Assignment - 2

(1) Create EC2 Instance

→ Step 1 : Sign in to the AWS Management Console and open the Amazon EC2 Console.

Step 2 Choose EC2 dashboard and then choose launch instance

Step 3 Choose the Amazon Linux 2 AMI

Step 4 Choose the microtypes and then choose next configures Instance details

Step 5 On the configure Instance details page. Shown following set these values and her the other values as their defaults

Step 6 Network : Choose the VPC with both public and private subnets that you choose for the DB instance such as the VPC identifier tutorial VPC.

Subnet : Choose an existing public subnet, such as us-west-2a Auto Assign public IP

Step 6 Choose next Add Storage

Step 7 On the add storage page keep the default values and choose next. Add type.

Step 8 On the add type page choose AS2 together enter name for key and enter tutorial sub services for value.

Step -9 Choose next configure security group.

Step 10 On the configure security group page choose select an existing security group then choose an existing security group such as the tutorial security group.

Step 11 Choose review and launch

Step 12 On the review Instance launch page verify your settings and then choose launch

Step 13 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

Step 14 Choose download key pair and then save the key pair file on your local machine use this key pair to connect to your EC2 Instance.

Step 15 To launch your EC2 Instance choose

launch instance on the launch status page note the identifier for your new EC2 Instance

Step 16 Choose new Instance to find your Instance

Step 17 Wait until Instance status for your instance reads as running before continuing

(2) Connect to windows Instance

Step 1 Open the Amazon EC2 console

Step 2 In the navigation pane, select instances. Select the instance and then choose Connect

Step 3 On the Connect to instance page Choose the RDP client tab, and then Choose get password

Step 4 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 window

Step 5 Choose Decrypt password The console displays the default administrator password for the instance under password, replacing the

Get password link showing previously. Save the Password in a safe place This Password is required to connect to the instance.

Step 6 Choose Download remote desktop file. Your browser prompts you to, either open or save the RDP shortcut file. When you have finished downloading the file Choose Cancel to return to the Instance page.

- If you opened the RDP file, you'll see the Remote desktop connection dialog Box
- If you saved the RDP file, navigate to your downloads directory, and open the RDP file to display the dialog box

Step 7 You may get a warning that the publisher of the remote connection is unknown Choose connect to continue to connect to your instance

Step 8 The Administrator account is chosen by default Copy and Paste the password that you saved previously

Step 9 Due to the nature of self signed certificates you may get a warning that the security certificate could not be authenticated. Use the following steps to verify the identity of the remote

computer, or simply choose Yes or continue if you trust the certificate.

(3) Connect to Linux Instance

→ In a terminal window use the ssh command to connect to the instance. You specify the path and file name of the private key, the user name for your instance, and the public DNS name or IPv6 address for your instance. For more info. about how to find the private key, the user name for your instance, and the DNS name or IPv6 address for an instance, see Locate the private key and set the permissions and Get information about your instance. To connect to your instance, use one of the following options.

- Public DNS to connect using your instance's public DNS name, enter the following command.

ssh -i /path/my-key-pair.pem my-instance-user-name@my-instance-public-dns-name

- IPv6 Alternatively, if your instance has an IPv6 address to connect using your instance's IPv6 address, enter the following command.

ssh -i /path/my-key-pair.pem my-instance-user-name@my-instance-IPv6-address

Step-2 Verify that the fingerprint in the security creds matches the fingerprint that you previously obtained in Cret the instance fingerprint. If these fingerprints don't match, someone might be attempting a "man-in-the-middle" attack. If they match, continue to the next step.

Step 3 Enter Yes

(b) Create S3 Bucket

Step 1 Sign in to the preview version of the AWS Management Console.

Step 2 Under Storage and content Delivery choose S3 to open the amazon S3 console.

Step 3 From the Amazon S3 console dashboard choose create bucket

Step 4 In a create bucket type a bucket name in Bucket Name

Step 5 In region choose Oregon

Step 6 Choose Create

PAGE NO.
DATE

(5) Send an email using SES

↳ Sign in to Amazon Web Services Management Console

Step 2 In the navigation pane on the left side of the Amazon SES console, under Identity Management choose Email Addresses to view the email address that you verified in Verifying email addresses in Amazon SES

Step 3 In the list of identities, check the box next to email address that you have verified

Step 4 Choose Send Test email

Step 5 For Send Test Email, choose the email format. Two choices are, Formatted and Raw

Step 6 For Send Test Email, fill out the rest of the fields. If you are still in the Amazon SES sandbox, make sure that the address in the To field is a verified email address ~~for more~~.

Step 7 Choose Send Test Email

Step 8 Sign in to the email client of the address you sent the email to. You will find the message that you sent.