your instance.

To connect your instance, use one by the following commands. To connect using your instance public DNS name, enter the following command

ssh -i \Path\my-key-pair my-instance-user-name!
my instance-public-dns-name

→ Verify that the fingerprint in the security alert matches the fingerprint that you previously obtained. If don't match someone might be attempting a man-in-the-middle-attack. If they match continue to the next step.

→ Enter yes.

☆ Create S3 Bucket

→ Sign in to Amazon AWS

→ Under storage & content delivery, choose S3 to open the Amazon S3 console

→ From the Amazon S3 console dashboard choose create bucket

→ In create a bucket type a bucket name to bucket name. The bucket name you choose must be globally unique across all existing bucket names in Amazon S3

→ In Region choose oregon

→ Choose create

Send an email using SES

→ Sign in to the AWS management console and open the Amazon SES console

→ In the navigation pane of the Amazon SES console under identity management, choose email addresses.

→ In the list of identities, select the checkbox of an email address that you have successfully verified with Amazon SES.

→ Choose send a test email

→ In the send test email dialog box for email format choose raw

→ For the to address type an address from the Amazon SES mailbox simulator

→ Copy and paste the following message in its entirety into the message textbox replacing configuration set name with the name of the configuration set you created in setup configuration set and replacing from address with the verified address you are sending this email from.

→ Choose send test email

→ Repeat this procedure a few times so that you generate multiple email sending events for a few of the emails change the value of the campaign message tag to simulate sending for a different email campaign.

Jasmit
20/12/2021