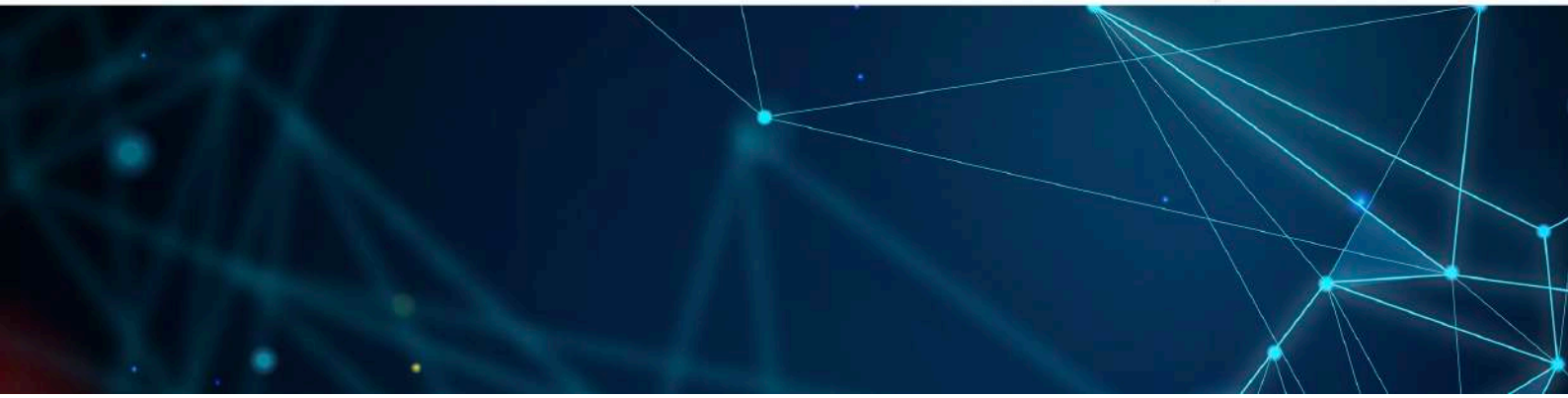
ENCRYPTION CONSULTING
www.encryptionconsulting.com



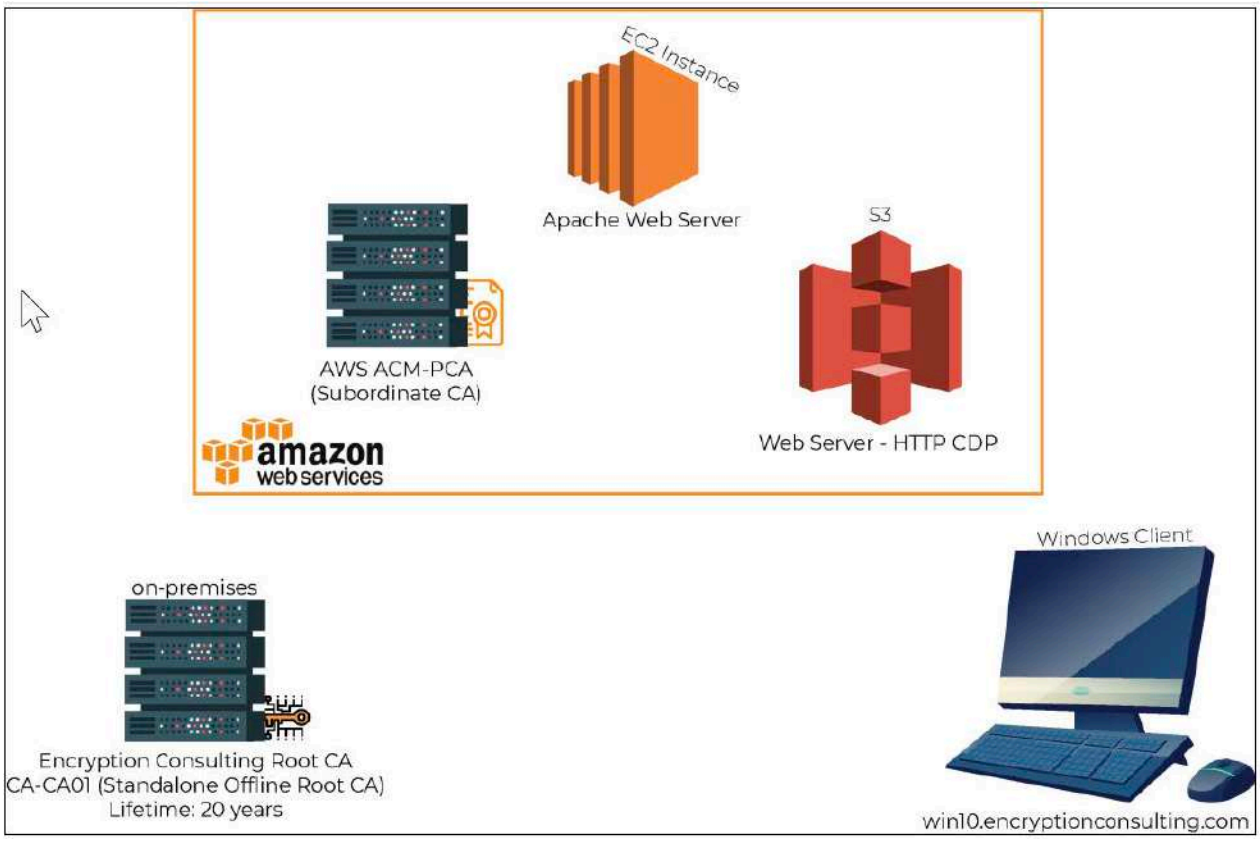
Hybrid (On-prem & AWS Cloud) Two Tier PKI Hierarchy Deployment

Detailed guide for Basic Configuration

Introduction and overview of the Test Lab:

There are two computers, one AWS Subordinate CA, one AWS EC2 instance, and one AWS S3 bucket, involved in this hybrid (On-prem & AWS) two tier PKI hierarchy lab:

1. One Standalone Offline Root CA (CA01).
2. One AWS Subordinate CA (Encryption Consulting Issuing CA)
3. One EC2 instance with RHEL8 distribution running an Apache Web Server (ec2-100-25-199-96.compute-1.amazonaws.com)
4. One S3 bucket with read/write permissions onto it (encryptionconsultingcrl)
5. One Windows 10 (Win 10) Client Computer (WIN10.encryptionconsulting.com)



Virtual Machine	Roles	OS Type	Public IP Address/FQDN	Scope
CA01	Standalone Offline Root CA	Windows Server 2016	NA	Windows Cloud
Encryption Consulting Issuing CA	Subordinate CA	AWS ACMPCA	NA	AWS Cloud
ec2-100-25-199-96.compute-1.amazonaws.com	Apache Web Server	RHEL-8	FQDN	AWS Cloud
encryptionconsultingcrl	CRL	AWS S3	FQDN	AWS Cloud
WIN10.encryptionconsulting.com	Windows Client Computer	Windows 10	Public IP	Internet Cloud

Major Steps:

There are eight major steps in this step-by-step guide as listed below (each includes several sub tasks).

1. Install the standalone offline root CA
2. Perform post installation configuration steps on the standalone offline root CA
3. Install Subordinate Issuing CA
4. Create a Key-Pair
5. Setup an EC2 instance
6. Issuing SSL/TLS Certificate for Web Server
7. Install the Apache Web Server
8. Verify the Hybrid PKI hierarchy health

Activity 1: Install the Standalone Offline Root CA

The standalone offline root CA should not be installed in the domain. As a matter of fact, it should not even be connected to a network at all.

Task 1: Create a CAPolicy.inf for the standalone offline root CA

To create a CAPolicy.inf for the standalone offline root CA:

1. Log onto CA01 as **CA01\Administrator.**
2. Click **Start**, click **Run** and then type **notepad C:\Windows\CAPolicy.inf** and press ENTER.
3. When prompted to create new file, click **Yes.**
4. Type in the following as the contents of the file.

```
[Version]
Signature="$Windows NT$"
[Certsrv_Server]
RenewalKeyLength=2048 ; recommended 4096
RenewalValidityPeriod=Years
RenewalValidityPeriodUnits=20
AlternateSignatureAlgorithm=0
```

5. Click File and Save to save CAPolicy.inf file under C:\Windows directory.

   Warning CAPolicy.inf with the .inf extension. Type .inf at the end of the file name and select the options as described, otherwise the file will be saved as a text file and will not be used during CA installation.

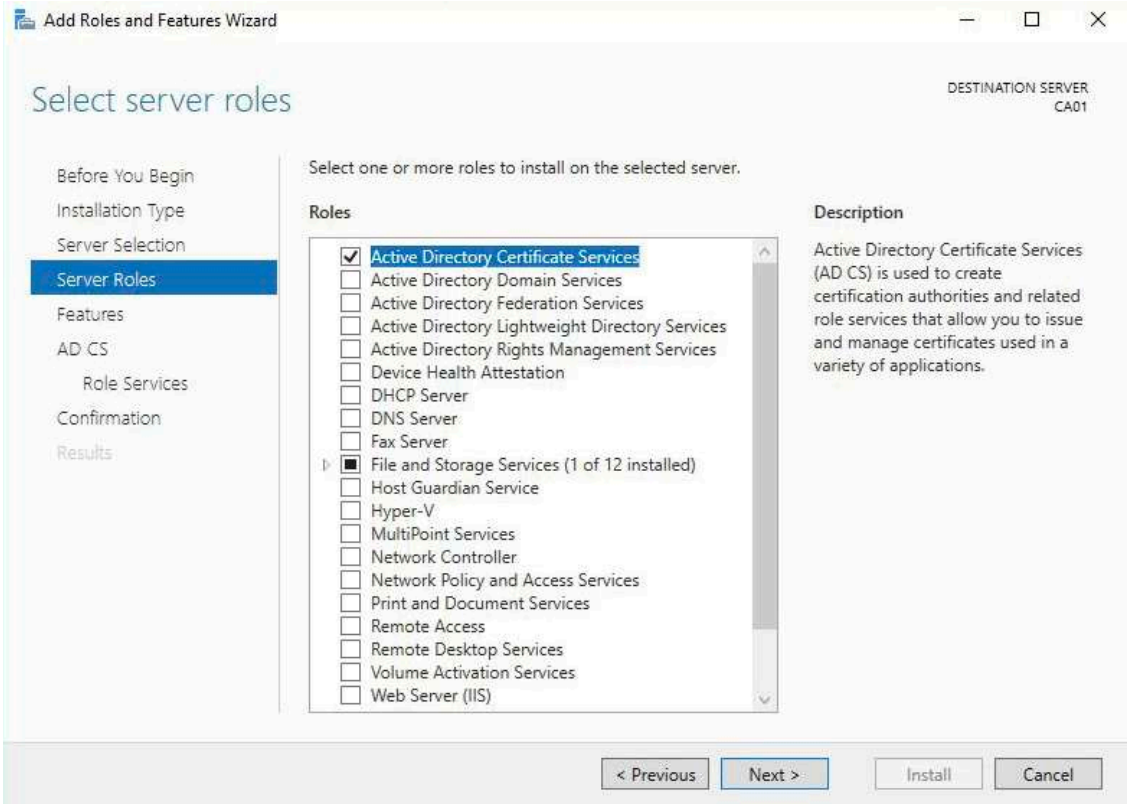
6. Close Notepad.

Task 2: Installing the Standalone Offline Root CA

To install the standalone offline root CA:

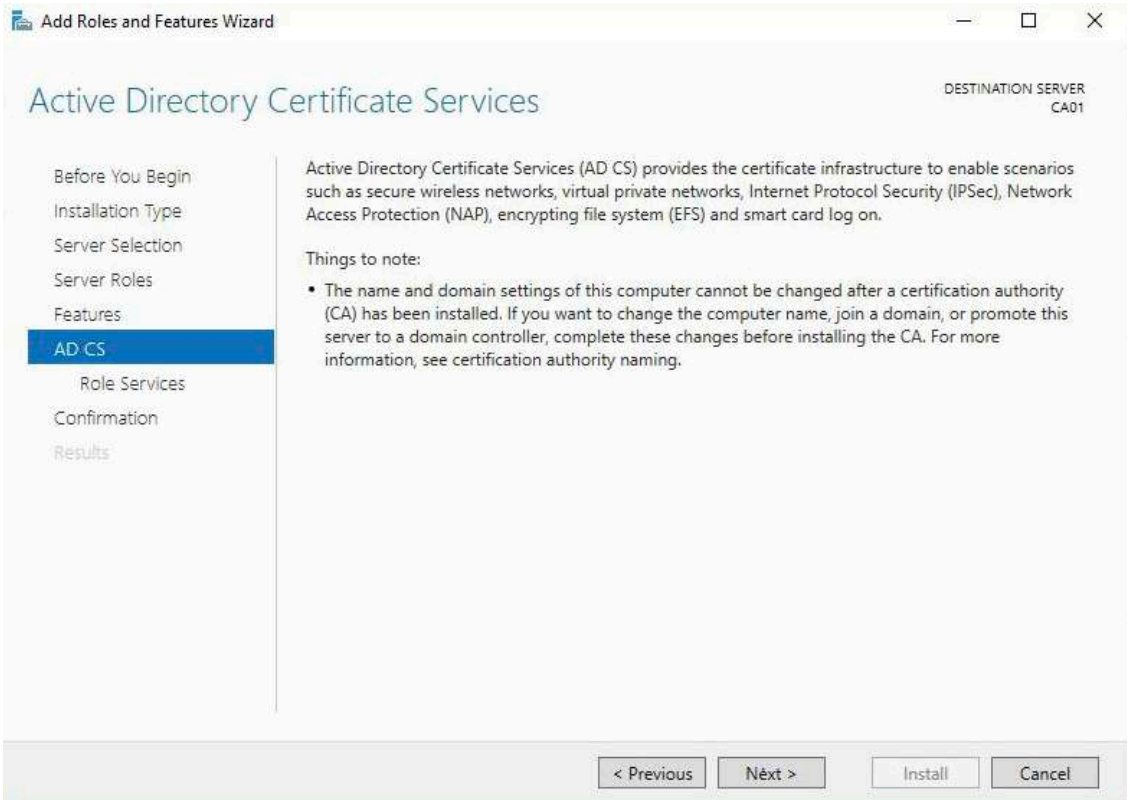
1. Log onto CA01 as CA01\Administrator.
2. Click **Start**, click **Administrative Tools**, and then click **Server Manager.**
3. Right-click on **Roles** and then click **Add Roles.**
4. On the **Before You Begin** page click **Next.**

5. On the **Select Server Roles** page select **Active Directory Certificate Services,** and then click **Next.**

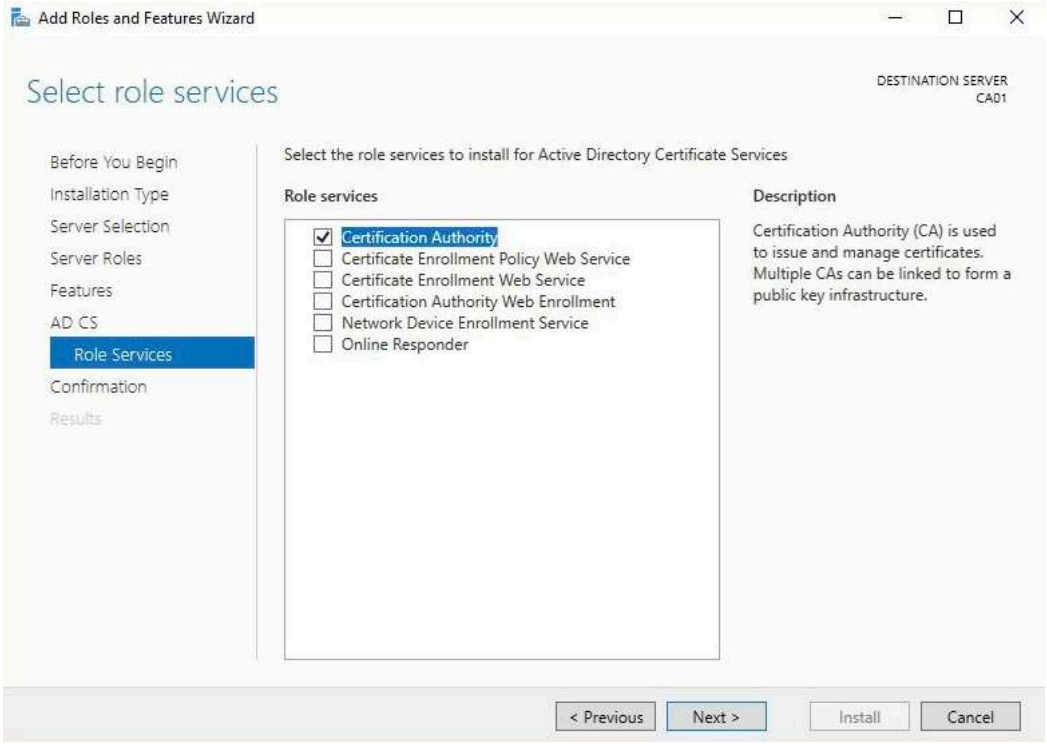


6. On the select features page, click next.

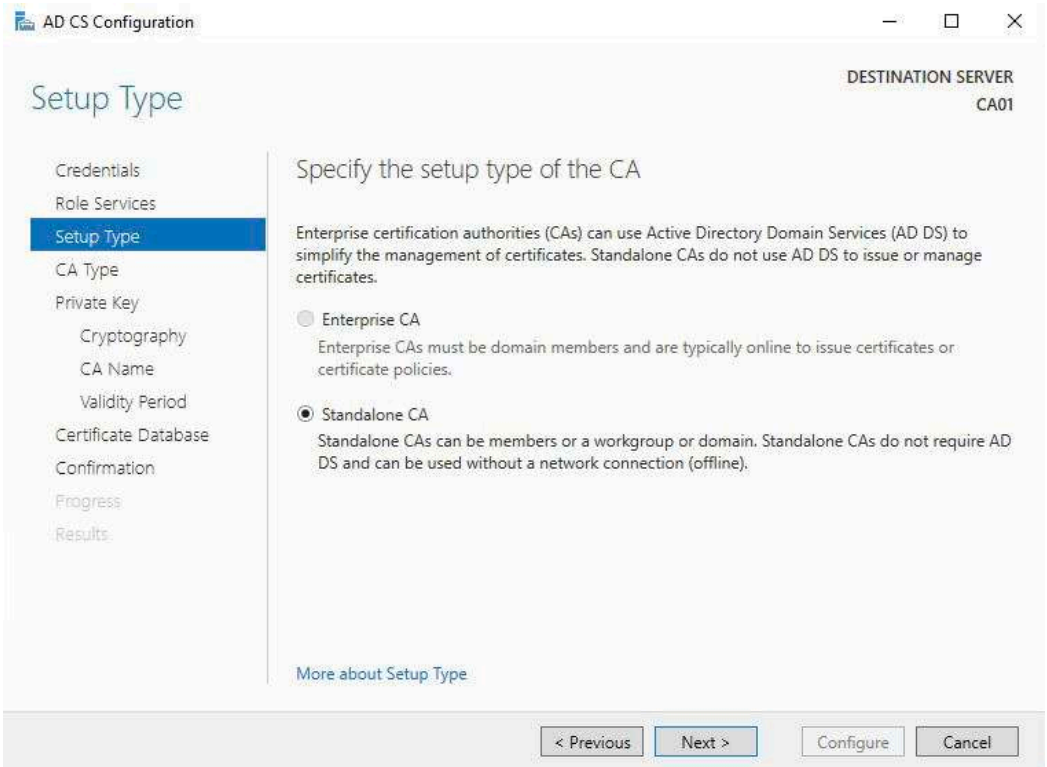
7. On the **Introduction to Active Directory Certificate Services** page, click **Next.**



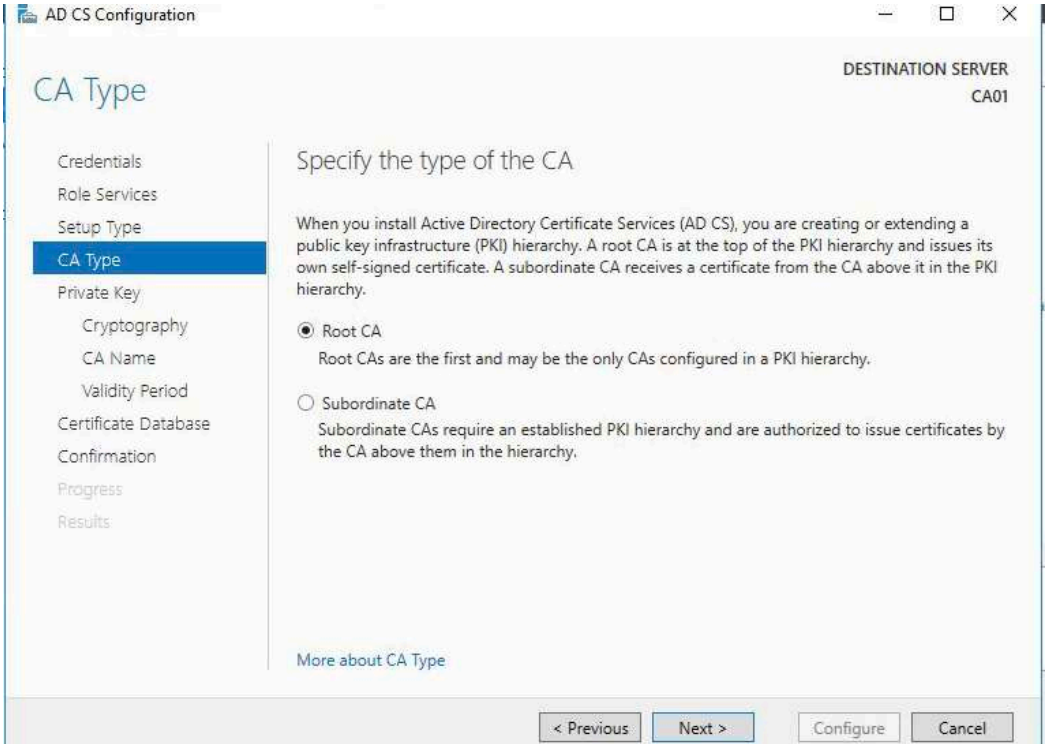
8. On the **Select Role Services** page, ensure that **Certification Authority** is selected, and then **Next.**



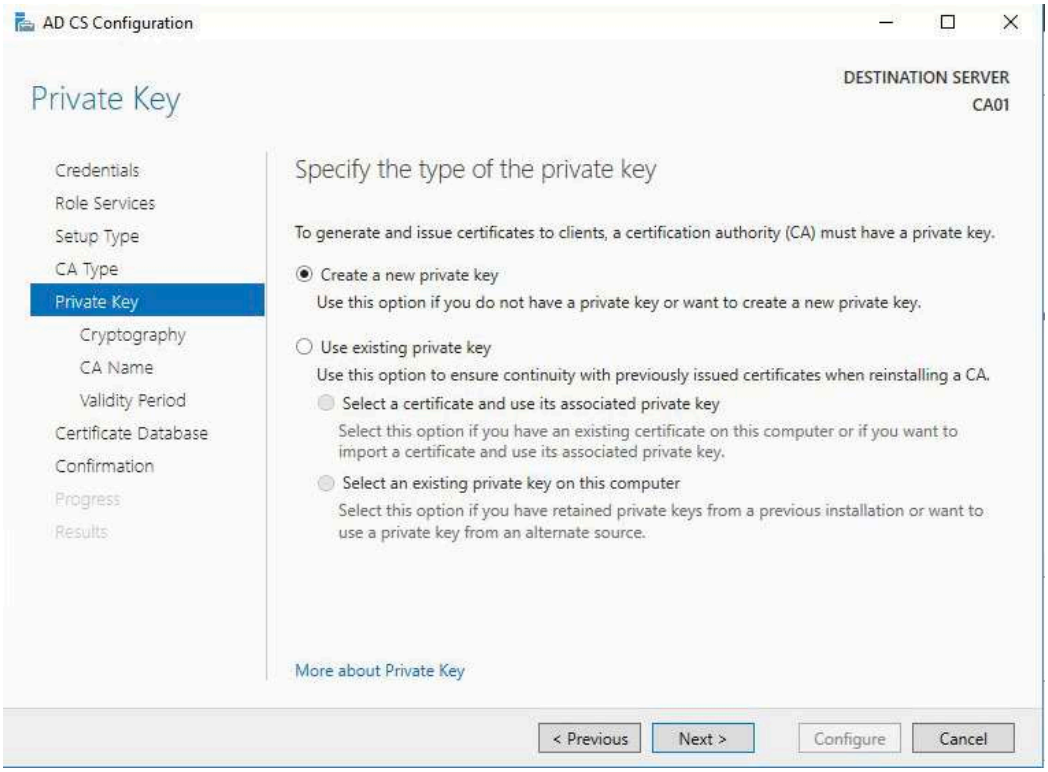
9. On the **Specify Setup Type** page, ensure that **Standalone** is selected, and then click **Next.**
    a. Note: Enterprise option is grayed out as CA01 server is not joined to an Active Directory domain.



10. On the **Specify CA Type** page, ensure that **Root CA** is selected, and then click **Next.**

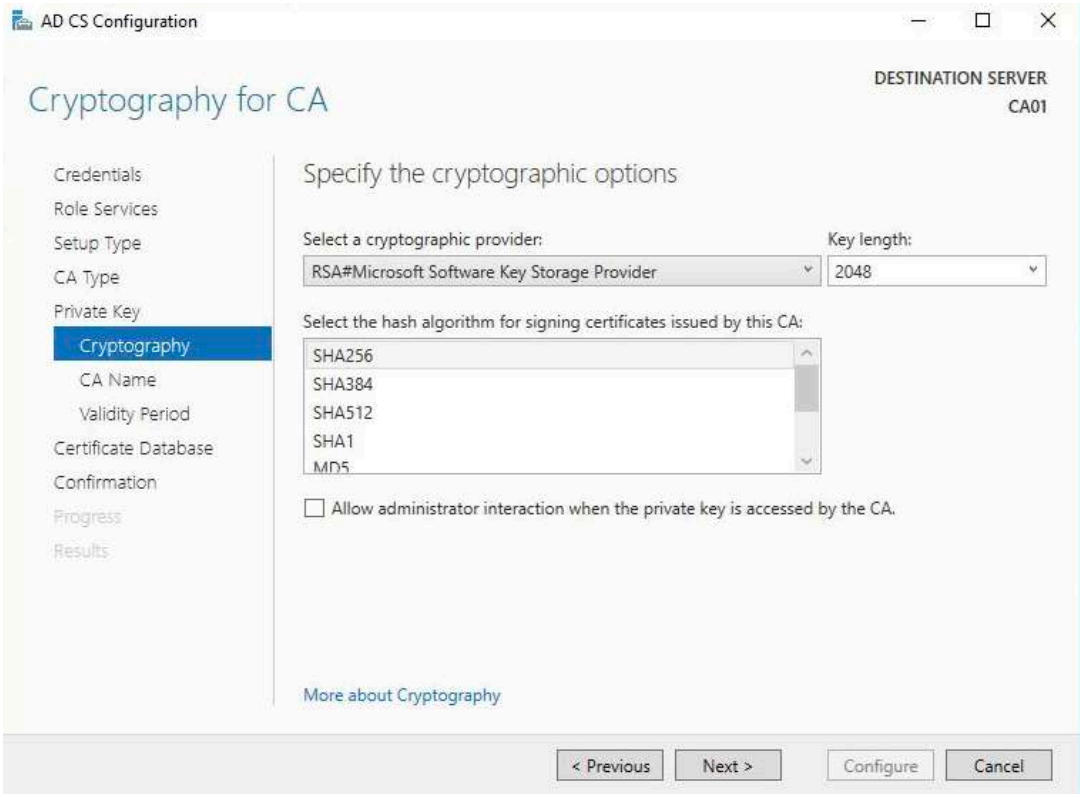


11. On the **Set Up Private Key** page, ensure that **Create a new private key** is selected, and then click **Next.**



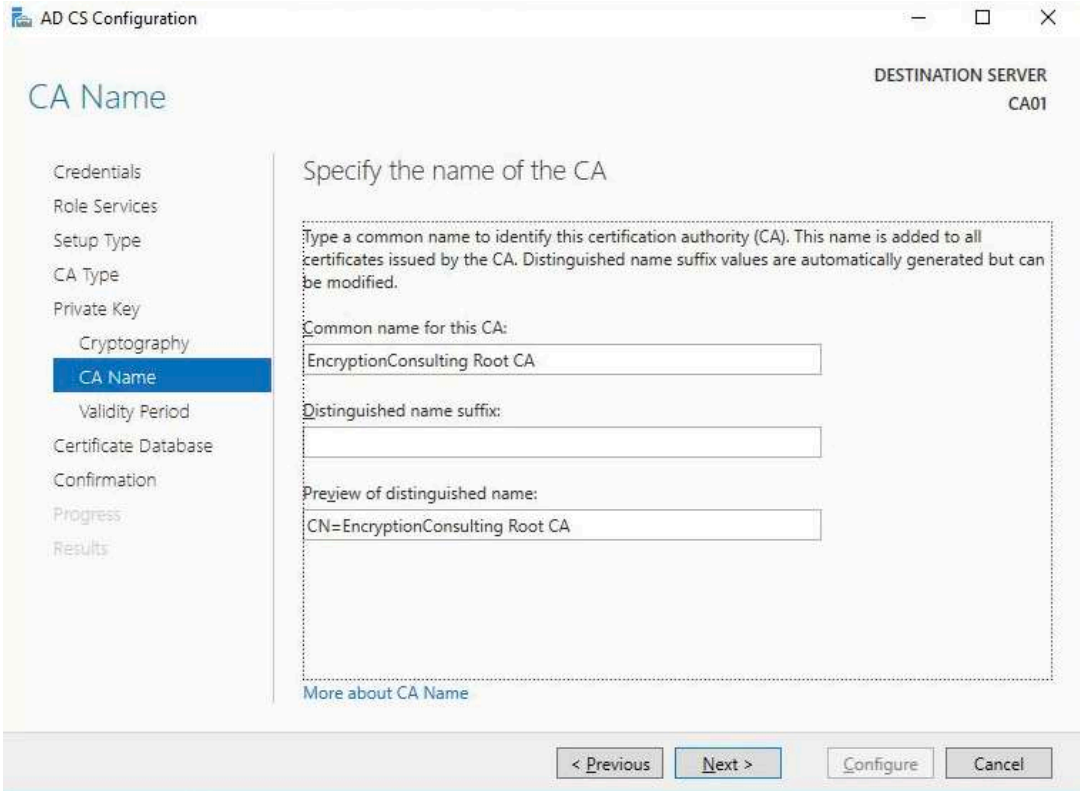
12. Leave the defaults on the **Configure Cryptography for CA** page, and then click **Next.**

    a. **Important**: In a production environment, you would set the CSP, Hash Algorithm, and Key length to meet application compatibility requirements.

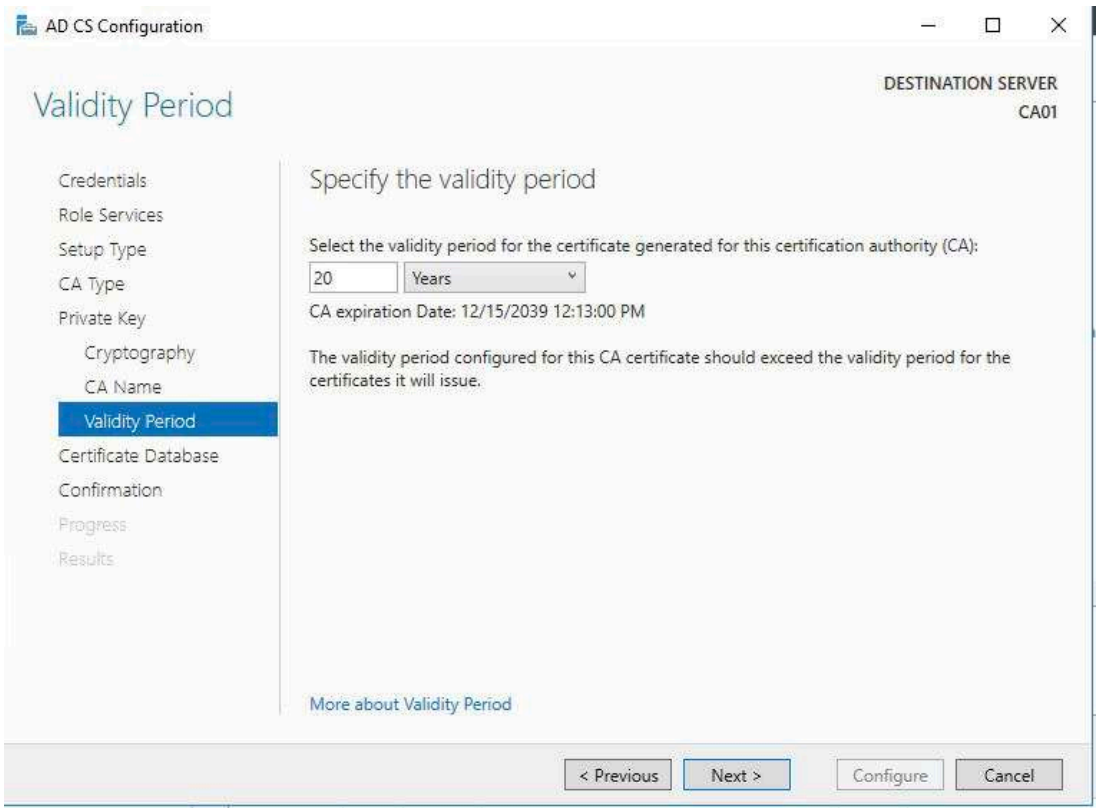


13. On **Configure CA Name** page, under Common name for this CA, clear the existing entry and type **EncryptionConsulting Root CA** Click **Next.**

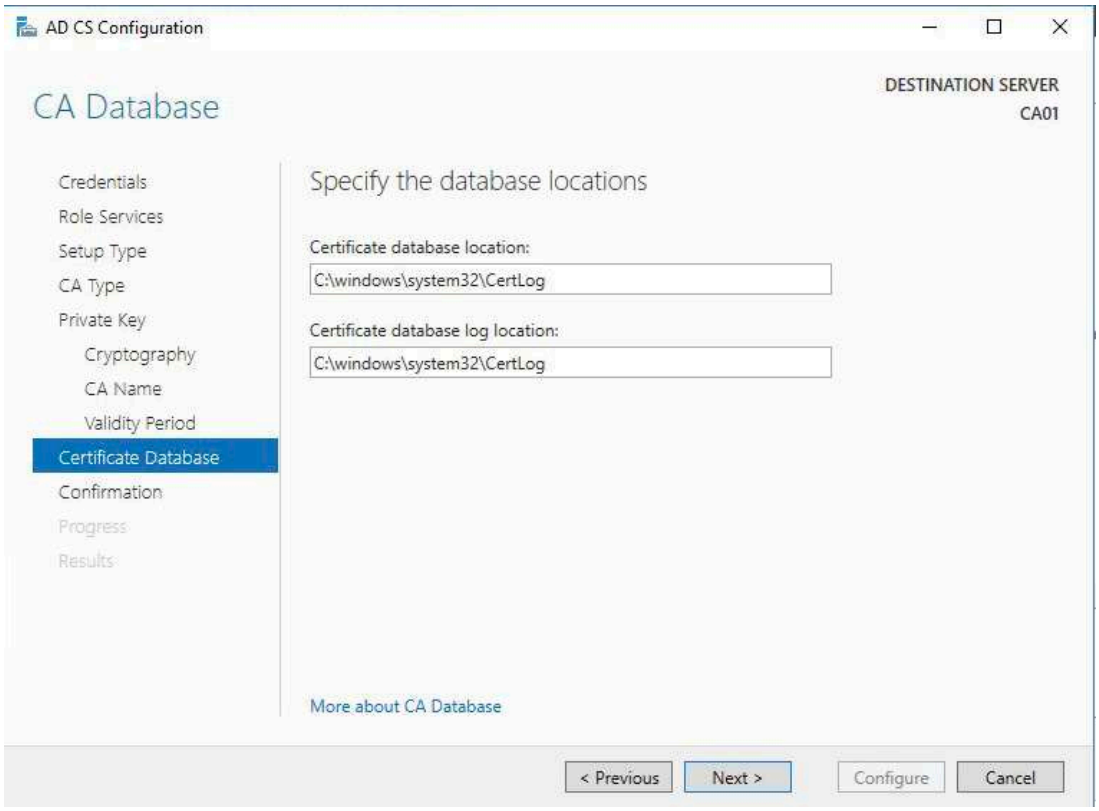
    a. Note: A Distinguished Name Suffix is optional for a root CA. This will be configured in a later step.



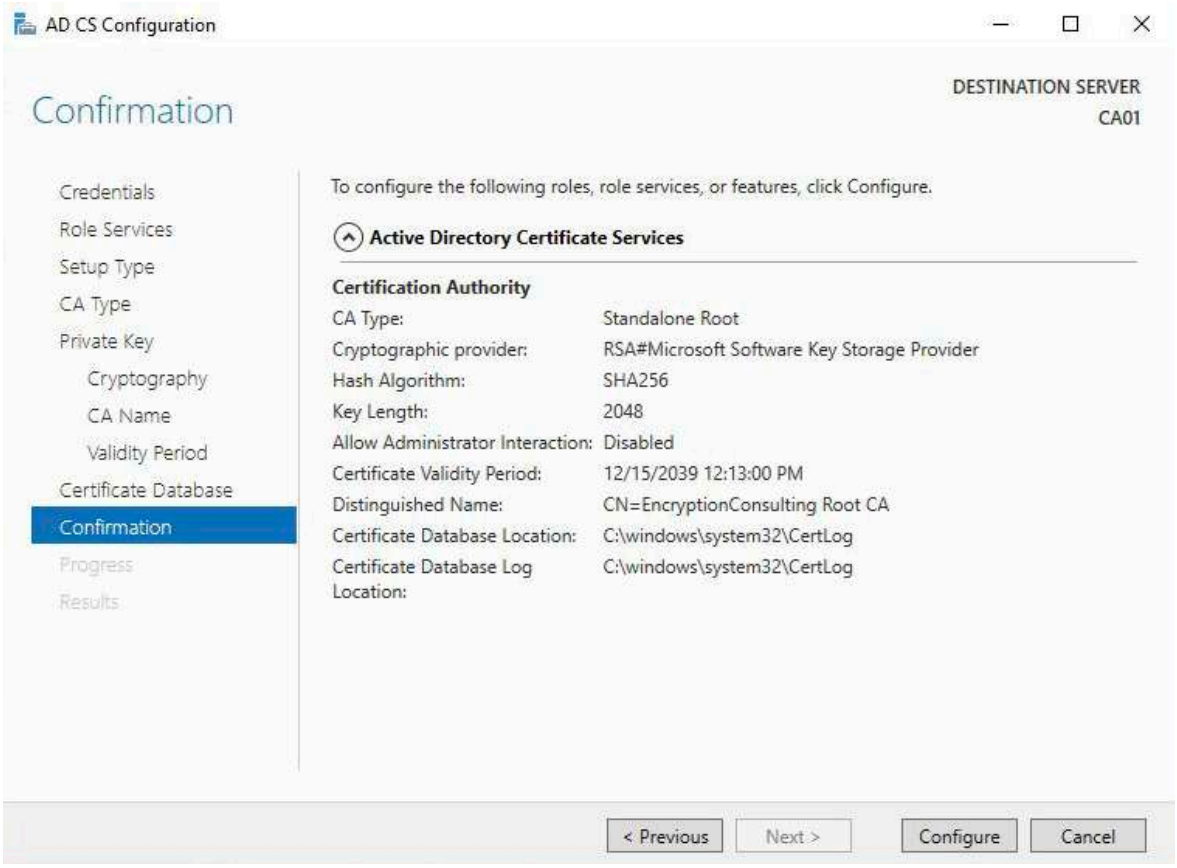
14. On **Set Validity Period** page, under **Select validity period for the certificate generated for this CA**, clear the existing entry and then type **20**. Leave the selection box set to **Years**. Click **Next**.



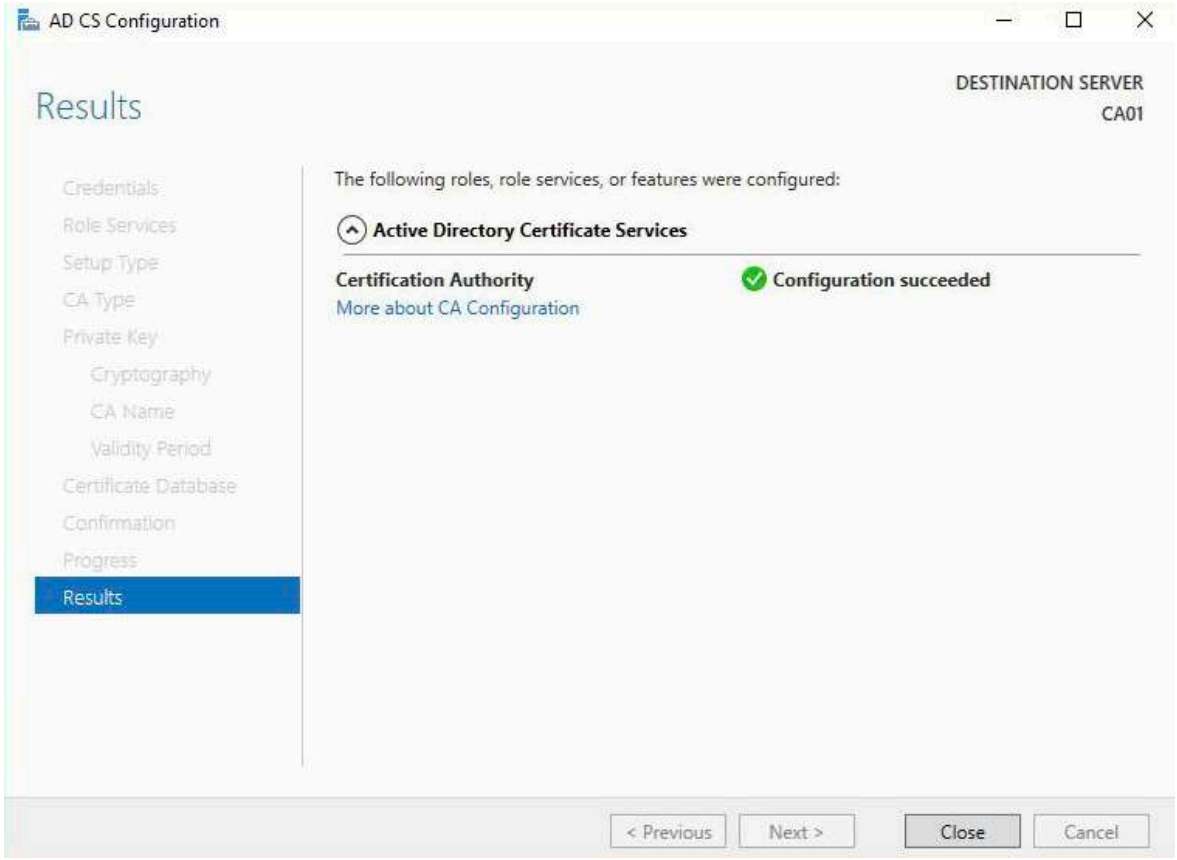
15. Keep the default settings on the **Configure Certificate Database** page, and then click **Next**.



16. On the **Confirm Installation Selections** page, review the settings, and then click **Install.**



17. Review the information on the **Installation Results** page to verify that the installation is successful and then click **Close.**



1. Activity 2: Perform post installation configuration steps on the standalone offline root CA

1. Ensure that you are logged on to **CA01** as **CA01\Administrator.**
2. Open a command prompt. To do so, you can click **Start**, click **Run**, type **cmd** and then click **OK**.
3. To define Active Directory Configuration Partition Distinguished Name, run the following command from an administrative command prompt:
    - **Certutil -setreg CA\DSConfigDN "CN=Configuration,DC=EncryptionConsulting,DC=com"**
4. To define **CRL Period Units** and **CRL Period**, run the following commands from an administrative command prompt:
    - **Certutil -setreg CA\CRLPeriodUnits 52**
    - **Certutil -setreg CA\CRLPeriod "Weeks"**
    - **Certutil -setreg CA\CRLDeltaPeriodUnits 0**
5. To define **CRL Overlap Period Units** and **CRL Overlap Period**, run the following commands from an administrative command prompt:
    - **Certutil -setreg CA\CRLOverlapPeriodUnits 12**
    - **Certutil -setreg CA\CRLOverlapPeriod "Hours"**
6. To define **Validity Period Units** for all issued certificates by this CA, type the following command and then press Enter. In this lab, the Enterprise Issuing CA should receive a 10 year lifetime for its CA certificate. To configure this, run the following commands from an administrative command prompt:
    - **Certutil -setreg CA\ValidityPeriodUnits 10**
    - **Certutil -setreg CA\ValidityPeriod "Years"**

Task 1: Enable Auditing on the Root CA

CA auditing depends on system **Audit Object Access** being enabled. The following instructions describe how to use Local Security Policy to enable object access auditing.

1. Click **Start,** click **Administrative Tools**, and then select **Local Security Policy.**
2. Expand **Local Policies** and then select **Audit Policy**.
3. Double click **Audit Object Access** and then select **Success** and **Failure** then click **OK**.
4. Close LocalPolicy .
5. Enable auditing for the CA by selecting which group of events to audit in the Certificate Authority MMC snap-in or by configuring AuditFilter registry key setting. To configure Auditing for all CA related events, run the following command from an administrative command prompt:

   Certutil -setreg CA\AuditFilter 127

Task 2: Configure the AIA and CDP

There are different methods for configuring the Authority Information Access (AIA) and certificate revocation list distribution point (CDP) locations. You can use the user interface (in the Properties of the CA object), certutil, or directly edit the registry. In this lab, we will be using "Certutil" method. The AIA is used to point to the public key for the certification authority (CA). The CDP is where the certificate revocation list is maintained, which allows client computers to determine if a certificate has been revoked. In this lab there will be three locations for the AIA and four locations for the CDP.

Configure the AIA

Using a certutil command is a quick and common method for configuring the AIA. When you run the following certutil command, you will be configuring a static file system location, a lightweight directory access path (LDAP) location, and an http location for the AIA. The certutil command to set the AIA modifies the registry, so ensure that you run the command from a command prompt run as Administrator. Run the following command:

certutil -setreg CA\CACertPublicationURLs "1:C:\Windows\system32\CertSrv\CertEnroll\ %1_%3%4.crt\n2:ldap:///CN=%7,CN=AIA, CN=Public Key Services,CN=Services,%6%11\n2:http://pki.EncryptionConsulting.com/CertEnroll/%1_%3%4.crt"

After you have run that command, run the following command to confirm your settings:

certutil -getreg CA\CACertPublicationURLs

If you look in the registry, under the following path: **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\CertSvc\Configuration\ EncryptionConsulting Root CA**, you can confirm the CACertPublicationURLs by opening that REG_MULTI_SZ value. You should see the following:

1:C:\Windows\system32\CertSrv\CertEnroll\%1_%3%4.crt

2:ldap:///CN=%7,CN=AIA,CN=Public Key Services,CN=Services,%6%11

2:http://pki.EncryptionConsulting.com/CertEnroll/%1_%3%4.crt

You can also see this in the the CA (certsrv) console. To open the console, click **Start**, click **Administrative Tools,** and then click **CertificationAuthority.** In the navigation pane, expand the C**ertificate Authority(Local)**. Right-click **EncryptionConsulting Root CA** and then click **Properties.** On the **Extensions** tab, under **Select extension**, click **Authority Information Access (AIA)** and you will see the graphical representation of the AIA settings.

Configure the CDP

The certutil command to set the CDP modifies the registry, so ensure that you run the command from acommand prompt:

certutil -setreg CA\CRLPublicationURLs "1:C:\Windows\system32\CertSrv\CertEnroll\%3%8%9.crl\n10:ldap:///CN=%7%8,CN=%2, CN=CDP,CN=Public Key Services,CN=Services,%6%10\n2:http://pki.EncryptionConsulting.com/CertEnroll/%3%8%9.crl"

After you run that command, run the following certutil command to verify your settings:

certutil -getreg CA\CRLPublicationURLs

In the registry

location: **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\EncryptionConsulting Root CA** you can open the REG_MULTI_SZ value and see the configuration of these values:

1:C:\Windows\system32\CertSrv\CertEnroll\%3%8%9.crl

10:ldap:///CN=%7%8,CN=%2,CN=CDP,CN=Public Key Services,CN=Services,%6%10

2:http://pki.EncryptionConsulting.com/CertEnroll/%3%8%9.crl

You can also see this in the the CA (certsrv) console. To open the console, click **Start**, click **Administrative Tools**, and then click **Certification Authority**. In the navigation pane, ensure that **Certificate Authority (Local)** is expanded. Right-click **EncryptionConsultng Root CA** and then click **Properties**. On the **Extensions** tab, under **Select extension**, click **CRL Distribution Point (CDP)** and you will see the graphical representation of the CDP settings.

At an administrative command prompt, run the following commands to restart Active Directory Certificate Services and to publish the CRL.

net stop certsvc

Net start certsvc

certutil -crl

Note: Before we start Activity 3, Make sure the time zone of the Root CA windows server is aligned with the time zone of AWS region in such a way that the "Subordinate CA Certificate" is valid while installing the "Subordinate CA Certificate" in ACM PCA

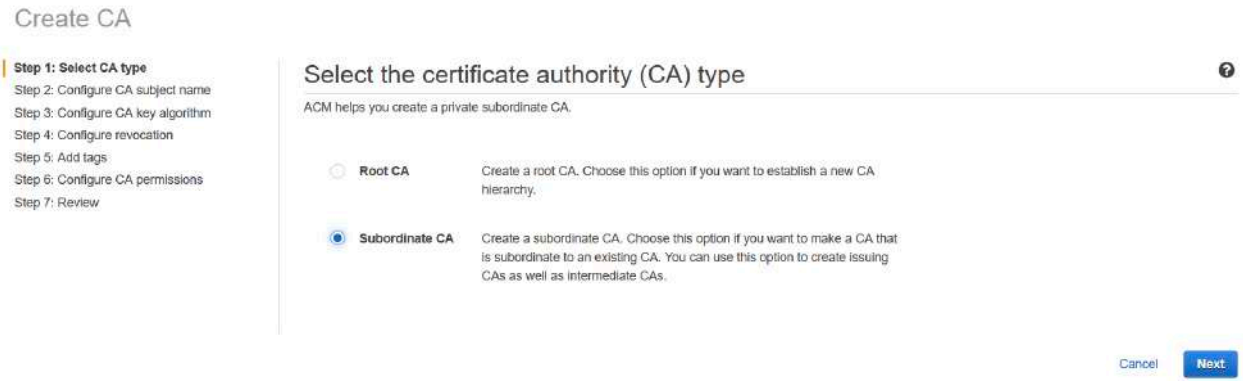
Activity 3: Install Subordinate Issuing CA

Task 1: Create the Subordinate CA

1. Sign into your AWS account and open the ACM Private CA console at https://console.aws.amazon.com/acm-pca/home. Kindly note that the user must have the permission to create/manage the ACM PCA service.

2. On the Select the certificate authority (CA) type page, select the type of the private certificate authority that you want to create (As the Root CA is on Prem, we will select the Subordinate CA option in the console):

ii. Subordinate CA



3. On the **Configure the certificate authority (CA) name** page, configure the subject name of your private CA. You must enter at least one of the following values:

i. Organization (O): Encryption Consulting

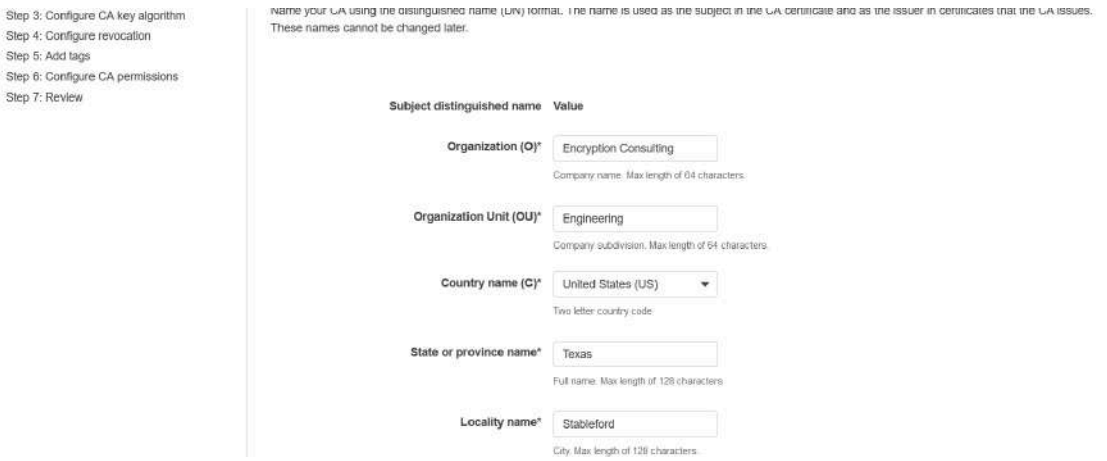
ii. Organization Unit (OU): Engineering

iii. Country name (C): USA

iv. State or province name: Texas

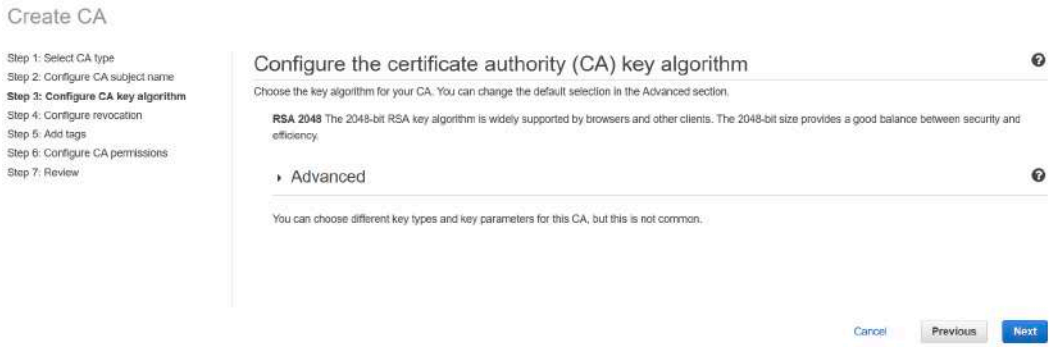
v. Locality name: Stableford

vi. Common Name (CN): Encryption Consulting Issuing CA



NOTE: make sure there are no spaces at the end of these subject names

4. On the **Configure the certificate authority (CA) key algorithm** page, select the key algorithm and the bit-size of the key. The default value is an RSA algorithm with a **2048-bit RSA key length as the** 2048-bit size provides a good balance between security and efficiency.



6. On the Configure certificate revocation page, you have the option of creating a certificate revocation list (CRL) managed by ACM Private CA in S3 bucket.

7. Create a new S3 bucket, choose Yes. On the S3 bucket name field type s3bucketforcrl (You may choose a different name for your S3 bucket, as with this name it will give an error"bucket already exists".

Note: You have an option to either create a new S3 bucket or use an existing S3 bucket with ACM which has the following IAM permissions to it:

"Action": [

"s3:PutObject",

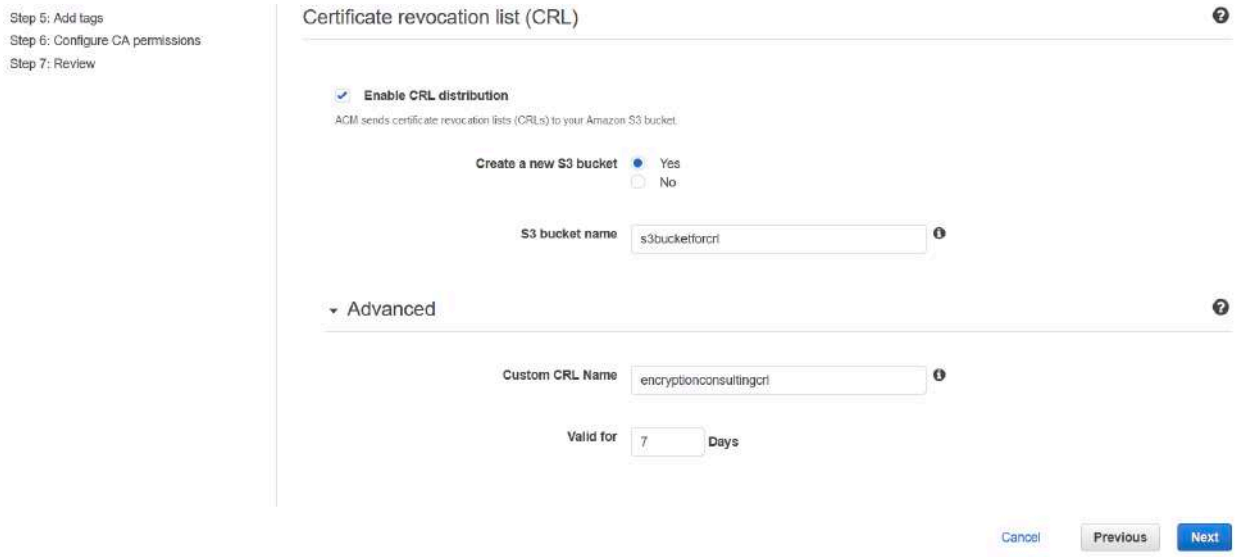
"s3:PutObjectAcl",

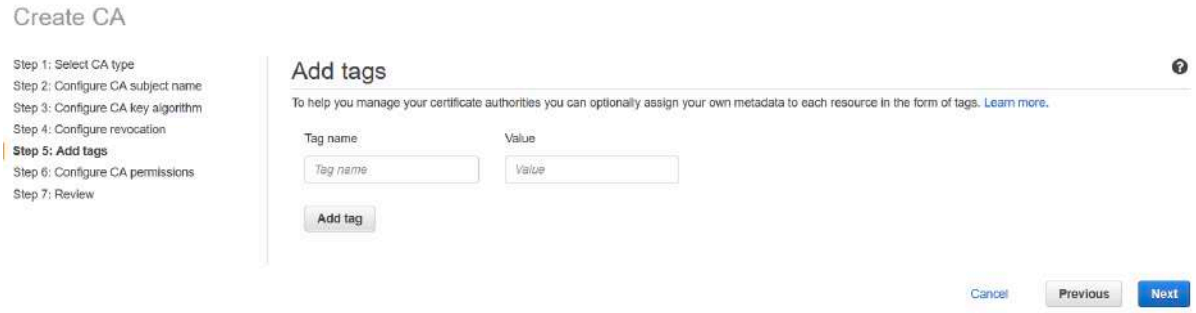
"s3:GetBucketAcl",

"s3:GetBucketLocation"

---

8. Expand the Advanced option and add the Custom CRL Name **encryptionconsultingcrl** to create an alias for your Amazon S3 bucket. This name is contained in certificates issued by the CA in the "CRL Distribution Points" extension that is defined by RFC 5280.



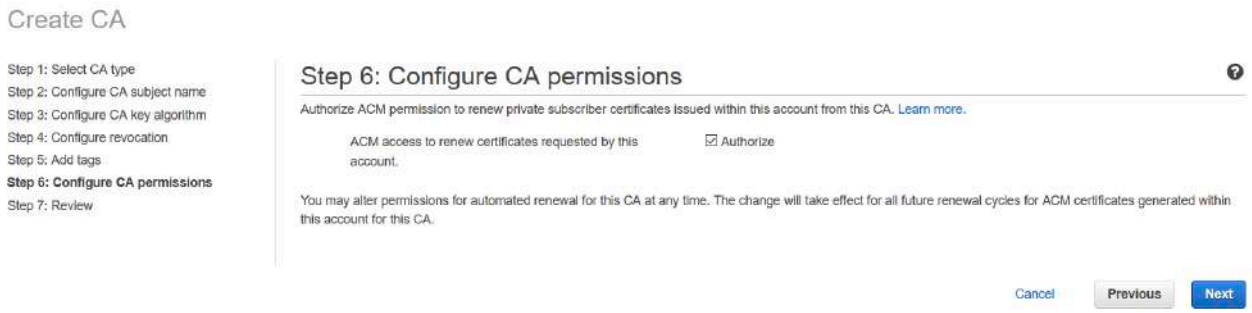


9. Type the number of days your CRL will remain valid. The default value is 7 days. Here, we are leaving it as default.

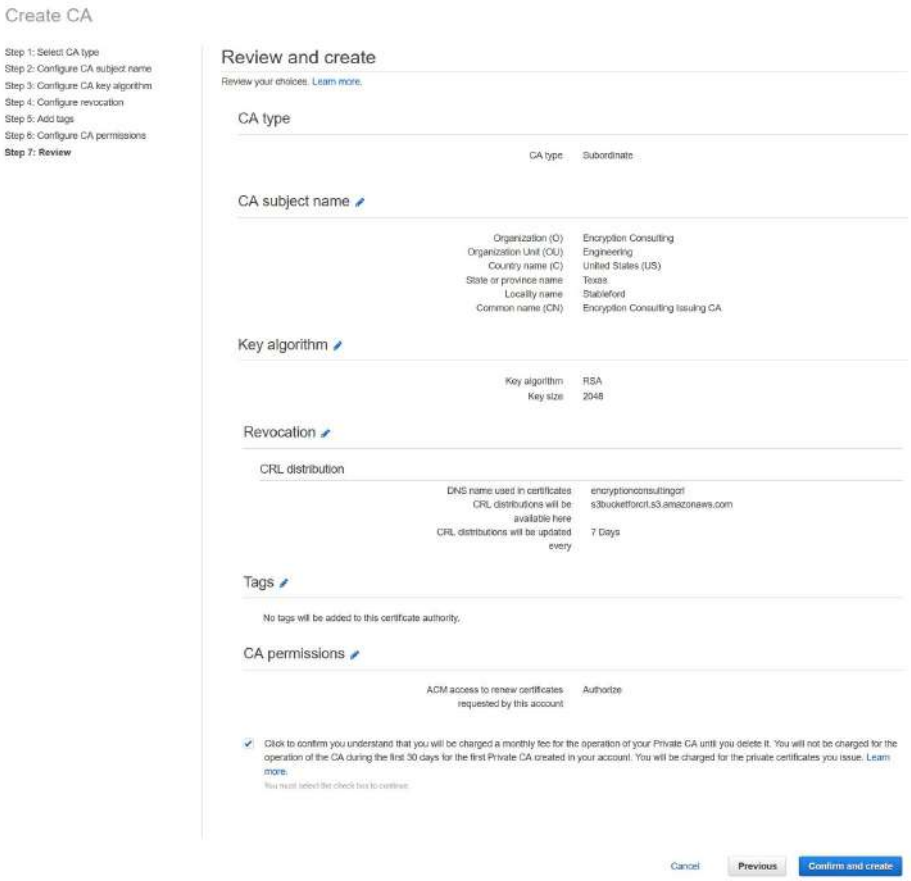
10. On the **Add tags** page, you can optionally tag your CA).

11. On the **Configure CA permissions** page, click Next.

ACM can automatically renew private end-entity certificates generated by this CA if this permission is granted. The default is to enable these permissions.



12. On the **Review and create** page, confirm that your configuration is correct, check the box to acknowledge pricing information, and choose Confirm and create.



Note: Optionally, you may opt for encrypting your CRL in the S3 bucket using various encryption options.

Success!

Your CA was created successfully.

Install a CA certificate to activate your CA.

Get started

You can also finish later

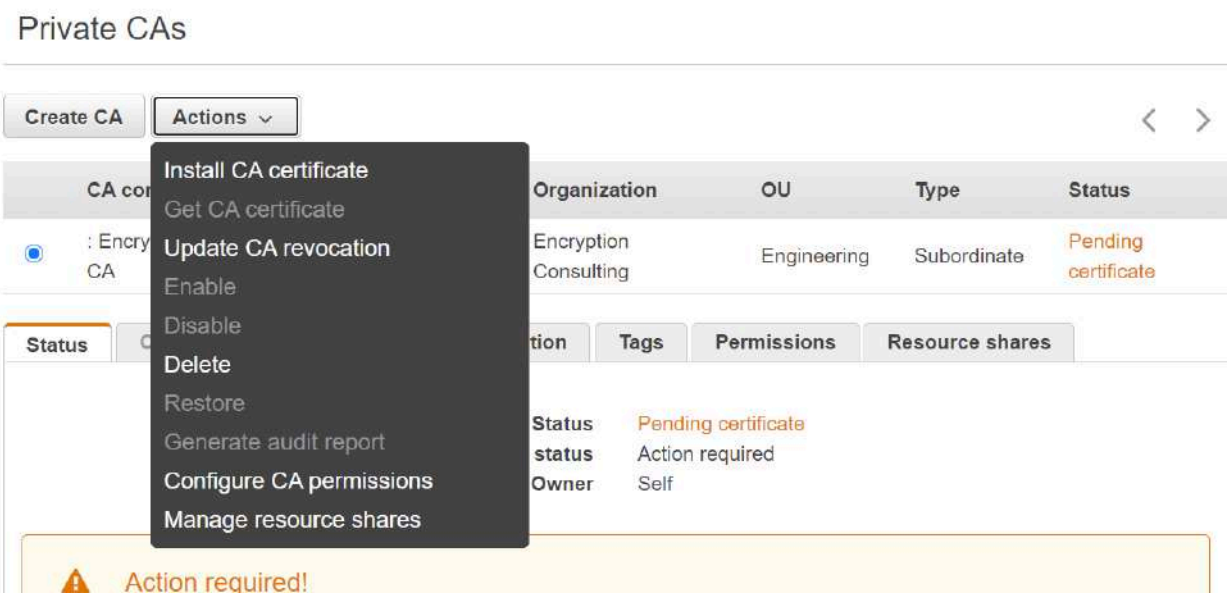
CA information

Type	Subordinate
CA common name	: Encryption Consulting Issuing CA
ARN	[redacted]

Task 2: CSR generation for EncryptionConsulting Issuing Subordinate CA

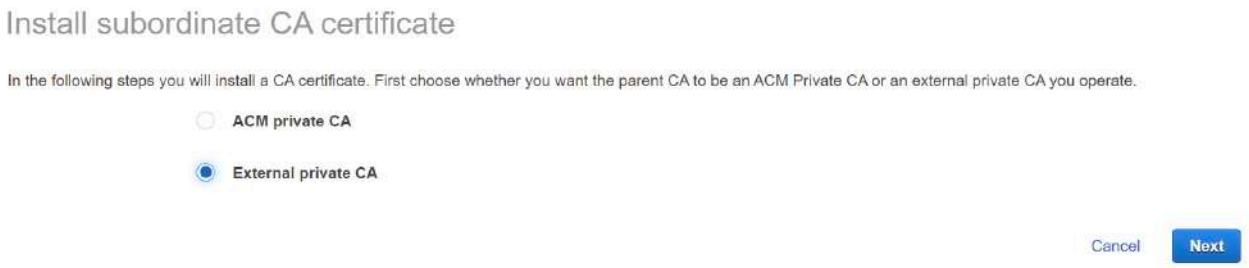
1. Open the ACM Private CA console at https://console.aws.amazon.com/acm-pca/home and begin installation by selecting the newly created subordinate CA (**Encryption Consulting issuing CA**) with status **"Pending Certificate".**

2. From the drop down of **Actions**, select Install CA Certificate. This opens the **Install subordinate CA** certificate wizard.

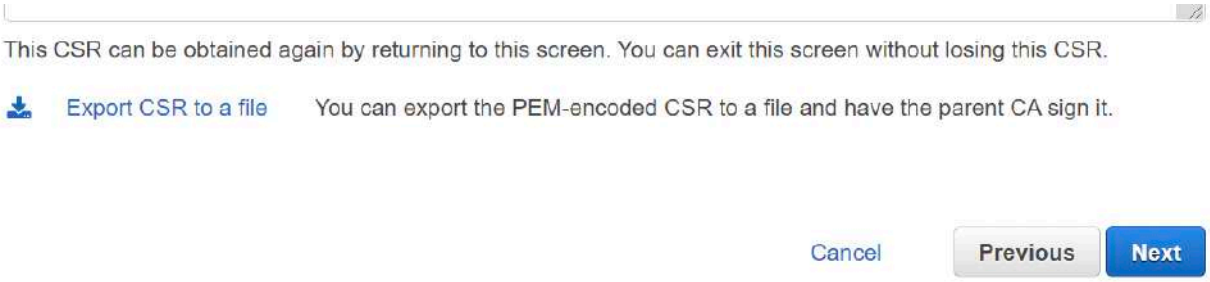


3. On the **Install subordinate CA certificate** page, select **External private CA.**

This installs a certificate signed by an external private CA that you own.



4. On the **Export a certificate signing request (CSR)** page, ACM Private CA generates and displays certificate information and a CSR. Scroll down and click on the option of **exporting the CSR to a file**.



5. Export the CSR to a file on your windows machine in **.PEM format.**
6. Copy this CSR file to your Root CA server (CA01).

Task 3: Sign the CSR and issue Certificate for EncryptionConsulting Issuing Subordinate CA

1. Ensure that you are logged on to CA01 as CA01\Administrator.

2. On CA01, open an administrative command prompt. Then, submit the request using the following command:

   certreq -submit "c:\CSR_subCA.pem"

   Note: Pay attention to the RequestID number that is displayed after you submit the request. You will use this number when retrieving the certificate.

3. In the **Certification Authority List dialog box**, ensure that **Encryption Consulting Root CA** is selected and then click **OK.**

4. Open the **Certification Authority** console. To do so, click Start, click Administrative Tools, click Certification Authority.

5. In the **certsrv** [Certification Authority (Local)] dialog box, in the console tree, expand Encryption Consulting Root CA.

6. Click **Pending Requests.** In the details pane, right-click the request you just submitted, click **All Tasks,** and then click **Issue.**

7. Return to the administrative command prompt to accept the issued certificate by running the following command:

   certreq -retrieve <ID> "c:\CSR_subCA.crt"

Task 4: Install the Encryption Consulting Issuing CA Certificate in AWS

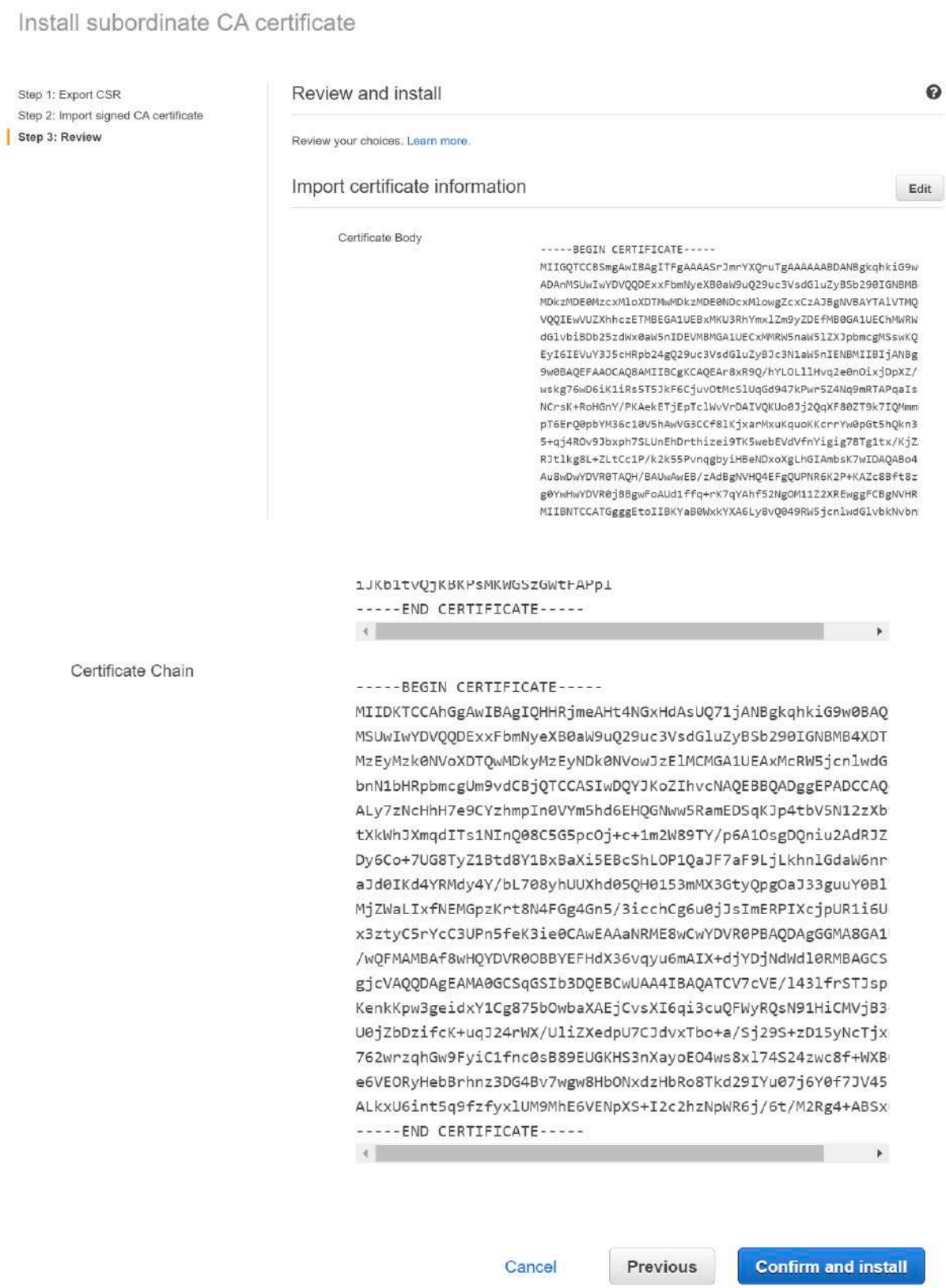
1. Go to your AWS console and continue from **"CSR generation for Subordinate CA".**

2. On the **Import a signed certificate authority (CA) certificate page**, import your signed CA certificate body (import CSR_subCA.crt) and your certificate chain (import your selfsigned Root CA Certificate - ECRootCA.crt) into the corresponding text boxes or import from files.

Note: **Signed CA Certificate (CSR_subCA.crt)** should be copied into a directory on a windows system where **AWS Console** is opened. **Root CA Certificate (ECRootCA.crt)** should be exported from **Root CA** through the **"Certificate Export Wizard"** in windows and should be copied into a directory on the same windows system where **AWS Console** is opened. Select both the certificate files from the stored directory while doing an import on the AWS Console page **"Import a signed certificate authority (CA) certificate"**

Note: Make sure the time zone of the Root CA windows server is aligned with the time zone of AWS region in such a way that the "Subordinate CA Certificate" should be valid while installing the "Subordinate CA Certificate" in ACM PCA.

3. On the Review and install page, confirm that your configuration is correct and choose Confirm and install. You should be returned to the Private CAs list page, displaying the status of the installation (success or failure) at the top. If the installation was successful, the newly completed Subordinate CA displays a status of Active in the list.



Activity 4: Create a Key-Pair

Task 1: Create a Public-Private Key-pair using an AWS EC2 Console

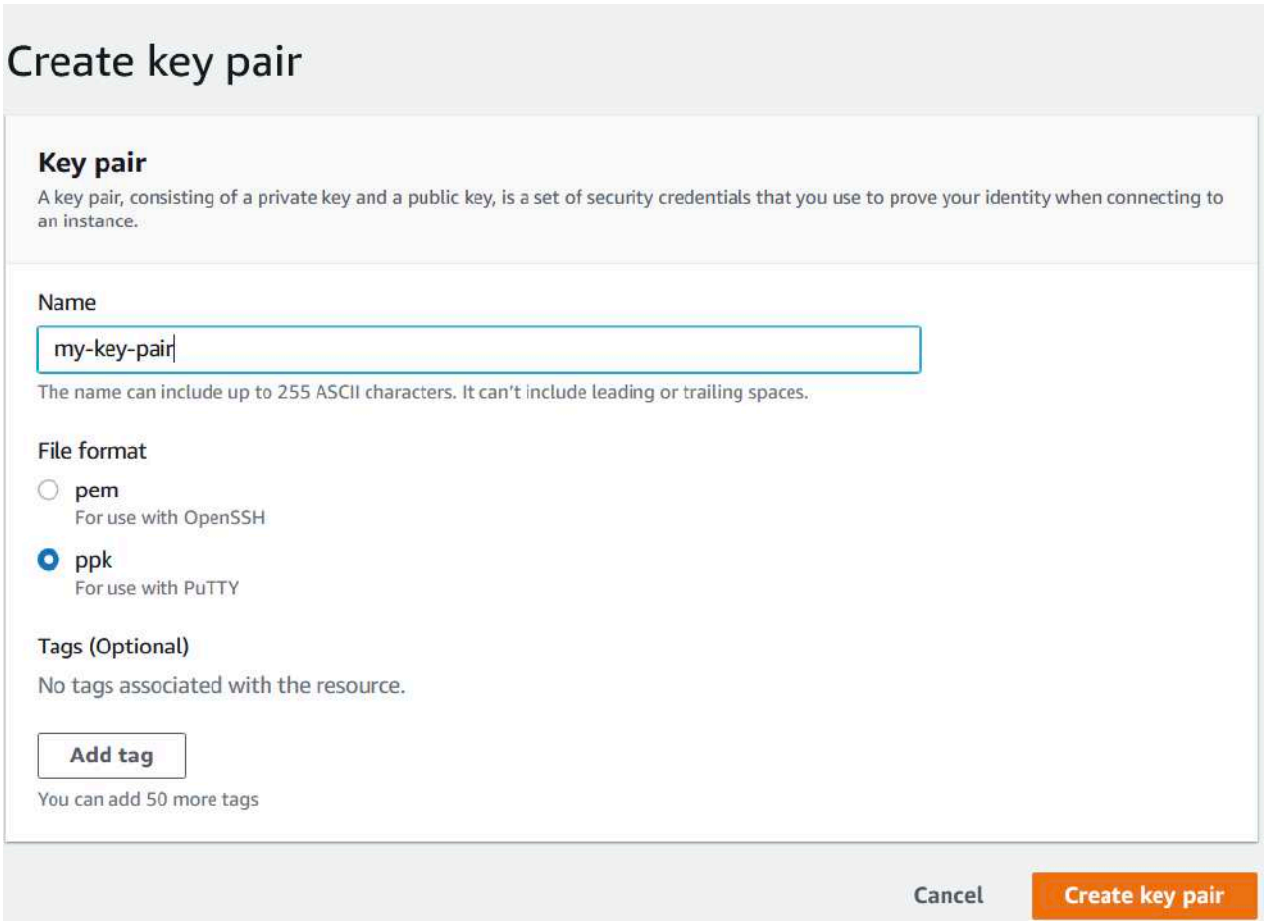
1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/

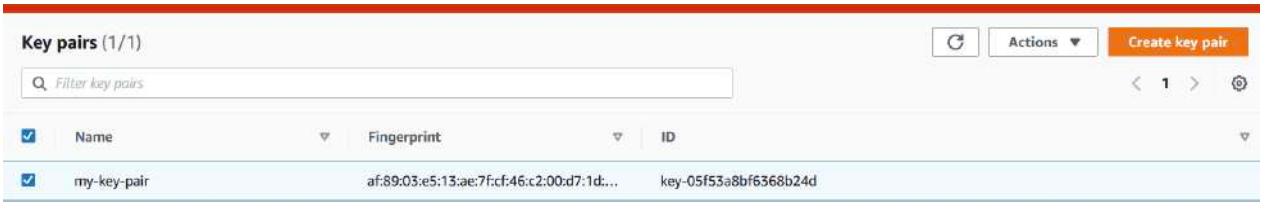
2. In the navigation pane, choose Key Pairs.

3. Choose Create key pair.

4. Enter a descriptive name for the key pair. Amazon EC2 associates the public key with the name that you specify as the key name.

5. Choose the format in which to save the private key. For Openssh, choose pem format and for Putty, choose ppk format. Here we are choosing ppk format.



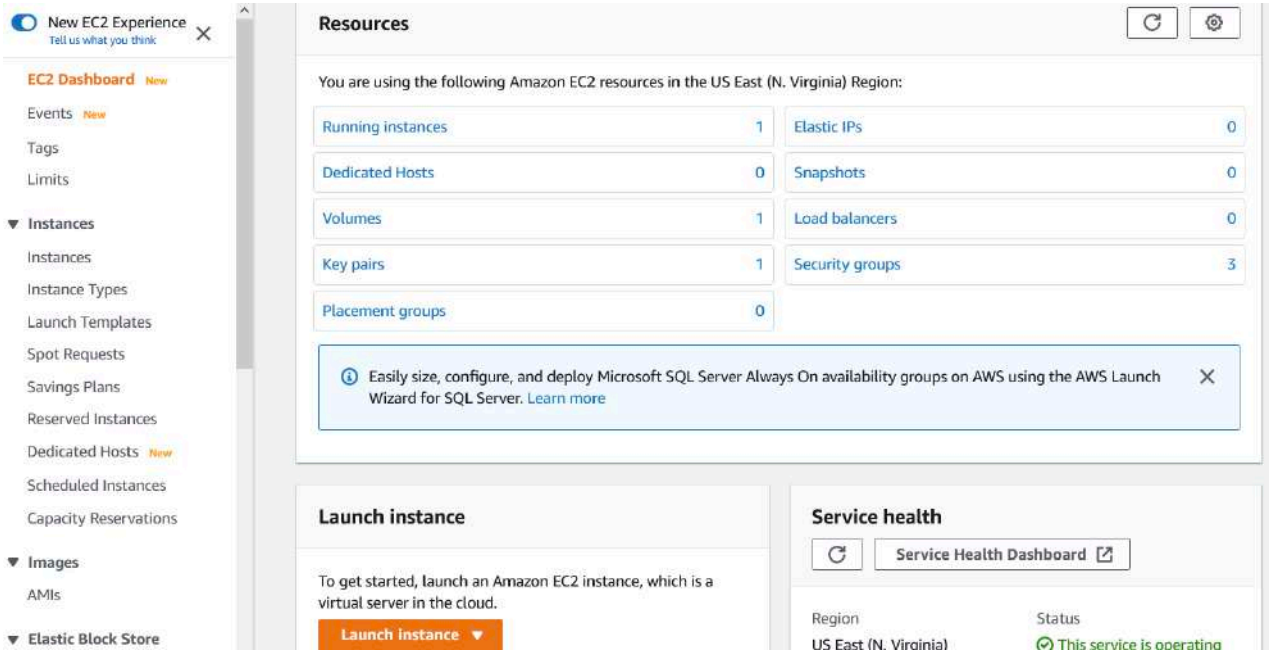


6. The private key file is automatically downloaded by your browser. Please save this file in a secure location as you will not get this file again.

Activity 5: Setup an EC2 instance

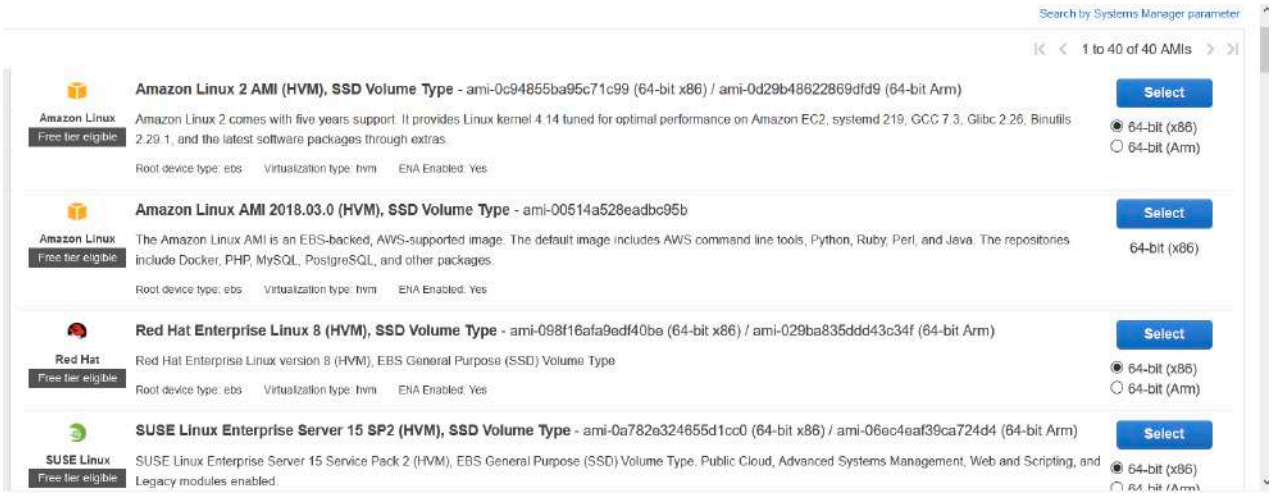
Task 1: Create and Setup an EC2 Instance to install the Apache Web Server on it.

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.

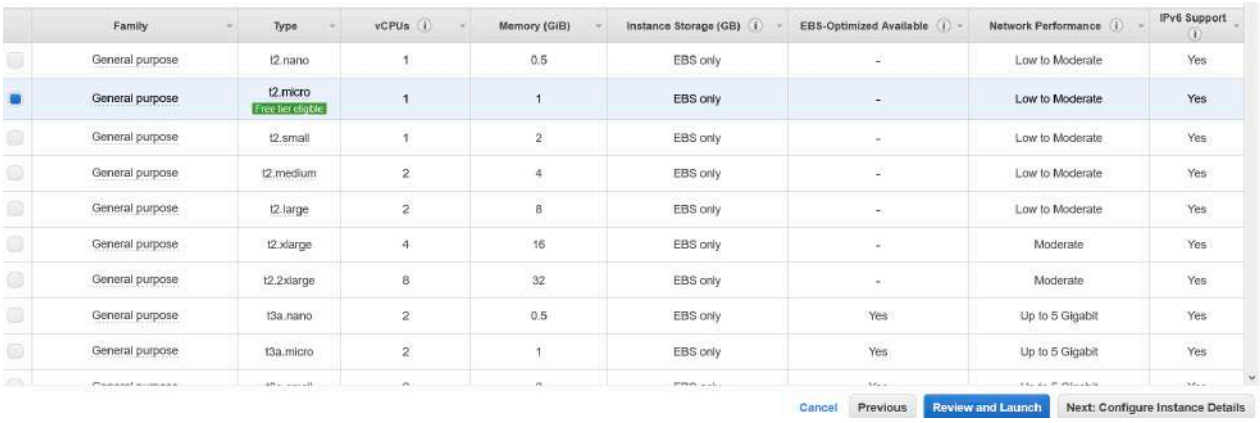


2. Choose Launch Instance.

3. Choose an Amazon Machine Image (AMI) select "Red Hat Enterprise Linux 8 (HVM), SSD Volume Type" (amzn2-ami-hvm-2.0.20200722.0-x86_64-gp2 (ami-02354e95b39ca8dec))



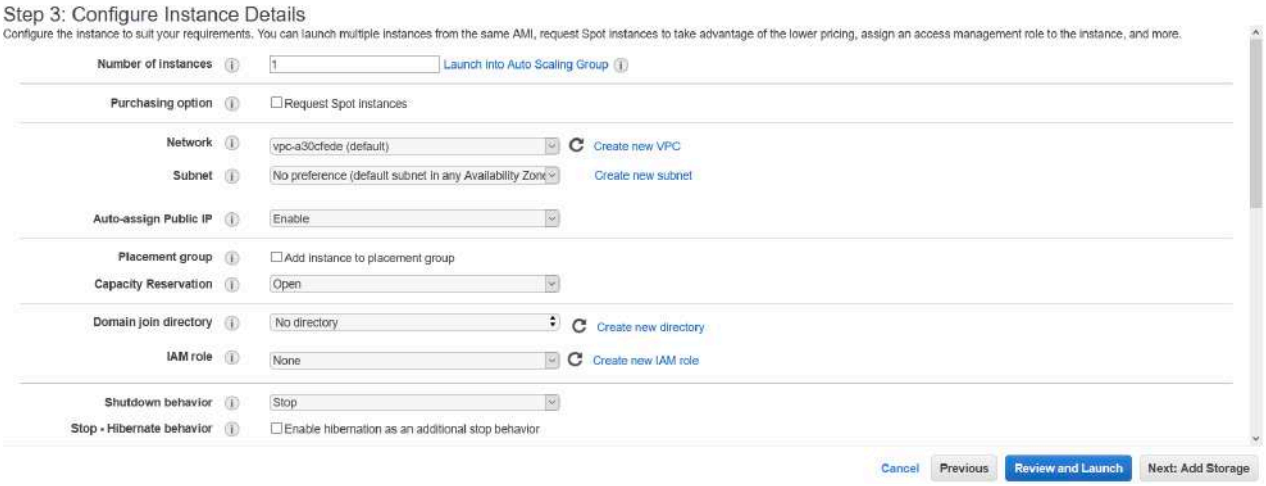
4. Choose an Instance Type "General Purpose: t2.micro", click Next: Configure Instance Details



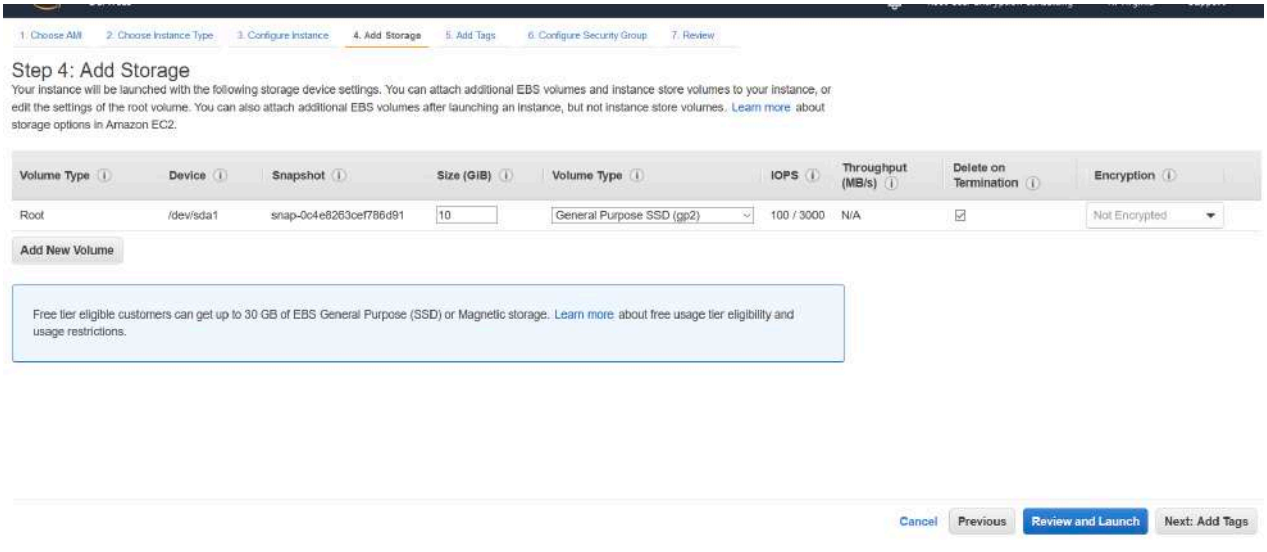
	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
	General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
■	General purpose	t2.micro (Free tier eligible)	1	1	EBS only	-	Low to Moderate	Yes
	General purpose	t2.small	1	2	EBS only	-	Low to Moderate	Yes
	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
	General purpose	t2.large	2	8	EBS only	-	Low to Moderate	Yes
	General purpose	t2.xlarge	4	16	EBS only	-	Moderate	Yes
	General purpose	t2.2xlarge	8	32	EBS only	-	Moderate	Yes
	General purpose	t3a.nano	2	0.5	EBS only	Yes	Up to 5 Gigabit	Yes
	General purpose	t3a.micro	2	1	EBS only	Yes	Up to 5 Gigabit	Yes

Cancel | Previous | Review and Launch | Next: Configure Instance Details

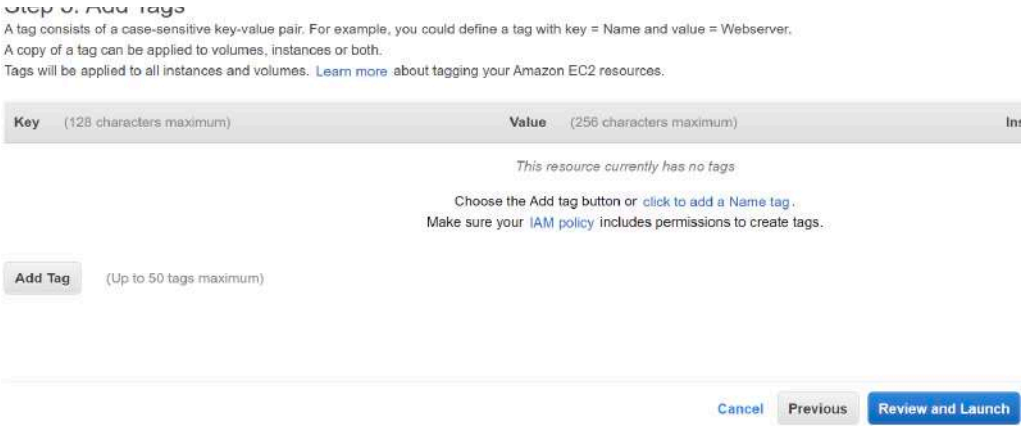
5. On the Auto Assign Public IP option drop down and select "Enable", leave the rest of the settings as "Default" and click Next: Add storage



6. Choose Next: Add Storage, for the lab purpose we are leaving this as default

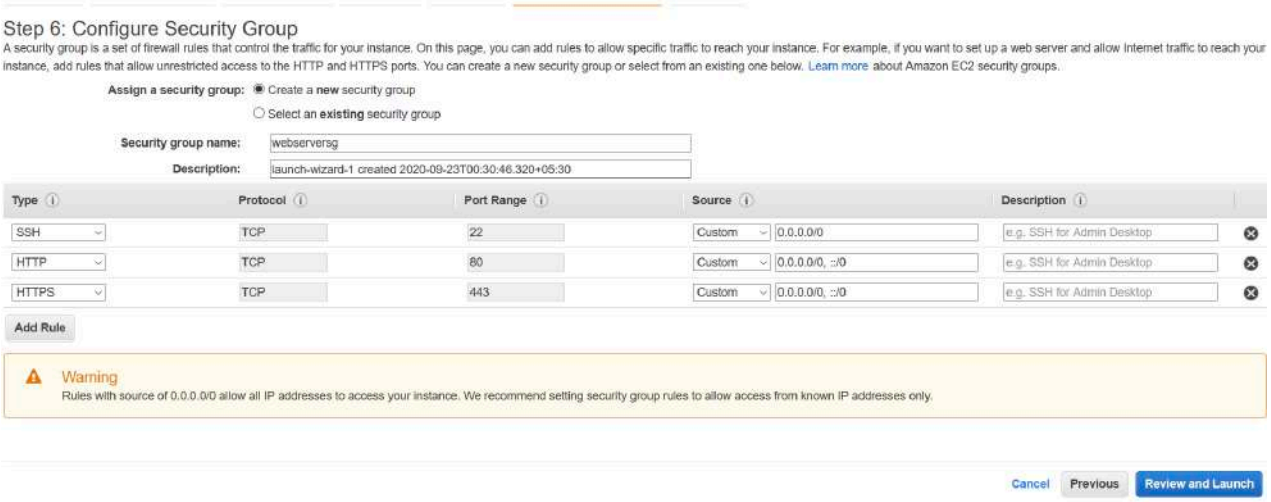


7. Choose Next: Add Tags (leave default)

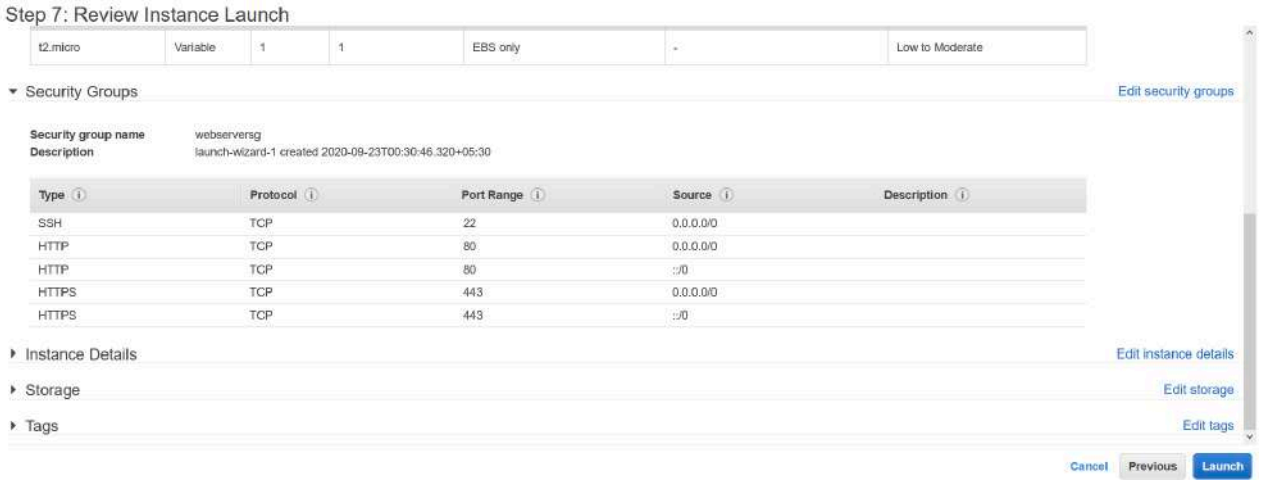


8. Choose Next: Configure Security Group. Add following inbound rules to the Security Group:

Type	Protocol	Port range	Source	Description - optional
HTTP	TCP	80	0.0.0.0/0	Web Server Access over http
SSH	TCP	22	0.0.0.0/0	SSH Access to the instance
HTTPS	TCP	443	0.0.0.0/0	Web Server Access over https

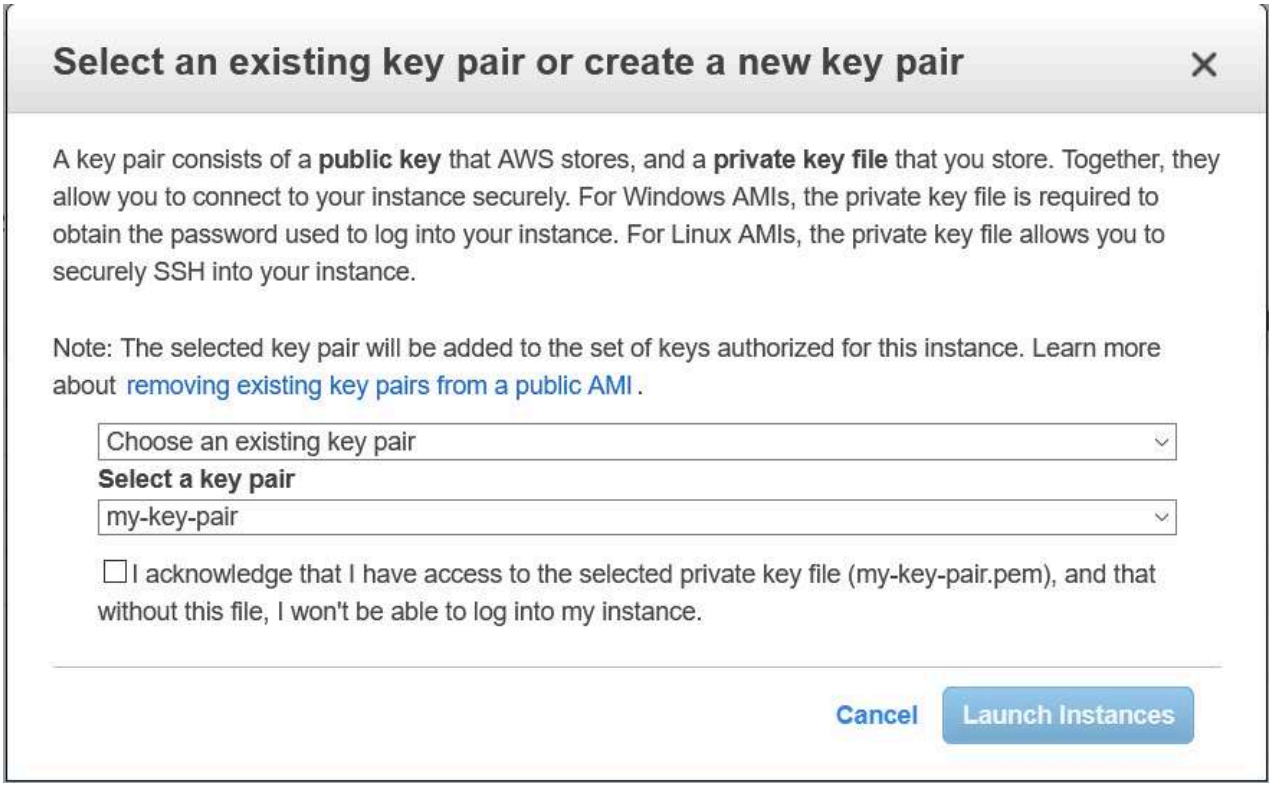


9. Choose Review and Launch.



10. Choose Launch.

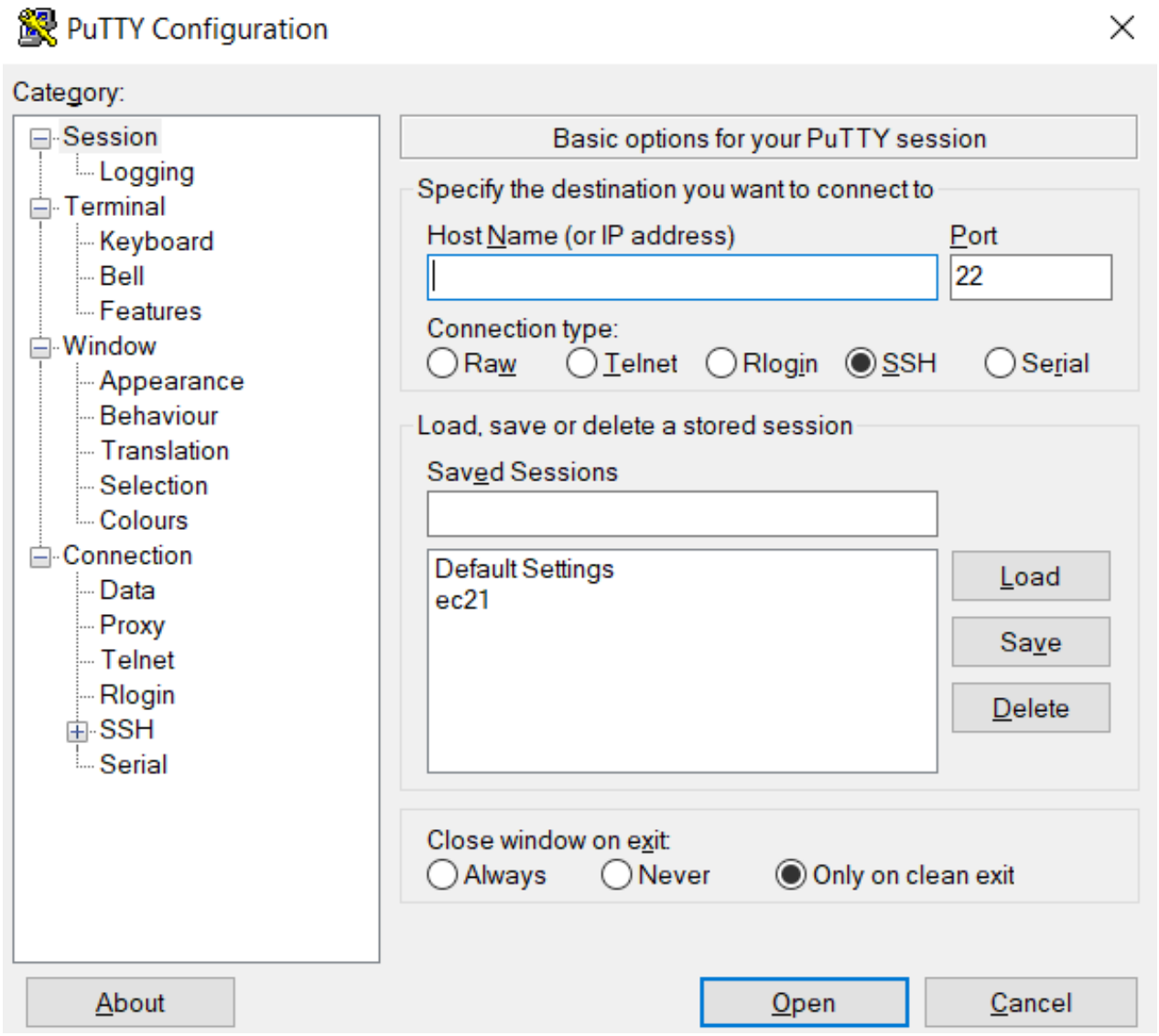
11. Select the check box for the key pair that you created, and then choose Launch Instances.



12. Wait for some time and then go to "EC2 dashboard --> Running Instances". Your instance should be running successfully with "Instance State: Running" and "Status Checks: 2/2 Checks Passed".

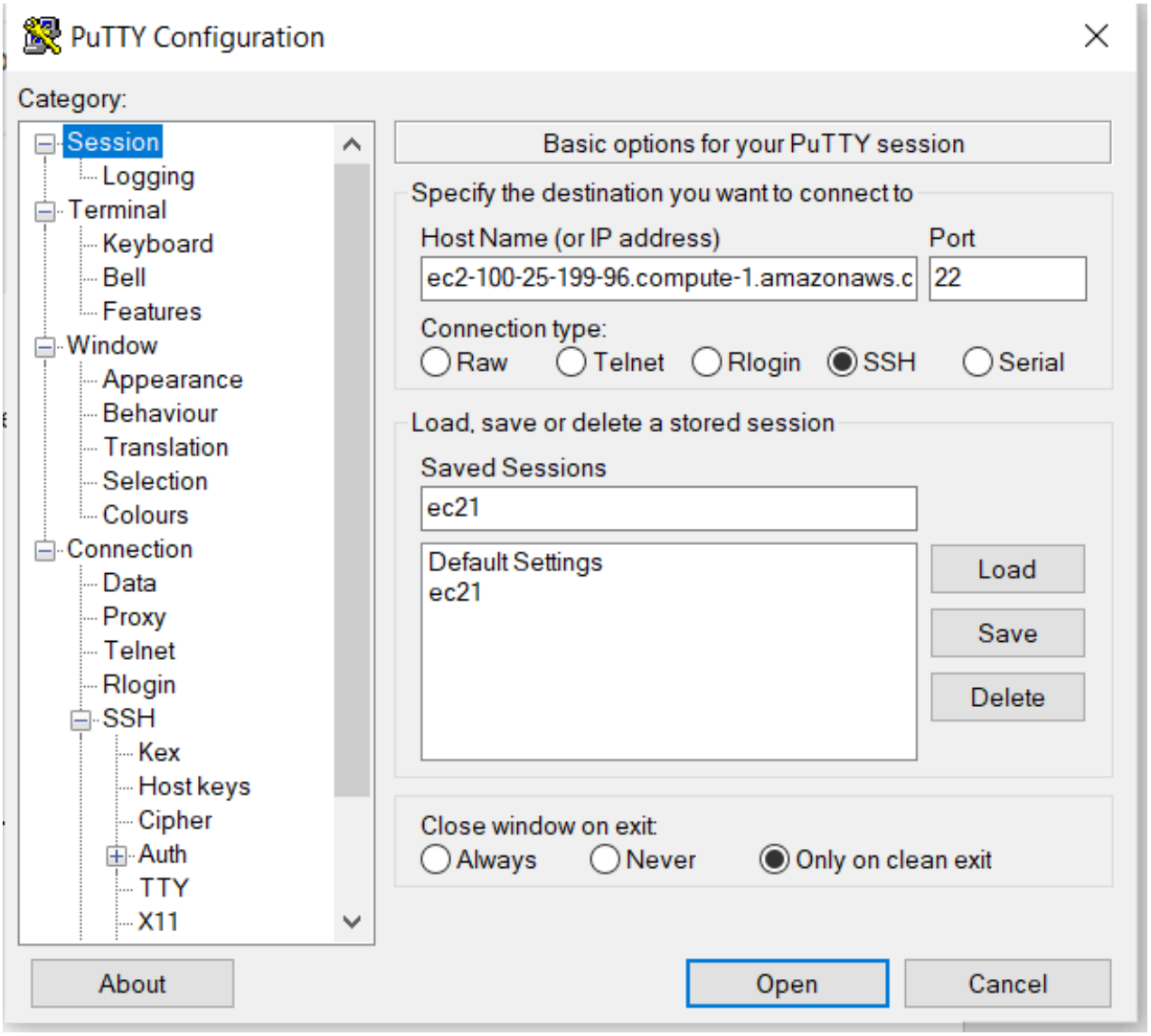
Task 2: Connect the EC2 instance using Putty client to install Apache Server on it.

1. Download and Open "Putty" on your windows machine.

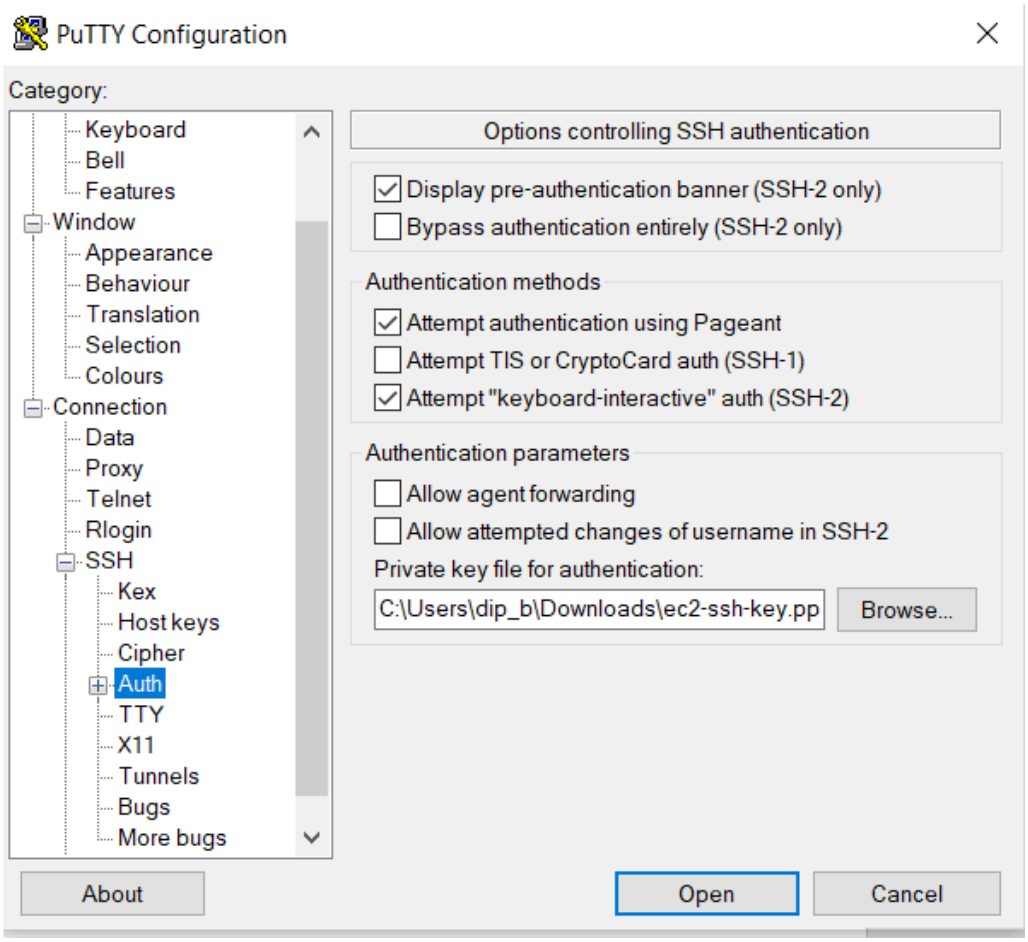


2. Enter Hostname: "ec2-100-25-199-96.compute-1.amazonaws.com" from "Public DNS (IPv4)" in AWS EC2 console and Port : 22 (ssh)

3.

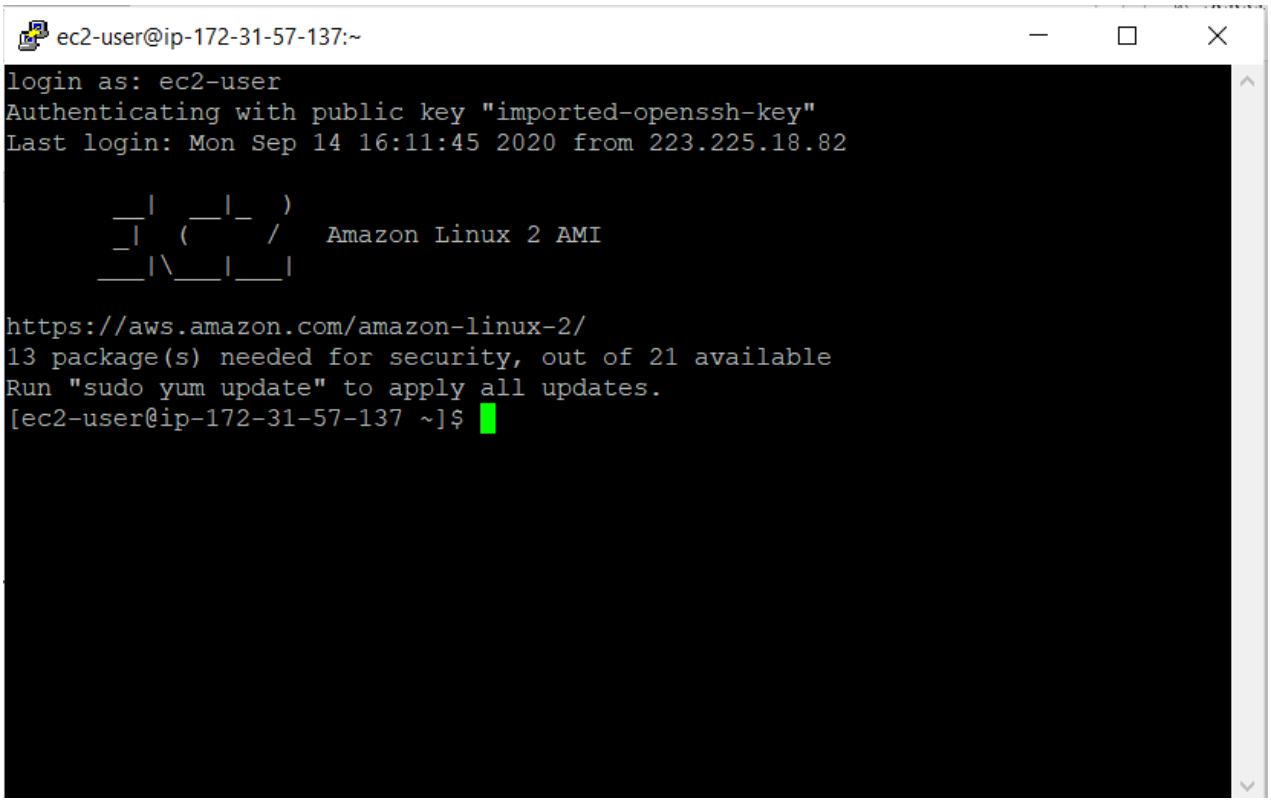


4. In Putty, Go to "Connections --> SSH --> Auth". Click browse and then upload the "Private Key" file in "ppk" format.



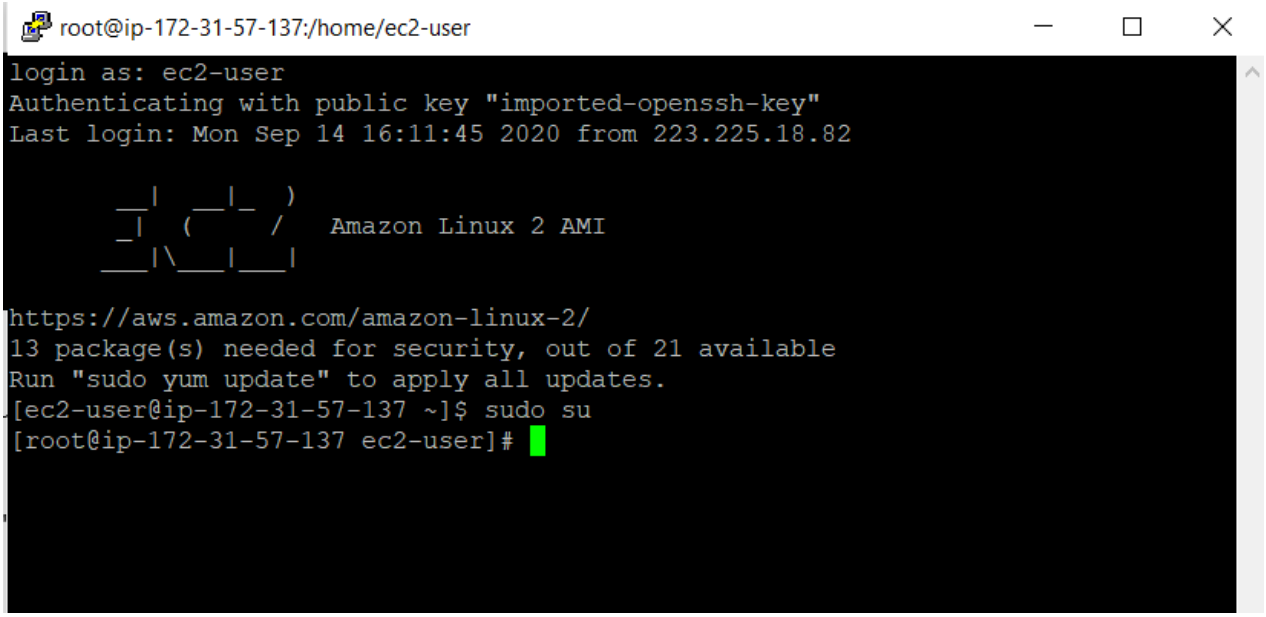
5. Click Open and then the Putty client connects to the EC2 instance in CLI mode.

7. Login as : “ec2-user”



7. Client will connect to "Amazon Linux 2 AMI"

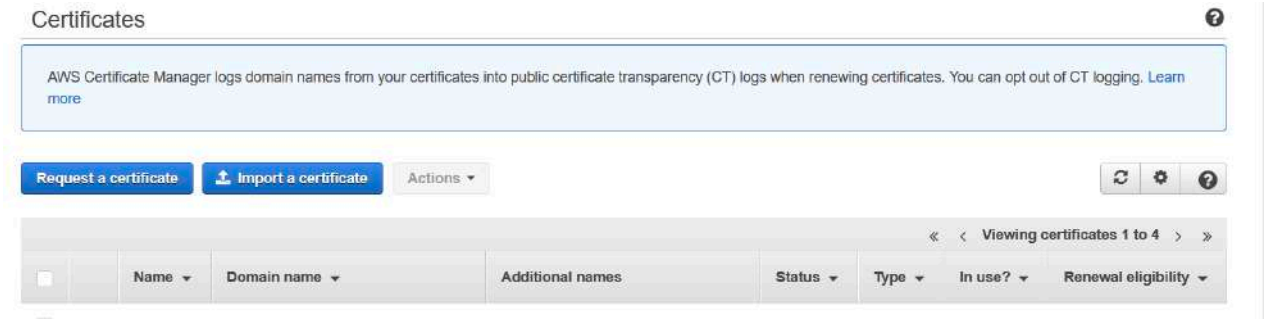
8. Type "Sudo su" to change to "root" user.



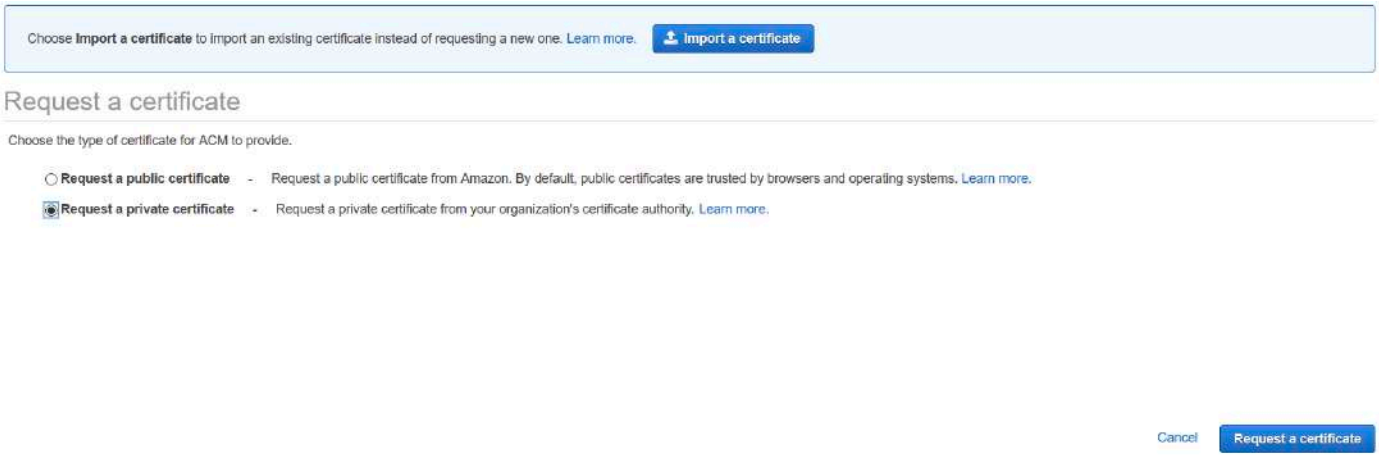
Activity 6: Issuing SSL/TLS Certificate for Web Server

Task 1: Issuing a Private SSL/TLS Certificate for Apache Web Server

1. Open the ACM Private CA console at https://console.aws.amazon.com/acm/home

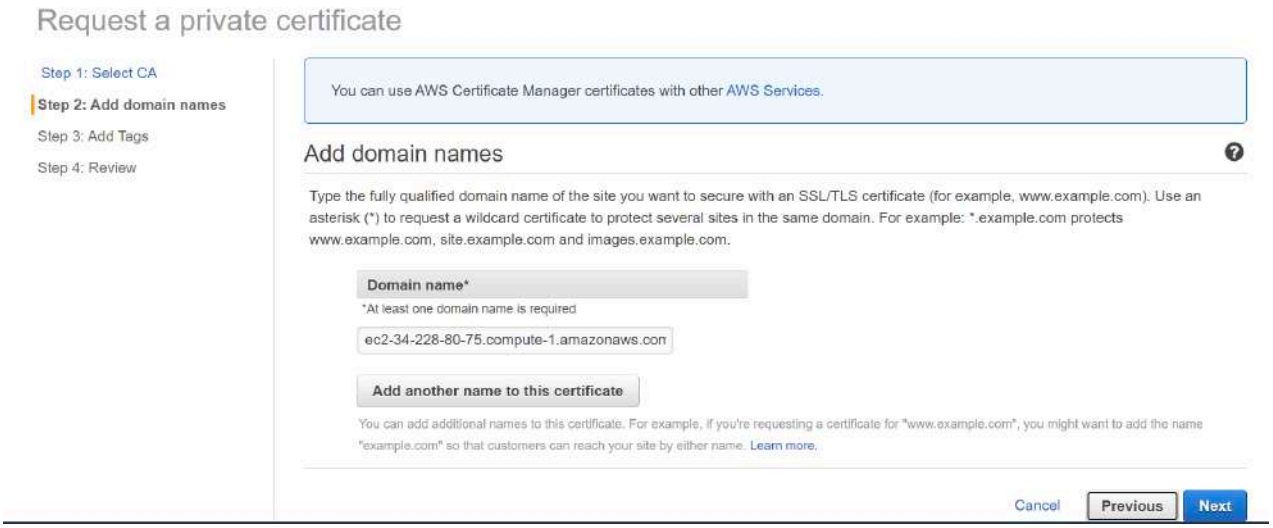


2. Click on "Request Certificate" and then "Request a Private Certificate".



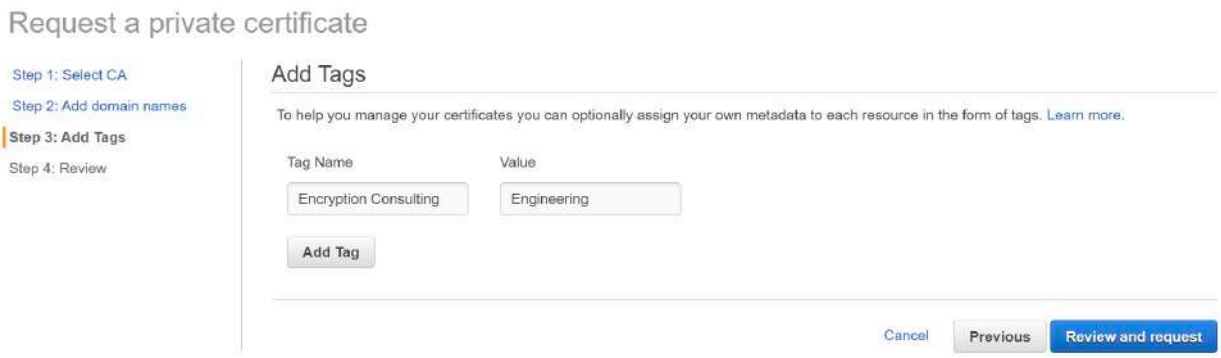
3. Select the CA from the drop-down list "EncryptionConsulting Issuing CA" and click "Next".

4. To add "Domain Names", type the FQDN for the Apache Web Server (your FQDN is same as what you used to login to putty)



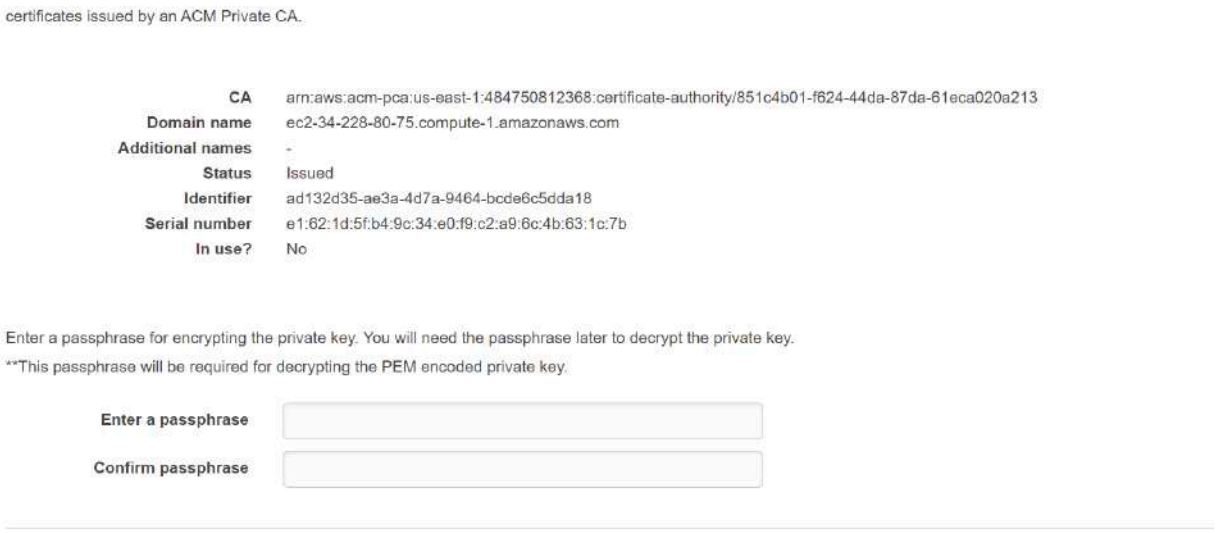
NOTE: You may add multiple names to attach to this Certificate

6. You may add "Tags" in the "Key-value" pair form.



7. On the Review and request page, confirm that your configuration is correct and choose Confirm and request. You should be returned to the Certificate list page, displaying the status of the successfully issued certificate.

8. Select the Issued certificate and Click on "Actions" and then select "Export (Private Certificates only)".



9. "Enter a passphrase" and "Confirm the Passphrase" to encrypt the private key of the certificate. Note: The same passphrase will be required to decrypt the Pem encoded private key.

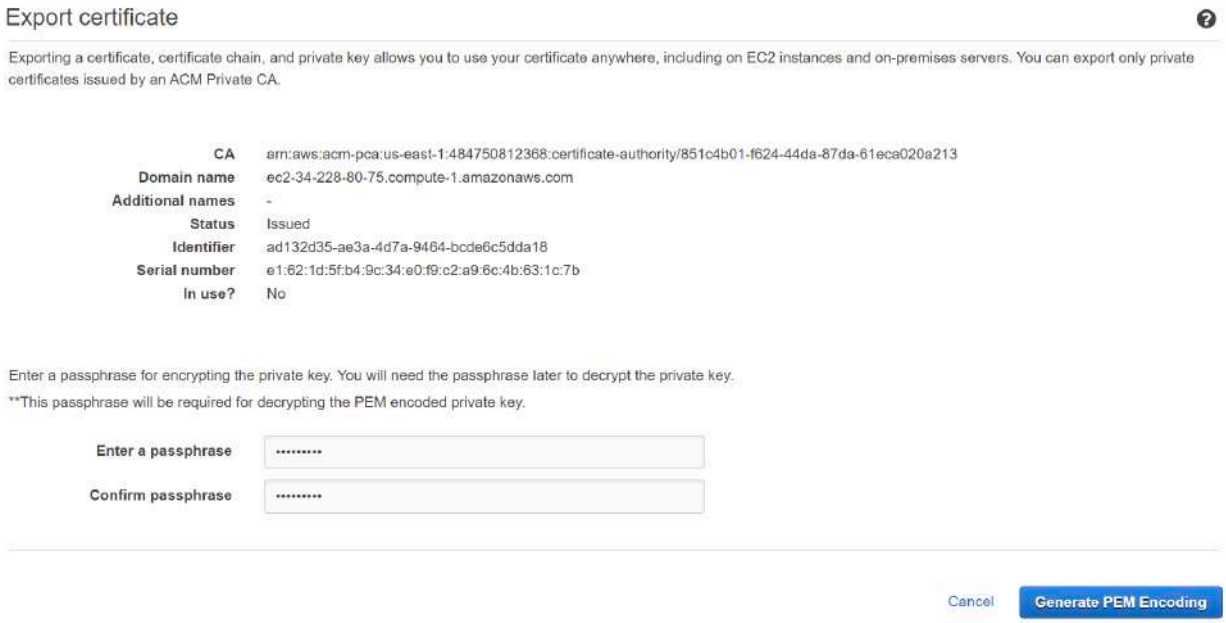


Figure-6

10. Select "Generate Pem Encoding" and then "Export Certificate" screen is shown.

11. Download the "Certificate", "Certificate Chain", and "Certificate Private Key" in pem encoded format on your windows machine.

12. Change the extension of **Certificate, Certificate chain** and ***Private Key*** file to **.crt** and **.key** respectively from. Pem as ACM PCA supports only .pem format for private key and certificate file

[to change the format from. pem to .crt and .key, go to the text file (e.g.; certificate.txt) > Right click > properties > General> delete .txt and update .crt/.key]

Activity 7: Install the Apache Web Server

Task 1: Install and Configure the Apache Web Server on EC2 instance

1. Connect to EC2 instance using Putty.

2. Type "**ec2-user**" for ""Login as"

3. Client will connect to "Amazon Linux 2 AMI"

4. Type "**Sudo su**" to change to "root" user.

5. Type "**yum install httpd**". This will install the http service on the instance. When popped for " IS IT OK" > type **Yes**

6. Type "**service httpd start**"

7. Type "**service httpd status**". Service httpd should be running.

8. Type "**netstat -tupan | grep -i http**". The output should include "**http**" running on port **80.**

```
[root@ip-172-31-28-208 ec2-user]# netstat -tupan | grep -i http
tcp6       0      0 :::80                   :::*                    LISTEN      13066/httpd
[root@ip-172-31-28-208 ec2-user]#
```

9. Open the web browser on your windows machine and type the hostname/dns name of the instance in the browser e.g.:

   http://ec2-100-25-199-96.compute-1.amazonaws.com

   9. This should open the default page of apache web server.

Task 2: Install the SSL/TLS Certificate to the Apache Web Server

1. Connect to EC2 instance using Putty.

2. Type "**ec2-user**" for ""Login as"

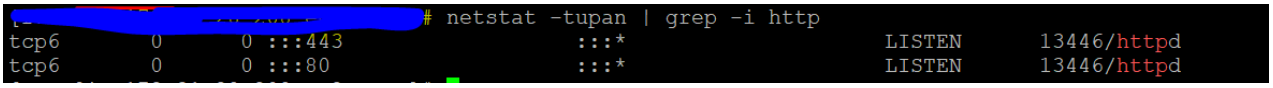
3. Client will connect to "Amazon Linux 2 AMI"

4. Type "**Sudo su**" to change to "root" user.

5. Type "**yum install mod_ssl**". This will install the ssl module on the instance.

6. Type "**service httpd restart**".

7. Type "**netstat -tupan | grep -i http**". The output should include "http" running on port **80** as well as on port **443.**



8. Type "**vi /etc/httpd/conf.d/ssl.conf**". This will open the "ssl.conf" in the editor:

9. Add below configuration to the "**ssl.conf**" file:

Listen 443 https

NameVirtualHost *:443

[Add the below snippet at the end of the ssl.conf file in the vi editor. Also, change the server and file names according to your customized set up]

<VirtualHost *:443>

SSLCertificateFile /etc/pki/tls/certs/Certificate.crt

SSLCertificateKeyFile /etc/pki/tls/private/private_key.key

sslEngine on

ServerName ec2-100-25-199-96.compute-1.amazonaws.com
ServerAdmin admin@ec2-100-25-199-96.compute-1.amazonaws.com
DocumentRoot /var/www/html/ec2-100-25-199-96.compute-1.amazonaws.com

</VirtualHost>

Press Esc

Save the file :wq!

10. Create a directory "**mkdir /var/www/html/ec2-100-25-199-96.compute-1.amazonaws.com**"

11. Create an "**index.html**" file with following html code: **vi /var/www/html/ec2-100-25-199-96.compute-1.amazonaws.com/index.html**

<h1>

Welcome to first AWS PCA Lab Setup

</h1>

12. Type "**service httpd restart**"

13. Type "**httpd -t**". This command will check the Apache configuration files for any syntax errors. Make sure there are no errors shown.

14. Now, copy the Certificate from your windows machine to "**/etc/pki/tls/certs/Certificate.crt**" on the EC2 instance.

15. Copy the Certificate Private key from your windows machine to "**/etc/pki/tls/private/private_key.key**" on the EC2 instance.

NOTE: User can choose any software or tools copy/download certificate and privatekey file from local windows machine to the above-mentioned path on the EC2 instance. [e.g., Winscp]

16. Type "**service httpd restart**"

17. Type "**systemctl enable httpd.service**"

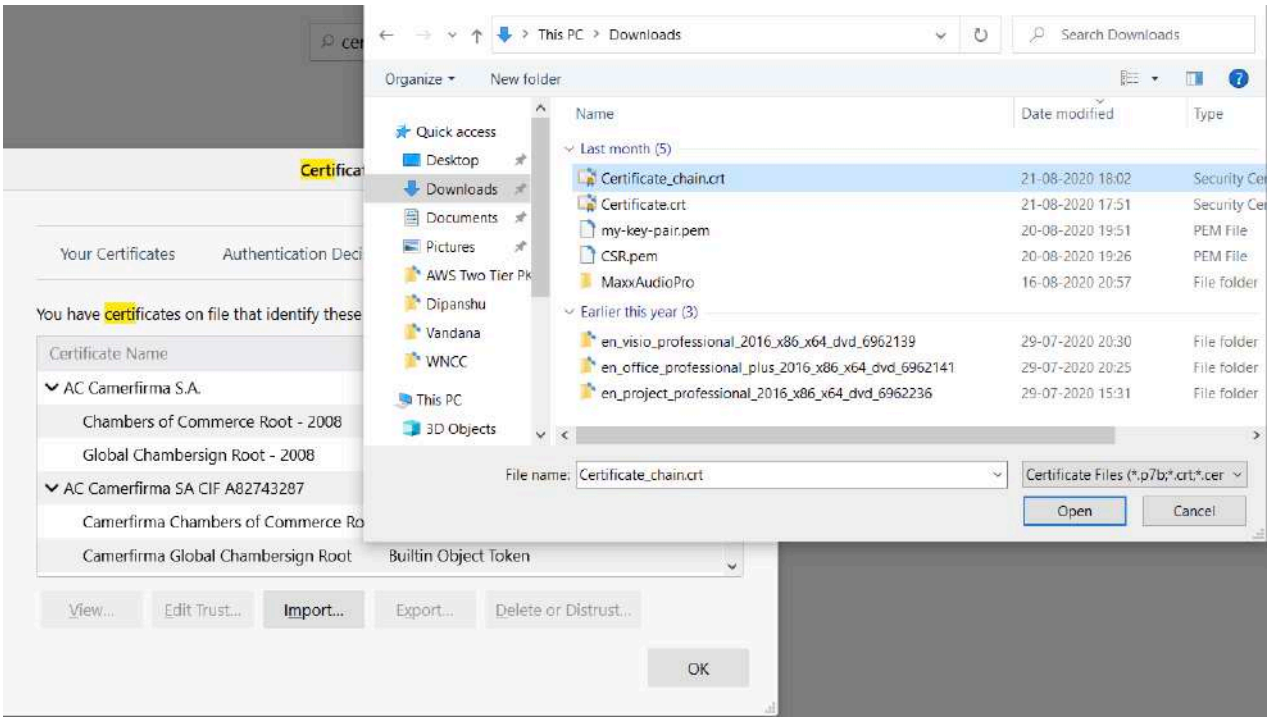
Task 2: Install the SSL/TLS Certificate Chain to the Client's Web browser

1. Open the Firefox web browser.

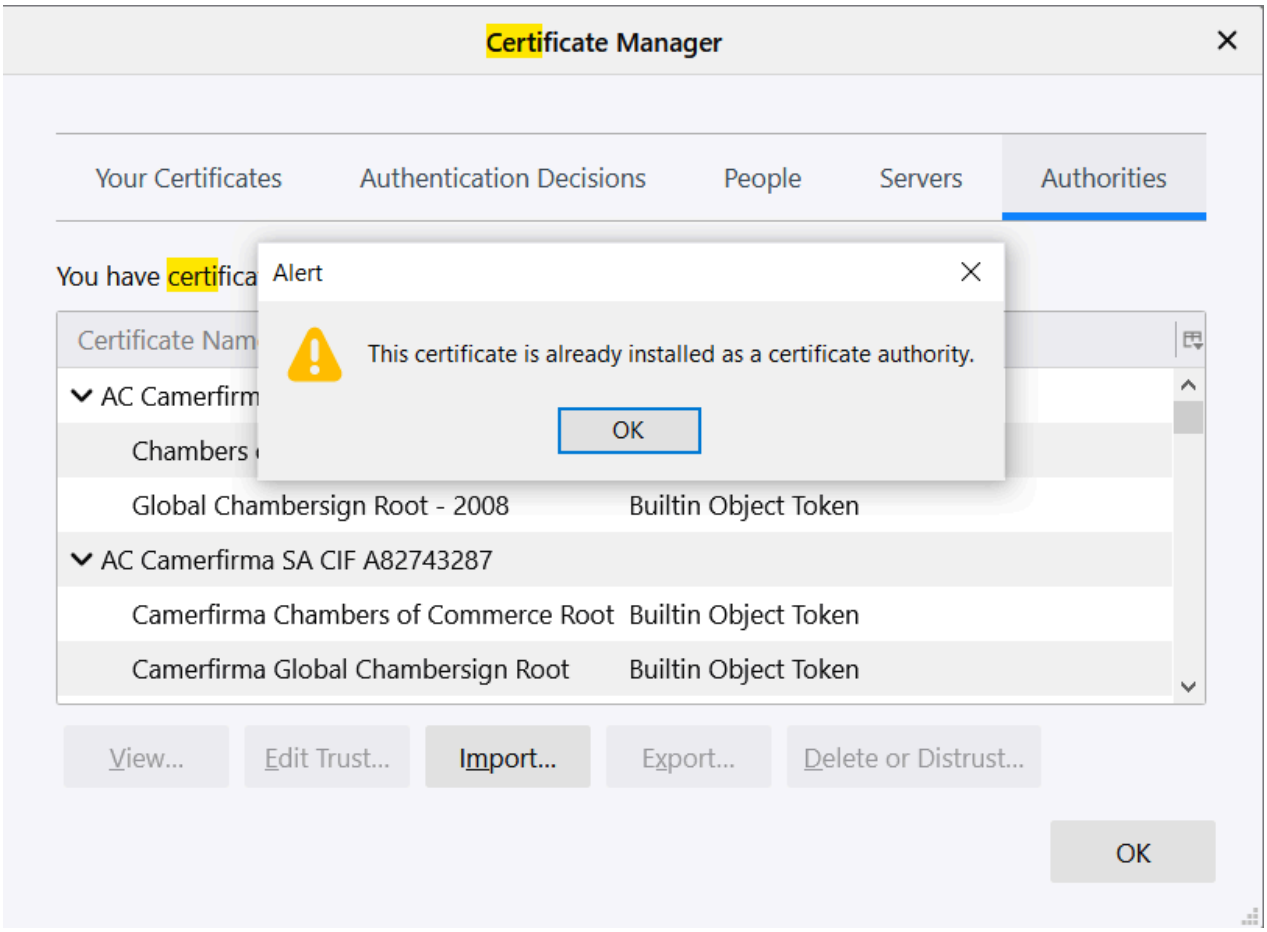
Note: You may add the SSL/TLS certificate to the browser of your choice. For the illustration purpose, I have taken Firefox browser.

2. Go to "Menu --> options ---> Privacy & Security --> Certificates --> View Certificates ---> Import".

3. Click "Import" and browse the Certificate Chain file. Choose the file and click open.



4. Certificate chain should be successfully installed in the browser and now, this browser should trust any certificate issued by the Subordinate CA and has trust relationship up-till Root CA.



Activity 8: Verify the Hybrid PKI Hierarchy Health

Task 1: Web Server Certificate validation

1. Open the Firefox web browser.
2. Type the following url name in the browser:

   https://ec2-100-25-199-96.compute-1.amazonaws.com

3. The custom web page should be shown with the following message:

   "Welcome to first AWS PCA Lab Setup"

4. Verify the "**Green Pad lock**" in the browser.

5. Click the Green Pad lock and verify the certificate by clicking "**More Information -->View Certificate**".

6. Verify the "**Issuer Name**", "**Validity**", "**Subject Name**", and "**CRL distribution points**".

7. Verify downloading the **CRL** and check the **CRL attributes** as well.

Task 2: CloudTrail logs for Certificate Issuance

1. Open the AWS CloudTrail console with the below link:
   "https://console.aws.amazon.com/cloudtrail/home"

2. Click ☰ on left hand corner and then go to "**Event History**".

3. Select "**Event Name**" in "**Lookup Attributes**" drop-down menu.

4. Type "**IssueCertificate**" in the text box and then press "Enter"

5. The logs entry should show the API call of "**IssueCertificate**"

6. Click on log entry "**IssueCertificate**" and verify the details of "**EventRecord**"

Task 3: CloudTrail logs for Certificate Retrieval

1. Open the AWS CloudTrail console with the below link:
   "https://console.aws.amazon.com/cloudtrail/home"

2. Click ☰ on left hand corner and then go to "**Event History**".

3. Select "**Event Name**" in "**Lookup Attributes**" drop-down menu.

4. Type "**GetCertificate**" in the text box and then press "Enter"

5. The logs entry should show the API call of "**GetCertificate**"

6. Click on log entry "**GetCertificate**" and verify the details of "**EventRecord**"

Task 4: Verify PKI Health for Web Server Certificate with "Certutil" utility

1. Log into Win7/10 as an Administrator.
2. Click **Start**, type **mmc** and then press ENTER.
3. Click **File**, and then click **Add/Remove Snap-in**.
4. Click **Certificates**, then click **Add**. Select **Computer Account**, and then click **Finish**. Click **OK**.
5. Expand **Certificates**, right click **Personal**, click **All Tasks**, and then click **Import**.
6. On the **Certificate Import Wizard** page, click **Next**.
7. On the **File to Import** page, browse the **Certificate** file click **Next**.
8. On the **Certificate Store** page, Click **Next**.
9. On the **Completing the Certificate Import Wizard** page, click then **Finish**, and then click **OK**.
10. Expand **Certificates**, right click **Personal**, click **All Tasks**, and then click **Import**.
11. On the **Certificate Import Wizard** page, click **Next**.
12. On the **File to Import** page, browse the **Certificate Chain file** click **Next**.
13. On the **Certificate Store** page, Click **Next**.
14. On the **Completing the Certificate Import Wizard** page, click then **Finish**, and then click **OK**.
15. Open a command prompt and run the following commands: (To open a command prompt, click **Start**, type **cmd**, and then press ENTER)
    - **cd**
    - **certutil -URL C:\win7.cer**
16. In the URL Retrieval Tool, perform the following steps, in the **Retrieve** section:
    - Select **CRLs (from CDP)** option and then click **Retrieve**. Confirm that it shows status as **Verified**.
17. Click **Exit** to close URL Retrieval Tool.
18. From command prompt run following command to thoroughly verify certificate chain retrieval and revocation status.
    - **certutil -verify -urlfetch c:\win7.cer**
19. Review the output and make sure all the chain retrieval and revocation status successfully verified.