


Services ▾

Resource Groups ▾



AppDevRole ▾

N. Virginia ▾

Support ▾

AWS Cloud9

×

Your environments

Shared with you

Account environments

How-to guide

AWS Cloud9 > Your environments

Your environments (1)

Open IDE

View details

Edit

Delete

Create environment

< 1 > ⚙

workshop-environment

•

Type

EC2

Permissions

Owner

Description

Cloud9 environment for the crypto builders python modules

Open IDE

Step 1:

- **Navigate to Cloud9 service**
- **Open the environment workshop-environment**
- **If you don't find the environment, you might not be in the right region for your workshop – this slide shows N.Virginia. Depending on where this workshop is being conducted the region might be different**

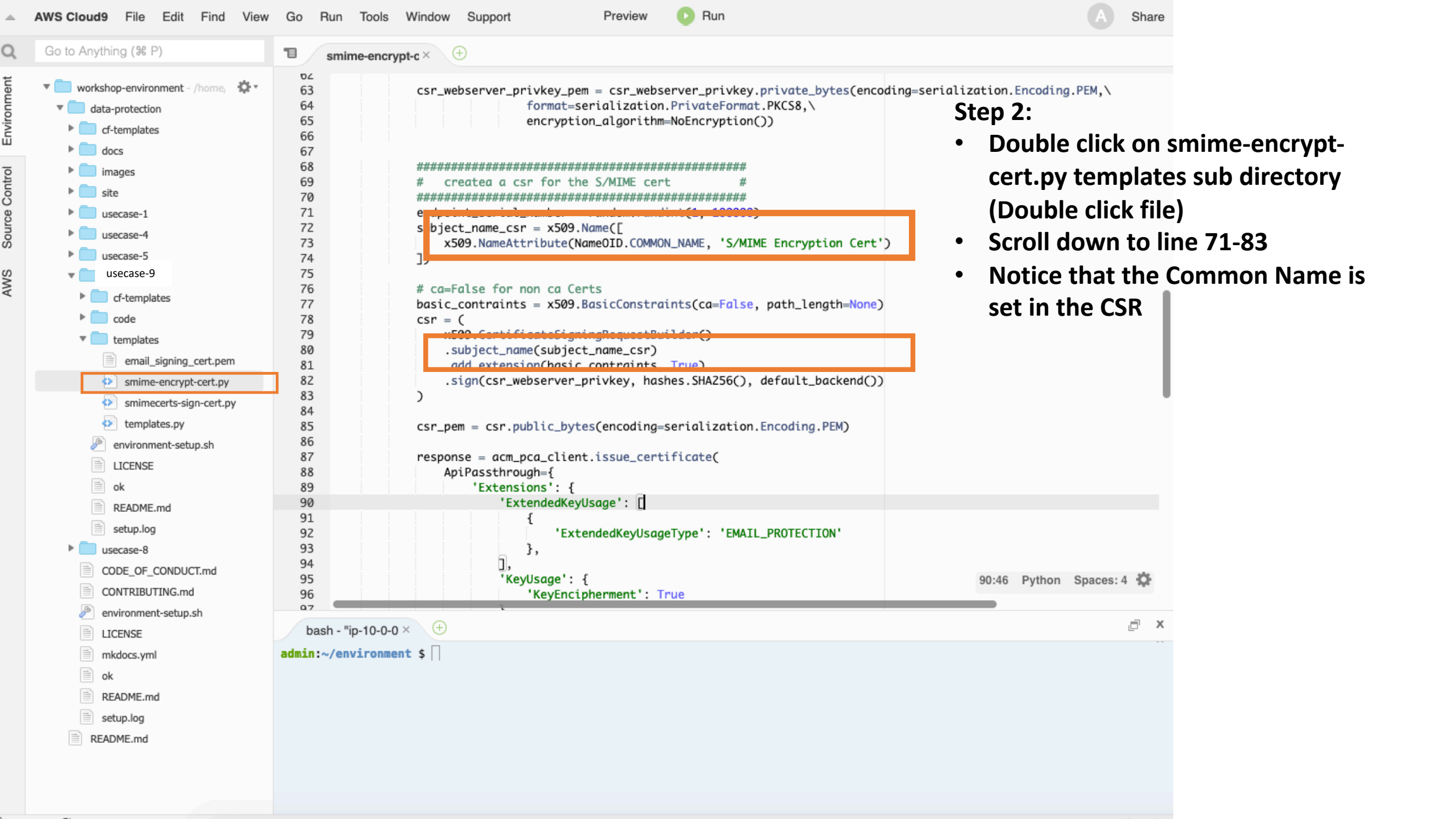
Feedback

English (US)

© 2008 - 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Privacy Policy

Terms of Use



AWS Cloud9 File Edit Find View Go Run Tools Window Support Preview Run

Go to Anything (% P)

workshop-environment - /home

- data-protection
 - cf-templates
 - docs
 - images
 - site
 - usecase-1
 - usecase-4
 - usecase-5
 - usecase-9
 - cf-templates
 - code
 - templates
 - email_signing_cert.pem
 - smime-encrypt-cert.py
 - smimecerts-sign-cert.py
 - templates.py
- environment-setup.sh
- LICENSE
- ok
- README.md
- setup.log

usecase-8

- CODE_OF_CONDUCT.md
- CONTRIBUTING.md
- environment-setup.sh
- LICENSE
- mkdocs.yml
- ok
- README.md
- setup.log
- README.md

smime-encrypt-c

```
80 .subject_name(subject_name_csr)
81 .add_extension(basic_constraints, True)
82 .sign(csr_webserver_privkey, hashes.SHA256(), default_backend())
83 )
84
85 csr_pem = csr.public_bytes(encoding=serialization.Encoding.PEM)
86
87 response = acm_pca_client.issue_certificate(
88     ApiPassthrough={
89         'Extensions': {
90             'ExtendedKeyUsage': [
91                 {
92                     'ExtendedKeyUsageType': 'EMAIL_PROTECTION'
93                 },
94             ],
95             'KeyUsage': {
96                 'KeyEncipherment': True
97             },
98             'SubjectAlternativeNames': [
99                 {
100                     'Rfc822Name': 'myemail@domain.com',
101                 },
102             ]
103         },
104         'Subject': {
105             'Country': 'US',
106             'Organization': 'customer',
107             'OrganizationalUnit': 'customerdept',
108             'State': 'Nevada',
109             'CommonName': 'S/MIME',
110             'SerialNumber': str(endpoint_serial_number),
111             'Locality': 'Las Vegas'
112         }
113     },
114     CertificateAuthorityArn=subordinate_pca_arn,
```

113:19 Python Spaces: 4

bash - "ip-10-0-0

admin:~/environment \$

Step 3:

- Scroll down to line 90
- Look through
 - ExtendedKeyUsage
 - KeyUsage
 - SubjectAlternativeNames
- Notice KeyUsage is using: *KeyEncipherment*
- This happens via [API Passthrough](#)

AWS Cloud9 File Edit Find View Go Run Tools Window Support Preview **Run** A Share

Go to Anything (% P)

Environment

- workshop-environment - /home
 - data-protection
 - cf-templates
 - docs
 - images
 - site
 - usecase-1
 - usecase-4
 - usecase-5
 - usecase-9
 - cf-templates
 - code
 - templates
 - email_encrypt_cert.pem
 - email_signing_cert.pem
 - smime-encrypt-cert.py**
 - smimecerts-sign-cert.py
 - templates.py
 - environment-setup.sh
 - LICENSE
 - ok
 - README.md
 - setup.log
 - usecase-8
 - CODE_OF_CONDUCT.md
 - CONTRIBUTING.md
 - environment-setup.sh
 - LICENSE
 - mkdocs.yml
 - ok
 - README.md
 - setup.log
 - README.md

Source Control

AWS

```
1 #####
2 # Learning about using templates #
3 #####
4
5 from datetime import datetime
6 from datetime import timedelta
7 import os
8 import subprocess
9 import sys
10 import random
11 import time
12 import boto3
13
14 from cryptography import x509
15 from cryptography.hazmat.primitives import hashes
16 from cryptography.hazmat.backends import default_backend
17 from cryptography.hazmat.primitives import serialization
18 from cryptography.hazmat.primitives.asymmetric import rsa
19 from cryptography.x509.oid import NameOID
20 from cryptography.hazmat.primitives.serialization import NoEncryption
21
22 def main():
23     """
24     #####
25     # Creating an S/MIME encryption certificate #
26     #####
27     """
28     try:
29         acm_pca_client = boto3.client('acm-pca')
30
31         current_directory_path = os.path.dirname(os.path.realpath(__file__)) + '/'
32         print("This step will take about 2 minutes to complete\n")
33
```

113:19 Python Spaces: 4

bash - "ip-10-0-0" data-protection/u

Run Command: data-protection/usecase-7/templates/smime-enci Runner: Python 3 CWD ENV

This step will take about 2 minutes to complete

Successfully created S/MIME encryption certificate called email_encrypt_cert.pem

Process exited with code: 0

Step 4:

- Run the python script smime-encrypt-cert.py by clicking on the Run button
- After about 2 mins you should see the print

“Successfully created ...”

Go to Anything (% P)

Environment

Source Control

AWS

workshop-environment - /home

data-protection

cf-templates

docs

images

site

usecase-1

usecase-4

usecase-5

usecase-9

cf-templates

code

templates

codesigning_cert.pem

email_cert.pem

smimecerts.py

templates.py

environment-setup.sh

LICENSE

ok

README.md

setup.log

usecase-8

cf-templates

files

environment-setup.sh

LICENSE

README.md


CODE_OF_CONDUCT.md

CONTRIBUTING.md

smimecerts.py

```
2 # Learning about
3 #####
4
5 from datetime import
6 from datetime import
7 import os
8 import subprocess
9 import sys
10 import random
11 import time
12 import boto3
13
14 from cryptography
15 from cryptography
16 from cryptography
17 from cryptography.hazmat.primitives import serialization
18 from cryptography.hazmat.primitives.asymmetric import rsa
19 from cryptography.x509.oid import NameOID
20 from cryptography.hazmat.primitives.serialization import NoEncryption
21
22 def main():
23     """
24     #####
25     # Creating an S/MIME certificate
26     #####
27     """
28     try:
```


New File ^ N

New Terminal  T

New Run Configuration

New Immediate Window

Output

Open Preferences  ,

Recently Closed Tabs

Preferences

Welcome

environment-setup.sh

templates.py

21:1 Python Spaces: 4

Run

Command: data-protection/usecase-7/templates/smimecerts.py

Runner: Python 3 CWD ENV

This step will take about 2 minutes to complete

Successfully created code signing cert email_cert.pem

Process exited with code: 0

Step 5:

- Open a new bash terminal

Step 6:

- Change directory to templates

cd data-protection/usecase-9/templates/

- Run the following command

openssl x509 -in email_encrypt_cert.pem -text -noout

The screenshot displays a code editor interface with a file explorer on the left and a terminal at the bottom. The file explorer shows a project structure with a 'data-protection' directory containing 'usecase-9' and a 'templates' subdirectory. The 'smimecerts.py' file is selected in the 'templates' directory. The code editor shows the following Python code:

```
2 # Learning about
3 #####
4
5 from datetime import
6 from datetime import
7 import os
8 import subprocess
9 import sys
10 import random
11 import time
12 import boto3
13
14 from cryptography
15 from cryptography
16 from cryptography
17 from cryptography.hazmat.primitives import serialization
18 from cryptography.hazmat.primitives.asymmetric import rsa
19 from cryptography.x509.oid import NameOID
20 from cryptography.hazmat.primitives.serialization import NoEncryption
21
22 def main():
23     """
24     #####
25     # Creating an S/MIME certificate #
26     #####
27     """
28     try:
```

A context menu is open over the code, showing options like 'New File', 'New Terminal', 'New Run Configuration', 'New Immediate Window', 'Output', and 'Open Preferences'. The 'New Terminal' option is highlighted.

The terminal window at the bottom shows the command 'data-protection/usecase-7/templates/smimecerts.py' being executed. The output indicates that the step will take about 2 minutes to complete and that a code signing certificate 'email_cert.pem' was successfully created. The process exited with code 0.

Go to Anything (% P)

Environment

Source Control

AWS

- workshop-environment - /home
 - data-protection
 - cf-templates
 - docs
 - images
 - site
 - usecase-1
 - usecase-4
 - usecase-5
 - usecase-9
 - cf-templates
 - code
 - templates
 - email_encrypt_cert.pem
 - email_signing_cert.pem
 - smime-encrypt-cert.py
 - smimecerts-sign-cert.py
 - templates.py
 - environment-setup.sh
 - LICENSE
 - ok
 - README.md
 - setup.log
 - usecase-8
 - CODE_OF_CONDUCT.md
 - CONTRIBUTING.md
 - environment-setup.sh
 - LICENSE
 - mkdocs.yml
 - ok
 - README.md
 - setup.log
 - README.md

smime-encrypt-c ×

```

61 )
62
63     csr_webserver_privkey_pem = csr_webserver_privkey.private_bytes(encoding=serialization.Encoding.PEM,\
64                               format=serialization.PrivateFormat.PKCS8,\
65                               encryption_algorithm=NoEncryption())
66
67
68     #####
69     #   create a csr for the S/MIME cert   #
70     #####
71     endpoint_serial_number = random.randint(1, 100000)
72     subject_name_csr = x509.Name([
73         x509.NameAttribute(NameOID.COMMON_NAME, 'S/MIME Encryption Cert')
74     ])
75
76     # ca=False for non ca Certs

```

113:19 Python Spaces: 4

bash - "ip-10-0-0 ×

data-protection/u ×

```

c1:1b:3f:65:61:ea:64:60:f1:95:b7:b2:d9:15:86:
1c:dc:a4:db:2b:f7:6b:a9:9f:59:57:62:2b:23:45:
65:49
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Basic Constraints:
CA:FALSE
X509v3 Authority Key Identifier:
keyid:43:A5:66:FD:76:ED:AB:11:24:E4:63:8C:D5:58:88:3C:7D:51:DE:52
X509v3 Subject Key Identifier:
X509v3 Key Usage: critical
Key Encipherment
X509v3 Extended Key Usage:
E-mail Protection
X509v3 Subject Alternative Name:
email:myemail@domain.com
Signature Algorithm: sha256WithRSAEncryption
92:fd:ce:5e:64:a2:e2:02:8a:a2:09:78:93:0d:2a:0f:c6:cc:
5d:26:86:e9:70:09:59:2b:b0:07:5e:c9:2f:2a:2f:7c:37:89:
55:f5:bc:af:c4:09:63:a9:e9:99:da:fa:87:18:43:96:b3:6b:
f1:99:2b:4c:27:5a:60:e5:4c:86:df:c6:f6:ed:52:0c:e2:e9:
70:43:ca:d2:2a:d4:61:06:4a:01:83:ab:7b:9c:69:20:a6:f5:
57:43:fb:23:0e:8d:f8:b3:83:b0:15:01:6e:36:3b:e8:6c:cd:
b8:31:ea:1d:ba:08:84:2f:00:e7:d4:bb:d0:d5:26:d8:89:30:
61:5c:4b:c2:c7:71:5d:ca:ad:40:03:f3:de:5f:03:9b:95:99:
56:2c:5f:8d:fa:7f:02:31:6b:98:73:a6:a2:fd:31:de:3c:a9:
2a:5d:ca:b1:7e:a5:d3:0b:dd:41:e2:61:44:7f:e8:37:89:47:
38:0b:7e:a5:53:4a:56:e5:ca:cb:4a:fb:ff:8a:ef:1d:10:34:

```

• Notice that:

- Key Usage and Extended Key Usage have been set by API Passthrough method