





## 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	ОЅ Туре	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.a mazonaws.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.

Add Roles and Features Wiza	rd	– 🗆 X
Select role servi	ces	DESTINATION SERVER CA01
Before You Begin Installation Type Server Selection Server Roles Features AD CS Role Services Confirmation Results	Select the role services to install for Active Directory Certi Role services           Certification Authority           Certificate Enrollment Policy Web Service           Certificate Enrollment Web Service           Certification Authority Web Enrollment           Network Device Enrollment Service           Online Responder	ficate Services Description Certification Authority (CA) is used to issue and manage certificates. Multiple CAs can be linked to form a public key infrastructure.

- 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.

New AD CS Connightation	
Setup Type	DESTINATION SERVER CA01
Credentials Role Services Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Confirmation Progress Results	<ul> <li>Specify the setup type of the CA</li> <li>Enterprise certification authorities (CAs) can use Active Directory Domain Services (AD DS) to simplify the management of certificates. Standalone CAs do not use AD DS to issue or manage certificates.</li> <li>Interprise CA</li> <li>Enterprise CAs must be domain members and are typically online to issue certificates or certificate policies.</li> <li>Standalone CA</li> <li>Standalone CAs can be members or a workgroup or domain. Standalone CAs do not require AD DS and can be used without a network connection (offline).</li> </ul>
	More about Setup Type
	< Previous Next > Configure Cancel



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.

AD CS Configuration			-		×
Cryptography fo	or CA		DESTINA	TION SER	VER CA01
Role Services	specify the cryptographic options				
Setup Type	Select a cryptographic provider:		Key length:		
CA Type	RSA#Microsoft Software Key Storage Provider	¥	2048		~
Private Key	Select the hash algorithm for signing certificates issued by	y this CA:			
Cryptography CA Name	SHA256 SHA384	^			
Validity Period Certificate Database	SHA512 SHA1 MD5	~			
Progress Results	☐ Allow administrator interaction when the private key i	s accessed	by the CA.		
	More about Cryptography				
	< Previous Next	t >	Configure	Cance	al

- 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.

AD CS Configuration	- L ×
CA Name	DESTINATION SERVER CA01
Credentials Role Services	Specify the name of the CA
Setup Type CA Type Private Key	Type a common name to identify this certification authority (CA). This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but can be modified.
CA Name	EncryptionConsulting Root CA
Validity Period Certificate Database	Distinguished name suffix:
Confirmation	Preview of distinguished name:
Progress Results	CN=EncryptionConsulting Root CA
	More about CA Name



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**.

AD CS Configuration		- 🗆 X
CA Database		DESTINATION SERVER CA01
Credentials Role Services Setup Type	Specify the database locations Certificate database location:	
CA Type Private Key	C:\windows\system32\CertLog	
Cryptography CA Name Validíty Period	C:\windows\system32\CertLog	
Certificate Database Confirmation Progress Results		
	More about CA Database	Configure Cancel



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

Credentials Role Services	To configure the following roles,	role services, or features, click Configure.
Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Confirmation Progress Results	Certification Authority CA Type: Cryptographic provider: Hash Algorithm: Key Length: Allow Administrator Interaction: Certificate Validity Period: Distinguished Name: Certificate Database Location: Certificate Database Log Location:	Standalone Root RSA#Microsoft Software Key Storage Provider SHA256 2048 Disabled 12/15/2039 12:13:00 PM CN=EncryptionConsulting Root CA C:\windows\system32\CertLog C:\windows\system32\CertLog

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:
  - O Certutil -setreg CA\CRLPeriodUnits 52
  - O Certutil -setreg CA\CRLPeriod "Weeks"
  - O 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:
  - O 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:
  - O Certutil -setreg CA\ValidityPeriodUnits 10
  - O 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:Idap:///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:Idap:///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:Idap:///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.



## Private certificate authority

You or your IT Administrator can establish a secure managed infrastructure for issuing and revoking private digital certificates. Private certificates identify and secure applications, services, devices and users within an organization.





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

Step 1: Select CA type	Select the cert	ificate authority (CA) type	0
Step 2: Configure CA subject name Step 3: Configure CA key algorithm Step 4: Configure revocation	ACM helps you create a priva	ate subordinate CA.	
Step 5: Add tags Step 6: Configure CA permissions Step 7: Review	💮 Root CA	Create a root CA. Choose this option if you want to establish a new CA hierarchy.	
	Subordinate CA	Create a subordinate CA. Choose this option if you want to make a CA that is subordinate to an existing CA. You can use this option to create issuing CAs as well as intermediate CAs.	

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 (0): 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

Step 3: Configure CA key algorithm Step 4: Configure revocation Step 5: Add tags	Name your UA using the disanguished name (UN) form These names cannot be changed later.	nal. The name is used as the subject in the UA certificate and as the issuer in certificates that the UA issues.
Step 5: Configure CA permissions		
Siep 1. Neview	Subject distinguished name	Value
	Organization (O)*	Encryption Consulting
		Company name. Max length of 64 characters.
	Organization Unit (OU)*	Engineering
		Company subdivision. Max length of 64 characters
	Country name (C)*	United States (US)
		Two letter country code
	State or province name*	Texas
		Full name. Max length of 128 characters
	Locality name*	Stableford
		City Max length of 128 characters

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.

tep 1: Select CA type tep 2: Configure CA subject name	Configure the certificate authority (CA) key algorithm	€
tep 3: Configure CA key algorithm	Choose the key algorithm for your CA. You can change the default selection in the Advanced section.	
tep 4: Configure revocation tep 5: Add tags tep 6: Configure CA permissions	RSA 2048 The 2048-bit RSA key algorithm is widely supported by browsers and other clients. The 2048-bit size provides a good balance between security a efficiency.	nd
tep 7: Review	Advanced	6
	You can choose different key types and key parameters for this CA, but this is not common.	

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.

Step 5: Add tags Step 6: Configure CA permissions	Certificate revocation list (CRL)			0
Step 7: Review	Enable CRL distribution  AGM sends certificate revocation lists (CRLs) to your Amazon S	3 bucket.		
	Create a new S3 bucket	Yes No		
	S3 bucket name	s3bucketforcri	0	
	- Advanced			Ø
	Custom CRL Name	encryptionconsultingcri	0	
	Valid for	7 Days		
			Cancel	Previous Next
Create CA				
Step 1: Select GA type Step 2: Configure GA subject name	Add tags			Ø
Step 3: Configure CA key algorithm	To help you manage your certificate authorities you can optional	y assign your own metadata to each resource in the fi	orm of tags. Learn more.	
Step 4: Configure revocation Step 5: Add tags	Tag name Value			
Step 6: Configure CA permissions	Tag name Value			
step /: Heview	Add tag			

- 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.

tep 1: Select CA type	Step 6 <sup>,</sup> Configure CA permissions		0
tep 2: Configure CA subject name tep 3: Configure CA key algorithm	Authorize ACM permission to renew private subscriber certificates iss	sued within this account from this CA. Learn more.	
tep 4: Configure revocation	ACM access to renew certificates requested by this account	☑ Authorize	
ep 6: Configure CA permissions			
tep 7: Review	You may alter permissions for automated renewal for this CA at any ti this account for this CA.	ime. The change will take effect for all future renewal cycles f	or ACM certificates generated within

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.

Step 1: Select CA type	Review and create
Step 3: Configure CA subject name Step 3: Configure CA key algorithm	Review your choices. Learn more.
Step 4: Configure revocation	CAllune
Step 6: Configure CA permissions	on the
Step 7: Review	C4 type Subordinate
	CA subject name 🥒
	Organization (O) Encryption Consulting Organization Unit (OU) Engineering
	Country name (C) United States (US) State or province name Texas
	Locally name Stableford
	Common name (CN) Encryption Consulting Issuing CA
	Key algorithm 🗡
	Key algorithm RSA
	Key size 2048
	Revocation 🦯
	CRL distribution
	DNS name used in cartificates encryptioncomsultingot CRU, distributions will be situationations and an encryption of the situation of the situ
	CFRL distributions will be updated 7 Clays every
	Tags 🖌
	No tags will be added to this certificate authority.
	CA permissions
	ACIM access to remew certificates Authorize requested by this account
	Clock to continu you understand that you will be charged a monthly tee for the operation of your Private CA until you detet it. You will not be charged for the operation of the CA during the lind 30 days for the first Private CA orealed in your account. You will be charged for the private certificates you issue. Learn more is used to check that be charged to the continue.

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.



You can also finish later

autiontyru

CA information

Type CA common name ARN Subordinate : Encryption Consulting Issuing CA



## 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".

C	A common name	Owner	Organization	OU	Туре	Status
: E C/	Encryption Consulting Issuing	Self	Encryption Consulting	Engineering	Subordinate	Pending certificate
Status	CA certificate Revo	ocation configu	ration Tags	Permissions	Resource shares	
		Detaile	Status Pend ed status Actio Owner Self	ling certificate n required		
4	Action required! Before issuing certificates	with your CA, yo	ou need to import a	CA certificate. Import	a CA certificate to a	ctivate your

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

Private CAs

CA cor Get CA certificate		Organization OU Encryption Consulting Engineering		Туре	Status		
CA     Encry     Update CA revocation     Enable				Engineering	Subordinate	Pending certificate	
Status	Disable Delete	tion	Tags	Permissions	Resource shares		
		Restore Generate audit report	Status status	s Pending certificate s Action required			
		Configure CA permissions Manage resource shares	Owner	Self			

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**.

This	CSR can be obtained a	gain by returning to this screen. You can exit this screen without	It losing this CSR.	
*	Export CSR to a file	You can export the PEM-encoded CSR to a file and have the	e parent CA sign it.	

- 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**.
- 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.

aws Services V			¢	Pama 🔻	N. Virginia 🔻
Step 1: Export CSR Step 2: Import signed CA certificate	Import a signed certificate	authority (CA) certificate			
Step 3: Review	Certificate body*	MIIGQTCCBSmgAwIBAgITFgAAAAS			
	Certificate chain*	File     Segin certificate			
		MIIDKTCCAhGgAwIBAgIQHHRjmeA Ht4NGxHdAsUQ71jANBgkqhkiG9w or import			
	*Required				
			Cancel	Previo	Next

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.

Step 1: Export CSR	Review and install		0
Step 3: Review	Review your choices. Learn more.		
	Import certificate inform	nation	Edit
	Certificate Body	<pre>MIIGQTCCBSmgAwIBAgITFgAAAASrJmrYXQruTgAAAAAABDA ADAnMSUwIwYDVQQDExxFbmNyeXB0aW9uQ29uc3VsdGluZyf MDkzMDE0HzcxMloXDTMwMDkzMDE0HDcxMlowgZcxCzA36g VQQIEwVUZXhhczETMBEGALUE8XMKU3RhYmxlZm9yZDEFM8G d6lvbiBD25zdMx0aW5nIDEVMBWGALUECXMMRWSnaW5IZX EyIGIEVUY3J5cHRpb24gQ29uc3VsdGluZyBJc3NlaW5nIEN 9w8BAQEFAAOCAQ8AMIIBCgKCAQEAr8xR9Q/hYLOL11Hvq2 wskg76wD6iX1iRsT515F6CjuvDtMc5LUgGd947kPur5Z4M NCrsK+RoHGnY/PKAekETjEpTc1WvTDAIVQKU08Jj2QXF6 pT6ErQ09bYM36c10V5hawVG3CCF81KjxarMxuKqu0KKcrr 5-qj4R0v9Jbxph75LUnEhDrthizej3TKSwebEVdVfnYigig R31Lkg8L+ZLtCc1P/k2K55PvnqgbyiHBeNDxoXgLhGIAmbi Au8wDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUPNR6K2f g0YHWw7DVR0j8BgwFoAUd1ffq+rK7qYAhF52NgO41Z2XRF MIIBNTCCATGgggEtoIIBKYaB0WxKYXA6Ly8vQ049RW5jcn</pre>	ANBgkqhkiG9w BSb290IGNBMB WUBAYTAIVTMQ DGALUECHMWRW JGALUECHMWRW JDpbmcgMSswKQ UBMIIBIJANBg #00ixjDpXZ/ UGMRTAPqaIs 802T9k7IQMmm rw0pGt5hQkn3 278Tg1tx/kjZ sk7wIDAQABo4 P+KAZc8Bft8z EwggFCBgNVHR LwdGlvbkNvbn
	ıjкbitvQjkBKP END CERT	SMKWGSZGWTFAPp1 IFICATE	
	4		•
Certificate Chain	BEGIN CE	RTIFICATE	
	MIIDKTCCAhGgA	wIBAgIQHHRjmeAHt4NGxHdAsUQ71jANBgkqhkiG9	WØBAQ
	MSUWIWYDVQQDE	xxFbmNyeXB0aW9uQ29uc3VsdG1uZyBSb290IGNBM	B4XDT
	MzEyMzkØNVoXD	TQwMDkyMzEyNDk0NVowJzElMCMGA1UEAxMcRW5jc	nlwdG
	bnN1bHRpbmcgU	m9vdCBiOTCCASIwDOYJKoZIhvcNAOEBBOADggEPA	
	51 (375)		DCCAQ
	ALy7zNcHhH7e9	CYzhmpIn0VYm5hd6EHQGNww5RamEDSqKJp4tbV5N	DCCAQ 12zXb
	ALy7zNcHhH7e9 tXkWhJXmqdITs	CYzhmpIn0VYm5hd6EHQGNww5RamEDSqKJp4tbV5N 1NInQ08C5G5pc0j+c+1m2W89TY/p6A10sgDQniu2.	DCCAQ 12zXb AdRJZ
	ALy7zNcHhH7e9 tXkWhJXmqdITs Dy6Co+7UG8TyZ	CYzhmpIn0VYm5hd6EHQGNww5RamEDSqKJp4tbV5N 1NInQ08C5G5pc0j+c+1m2W89TY/p6A1OsgDQniu2 1Btd8Y1BxBaXi5EBcShLOP1QaJF7aF9LjLkhnlGd	DCCAQ 12zXb AdRJZ aW6nr
	ALy7zNcHhH7e9 tXkWhJXmqdITs Dy6Co+7UG8TyZ aJd0IKd4YRMdy	CYzhmpIn0VYm5hd6EHQGNww5RamEDSqKJp4tbV5N 1NInQ08C5G5pcOj+c+1m2W89TY/p6A10sgDQniu2 1Btd8Y1BxBaXi5EBcShLOP1QaJF7aF9LjLkhnlGd 4Y/bL708yhUUXhd05QH0153mMX3GtyQpgOaJ33gu	DCCAQ 12zXb AdRJZ aW6nr uY0Bl
	ALy7zNcHhH7e9 tXkWhJXmqdITs Dy6Co+7UG8TyZ aJd0IKd4YRMdy MjZWaLIxfNEMG	CYzhmpIn0VYm5hd6EHQGNww5RamEDSqKJp4tbV5N 1NInQ08C5G5pcOj+c+1m2W89TY/p6A1OsgDQniu2 1Btd8Y1BxBaXi5EBcShLOP1QaJF7aF9LjLkhnlGd 4Y/bL708yhUUXhd05QH0153mMX3GtyQpgOaJ33gu pzKrt8N4FGg4Gn5/3icchCg6u0jJsImERPIXcjpU	DCCAQ 12zXb AdRJZ aW6nr uY0B1 R1i6U
	ALy7zNcHhH7e9 tXkWhJXmqdITs Dy6Co+7UG8TyZ aJd0IKd4YRMdy MjZWaLIxfNEMG x3ztyC5rYcC3U	CYzhmpIn0VYm5hd6EHQGNww5RamEDSqKJp4tbV5N 1NInQ08C5G5pcOj+c+1m2W89TY/p6A1OsgDQniu2 1Btd8Y1BxBaXi5EBcShLOP1QaJF7aF9LjLkhnlGd 4Y/bL708yhUUXhd05QH0153mMX3GtyQpgOaJ33gu pzKrt8N4FGg4Gn5/3icchCg6u0jJsImERPIXcjpU Pn5feK3ie0CAwEAAaNRME8wCwYDVR0PBAQDAgGGM	DCCAQ 12zXb AdRJZ aW6nr uY0Bl R1i6U A8GA1
	ALy7zNcHhH7e9 tXkWhJXmqdITs Dy6Co+7UG8TyZ aJd0IKd4YRMdy MjZWaLIxfNEMG x3ztyC5rYcC3U /wQFMAMBAf8wHi	CYzhmpIn0VYm5hd6EHQGNww5RamEDSqKJp4tbV5N 1NInQ08C5G5pc0j+c+1m2W89TY/p6A10sgDQniu2 1Btd8Y1BxBaXi5EBcShLOP1QaJF7aF9LjLkhnlGd 4Y/bL708yhUUXhd05QH0153mMX3GtyQpgOaJ33gu pzKrt8N4FGg4Gn5/3icchCg6u0jJsImERPIXcjpU Pn5feK3ie0CAwEAAaNRME8wCwYDVR0PBAQDAgGGM QYDVR00BBYEFHdX36vqyu6mAIX+djYDjNdWd10RM	DCCAQ 12zXb AdRJZ aW6nr uY0B1 R1i6U A8GA1 BAGCS
	ALy7zNcHhH7e9 tXkWhJXmqdITs Dy6Co+7UG8TyZ aJd0IKd4YRMdy MjZWaLIxfNEMG x3ztyC5rYcC3U /wQFMAMBAf8wH gjcVAQQDAgEAM	CYzhmpIn0VYm5hd6EHQGNww5RamEDSqKJp4tbV5N 1NInQ08C5G5pc0j+c+1m2W89TY/p6A10sgDQniu2 1Btd8Y1BxBaXi5EBcShLOP1QaJF7aF9LjLkhnlGd 4Y/bL708yhUUXhd05QH0153mMX3GtyQpgOaJ33gu pzKrt8N4FGg4Gn5/3icchCg6u0jJsImERPIXcjpU Pn5feK3ie0CAwEAAaNRME8wCwYDVR0PBAQDAgGGM QYDVR00BBYEFHdX36vqyu6mAIX+djYDjNdWd10RM A0GCSqGSIb3DQEBCwUAA4IBAQATCV7cVE/1431fr	DCCAQ 12zXb AdRJZ aW6nr uY0B1 R1i6U A8GA1 BAGCS STJSp
	ALy7zNcHhH7e9 tXkWhJXmqdITs Dy6Co+7UG8TyZ aJd0IKd4YRMdy MjZWaLIxfNEMG x3ztyC5rYcC3U /wQFMAMBAf8wH gjcVAQQDAgEAM KenkKpw3geidx	CYzhmpIn0VYm5hd6EHQGNww5RamEDSqKJp4tbV5N 1NInQ08C5G5pcOj+c+1m2W89TY/p6A10sgDQniu2 1Btd8Y1BxBaXi5EBcShLOP1QaJF7aF9LjLkhnlGd 4Y/bL708yhUUXhd05QH0153mMX3GtyQpgOaJ33gu pzKrt8N4FGg4Gn5/3icchCg6u0jJsImERPIXcjpU Pn5feK3ie0CAwEAAaNRME8wCwYDVR0PBAQDAgGGM. QYDVR00BBYEFHdX36vqyu6mAIX+djYDjNdWd10RM A0GCSqGSIb3DQEBCwUAA4IBAQATCV7cVE/1431fr Y1Cg875b0wbaXAEjCvsXI6qi3cuQFWyRQsN91HiC	DCCAQ 12zXb AdRJZ aW6nr uY0B1 R1i6U A8GA1 BAGCS STJsp MVjB3
	ALy7zNcHhH7e9 tXkWhJXmqdITs Dy6Co+7UG8TyZ aJd0IKd4YRMdy MjZWaLIxfNEMG x3ztyC5rYcC3U /wQFMAMBAf8wH gjcVAQQDAgEAM KenkKpw3geidx U0jZbDzifcK+u	CYzhmpIn0VYm5hd6EHQGNww5RamEDSqKJp4tbV5N 1NInQ08C5G5pcOj+c+1m2W89TY/p6A1OsgDQniu2 1Btd8Y1BxBaXi5EBcShLOP1QaJF7aF9LjLkhnlGd 4Y/bL708yhUUXhd05QH0153mMX3GtyQpgOaJ33gu pzKrt8N4FGg4Gn5/3icchCg6u0jJsImERPIXcjpU Pn5feK3ie0CAwEAAaNRME8wCwYDVR0PBAQDAgGGM. QYDVR00BBYEFHdX36vqyu6mAIX+djYDjNdWd10RM A0GCSqGSIb3DQEBCwUAA4IBAQATCV7cVE/1431fr: Y1Cg875bOwbaXAEjCvsXI6qi3cuQFWyRQsN91HiCi qJ24rWX/U1iZXedpU7CJdvxTbo+a/Sj29S+zD15y	DCCAQ 12zXb AdRJZ aW6nr uY0B1 R1i6U A8GA1 BAGCS STJSp MVjB3 NcTjx
	ALy7zNcHhH7e9 tXkWhJXmqdITs Dy6Co+7UG8TyZ aJd0IKd4YRMdy MjZWaLIxfNEMG x3ztyC5rYcC3U /wQFMAMBAf8wH gjcVAQQDAgEAM KenkKpw3geidx U0jZbDzifcK+u 762wrzqhGw9Fy	CYzhmpIn0VYm5hd6EHQGNww5RamEDSqKJp4tbV5N 1NInQ08C5G5pcOj+c+1m2W89TY/p6A1OsgDQniu2 1Btd8Y1BxBaXi5EBcShLOP1QaJF7aF9LjLkhnlGd 4Y/bL708yhUUXhd05QH0153mMX3GtyQpgOaJ33gu pzKrt8N4FGg4Gn5/3icchCg6u0jJsImERPIXcjpU Pn5feK3ie0CAwEAAaNRME8wCwYDVR0PBAQDAgGGM. QYDVR00BBYEFHdX36vqyu6mAIX+djYDjNdWdl0RM A0GCSqGSIb3DQEBCwUAA4IBAQATCV7cVE/1431fr Y1Cg875b0wbaXAEjCvsXI6qi3cuQFWyRQsN91HiCl qJ24rWX/UliZXedpU7CJdvxTbo+a/Sj29S+zD15y iC1fnc0sB89EUGKHS3nXayoEO4ws8x174S24zwc8	DCCAQ 12zXb AdRJZ aW6nr uY0B1 R1i6U A8GA1 BAGCS STJsp MVjB3 NcTjx f+WXB
	ALy7zNcHhH7e9 tXkWhJXmqdITs Dy6Co+7UG8TyZ aJd0IKd4YRMdy MjZWaLIxfNEMG x3ztyC5rYcC3U /wQFMAMBAf8wH gjcVAQQDAgEAM KenkKpw3geidx U0jZbDzifcK+u 762wrzqhGw9Fy e6VEORyHebBrh	CYzhmpIn0VYm5hd6EHQGNww5RamEDSqKJp4tbV5N 1NInQ08C5G5pcOj+c+1m2W89TY/p6A1OsgDQniu2 1Btd8Y1BxBaXi5EBcShLOP1QaJF7aF9LjLkhnlGd 4Y/bL708yhUUXhd05QH0153mMX3GtyQpgOaJ33gu pzKrt8N4FGg4Gn5/3icchCg6u0jJsImERPIXcjpU Pn5feK3ie0CAwEAAaNRME8wCwYDVR0PBAQDAgGGM. QYDVR00BBYEFHdX36vqyu6mAIX+djYDjNdWd10RM A0GCSqGSIb3DQEBCwUAA4IBAQATCV7cVE/1431fr Y1Cg875b0wbaXAEjCvsXI6qi3cuQFWyRQsN91HiCl qJ24rWX/UliZXedpU7CJdvxTbo+a/Sj29S+zD15y/ iC1fnc0sB89EUGKHS3nXayoEO4ws8x174S24zwc8 nz3DG4Bv7wgw8HbONxdzHbRo8Tkd29IYu07j6Y0f	DCCAQ 12zXb AdRJZ aW6nr uY0B1 R1i6U A8GA1 BAGCS STJsp MVjB3 NcTjx f+WXB 7JV45
	ALy7zNcHhH7e9 tXkWhJXmqdITs Dy6Co+7UG8TyZ aJd0IKd4YRMdy MjZWaLIxfNEMG x3ztyC5rYcC3U /wQFMAMBAf8wH gjcVAQQDAgEAM KenkKpw3geidx U0jZbDzifcK+u 762wrzqhGw9Fy e6VEORyHebBrh ALkxU6int5q9f	CYzhmpIn0VYm5hd6EHQGNww5RamEDSqKJp4tbV5N 1NInQ08C5G5pcOj+c+1m2W89TY/p6A1OsgDQniu2 1Btd8Y1BxBaXi5EBcShLOP1QaJF7aF9LjLkhnlGd 4Y/bL708yhUUXhd05QH0153mMX3GtyQpgOaJ33gu pzKrt8N4FGg4Gn5/3icchCg6u0jJsImERPIXcjpU Pn5feK3ie0CAwEAAaNRME8wCwYDVR0PBAQDAgGGM QYDVR00BBYEFHdX36vqyu6mAIX+djYDjNdWd10RM A0GCSqGSIb3DQEBCwUAA4IBAQATCV7cVE/1431fr Y1Cg875bOwbaXAEjCvsXI6qi3cuQFWyRQsN91HiC qJ24rWX/U1iZXedpU7CJdvxTbo+a/Sj29S+zD15y iC1fnc0sB89EUGKHS3nXayoEO4ws8x174S24zwc8 nz3DG4Bv7wgw8HbONxdzHbRo8Tkd29IYu07j6Y0f zfyx1UM9MhE6VENpXS+I2c2hzNpWR6j/6t/M2Rg4	DCCAQ 12zXb AdRJZ aW6nr uY0B1 R1i6U A8GA1 BAGCS STJsp MVjB3 NcTjx f+WXB 7JV45 +ABSX
	ALy7zNcHhH7e9 tXkWhJXmqdITs Dy6Co+7UG8TyZ aJd0IKd4YRMdy MjZWaLIxfNEMG x3ztyC5rYcC3U /wQFMAMBAf8wH gjcVAQQDAgEAM KenkKpw3geidx U0jZbDzifcK+u 762wrzqhGw9Fy e6VEORyHebBrh ALkxU6int5q9f END CERT	CYzhmpIn0VYm5hd6EHQGNww5RamEDSqKJp4tbV5N 1NInQ08C5G5pcOj+c+1m2W89TY/p6A10sgDQniu2 1Btd8Y1BxBaXi5EBcShLOP1QaJF7aF9LjLkhnlGd 4Y/bL708yhUUXhd05QH0153mMX3GtyQpgOaJ33gu pzKrt8N4FGg4Gn5/3icchCg6u0jJsImERPIXcjpU Pn5feK3ie0CAwEAAaNRME8wCwYDVR0PBAQDAgGGM. QYDVR00BBYEFHdX36vqyu6mAIX+djYDjNdWd10RM A0GCSqGSIb3DQEBCwUAA4IBAQATCV7cVE/1431fr Y1Cg875b0wbaXAEjCvsXI6qi3cuQFWyRQsN91HiCu qJ24rWX/U1iZXedpU7CJdvxTbo+a/Sj29S+zD15y iC1fnc0sB89EUGKHS3nXayoEO4ws8x174S24zwc8 nz3DG4Bv7wgw8HbONxdzHbRo8Tkd29IYu07j6Y0f zfyx1UM9MhE6VENpXS+I2c2hzNpWR6j/6t/M2Rg4 IFICATE	DCCAQ 12zXb AdRJZ aW6nr uY0B1 R1i6U A8GA1 BAGCS STJSp MVjB3 NcTjx f+WXB 7JV45 +ABSx

#### Install subordinate CA certificate

Cancel

Previous



## 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.

Running instances	1	Elastic IPs	0
Dedicated Hosts	0	Snapshots	0
/olumes	1	Load balancers	0
Key pairs	1	Security groups	3
Placement groups	0		

#### 3. Choose Create key pair.

Q. Filter key pairs      1       Name     V     Fingerprint     V		
Name v Fingerprint v ID	>	0
		V
my-key-pair af:89:03:e5:13:ae:7f:cf:46:c2:00:d7:1d: key-05f53a8bf6368b24d		

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.

Create key pair	
Key pair A key pair, consisting of a private key and a public key, is a set of security cre an instance.	dentials that you use to prove your identity when connecting to
Name	
my-key-pair	
The name can include up to 255 ASCII characters. It can't include leading or	trailing spaces.
File format	
O pem For use with OpenSSH	
• ppk For use with PuTTY	
Tags (Optional)	
No tags associated with the resource.	
Add tag	
You can add 50 more tags	
	Cancel Create key pair
Key pairs (1/1)	C Actions  Create key pair
Q Filter key pairs	< 1 > @
☑ Name ♥ Fingerprint ♥ ID	4
☑ my-key-pair af:89:03:e5:13:ae:7f:cf:46:c2:00:d7:1d: key	-05f53ə8bf6368b24d

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/.

New EC2 Experience Tell us what you think	Resources			© ©
EC2 Dashboard New	You are using the following Amazon EC2 resources in the US Ea	(N. Virginia)	) Region:	
Events New	Running instances	Elastic I	IPs	0
Tags	Definited lines	Course		0
Limits	Dedicated Hosts	Snapsn	OTS	U
/ Instances	Volumes	Load ba	alancers	0
Instances	Key pairs	Security	y groups	3
Instance Types				
Launch Templates	Placement groups			
Spot Requests Savings Plans Reserved Instances	Easily size, configure, and deploy Microsoft SQL Server, Wizard for SQL Server. Learn more	ways On ava	ilability groups on AWS using the AWS La	unch X
Dedicated Hosts New				
Capacity Reservations	Launch instance	Ser	vice health	
		C	Service Health Dashboard	1
Images	To get started, launch an Amazon EC2 instance, which is a			_
AMIS	virtual server in the cloud.	Regio	on Status	
Flastic Block Store	Launch instance 🔻	negn	50003	

- 2. Choose Launch Instance.
- 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	- Туре -	vCPUs (j) -	Memory (GiB) -	Instance Storage (GB) 🤅 🔹	EBS-Optimized Available () -	Network Performance (j) -	IPv6 Support
General purpose	t2.nano	1	0.5	EBS only	2	Low to Moderate	Yes
General purpose	12.micro	1	1	EBS only	-	Low to Moderate	Yes
General purpose	t2.small	1	2	EBS only		Low to Moderate	Yes
General purpose	12.medium	2	4	EBS only	2	Low to Moderate	Yes
General purpose	t2.large	2	8	EBS only		Low to Moderate	Yes
General purpose	t2.xlarge	4	16	EBS only	ž.	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	t	EBS only	Yes	Up to 5 Gigabit	Yes
Consideration	40 x xxx x0			PRA	Max	THE REPORT AND	Max

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

Number of instances		1 Launch Into Auto Scali	ng Gr	roup ①
Purchasing option	٢	Request Spot Instances		
Network		vpc-a30cfede (default)	C	Create new VPC
Subnet	$^{\odot}$	No preference (default subnet in any Availability Zon(		Create new subnet
Auto-assign Public IP	•	Enable		
Placement group	$\oplus$	Add Instance to placement group		
Capacity Reservation		Open y		
Domain join directory	٢	No directory	C	Create new directory
IAM role		None	C	Create new IAM role
Shutdown behavior	(j)	Stop		
Ston - Hibernate behavior	(P)	Enable bibernation as an additional stop behavior		

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

<b>X</b> 230								<b></b>	Constraint and a second	ist statistics	500000
1. Choose AM 2	2. Choose Instance Type	3. Configure Instance	4. Add Storage	5 Add Tags	6. Configure Security Group	7. Review					
Step 4: Add our instance will be dit the settings of t torage options in A	Storage e launched with the fol the root volume. You c Amazon EC2.	lowing storage device an also attach addition	settings. You can al EBS volumes a	attach additional fter launching an	EBS volumes and instance instance, but not instance :	store volumes to store volumes. Les	your instance, or am more about				
Volume Type 🕕	Device (]	Snapshot (	D	Size (GiB) 🕕	Volume Type (1)			Throughput (MB/s)	Delete on Termination (j)	Encryption ①	
Root	/dev/sda1	snap-0c4e82	63cef786d91	10	General Purpose S	SD (gp2)	100 / 3000	N/A		Not Encrypted	*
Add New Volume	2										
Add New Volume	e customers can get u	p to 30 GB of EBS Ger	neral Purpose (SS	D) or Magnetic s	storage. Learn more about t	ree usage tier elig	ibility and				



## 7. Choose Next: Add Tags (leave default)

 Step 5. Fee rags

 A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.

 A copy of a tag can be applied to volumes, instances or both.

 Tags will be applied to all instances and volumes. Learn more about tagging your Amazon EC2 resources.

 Key
 (128 characters maximum)

 Value
 (256 characters maximum)

 Instances and volumes. Learn more about tagging your Amazon EC2 resources.

 Key
 (128 characters maximum)

 Value
 (256 characters maximum)

 Instances
 This resource currently has no tags

 Choose the Add tag button or click to add a Name tag.

 Make sure your IAM policy includes permissions to create tags.

 Add Tag
 (Up to 50 tags maximum)

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

Туре	Protocol	Port range	Source	Description - optional
HTTP	ТСР	80	0.0.0/0	Web Server Access over http
SSH	ТСР	22	0.0.0.0/0	SSH Access to the instance
HTTPS	ТСР	443	0.0.0/0	Web Server Access over https

	O Select an existing s	ecurity group		
Securit	y group name: webserversg			
	Description: launch-wizard-1 cre	ated 2020-09-23T00:30:46.320+05:30		
Туре ()	Protocol (j)	Port Range (i)	Source (1)	Description (i)
SSH ~	TCP	22	Custom ~ 0.0.0/0	e.g. SSH for Admin Desktop
	TCP	80	Custom ~ 0.0.0.0/0, ::/0	e.g. SSH for Admin Desktop
HTTPS V	TCP	443	Custom ~ 0.0.0.0/0, ::/0	e.g. SSH for Admin Desktop
Add Rule				
Add Rule				

Cancel Previous Review and Launch



#### 9. Choose Review and Launch.

#### Step 7: Review Instance Launch

AMI Details				00410-4-0-4400-			Edit AMI
Free tier Red Hat En eligible Root Device	tarprise Linux versi Type: ebs Virtualza	on 8 (HVM), SSL on 8 (HVM), EBS ton type: hvm	S General Purpose (SSD) V	folume Type			
Instance Type							Edit instance type
Instance Type	ECUs	vCPUs	Memory (GIB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	
t2.micro	Variable	1	1	EBS only	71	Low to Moderate	
Security Groups							Edit security groups
Security group name Description	websen launch-	versg wizard+1 creater	d 2020-09-23T00:30:46.3	120+05:30			
Туре 🕕		Protocol ()		Port Range ①	Source (1)	Description ()	
		TCP		22	0.0.0.0/0		
SSH							

t2.micro	Variable	81	1	EBS only	÷	Low to Moderate	
<ul> <li>Security Groups</li> </ul>							Edit security groups
Security group name Description	websen launch-	versg wizard-1 crea	ted 2020-09-23T00:	30:46.320+05:30			
Type (j)		Protocol	(i)	Port Range (j)	Source (j)	Description (j)	
SSH		TCP		22	0.0.0/0		
HTTP		TCP		80	0.0.0.0/0		
HTTP		TCP		80	::/0		
HTTPS		TCP		443	0.0.0.0/0		
HTTPS		TCP		443	: <b>/</b> 0		
Instance Details							Edit instance details
Storage							Edit storage
							Edit tags

10. Choose Launch.



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

	elect an existing key pair or create a new key pair
A k allo obi seo	ey pair consists of a <b>public key</b> that AWS stores, and a <b>private key file</b> that you store. Together, the wy you to connect to your instance securely. For Windows AMIs, the private key file is required to ain the password used to log into your instance. For Linux AMIs, the private key file allows you to curely SSH into your instance.
٧o	te: The selected key pair will be added to the set of keys authorized for this instance. Learn more
ab	out removing existing key pairs from a public AMI.
	Choose an existing key pair ~
	Select a key pair
	my-key-pair ~
	□ I acknowledge that I have access to the selected private key file (my-key-pair.pem), and that without this file, I won't be able to log into my instance.

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".

Laun	ch Instance 👻 🔍	Connect Actio	ns v							
Q,	liter by tags and attribute	es or search by key	word						Ø	
	Instance ID	Instance Type	<ul> <li>Availability Zone -</li> </ul>	Instance State 👻	Status Checks	 Alarm Statu	6	Public DNS (IPv4)	*	
	i-0fdb95c000e466090	t2.micro	us-east-1e	🥹 running	2/2 checks passed	None	7	ec2-100-25-199-96.cc	0	



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

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

#### RuTTY Configuration $\times$ Category: Session Basic options for your PuTTY session Logging Specify the destination you want to connect to 📥 Terminal Host Name (or IP address) <u>P</u>ort Keyboard Bell 22 - Features Connection type: Window ○<u>I</u>elnet ○ Rlogin ● SSH O Serial Appearance - Behaviour Load, save or delete a stored session - Translation Saved Sessions - Selection - Colours Connection Default Settings Load --- Data ec21 - Proxy Save Telnet Rlogin Delete . In SSH Serial Close window on exit: O Never Only on clean exit About Cancel Open



- 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.

Reputry Configuration	×
Category:	
Session Cogging Commonstant Cogging Commonstant Commo	Basic options for your PuTTY session         Specify the destination you want to connect to         Host Name (or IP address)         Port         ec2-100-25-199-96.compute-1.amazonaws.c         22         Connection type:         Raw       Telnet         Rogin       SSH         Serial
E Behaviour Translation Selection Colours Connection Data Proxy Telnet Rlogin SSH Kex	Load, save or delete a stored session Saved Sessions ec21 Default Settings ec21 Save Delete
- Host keys - Cipher - Auth - TTY - X11	Close window on exit: Always Never Only on clean exit
About	Open Cancel



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

Certifie	cates									G
AWS C	ertificate Manage	r logs domain names from y	our certificates i	into public certificate transparenc	/ (CT) logs when renewir	ng certificates	. You can opt ou	t of CT loggi	ng, Lear	n
Request	a certificate	1 Import a certificate	Actions •					2	¢	0
						«	< Viewing o	certificates 1	to 4	> »
	Name 👻	Domain name 👻		Additional names	Status 👻	Туре 👻	In use? 👻	Renewal	eligibili	ty 👻



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)

#### Request a private certificate

Step 1: Select CA Step 2: Add domain names	You can use AWS Certificate Manager certificates with other AWS Services.	
Step 3: Add Tags Step 4: Review	Add domain names	6
	Type the fully qualified domain name of the site you want to secure with an SSL/TLS certificate (for example, www.exan asterisk (*) to request a wildcard certificate to protect several sites in the same domain. For example: *.example.com prove www.example.com, site.example.com and images.example.com.	nple.com). Use an otects
	Domain name*	
	"At least one domain name is required	
	ec2-34-228-80-75.compute-1.amazonaws.com	
	Add another name to this certificate	
	You can add additional names to this certificate. For example, if you're requesting a certificate for "www.example.com", you might v "example.com" so that customers can reach your site by either name. Learn more.	want to add the name
	Cancel	Previous

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



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

#### Request a private certificate

Step 2: Add domain names Step 3: Add Tags	To help you manage your certi	ates you can optionally assign your own metadata to each resource in the form of t	ags. Learn more.
Step 4: Review	Tag Name	Value	
	Encryption Consulting	Engineering	
	Add Tag		
		Cancel Previo	us Review and request

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.

Certificates		Certificates	0
Certificate Manager	•	AWS Certificate Manager logs domain names from your certificates into public certificate transparency (CT) logs when renewing certificates. You can opt out of CT logging. Learn more	
Private certificate authority	2		

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

certificates issued by an ACM Private	CA.
CA Domain name	arn:aws:acm-pca:us-east-1:484750812368:certificate-authority/851c4b01-f624-44da-87da-61eca020a213 ec2-34-228-80-75.compute-1.amazonaws.com
Additional names	
Status	Issued
Identifier	ad132d35-ae3a-4d7a-9464-bcde6c5dda18
Serial number	e1:62:1d:5f:b4:9c:34:e0:f9:c2:a9:6c:4b:63:1c:7b
In use?	No
Enter a passphrase for encrypting the	private key. You will need the passphrase later to decrypt the private key.
**This passphrase will be required for	decrypting the PEM encoded private key.
Enter a passphrase	
Confirm passphrase	



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.

ertificates issued by an ACM Private	in, and private key allows you to use your certificate anywhere, including on EC2 instances and on-premises servers. You can export only private CA.
CA	arn:aws:acm-pca:us-east-1:484750812368:certificate-authority/851c4b01-f624-44da-87da-61eca020a213
Domain name	ec2-34-228-80-75.compute-1.amazonaws.com
Additional names	
Status	Issued
Identifier	ad132d35-ae3a-4d7a-9464-bcde6c5dda18
Serial number	e1:62:1d:5f:b4;9c:34:e0:f9:c2:a9:6c:4b:63:1c:7b
In use?	No
Enter a passphrase for encrypting the *This passphrase will be required for	e private key. You will need the passphrase later to decrypt the private key. r decrypting the PEM encoded private key.
Enter a passphrase for encrypting the "This passphrase will be required fo Enter a passphrase	e private key. You will need the passphrase later to decrypt the private key. decrypting the PEM encoded private key.
Enter a passphrase for encrypting the *This passphrase will be required fo Enter a passphrase Confirm passphrase	e private key. You will need the passphrase later to decrypt the private key. decrypting 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.

#### Red Hat Enterprise Linux Test Page

This page is used to test the proper operation of the Apache HTTP server after it has been installed. If you can read this page, it means that the Apache HTTP server installed at this site is working properly.

#### If you are a member of the general public:

The fact that you are seeing this page indicates that the website you just visited is either experiencing problems, or is undergoing routine maintenance.

If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster" and directed to the website's domain should reach the appropriate person.

For example, if you experienced problems while visiting www.example.com, you should send e-mail to "webmaster@example.com".

For information on Red Hat Enterprise Linux, please visit the <u>Red Hat. Inc. website</u>. The documentation for Red Hat Enterprise Linux is <u>available on the Red Hat. Inc.</u> <u>website</u>. If you are the website administrator:

You may now add content to the directory /var/www/html/. Note that until you do so, people visiting your website will see this page, and not your content. To prevent this page from ever being used, follow the instructions in the file /etc/httpl/conf.d/wellowe.conf.

You are free to use the image below on web sites powered by the Apache HTTP 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.

			📕 netstat -tupan   grep -i http		
tcp6	0	0 :::443	:::*	LISTEN	13446/httpd
tcp6	0	0 :::80	:::*	LISTEN	13446/httpd

- 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>

|--|

SSLCertificateKeyFile /etc/pki/tls/private/private\_key.key

sslEngineonServerNameec2-100-25-199-96.compute-1.amazonaws.comServerAdminadmin@ec2-100-25-199-96.compute-1.amazonaws.comDocumentRoot/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.

₽ cer	← → × ↑ 🗣 > This PC > Downloads 🛛 👻 👌	P Search Downl	loads
	Organize - New folder		• 🔳 🔞
	Quick access     Last month (5)	Date modified	Туре
Certifica	Downloads	21-08-2020 18:02	Security Ce
	Certificate.crt	21-08-2020 17:51	Security Cer
	Documents my-key-pair.pem	20-08-2020 19:51	PEM File
Your Certificates Authentication Deci	CSR.pem	20-08-2020 19:26	PEM File
-	AWS Two Tier Pk MaxxAudioPro	16-08-2020 20:57	File folder
You have certificates on file that identify these	Dipanshu v Earlier this year (3)		
an and the second	Vandana en_visio_professional_2016_x86_x64_dvd_6962139	29-07-2020 20:30	File folder
Certificate Name	WNCC professional_plus_2016_x86_x64_dvd_6962141	29-07-2020 20:25	File folder
✓ AC Camerfirma S.A.	This PC	29-07-2020 15:31	File folder
Chambers of Commerce Root - 2008	3 3D Objects		>
Global Chambersign Root - 2008			
✓ AC Camerfirma SA CIF A82743287	File name: Certificate_chain.crt	Certificate Files (*.p7b;*.crt;*.cer ~	
Camerfirma Chambers of Commerce Ro		Open	Cancel
Camerfirma Global Chambersign Root	Builtin Object Token		
View Edit Trust Import	Export Delete or Distrust		
	ОК		
	al and a second s		



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.

	<mark>Certi</mark> ficate	Manager		
Your Certificates	Authentication Decision	ons Peop	le Servers	Authorities
You have certifica Alert	:		×	
Certificate Nam	This certificate is alread	y installed as a c	ertificate authority.	Ę
✓ AC Camerfirm	•	0.11		^
Chambers		OK		
Global Chamber	sign Root - 2008	Builtin Object	Token	
$\checkmark$ AC Camerfirma SA	CIF A82743287			
Camerfirma Cha	mbers of Commerce Root	t Builtin Object	Token	
Camerfirma Glob	oal Chambersign Root	Builtin Object	Token	~
<u>V</u> iew <u>E</u> dit	Trust I <u>m</u> port	E <u>x</u> port	<u>D</u> elete or Distrust	
				ОК

# 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  $\equiv$  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  $\equiv$  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)
  - 0 **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.
  - o certutil -verify -urlfetch c:\win7.cer
- 19. Review the output and make sure all the chain retrieval and revocation status successfully verified.