ENCRYPTION CONSULTING
www.encryptionconsulting.com

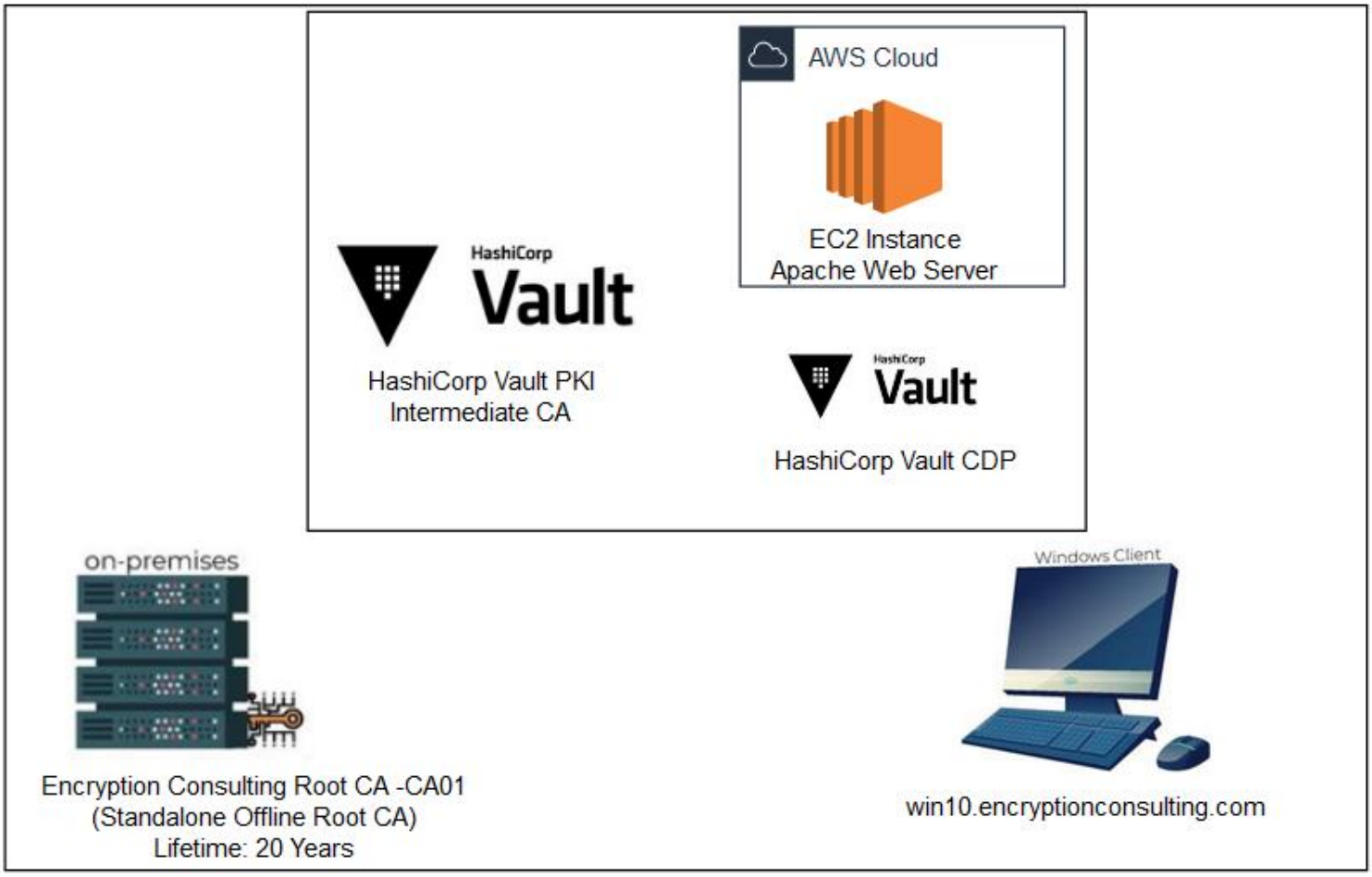
Two Tier PKI Hierarchy Deployment with Windows and HashiCorp

Detailed guide for Basic Configuration

Introduction and overview of the Test Lab:

There are three computers, one Standalone Root CA, one HashiCorp Issuing CA instance, and one Windows machine involved in this two-tier PKI hierarchy lab:

1. One Standalone Offline Root CA (CA01).
2. One HashiCorp Issuing CA (Encryption Consulting Issuing CA) instance
3. One EC2 instance with RHEL8 distribution running an Apache Web Server (ec2-107-22-163-176.compute-1.amazonaws.com)
4. HashiCorp CRL location
5. One Windows Client Computer



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	Issuing CA	HashiCorp OSS	NA	HashiCorp
ec2-107-22-163-176.compute-1.amazonaws.com	Apache Web Server	RHEL-8	FQDN	AWS Cloud
HashiCorp CRL	CRL	HashiCorp	NA	HashiCorp
Windows	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 HashiCorp 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.

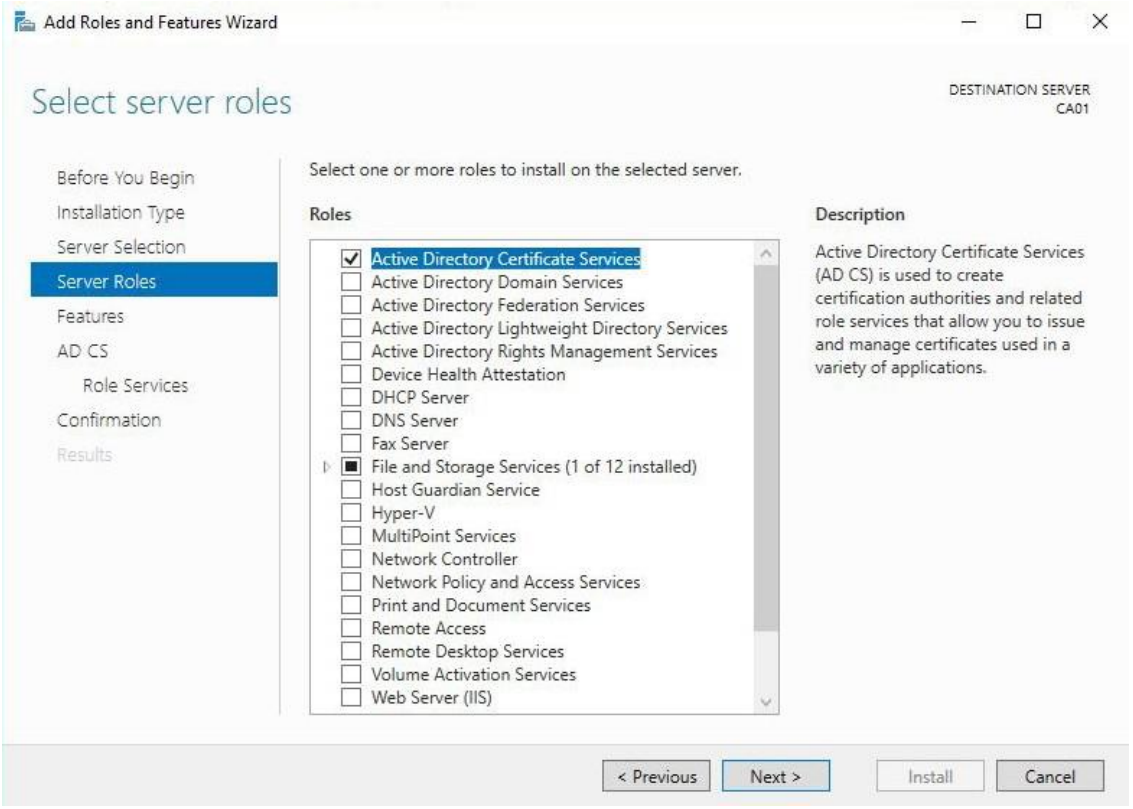
6. Close Notepad.

Task 2: Installing the Standalone Offline Root CA

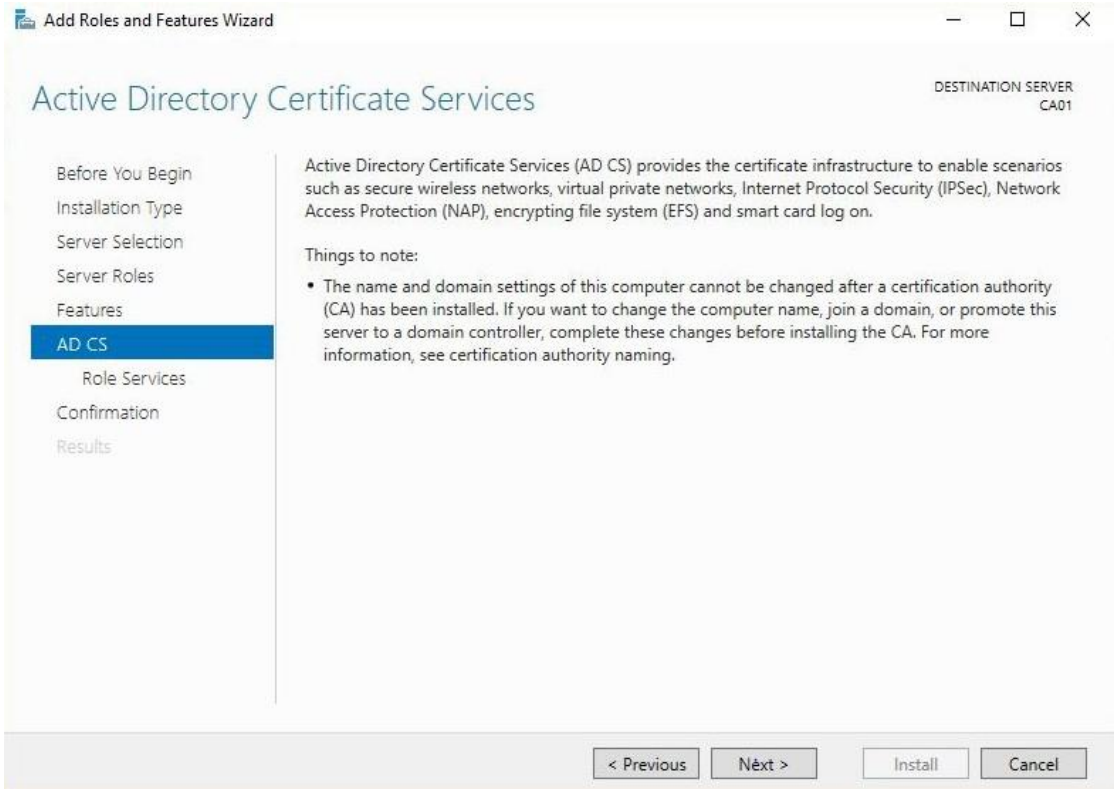
To install the standalone offline root CA:

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**.

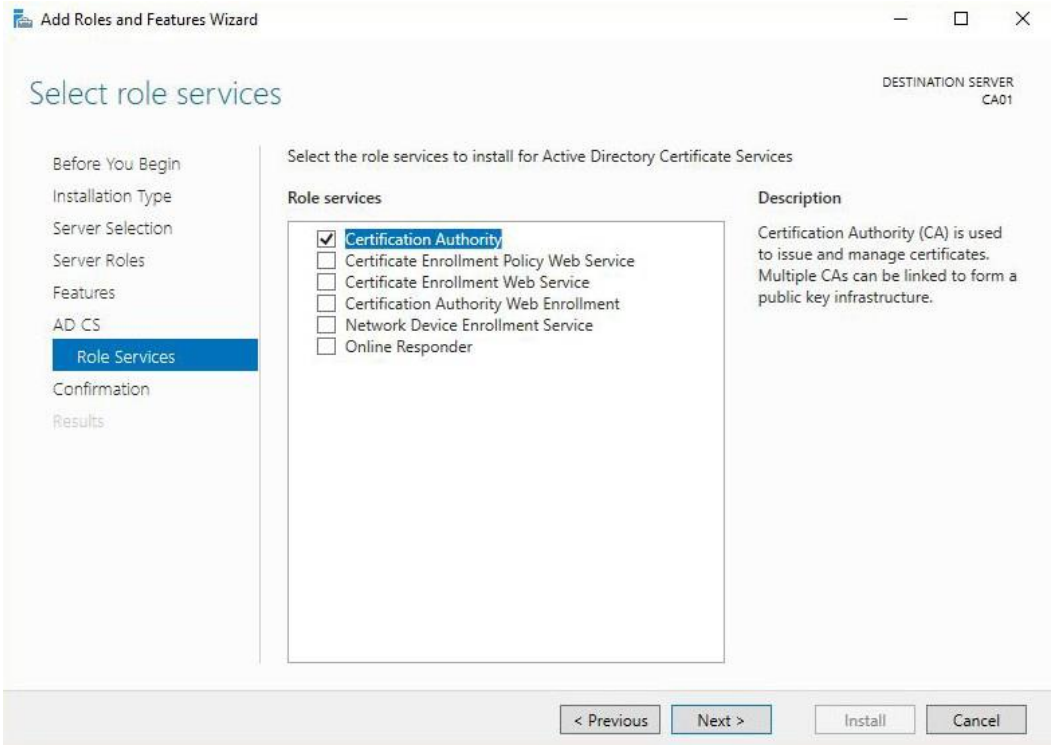
5. On the **Select Server Roles** page select **Active Directory Certificate Services**, and then click **Next.**



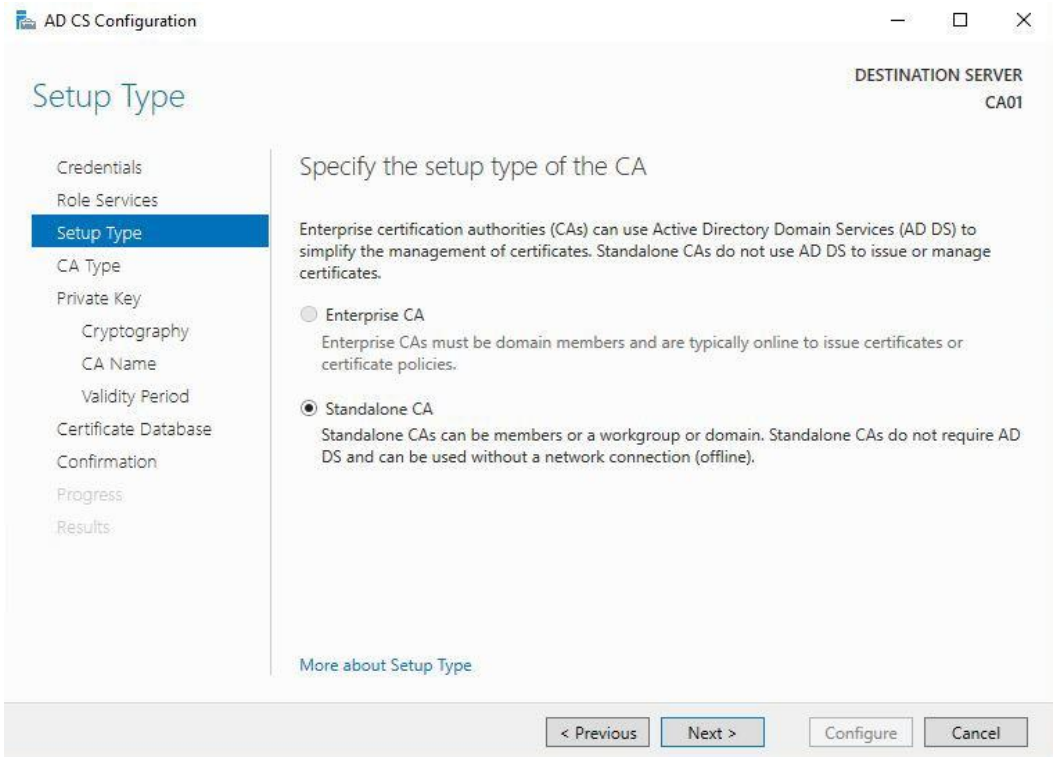
6. On the select features page, click next.
7. On the **Introduction to Active Directory Certificate Services** page, click **Next.**



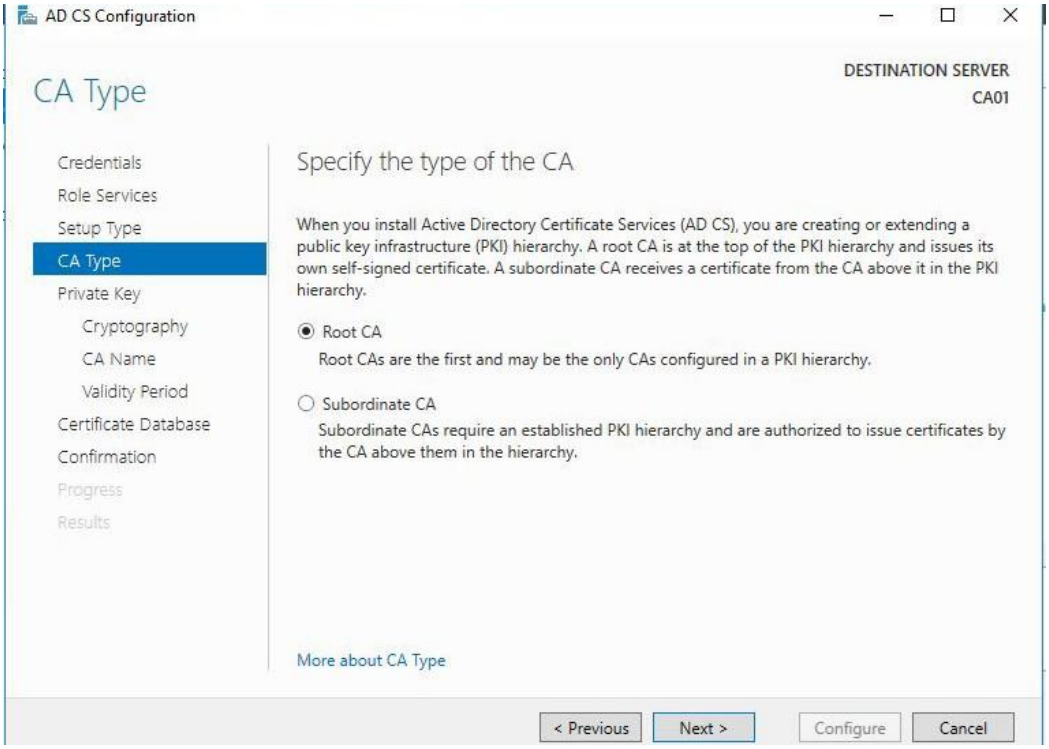
8. On the **Select Role Services** page, ensure that **Certification Authority** is selected, and then **Next.**



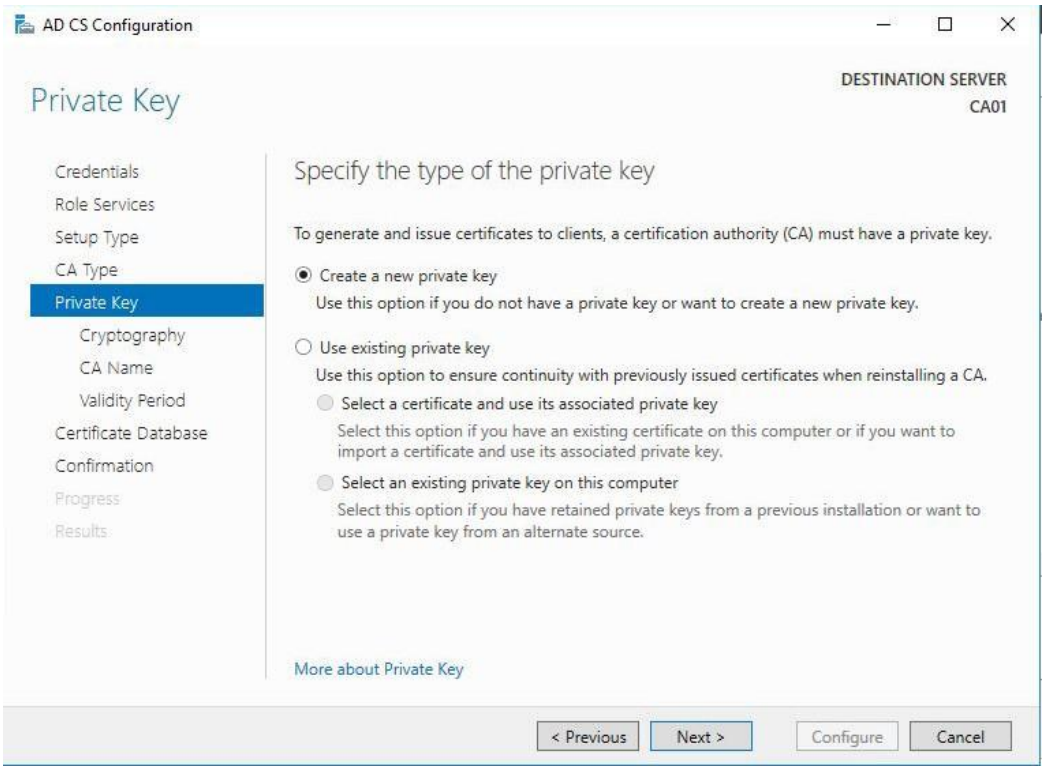
9. On the **Specify Setup Type** page, ensure that **Standalone** is selected, and then click **Next.**
    - Note: Enterprise option is grayed out as CA01 server is not joined to an Active Directory domain.



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.**

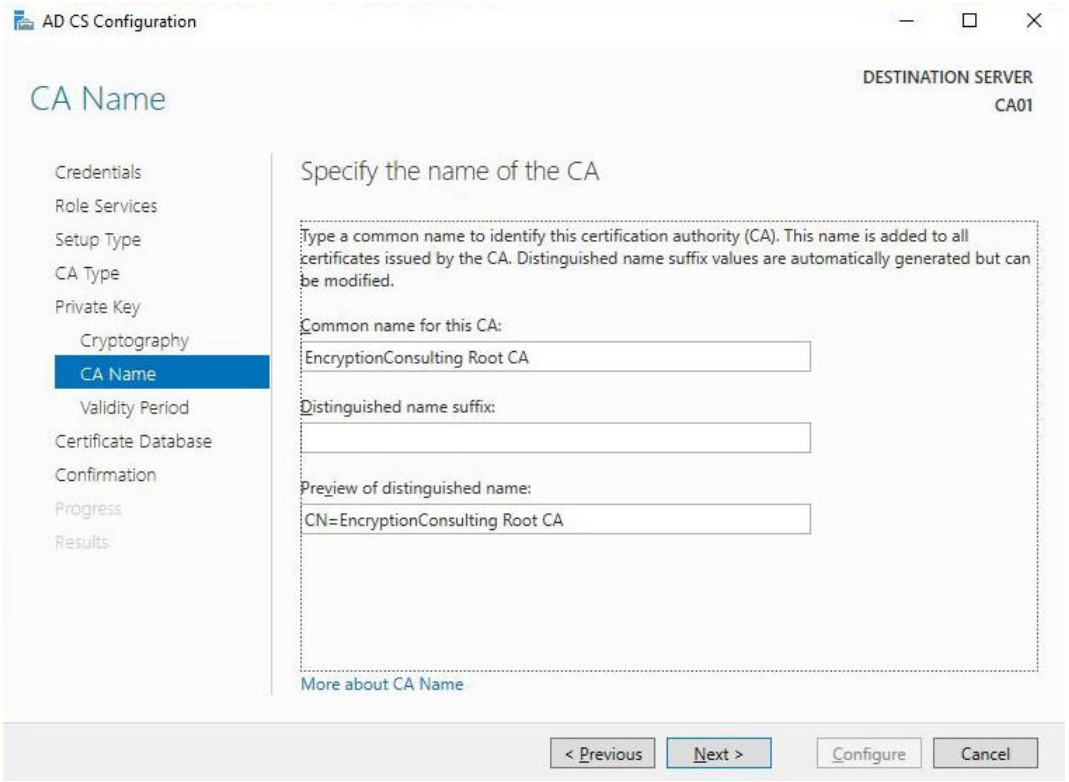


12. Leave the defaults on the **Configure Cryptography for CA** page, and then click **Next.**

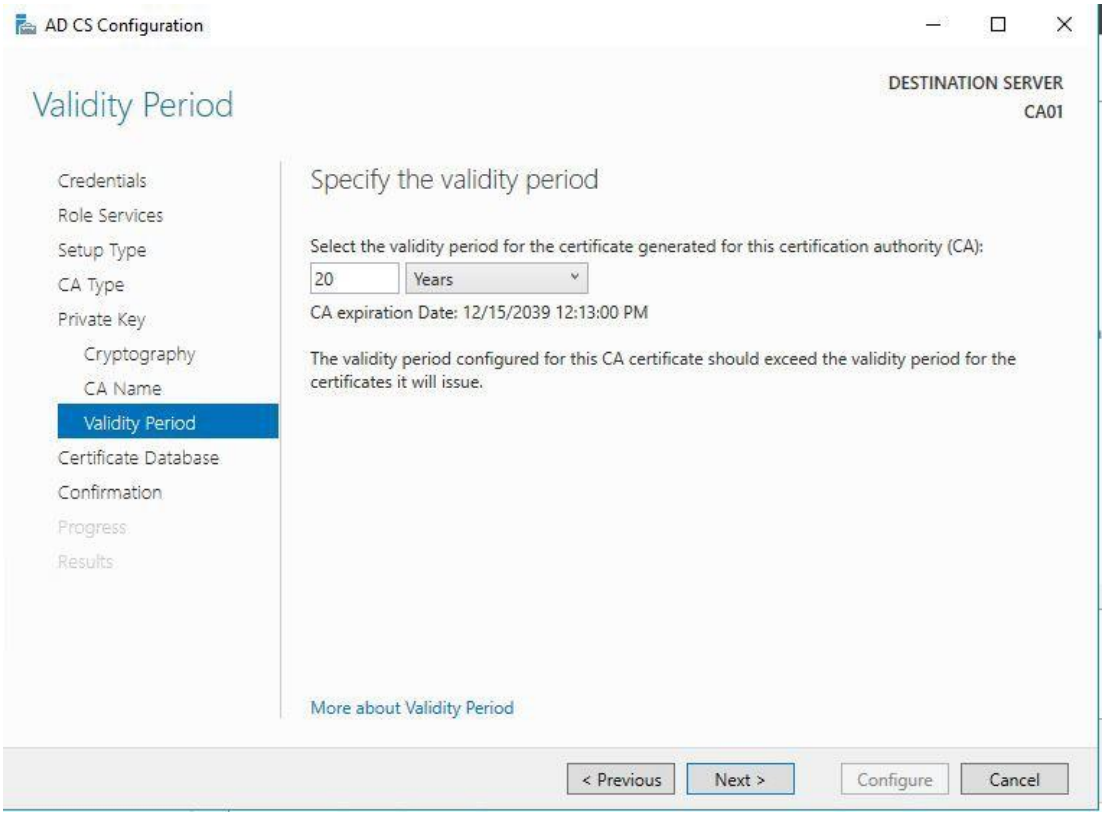
- **Important:** In a production environment, you would set the CSP, Hash Algorithm, and Key length to meet application compatibility requirements.

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

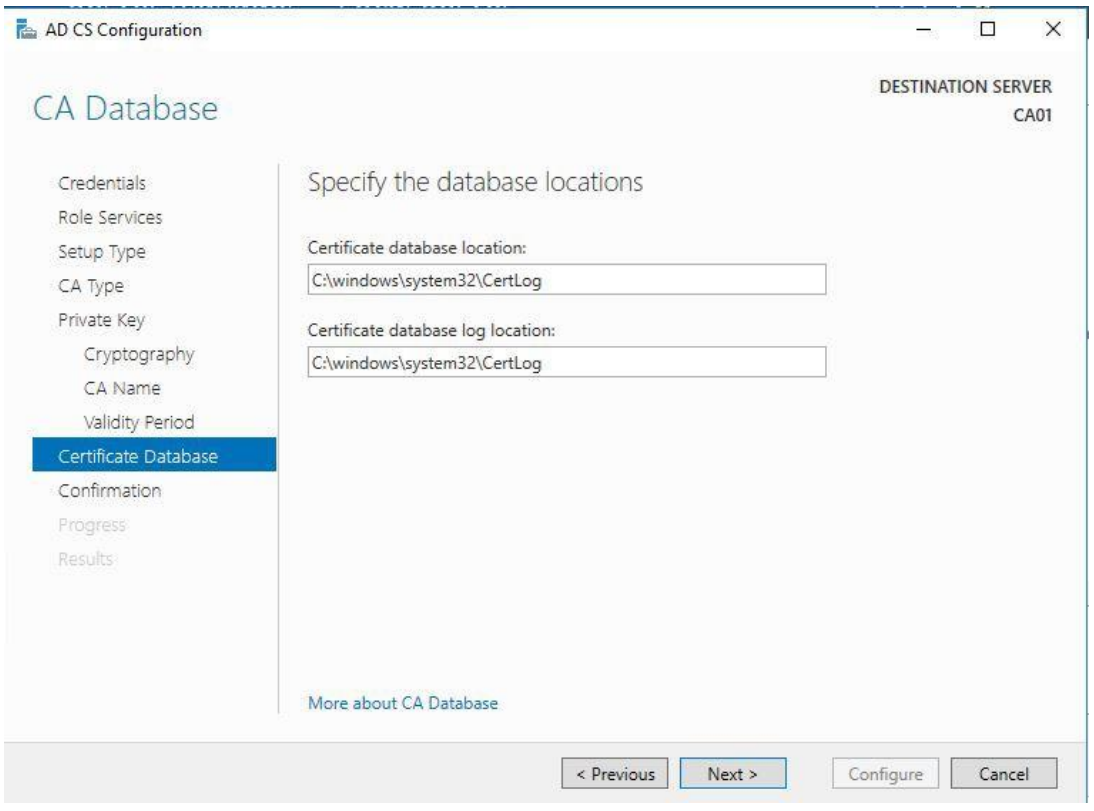
- Note: A Distinguished Name Suffix is optional for a root CA. This will be configured in a later step.



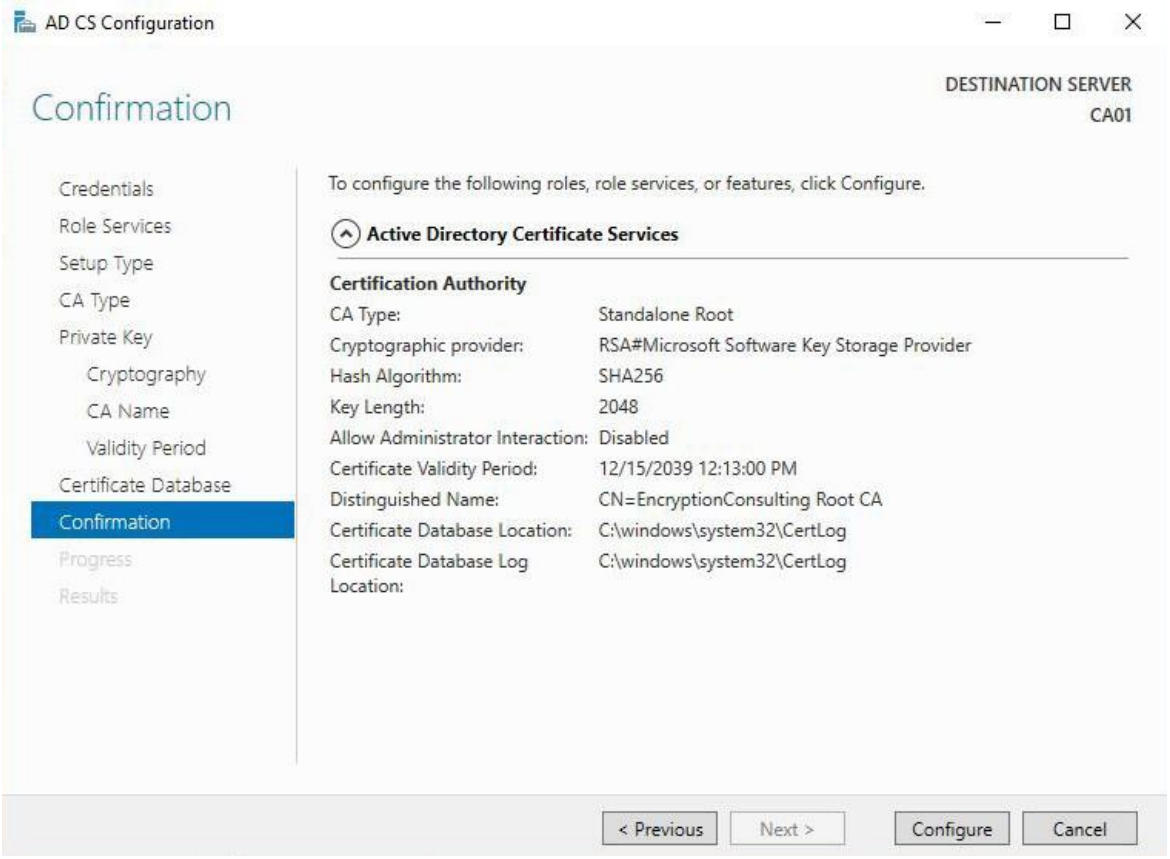
14. On **Set Validity Period** page, under **Select validity period for the certificate generated for this CA**, clear the existing entry, and then type **20**. Leave the selection box set to Years. Click **Next.**



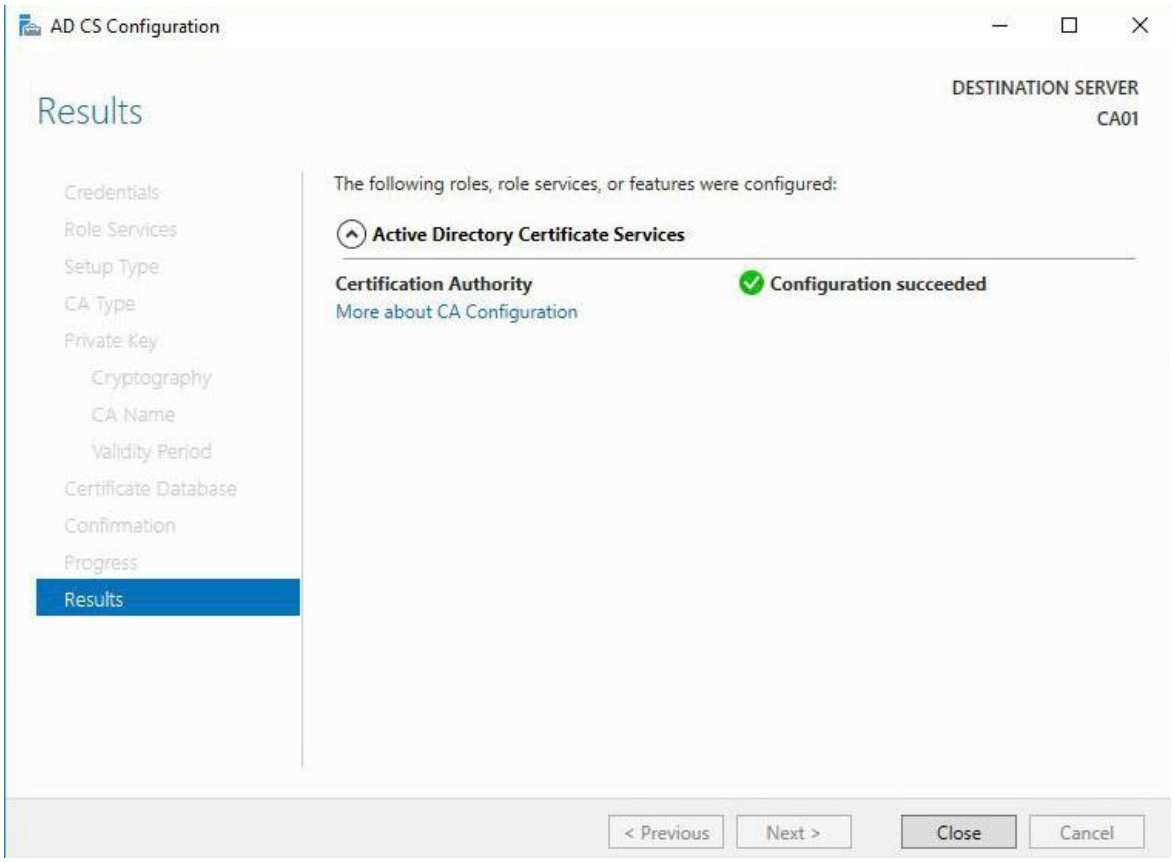
15. Keep the default settings on the **Configure Certificate Database** page, and then click **Next.**



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**.**



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 **Certificate 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 command 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 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 **EncryptionConsulting 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

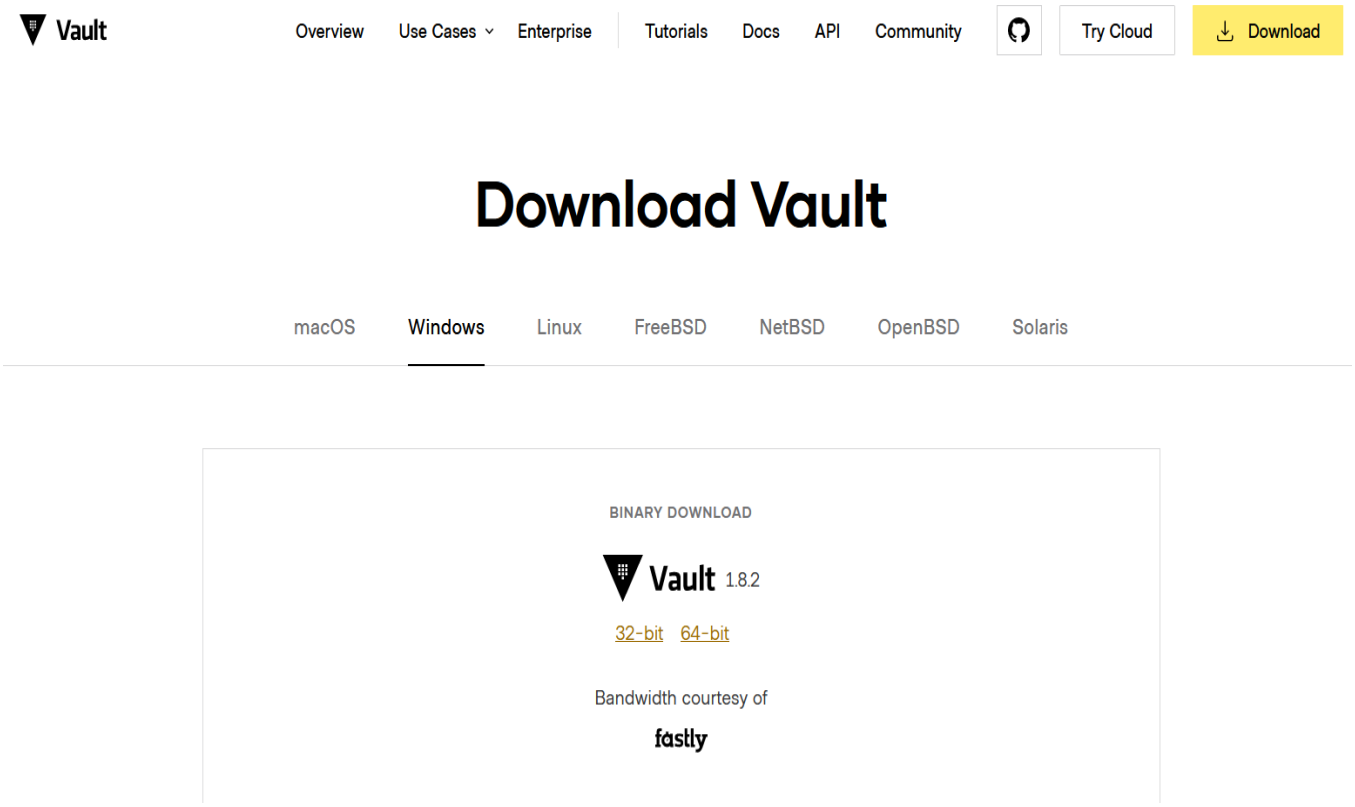
net start certsvc

certutil -crl

Activity 3: Install HashiCorp OSS on windows machine

Task1: Download and install the HashiCorp OSS on windows Machine

1. Download the HashiCorp OSS from HashiCorp portal to windows machine to be used as an Issuing CA.



2. Download the 32-bit/64-bit as per your setup.

3. Go to the installation directory and start the HashiCorp server with the following command on windows command prompt:

```
c:\>vault server -dev
==> Vault server configuration:

            Api Address: http://127.0.0.1:8200
                    Cgo: disabled
        Cluster Address: https://127.0.0.1:8201
             Go Version: go1.16.7
             Listener 1: tcp (addr: "127.0.0.1:8200", cluster address: "127.0.0.1:8201", max_request_duration: "1m30s",
max_request_size: "33554432", tls: "disabled")
              Log Level: info
                  Mlock: supported: false, enabled: false
          Recovery Mode: false
                Storage: inmem
                Version: Vault v1.8.2
            Version Sha: aca76f63357041a43b49f3e8c11d67358496959f

==> Vault server started! Log data will stream in below:
```

4. Stop the server with ctrl+c.

5. Set the environment variable:

```
c:\>set VAULT_ADDR=http://127.0.0.1:8200
```

Note: Kindly note that once you stop the HashiCorp instance, any configuration performed will be wiped out.

6. Start the server once again:

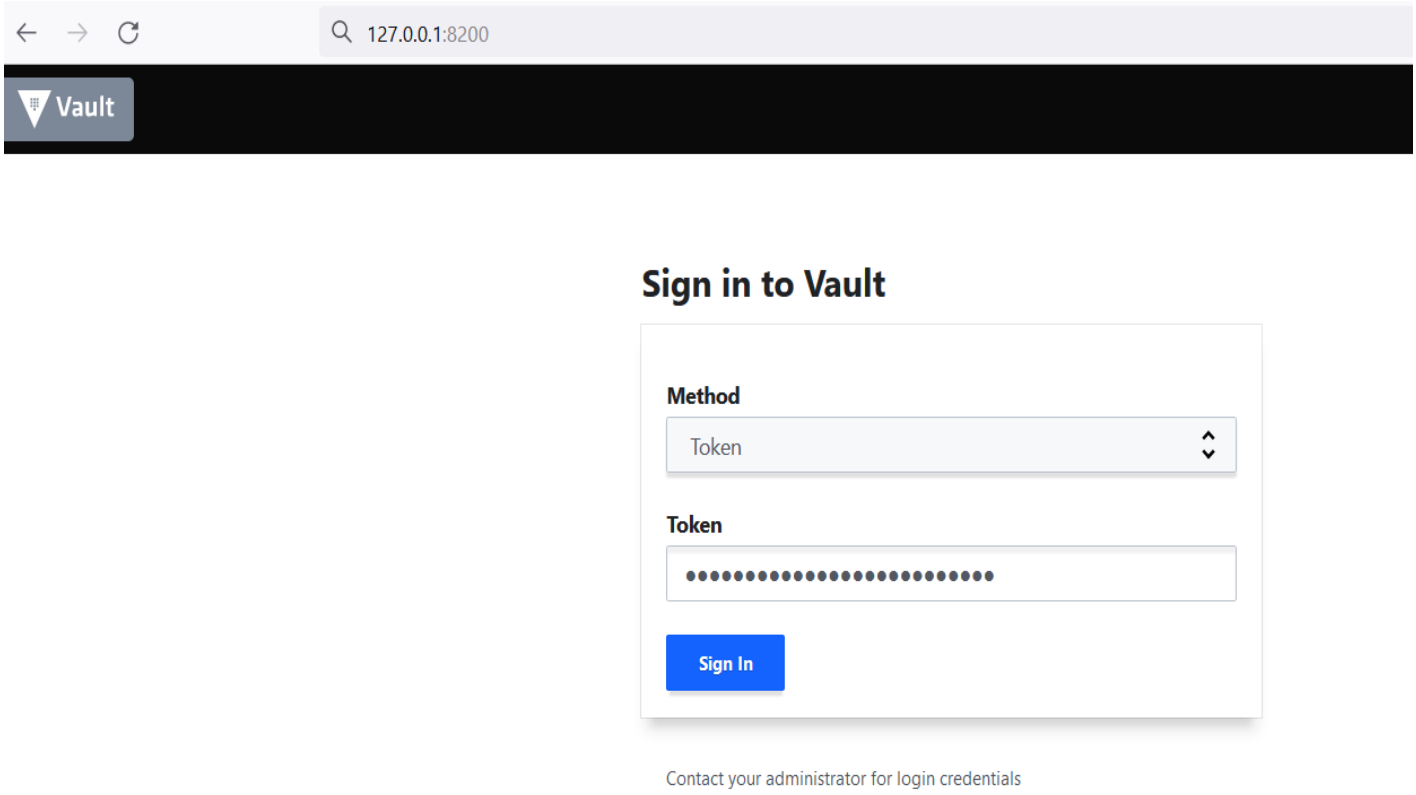
```
c:\>vault server -dev
==> Vault server configuration:

            Api Address: http://127.0.0.1:8200
                    Cgo: disabled
        Cluster Address: https://127.0.0.1:8201
             Go Version: go1.16.7
             Listener 1: tcp (addr: "127.0.0.1:8200", cluster address: "127.0.0.1:8201", max_request_duration: "1m30s",
max_request_size: "33554432", tls: "disabled")
              Log Level: info
                  Mlock: supported: false, enabled: false
          Recovery Mode: false
                Storage: inmem
                Version: Vault v1.8.2
            Version Sha: aca76f63357041a43b49f3e8c11d67358496959f

==> Vault server started! Log data will stream in below:
```

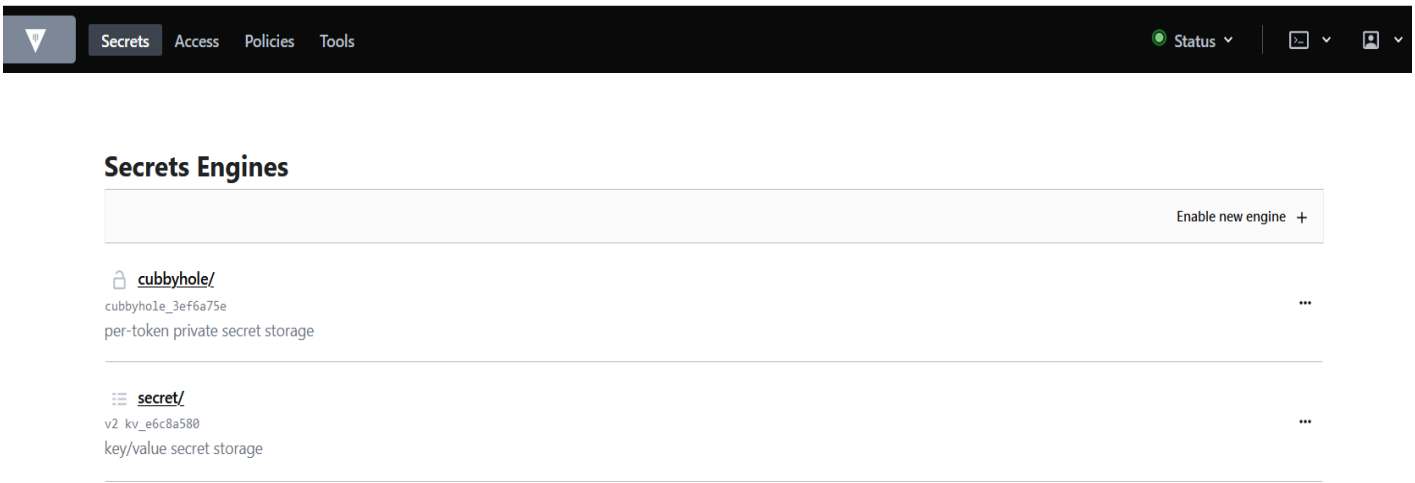
7. Open the web browser and paste the following:

http://127.0.0.1:8200/ui



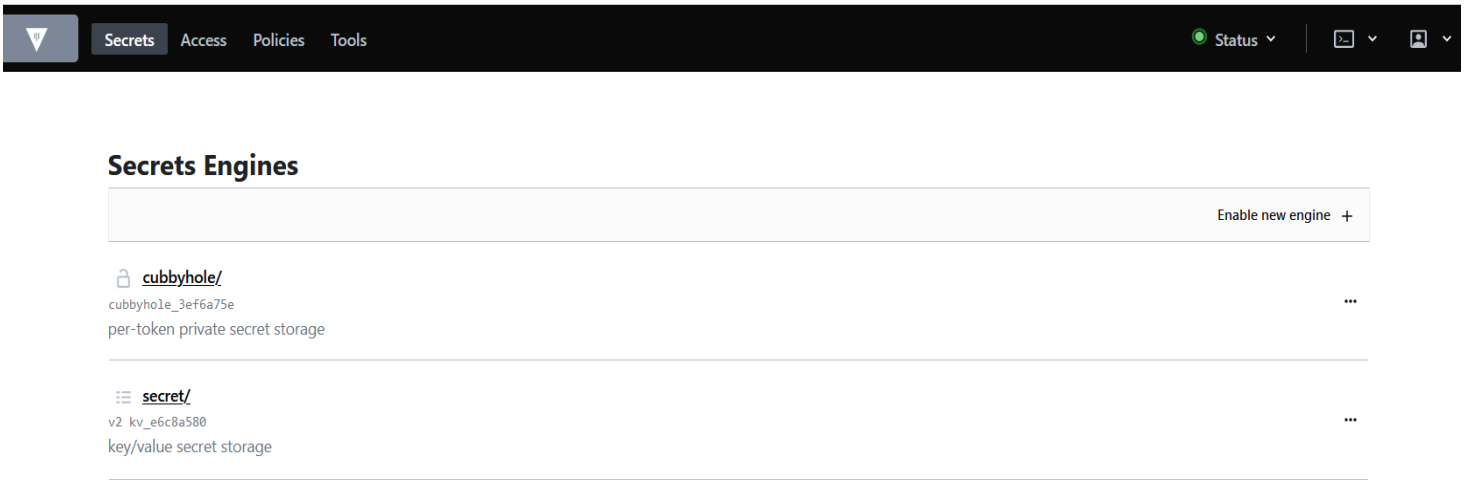
8. Select the Method as Token and copy the Root token from the command prompt and paste it in the Token field and click Sign In.

9. The login should be successful and following screen is observed:

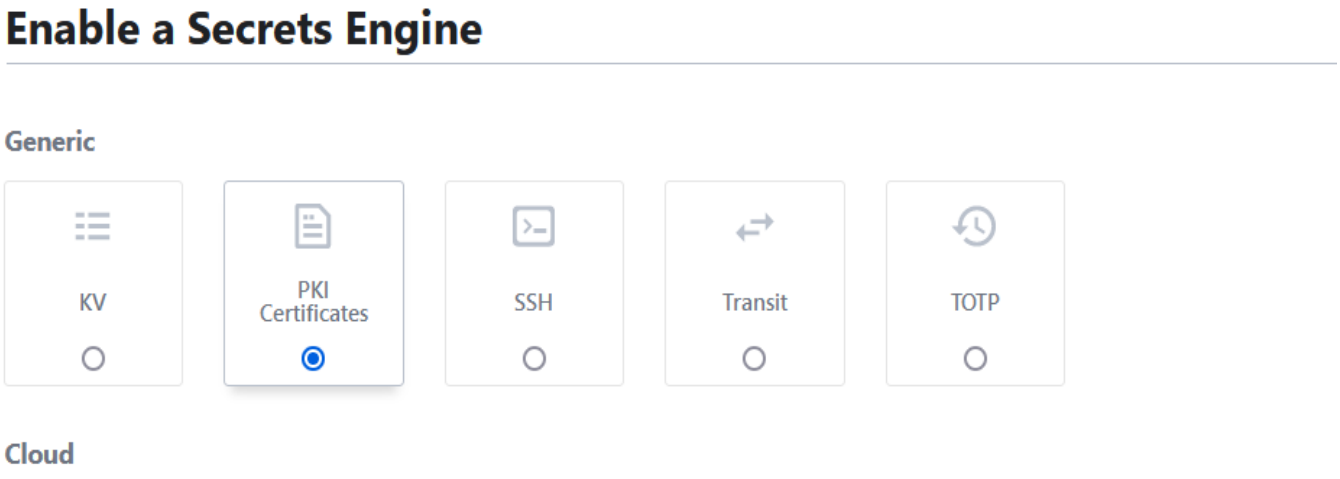


Task 2: Create the Issuing CA in HashiCorp OSS installation

1. Sign into your HashiCorp server with the Token and Root token credentials as mentioned in previous step.

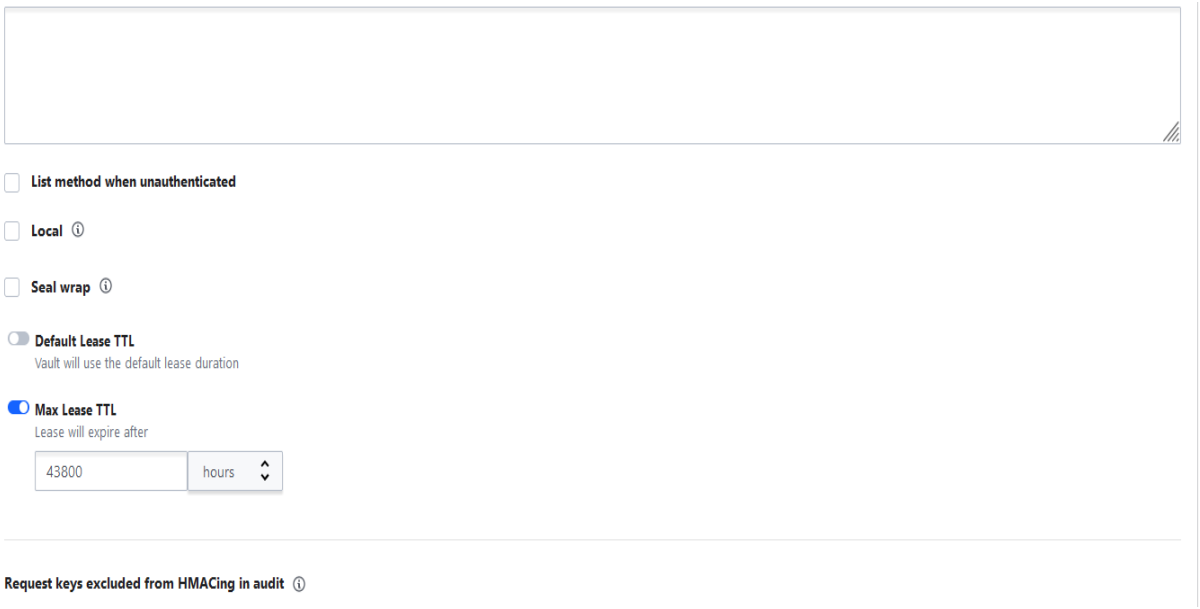


2. Click on “Enable new engine” and select PKI certificates and click next.



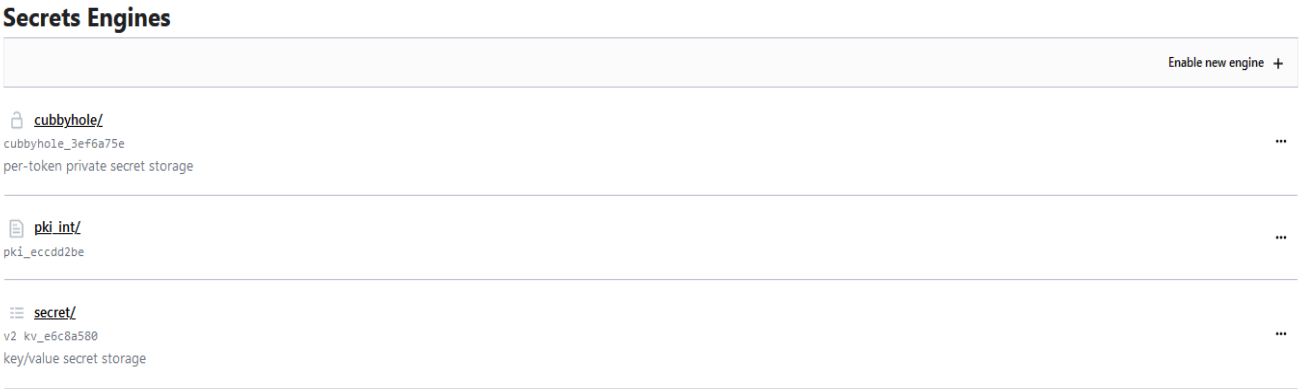
3. Enter pki_int in the Path field.

4. Click More options to expand and set the Maximum lease TTL to 43800 hours.



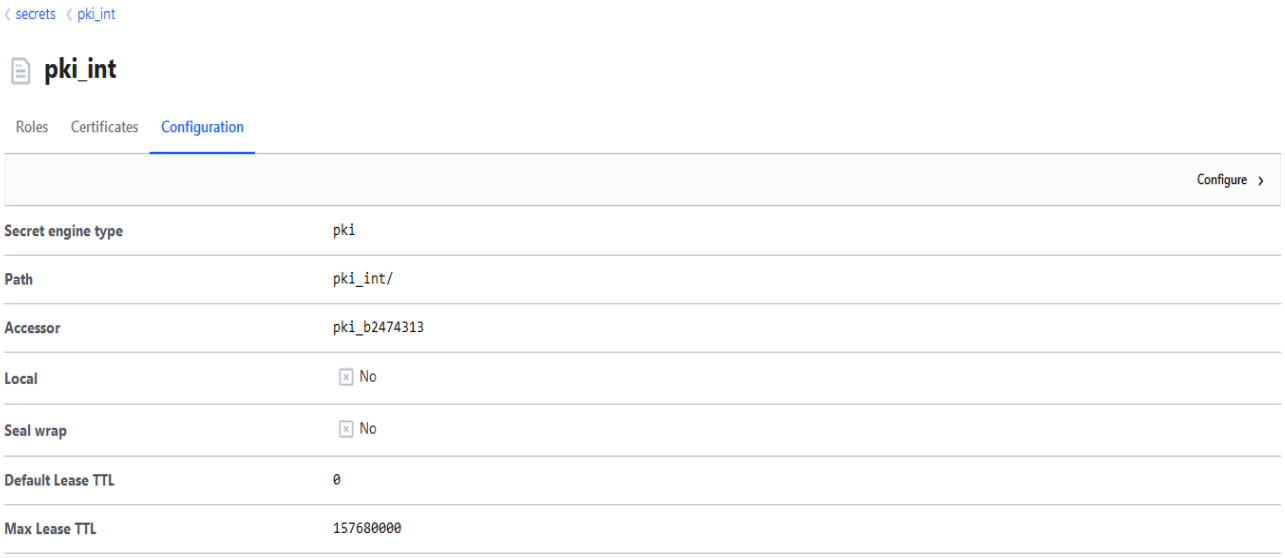
5. Click Enable Engine.

6. A new PKI engine is created in HashiCorp OSS:



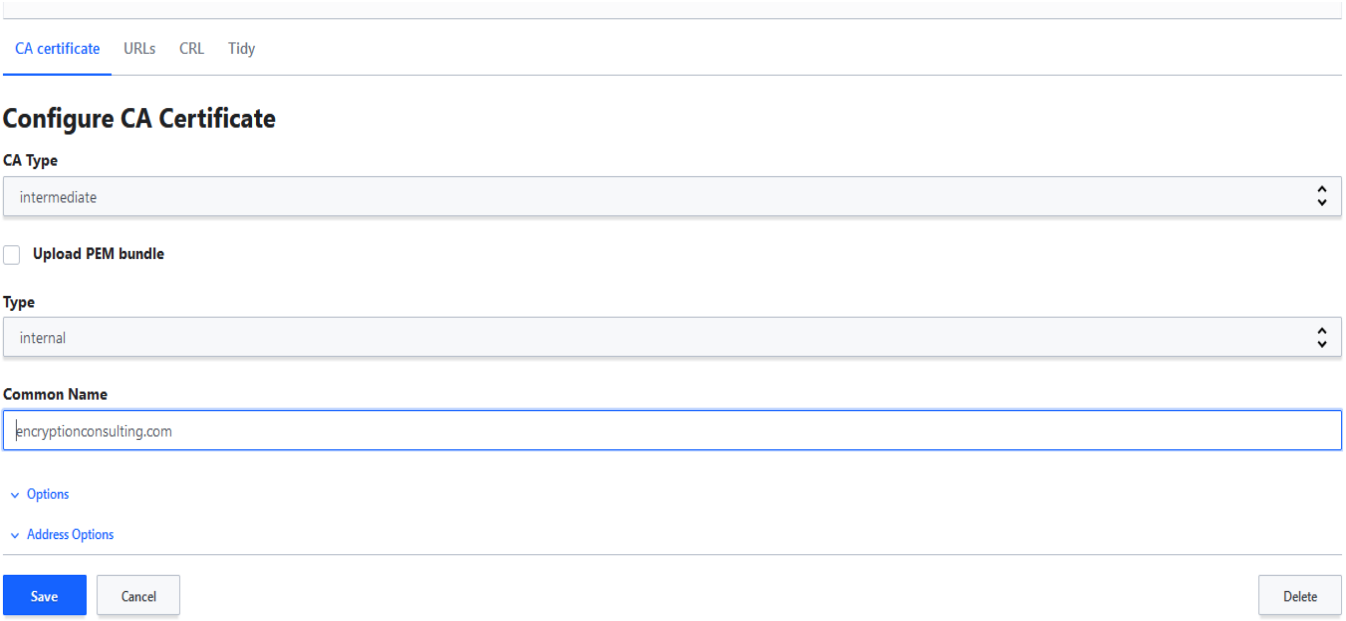
Task 3: Issue the CSR from HashiCorp Issuing (intermediate) CA for EncryptionConsulting domain

1. Select the **Configuration** tab and then **Configure**:

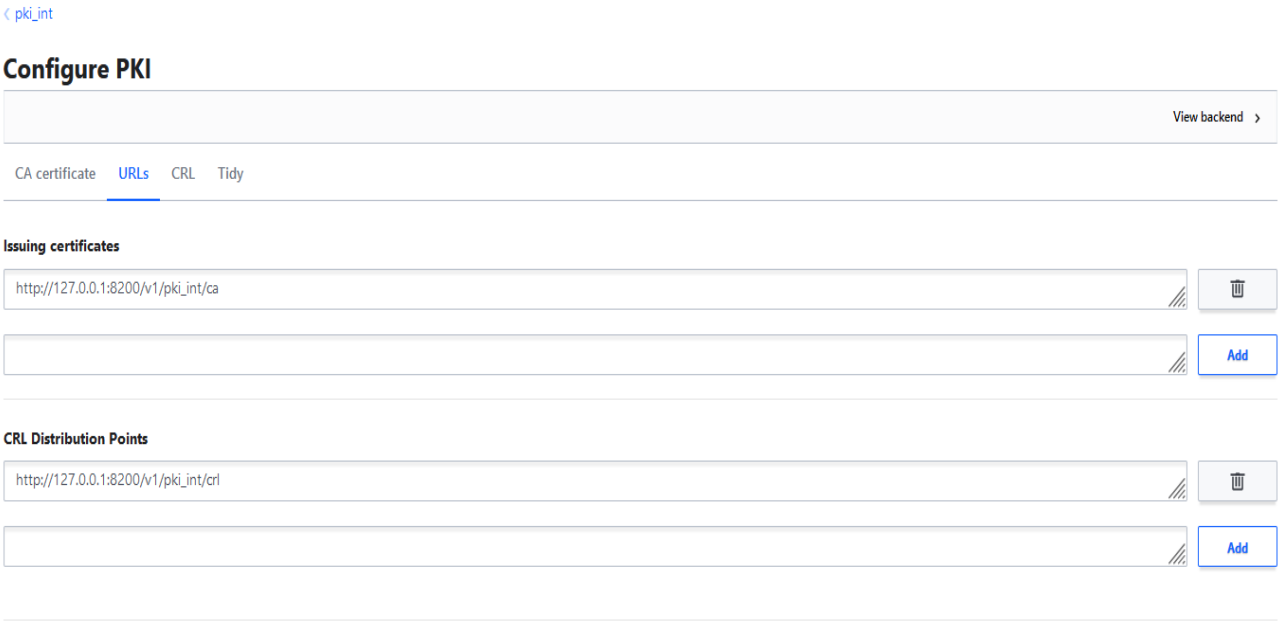


2. Click **Configure CA** and Select **intermediate** from CA Type drop-down list.

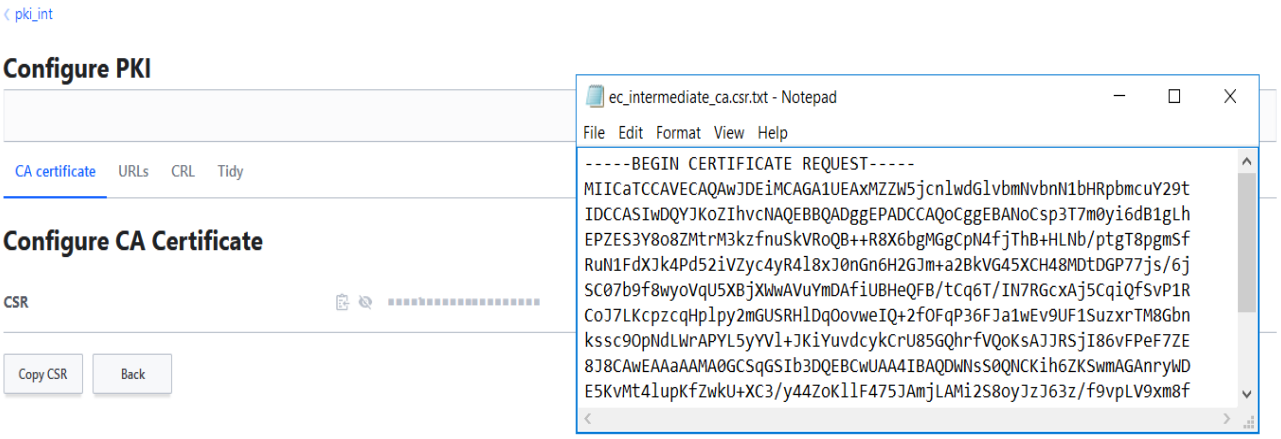
3. Enter **encryptionconsulting.com** Intermediate Authority in the Common Name field, Internal in Type field and Click **Save**.



4. Enter the following urls under the URLs tab and Click Save.



5. Click **Copy CSR** and save it in a file, ec_intermediate_ca.csr



Task 4: Sign the CSR through OpenSSL utility

1. Ensure that you are logged on to a windows machine as an Administrator.
2. Install the OpenSSL package on a windows machine.
3. Create a folder named “HashiCorp_Intermediate_Cert” on the windows machine.
4. Copy following files in the above-mentioned folder:
    - ec_intermediate_ca.csr
    - root_ca.crt (Extract the root CA (offline) certificate from Microsoft root CA)
    - root_ca.key (Extract the root CA (offline) private key from Microsoft root CA)
    - extfile.cnf
5. Open the extfile.cnf in text editor and paste following text and save the file.

    basicConstraints=CA:TRUE
6. Run the following command on the OpenSSL prompt:

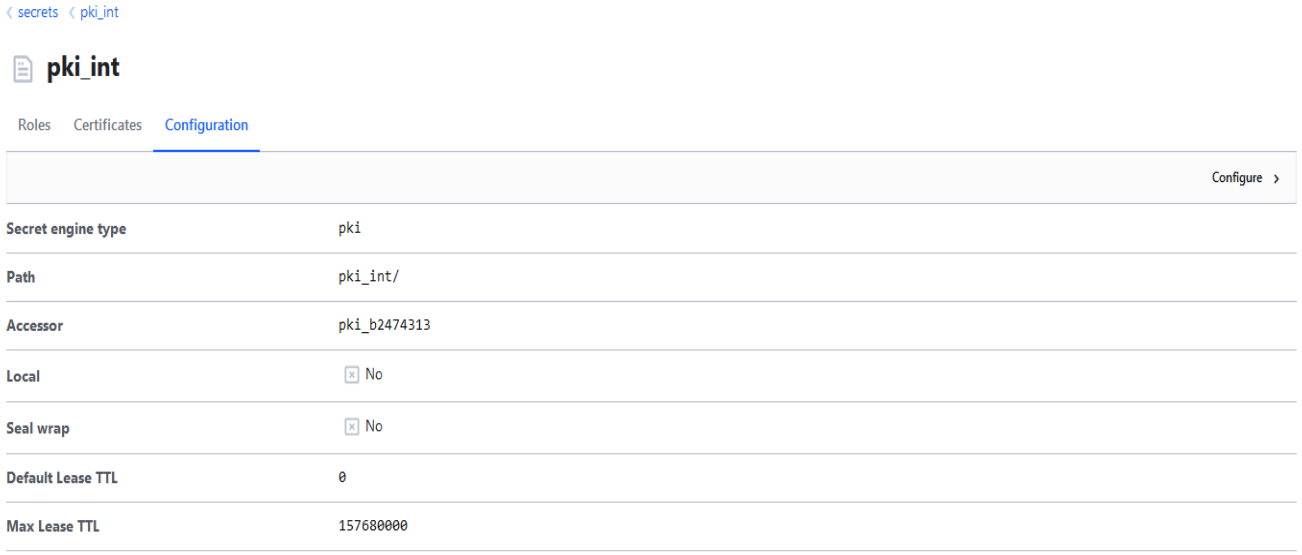
```
c:\hashicorp>openssl x509 -req -in ec_intermediate_ca.csr -CA root.crt -CAkey root.key -extfile extfile.cnf -CAcreateserial -out intermediate-cert.pem

c:\hashicorp>
```

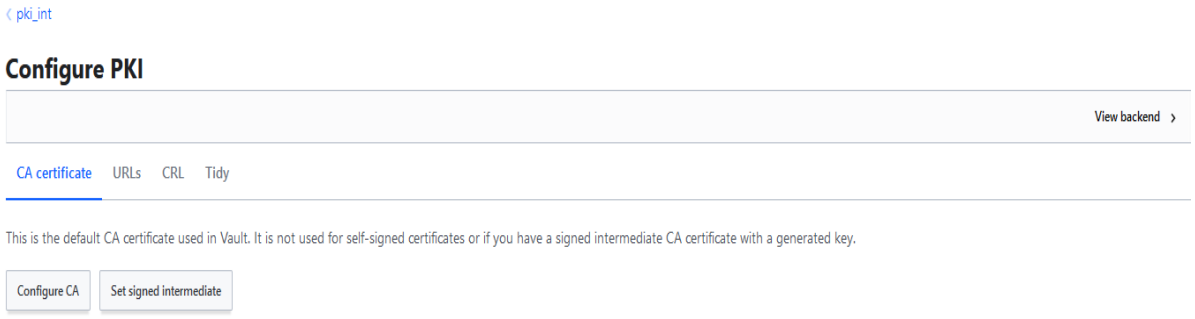
7. The Encryption Consulting Issuing CA certificate (Intermediate-cert.pem) file will be generated at the same location.

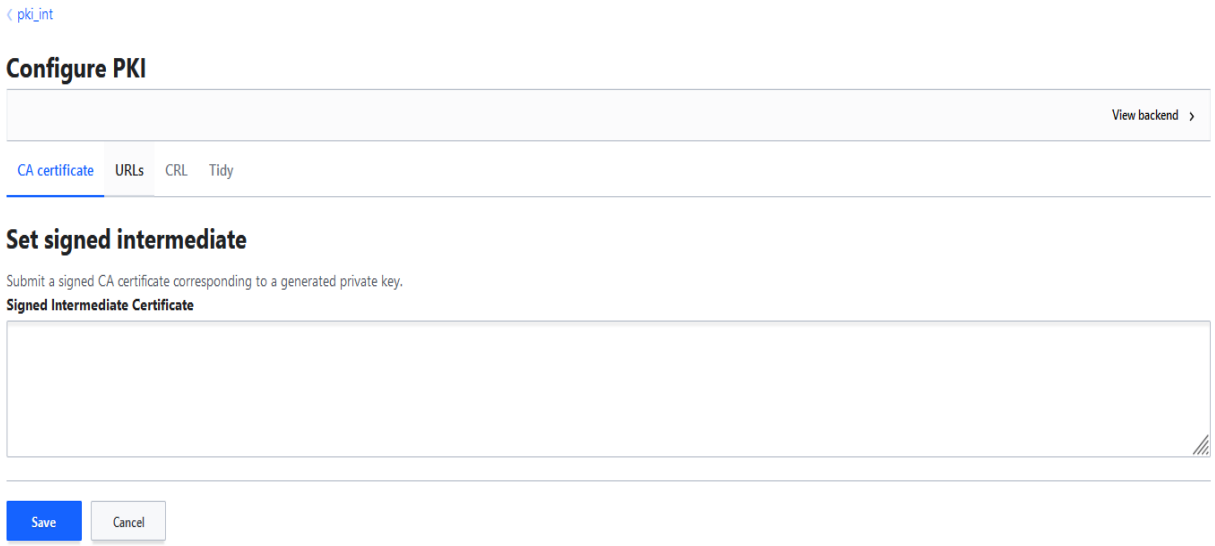
Task 5: Install the Encryption Consulting Issuing CA Certificate in HashiCorp OSS

1. Go to HashiCorp Issuing (intermediate) CA and login with administrator credentials.
2. Copy the Encryption Consulting Issuing CA certificate to the HashiCorp windows machine.
3. Go to HashiCorp WenUI and select **pki_int** from the **Secrets** tab to return to the HashiCorp Issuing (intermediate) CA:

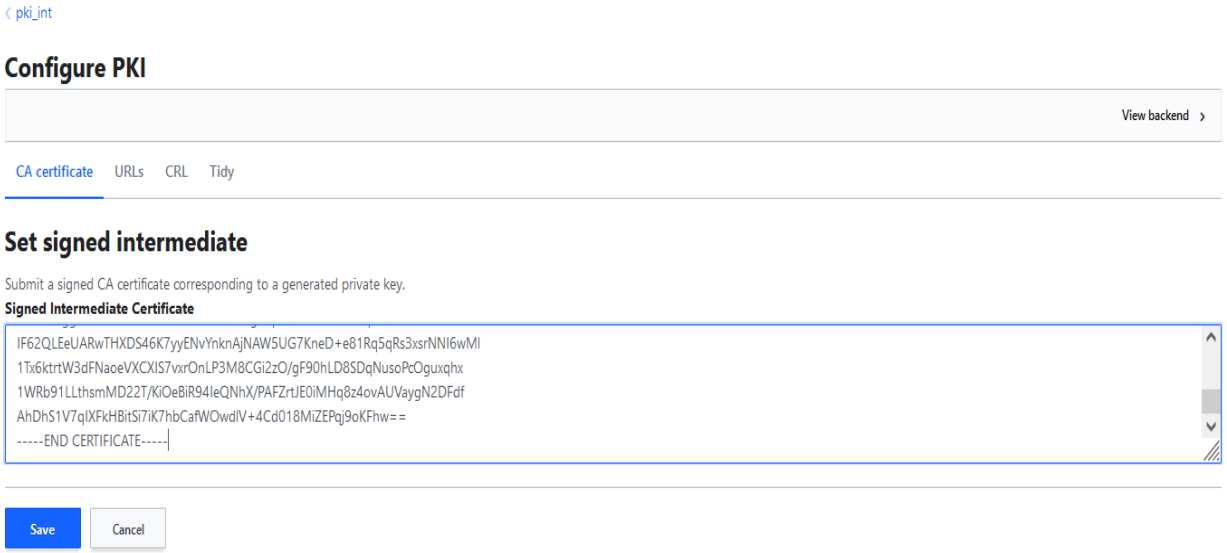


4. Select the **Configuration** tab and then **Configure** and Click **Set signed intermediate**.

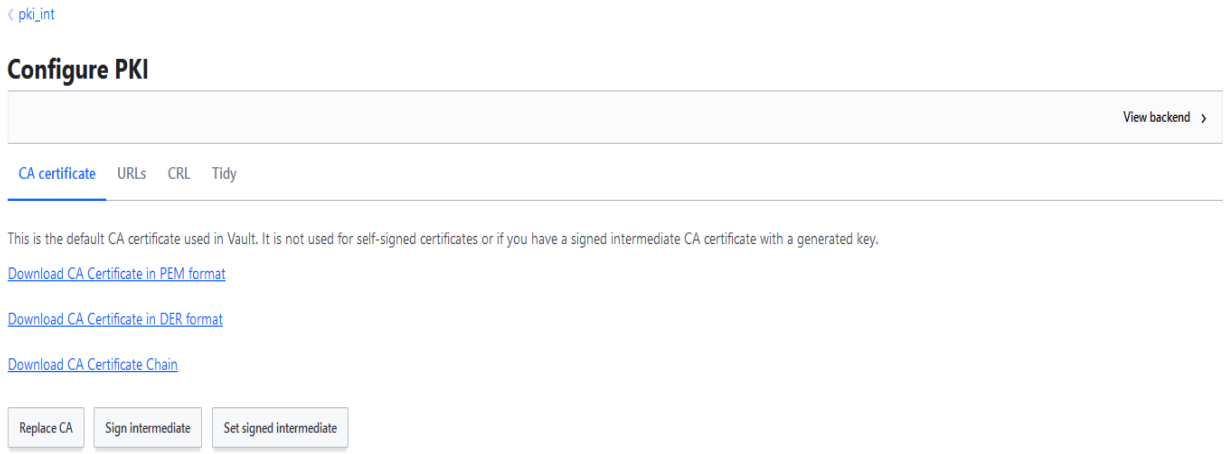




5. Open the Issuing CA certificate in text editor and paste in the above text box and click Save:

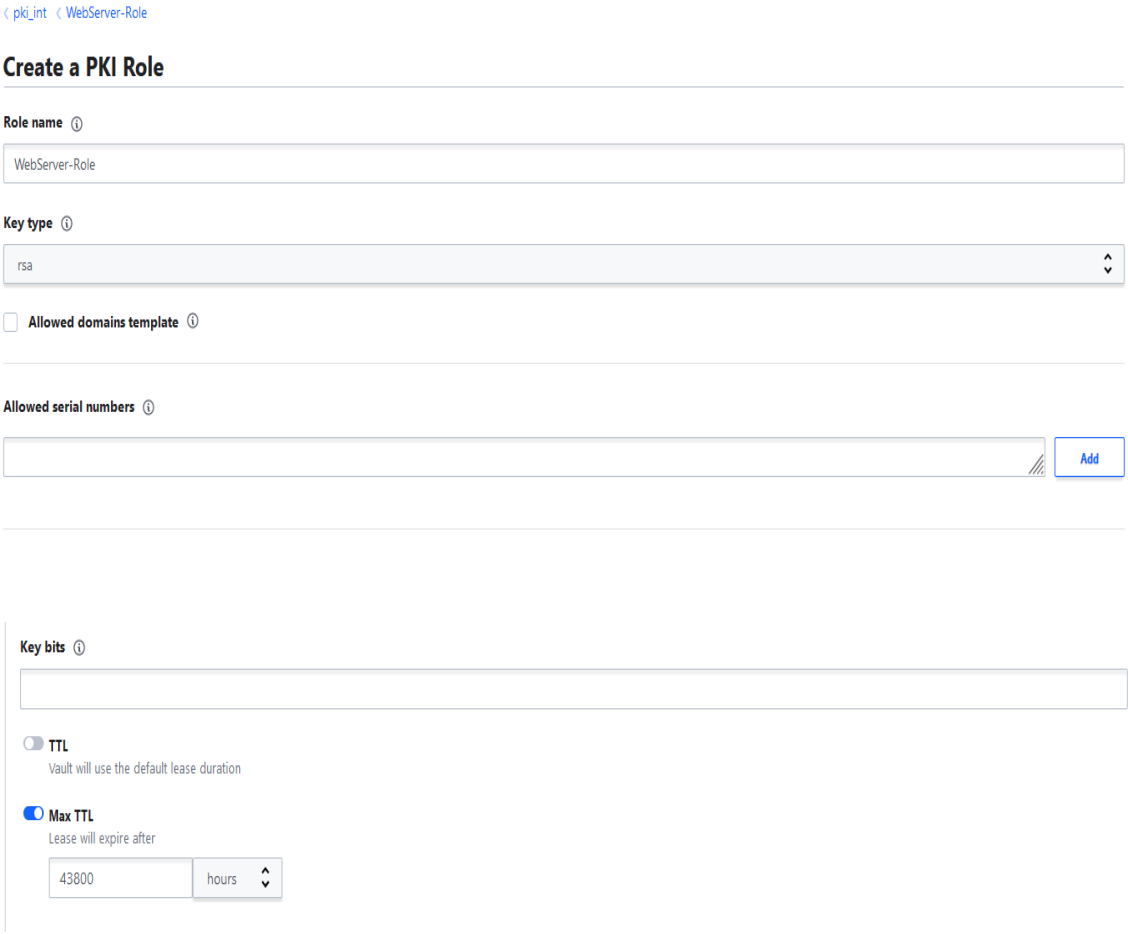


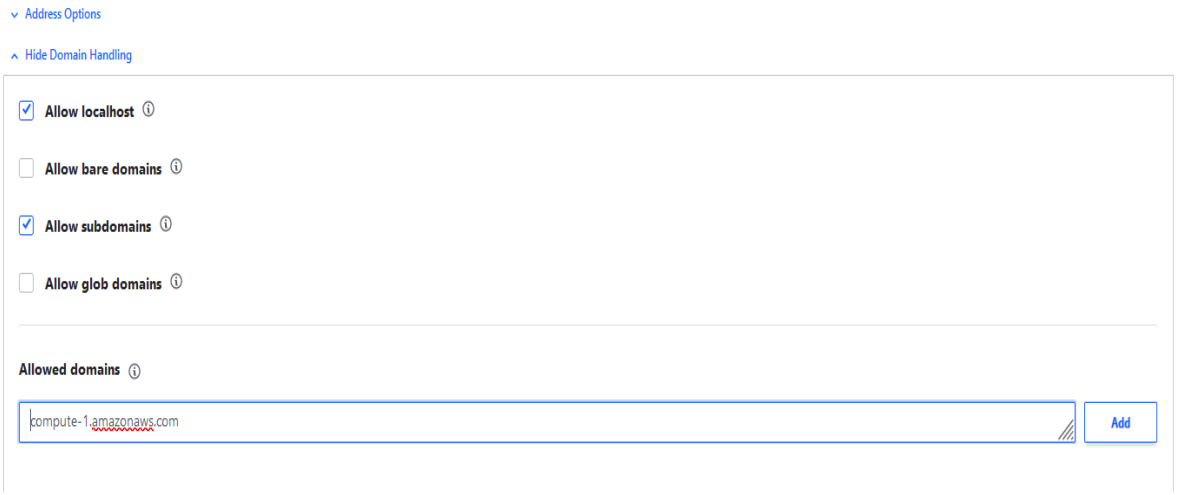
6. The Issuing CA Certificate will be uploaded successfully.



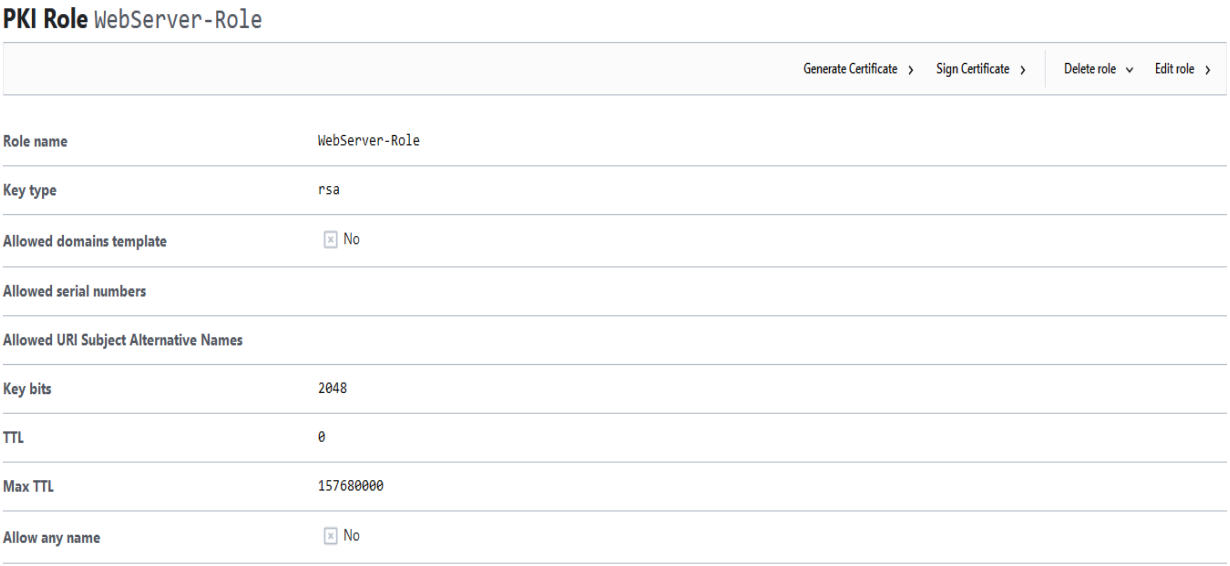
Task 6: Create a Role under HashiCorp intermediate CA

1. Go to HashiCorp Issuing (intermediate) CA and login with administrator credentials
2. Click pki_int and then select Create role and Enter WebServer-Role in the Role name field:





3. Role created successfully

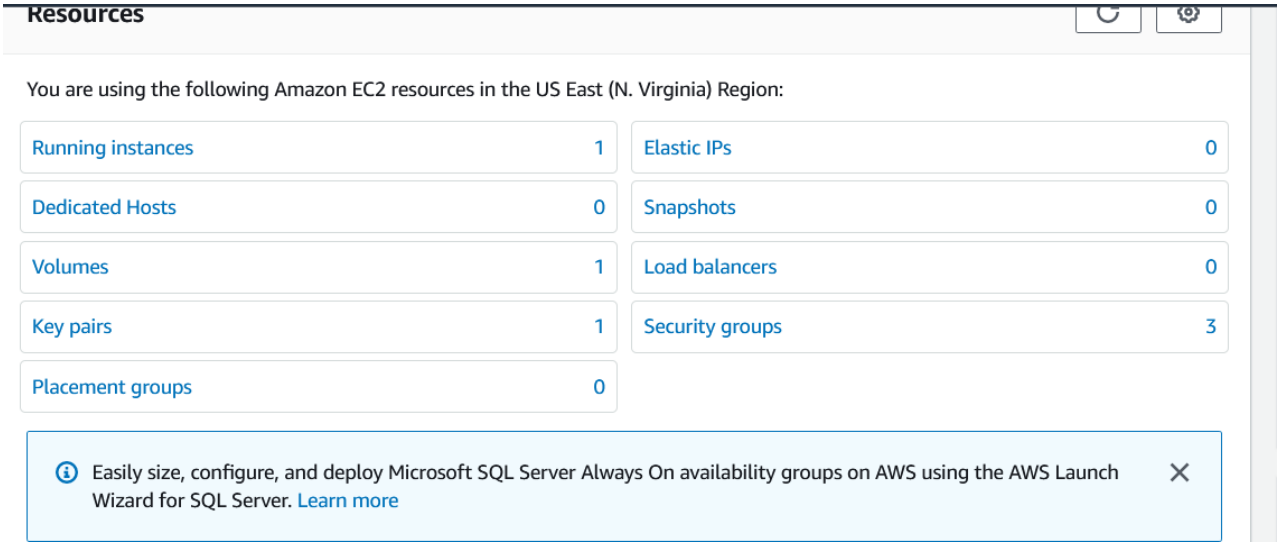


Activity 4: Create a Key-Pair

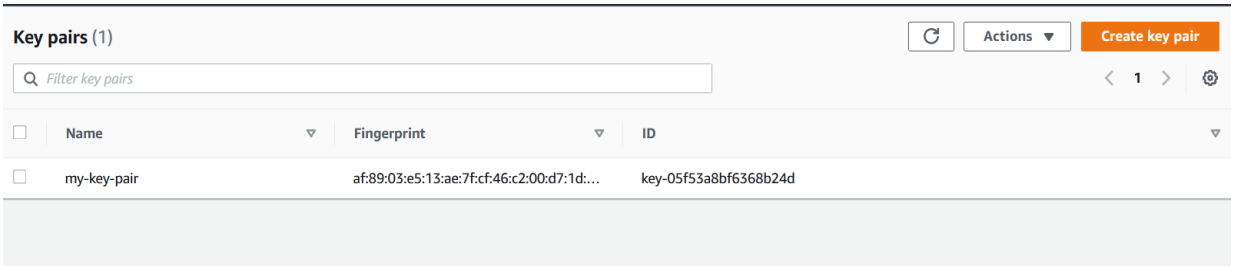
Task 1: Create a Public-Private Key-pair using an AWS EC2 Console

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

2. In the navigation pane, choose Key Pairs.

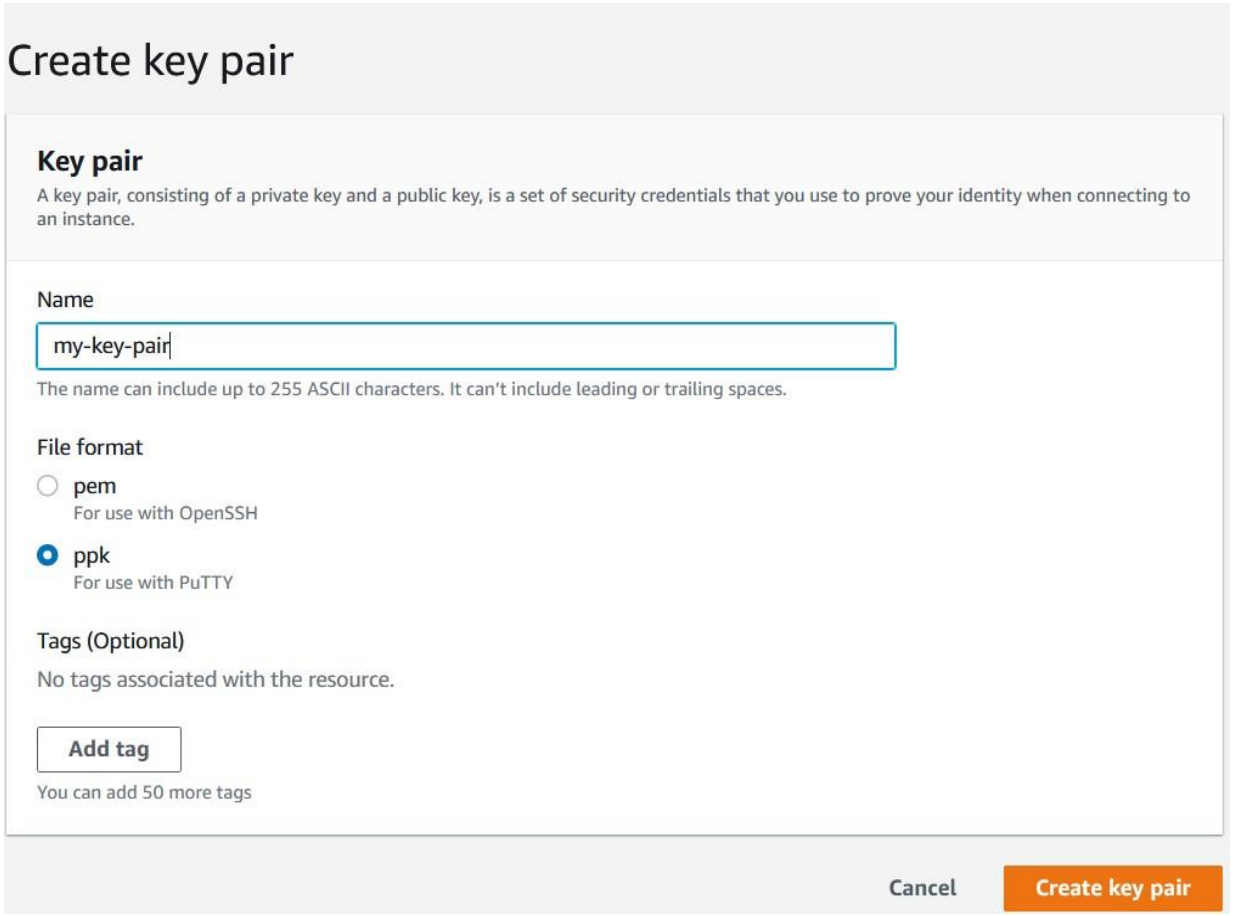


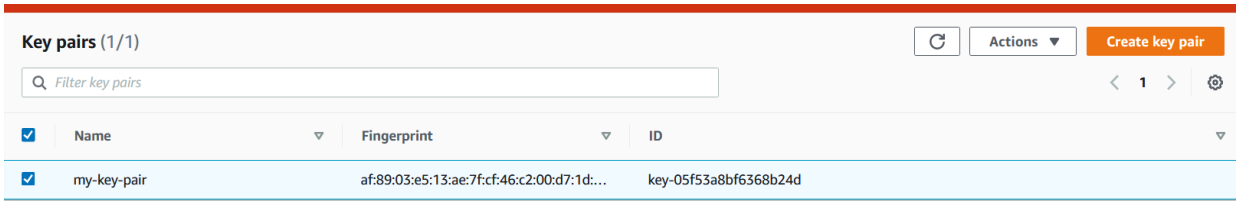
3. Choose Create key pair.



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.





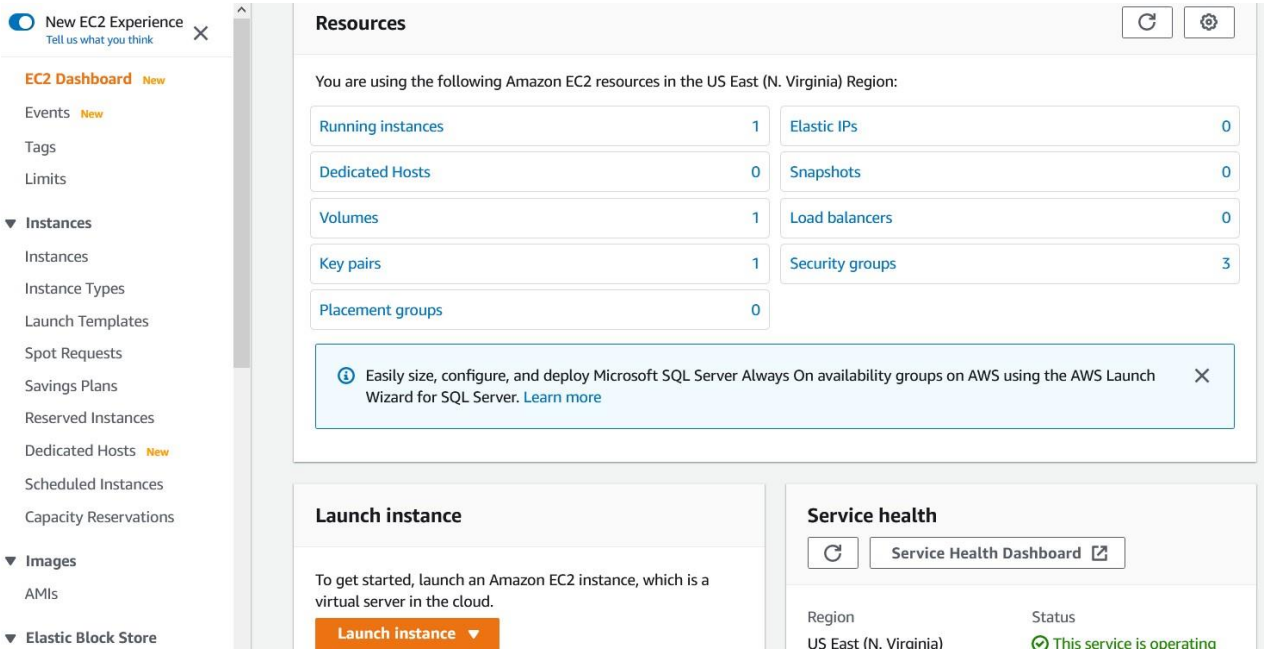
6. The private key file is automatically downloaded by your browser. Please save this file in a secure location as you will not get this file again.

Note: Key-pair creation will be specific to the user's environment and above steps are for illustration purposes, hence store the ssh-keys at a secure place for further usage as it won't be available for download if not saved.

Activity 5: Setup an EC2 instance

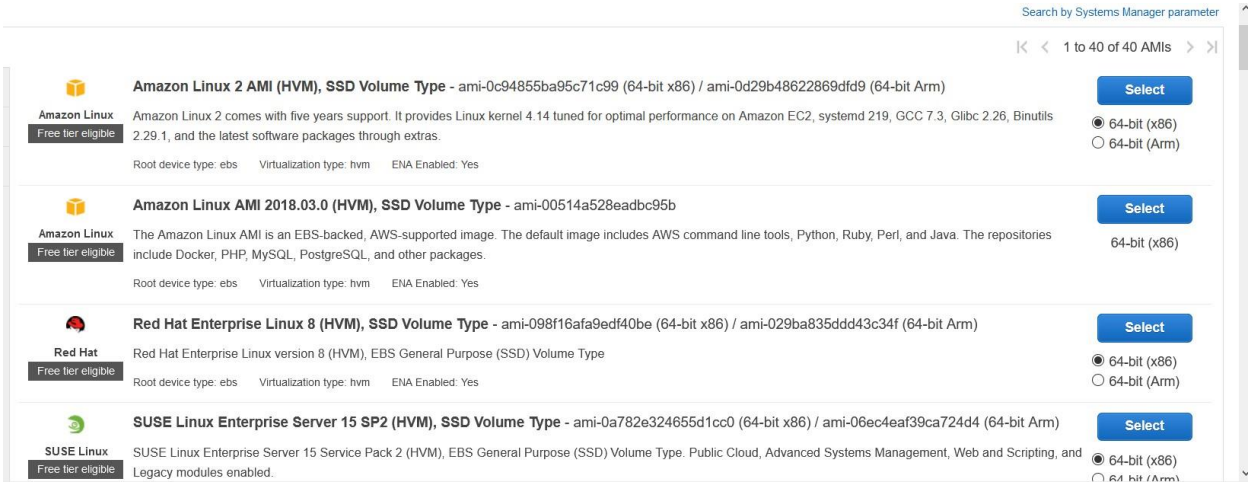
Task 1: Create and Setup an EC2 Instance to install the Apache Web Server on it

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

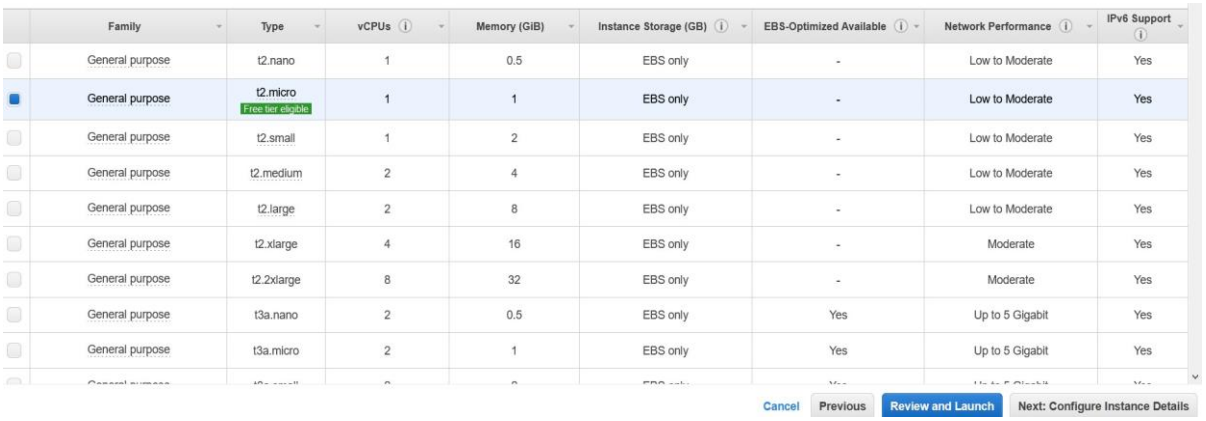


2. Choose Launch Instance.

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))



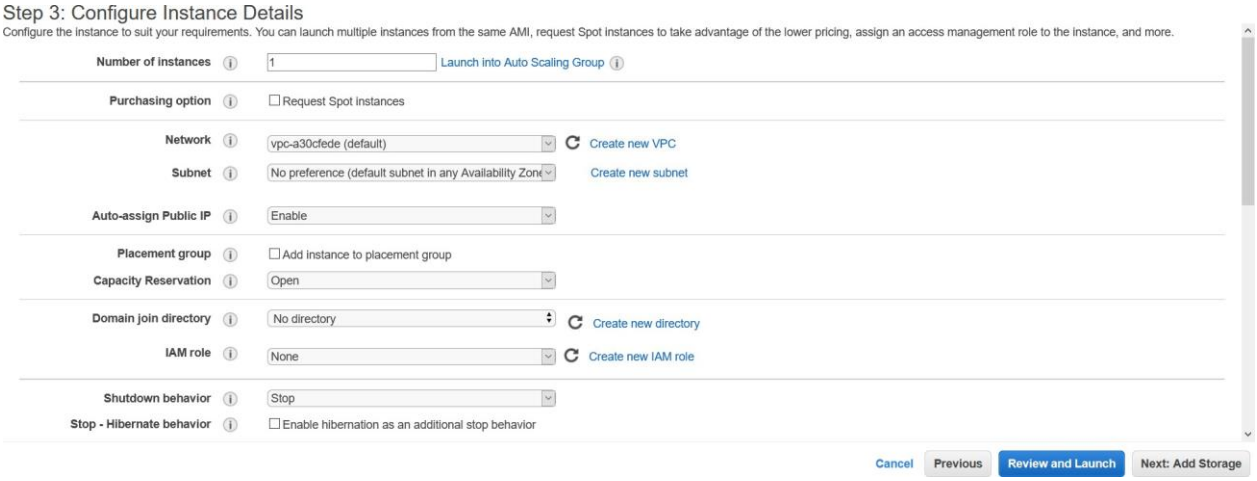
4. Choose an Instance Type “General Purpose: t2.micro”, click Next: Configure Instance Details



	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



Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances: 1 — Launch into Auto Scaling Group

Purchasing option: ☐ Request Spot instances

Network: vpc-a30cfede (default) — Create new VPC

Subnet: No preference (default subnet in any Availability Zone) — Create new subnet

Auto-assign Public IP: Enable

Placement group: ☐ Add instance to placement group

Capacity Reservation: Open

Domain join directory: No directory — Create new directory

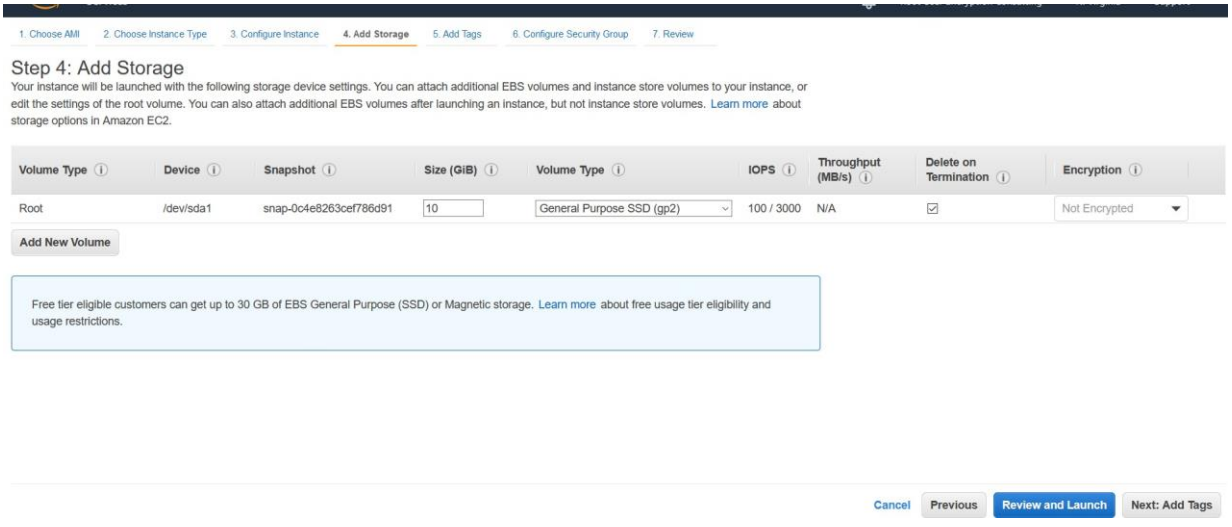
IAM role: None — Create new IAM role

Shutdown behavior: Stop

Stop - Hibernate behavior: ☐ Enable hibernation as an additional stop behavior

Cancel | Previous | Review and Launch | Next: Add Storage

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



1. Choose AMI | 2. Choose Instance Type | 3. Configure Instance | 4. Add Storage | 5. Add Tags | 6. Configure Security Group | 7. Review

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. Learn more about storage options in Amazon EC2.

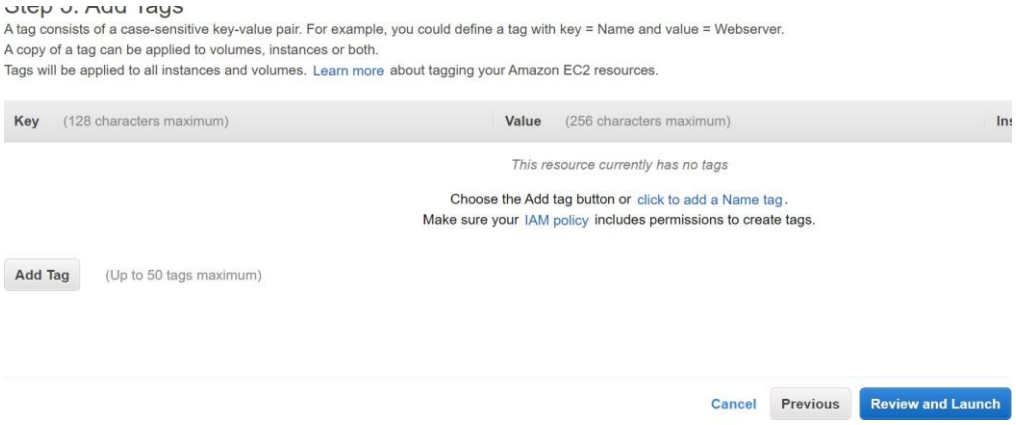
Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encryption
Root	/dev/sda1	snap-0c4e8263cef786d91	10	General Purpose SSD (gp2)	100 / 3000	N/A	☑	Not Encrypted

Add New Volume

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. Learn more about free usage tier eligibility and usage restrictions.

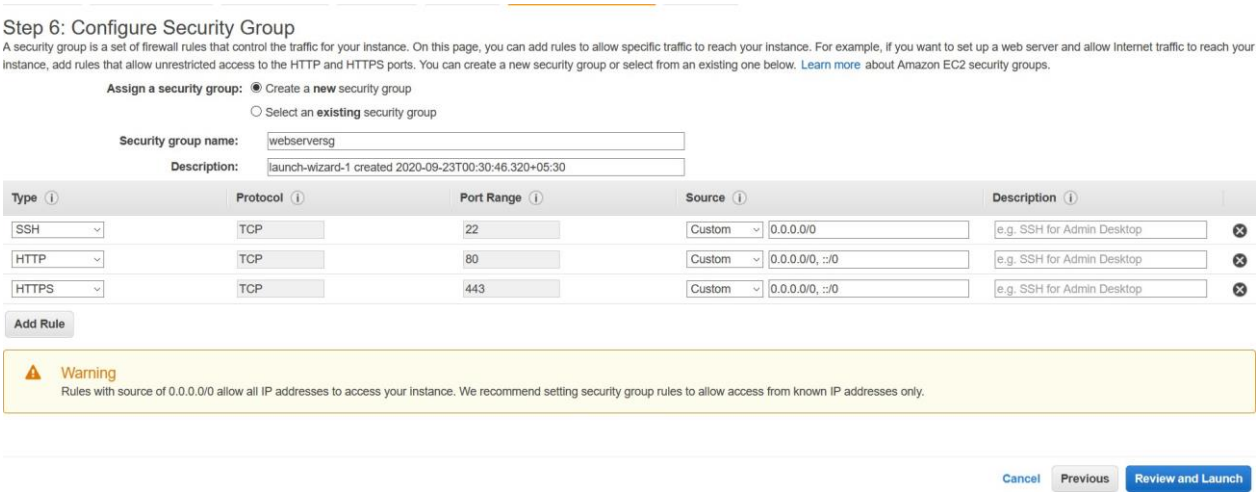
Cancel | Previous | Review and Launch | Next: Add Tags

7. Choose Next: Add Tags (leave default)

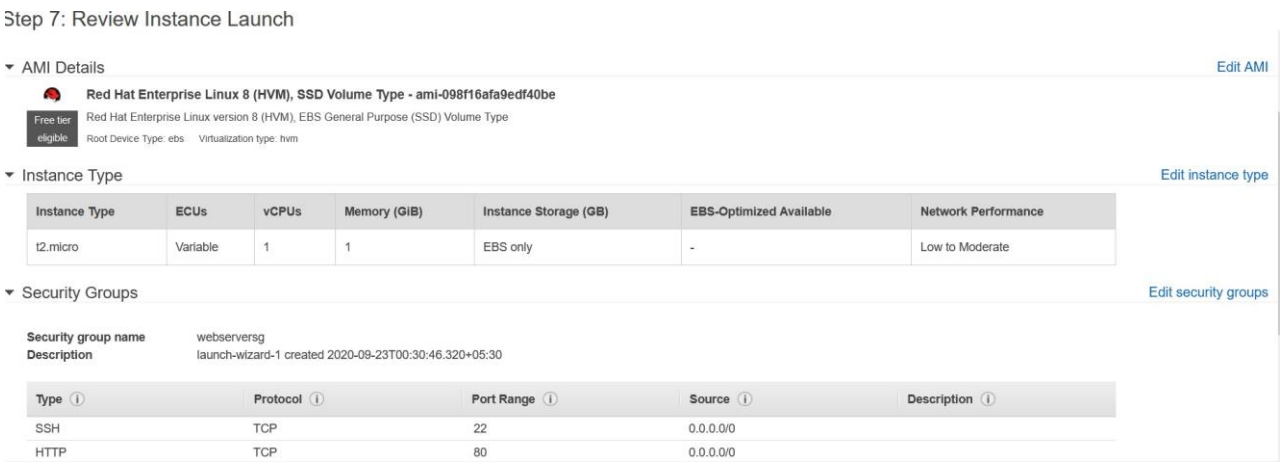


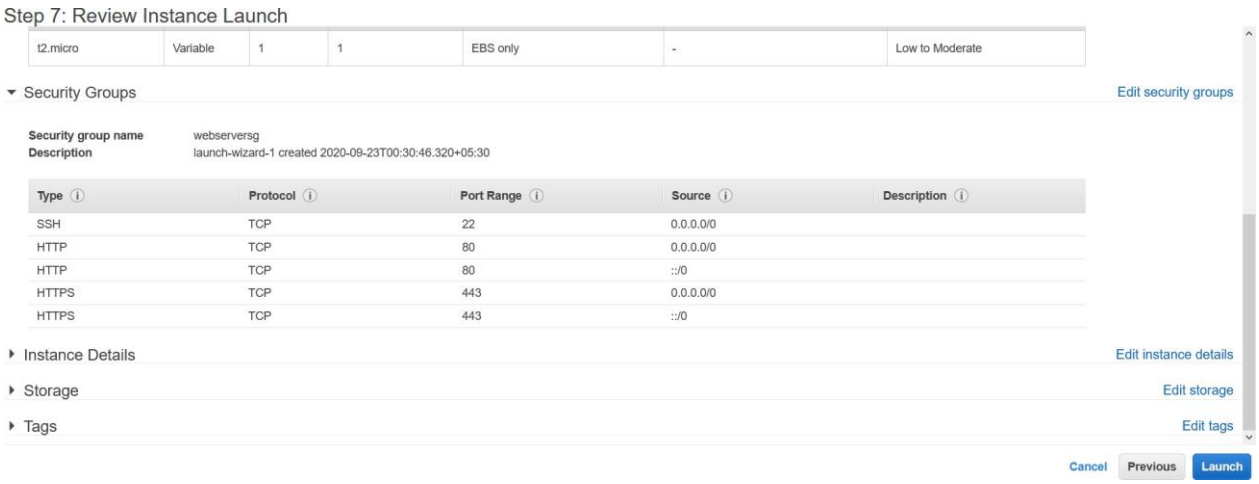
8. Choose Next: Configure Security Group. Add following inbound rules to the Security Group:

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



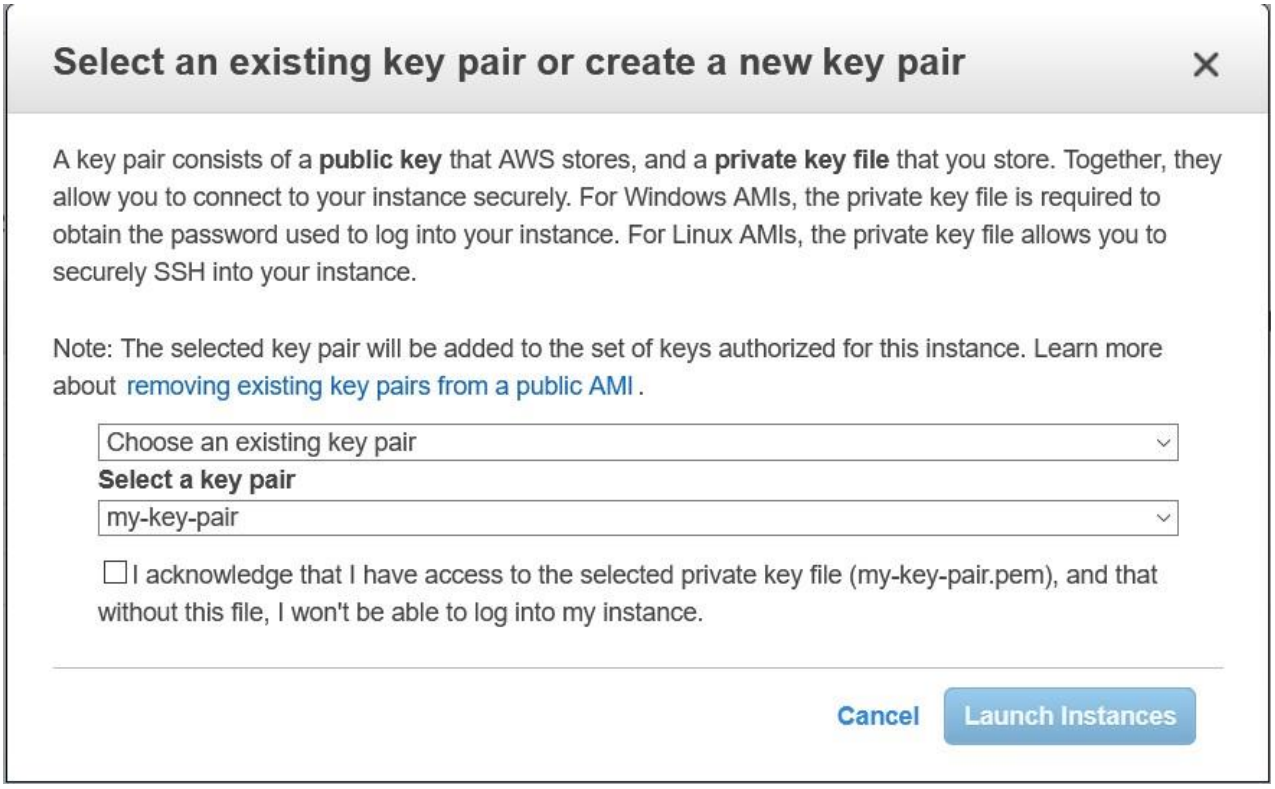
9. Choose Review and Launch.



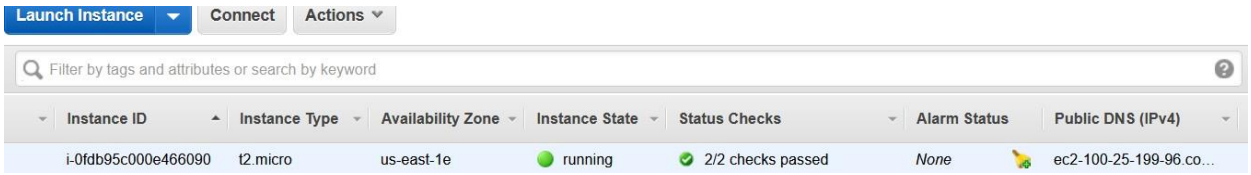


10. Choose Launch.

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



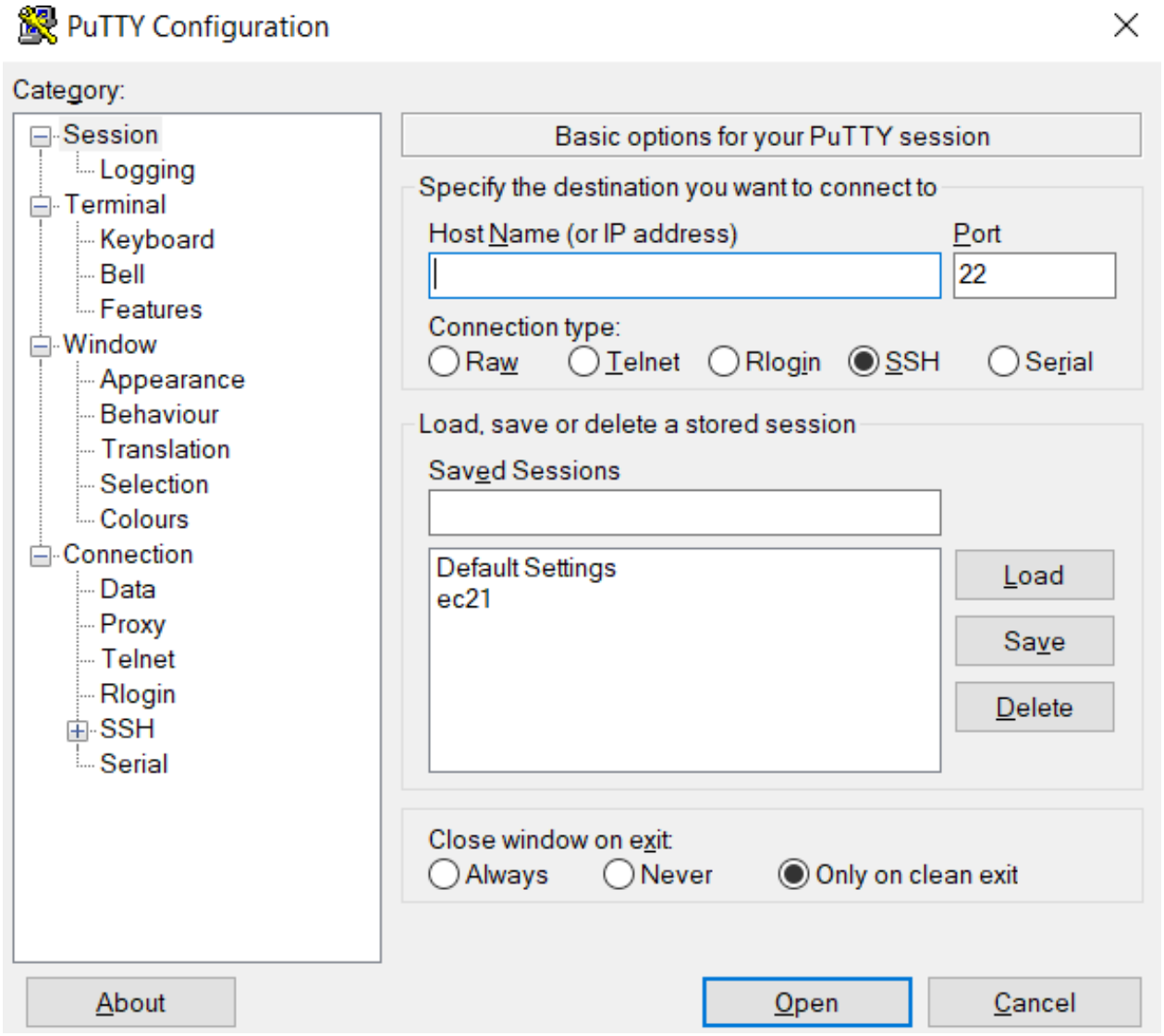
12. Wait for some time and then go to "EC2 dashboard --> Running Instances". Your instance should be running successfully with "Instance State: Running" and "Status Checks: 2/2 Checks Passed".



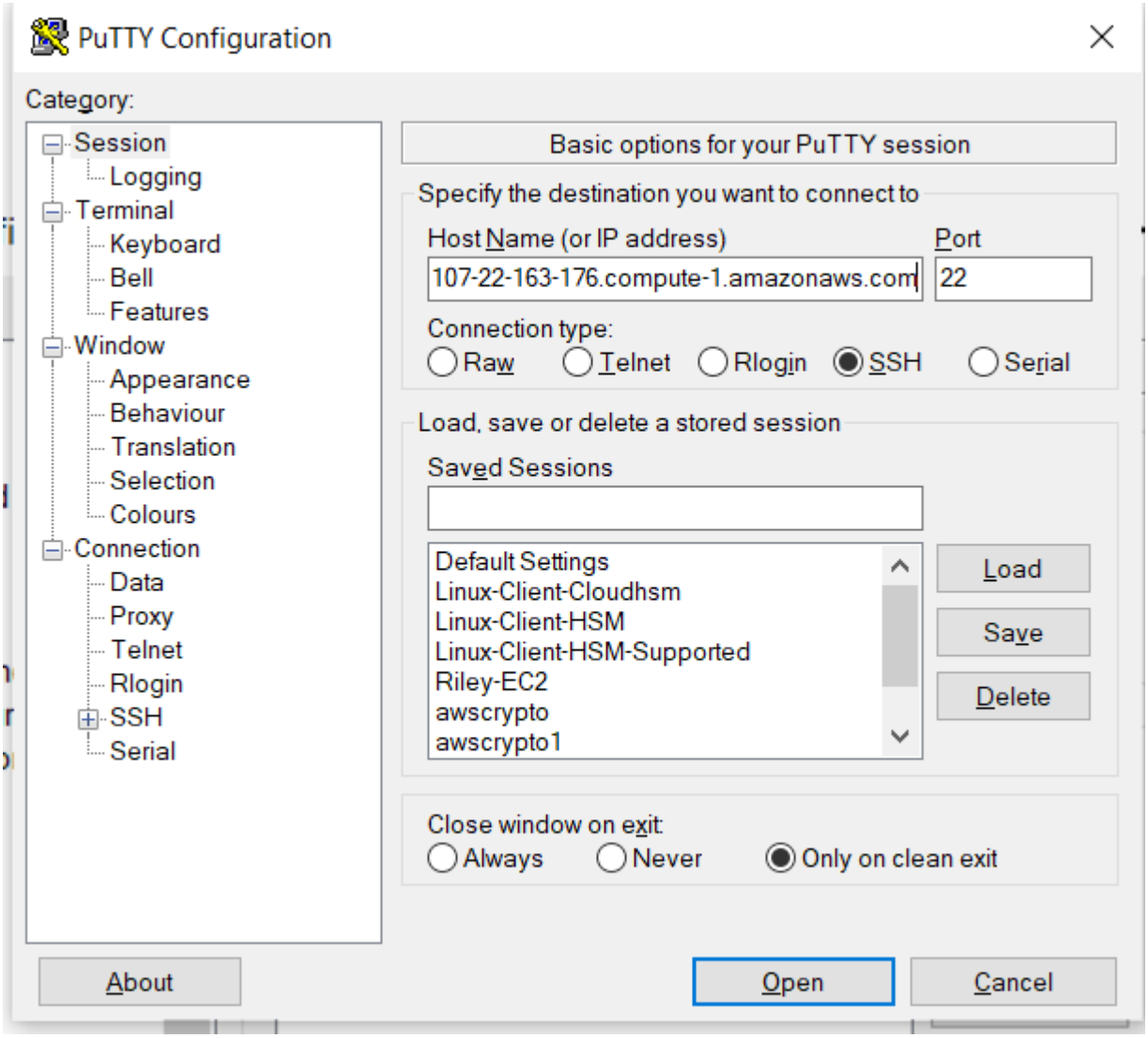
Note: EC2 instance creation will be specific to the user's environment and above steps are for illustration purposes, hence use the Public-DNS name of the EC2 instance as per your environment.

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

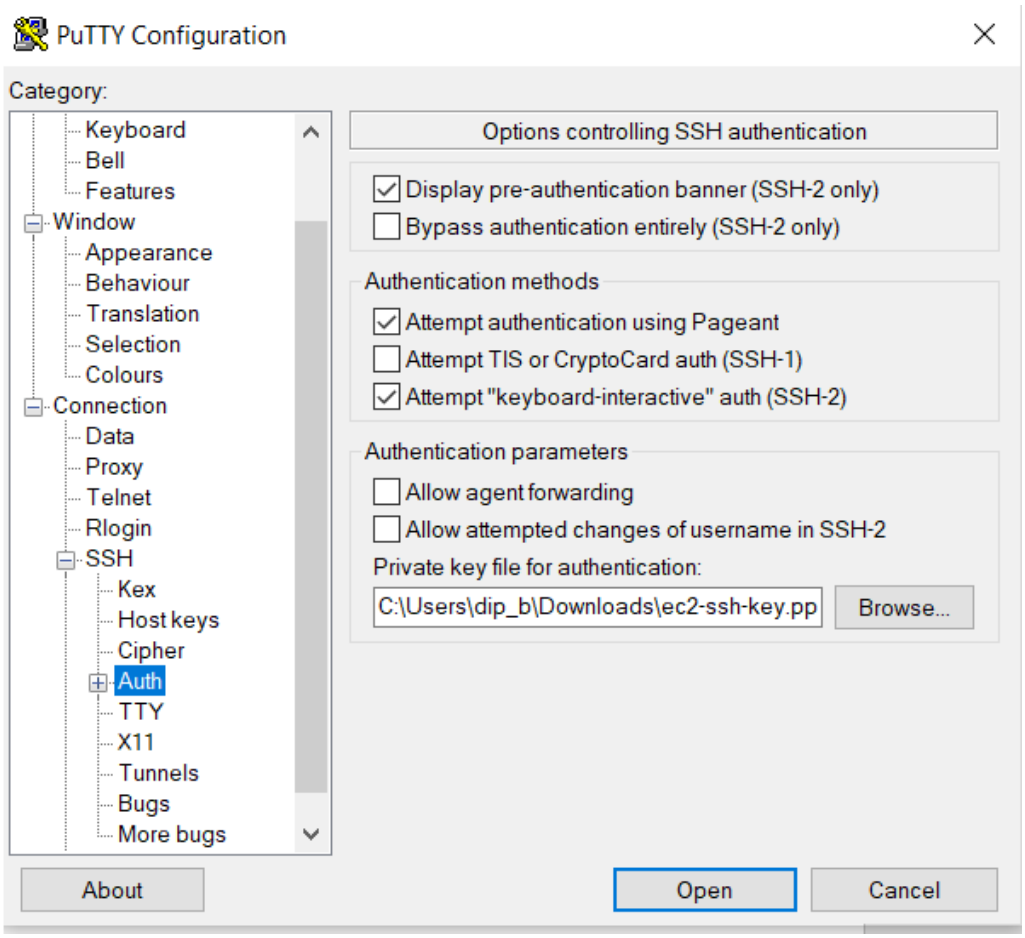
1. Download and Open “Putty” on your windows machine.



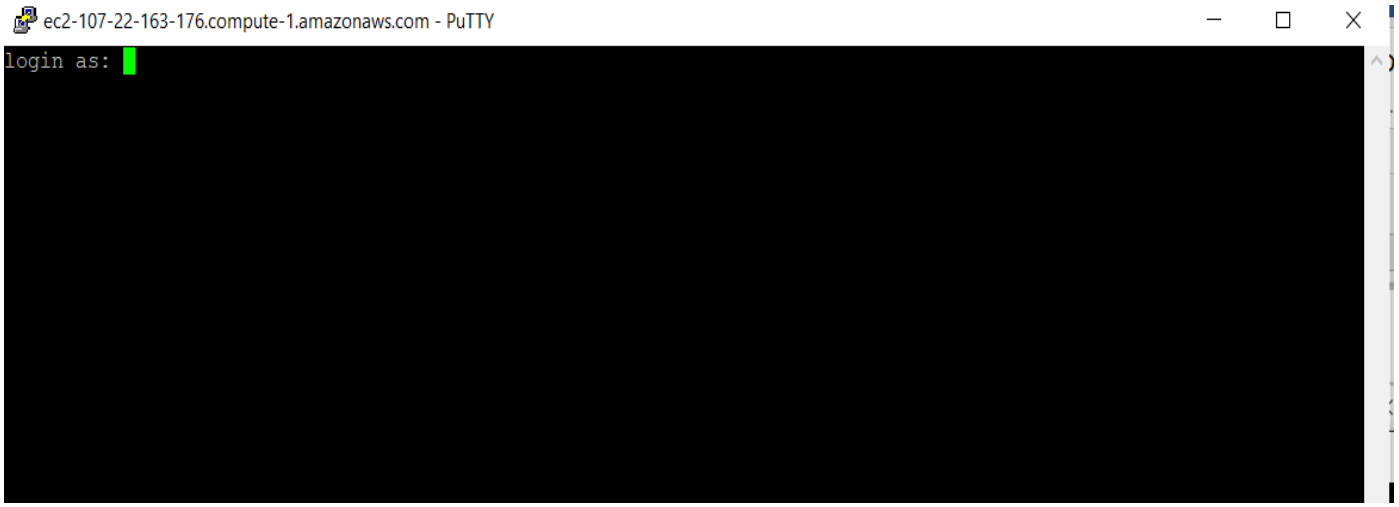
2. Enter Hostname: “ec2-107-22-163-176.compute-1.amazonaws.com” from “Public DNS (IPv4)” in AWS EC2 console and Port : 22 (ssh)



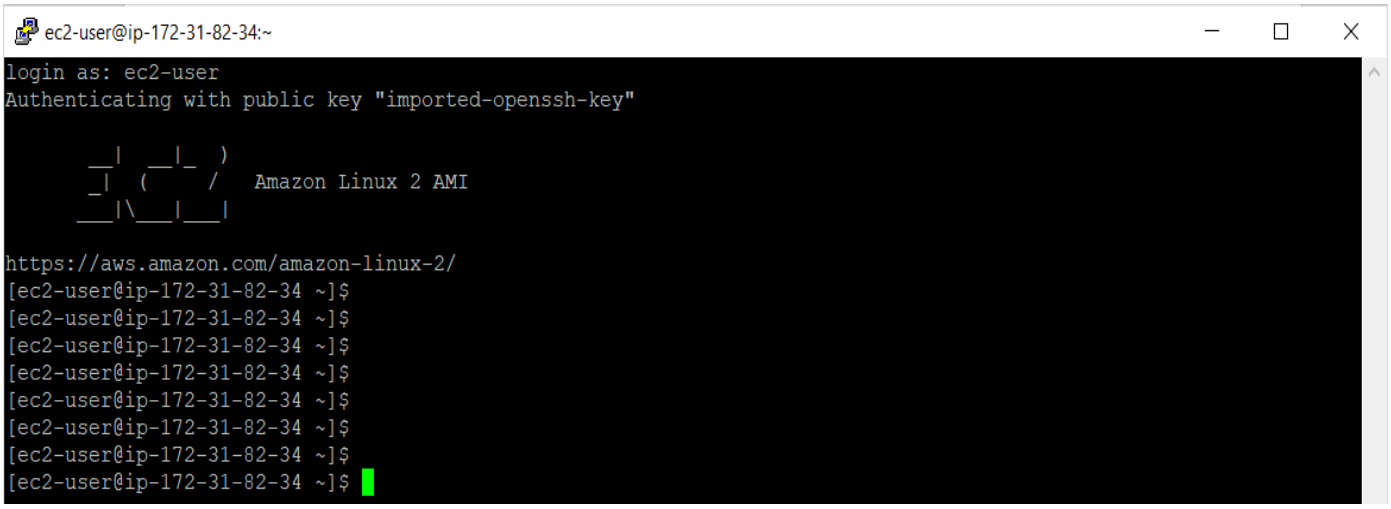
3. In Putty, Go to “Connections --> SSH --> Auth”. Click browse and then upload the “Private Key” file in “ppk” format.



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



5. Login as : “ec2-user”



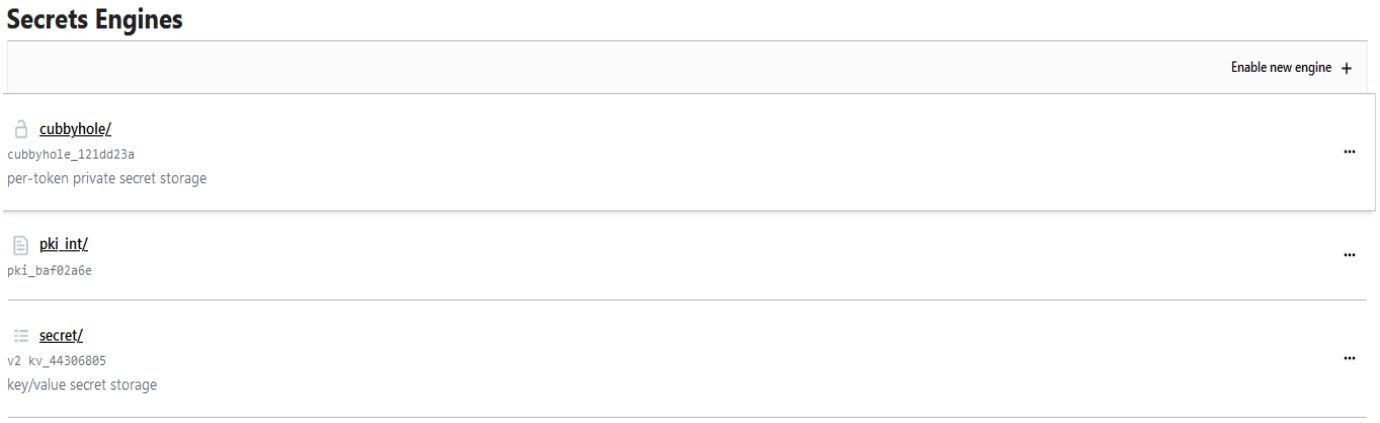
6. Type “Sudo su” to change to “root” user.

Note: EC2 instance creation/connection will be specific to the user’s environment and above steps are for illustration purposes, hence use the Public-DNS name of the EC2 instance as per your environment.

Activity 6: Issuing SSL/TLS Certificate for Web Server

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

1. Login to HashiCorp server with the root credentials

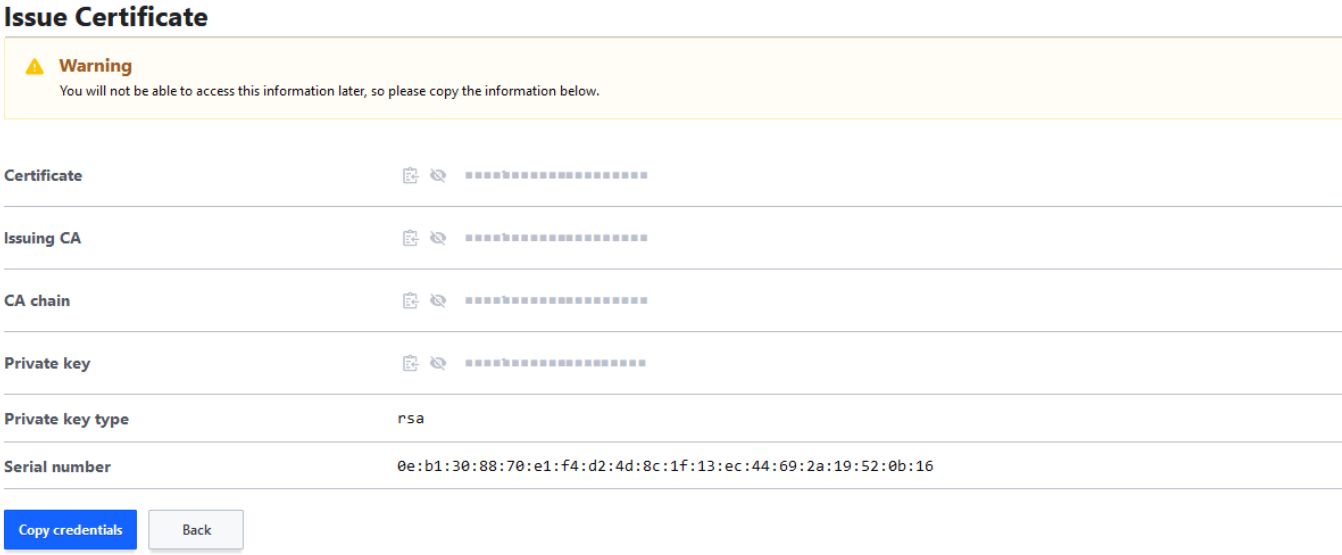


2. Select **Secrets → pki_int** from the **Secrets Engines** list.

3. Select **WebServer Role** under **Roles.**

4. Enter ec2-107-22-163-176.compute-1.amazonaws.com in the Common Name field and TTL 365 days

5. Click Generate:



6. Click **Copy credentials** and save it to a file named “webserver-cert.pem”

Note: Change the extension of **Certificate, Certificate chain** and ***Private Key*** file to **.crt** and **.key** respectively from. Pem

[to change the format from. pem to .crt and .key, go to the text file (e.g.; certificate.txt)>Rightclick>properties>General>delete.txtandupdate.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**.

```
# 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.:

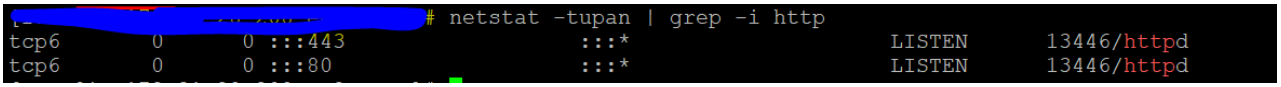
   http://ec2-107-22-163-176.compute-1.amazonaws.com

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

Note: Usage of EC2 instance Public DNS name will be specific to the user’s environment and above steps are for illustration purposes, hence use the Public-DNS name of the EC2 instance as per your environment.

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 ec2-107-22-163-176.compute-1.amazonaws.com

ServerAdmin admin@ec2-107-22-163-176.compute-1.amazonaws.com

DocumentRoot /var/www/html/ec2-107-22-163-176.compute-1.amazonaws.com

</VirtualHost>

Press Esc

Save the file :wq!

10.

10. Create a directory "**mkdir /var/www/html/ec2-107-22-163-176.compute-1.amazonaws.com**"

11. Create an "**index.html**" file with following html code: **vi /var/www/html/ec2-107-22-163-176.compute-1.amazonaws.com/index.html**

<h1>

Welcome to 2 Tier PKI Lab Setup with HashiCorp

</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"**

Note: Usage of EC2 instance Public DNS name will be specific to the user's environment and above steps are for illustration purposes, hence use the Public-DNS name of the EC2 instance as per your environment.

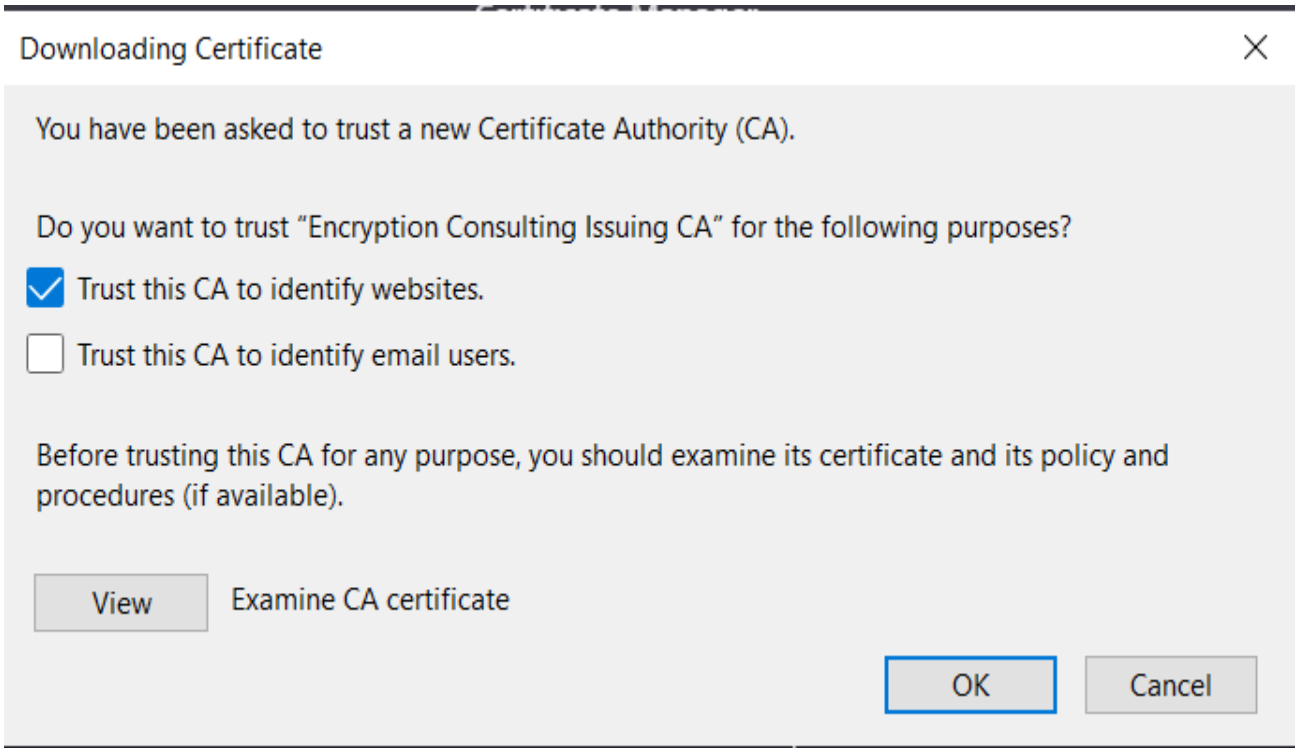
Task 3: Install the SSL/TLS Certificate Chain to the Client's Web browser

1. Open the Firefox web browser.

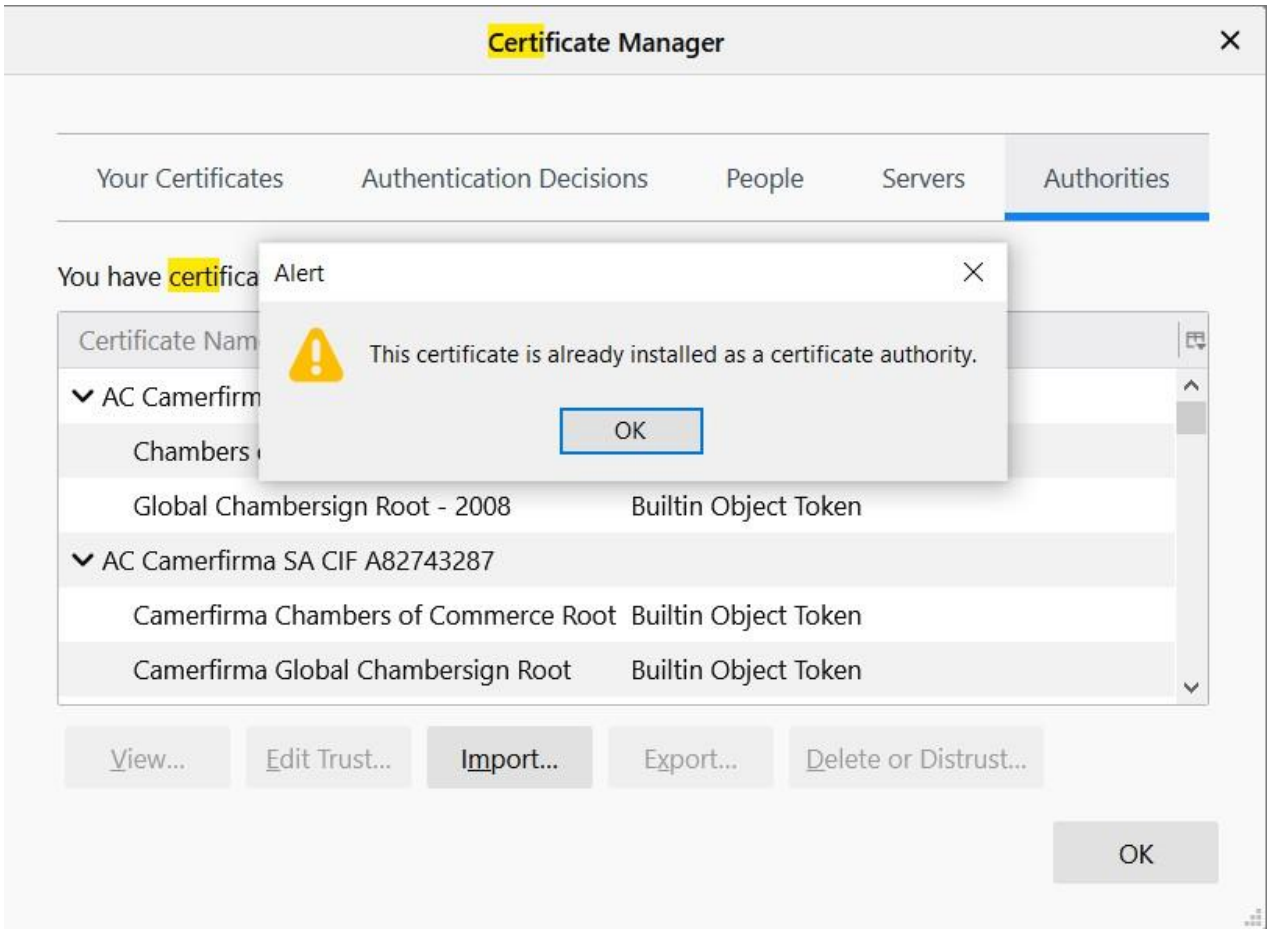
Note: You may add the SSL/TLS certificate to the browser of your choice. For the illustration purpose, I have taken Firefox browser.

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 HashiCorp Intermediate CA and has trust relationship up-till Microsoft 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://ec2-107-22-163-176.compute-1.amazonaws.com

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

   "Welcome to 2 Tier PKI Lab Setup with HashiCorp"

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".**

Task 2: Verify PKI Health for Web Server Certificate with "Certutil" utility

1. Log into Windows machine 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:\web-server-cert.crt**
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:\web-server-cert.crt**
19. Review the output and make sure all the chain retrieval and revocation status successfully verified.