1. Login to pgv010188 via SSH

```
[aalci00@pgv010188 ~]$ whoami
aalci00
```

2. Generate PEM files.

```
[aalci00@pgv010188 ~]$ openssl s_client -showcerts -verify 5 -connect zquw-itka1br01.safeway.com:9095
< /dev/null | awk '/BEGIN/,/END/{ if(/BEGIN/){a++}; out="cert"a".pem"; print >out}'
verify depth is 5
depth=2 C = GB, ST = Greater Manchester, L = Salford, O = COMODO CA Limited, CN = COMODO RSA
Certification Authority
verify return:1
depth=1 C = GB, ST = Greater Manchester, L = Salford, O = COMODO CA Limited, CN = COMODO RSA
Organization Validation Secure Server CA
verify return:1
depth=0 C = US, ST = California, O = "Safeway, Inc.", OU = Venafi API, CN = zquw-itka1br01.safeway.com
verify return:1
DONE
```

3. Validate the PEM files. The smallest is the Top Level Cert included in the chain.

```
[aalci00@pgv010188 ~]$ ls -l *.pem
-rw-r--r-- 1 aalci00 unix_users 2476 Aug 22 23:21 cert1.pem
-rw-r--r-- 1 aalci00 unix_users 2159 Aug 22 23:21 cert2.pem
-rw-r--r-- 1 aalci00 unix_users 2086 Aug 22 23:21 cert3.pem
```

4. Run this command to rename the certificates.

```
[aalci00@pgv010188 ~]$ for cert in *.pem; do newname=$(openssl x509 -noout -subject -in $cert | sed -n
's/^.*CN=\(.*\)$/\1/; s/[ ,.*]/_/g; s/__/_/g; s/^_//g;p').pem; mv $cert $newname; done

[aalci00@pgv010188 ~]$ ls -l *.pem
-rw-r--r-- 1 aalci00 unix_users 2086 Aug 22 23:21 COMODO_RSA_Certification_Authority.pem
-rw-r--r-- 1 aalci00 unix_users 2159 Aug 22 23:21
COMODO_RSA_Organization_Validation_Secure_Server_CA.pem
-rw-r--r-- 1 aalci00 unix_users 2476 Aug 22 23:21 zquw-itka1br01_safeway_com.pem
```

5. Create a trust store and import the certificates using “keytool” command.

5.1. If “keytool” if available on pgv010188. Follow this step and move to step number 6.

Run the keytool command below to create trust store and import root certificate into the trust store.
Input your desired password. Keep this as this will be used for the trust store password.

```
[aalci00@pgv010188 ~]$ /opt/vmware-jre/bin/keytool -keystore KafkaTrust.jks -alias comodo_ca -import -
file COMODO_RSA_Certification_Authority.pem
Enter keystore password:
Re-enter new password:
Owner: CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester,
C=GB
Issuer: CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester,
C=GB
Serial number: 4caaf9cadb636fe01ff74ed85b03869d
Valid from: Mon Jan 18 17:00:00 MST 2010 until: Mon Jan 18 16:59:59 MST 2038
Certificate fingerprints:
         SHA1: AF:E5:D2:44:A8:D1:19:42:30:FF:47:9F:E2:F8:97:BB:CD:7A:8C:B4
         SHA256:
52:F0:E1:C4:E5:8E:C6:29:29:1B:60:31:7F:07:46:71:B8:5D:7E:A8:0D:5B:07:27:34:63:53:4B:32:B4:02:34
Signature algorithm name: SHA384withRSA
Subject Public Key Algorithm: 4096-bit RSA key
Version: 3

Extensions:

#1: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
  CA:true
  PathLen:2147483647
```

```
]

#2: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
  Key_CertSign
  Crl_Sign
]

#3: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: BB AF 7E 02 3D FA A6 F1   3C 84 8E AD EE 38 98 EC  ....=...<....8..
0010: D9 32 32 D4                                        .22.
]
]

Trust this certificate? [no]:  yes
Certificate was added to keystore

[aalci00@pgv010188 ~]$ ls -l KafkaTrust.jks
-rw-r--r-- 1 aalci00 unix_users 1566 Aug 22 23:27 KafkaTrust.jks
```

Transfer the JKS file to AKS Jump host (172.25.227.100)

```
[aalci00@pgv010188 ~]$ ls -l KafkaTrust.jks
KafkaTrust.jks
[aalci00@pgv010188 ~]$ scp KafkaTrust.jks aalci00@safeway.com@172.25.227.100:~
This feature is now deprecated. Learn more at https://aka.ms/AADSSHLogin

To sign in, use a web browser to open the page https://microsoft.com/devicelogin and enter the code
RYZGJPQJ9 to authenticate.

Press ENTER when ready.
KafkaTrust.jks                                          100% 1566     1.5KB/s   00:00
[aalci00@pgv010188 ~]$
```

5.2. If “keytool” is not available on pgv010188 follow this section and move to step number 6 once completed.

Open command promot and copy the PEM files to your workstation.
You can place it on C:\Users\<ldap> directory

```
Microsoft Windows [Version 10.0.19042.1826]
(c) Microsoft Corporation. All rights reserved.

C:\Users\aalci00>scp aalci00@pgv010188.albertsons.com:/home/aalci00/*.pem .
The authenticity of host 'pgv010188.albertsons.com (172.26.40.20)' can't be established.
ECDSA key fingerprint is SHA256:XtqC4GED+oUq1varwej8zp6NDcqS3xt+VFEMJclvwFk.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'pgv010188.albertsons.com,172.26.40.20' (ECDSA) to the list of known hosts.
============================================================
          ========== W A R N I N G ==========

This is a private network - server for use by Safeway Inc.
and its designated customers only.

All access to this system is monitored and any abuse or
non-authorized access will be prosecuted to the full extent
that the laws of the United States of America will allow.

All information on this site becomes the property of Safeway
Inc. or one of its subsidiaries.
============================================================

aalci00@pgv010188.albertsons.com's password:
COMODO_RSA_Certification_Authority.pem                      100% 2086    12.3KB/s   00:00
COMODO_RSA_Organization_Validation_Secure_Server_CA.pem     100% 2159    12.7KB/s   00:00
zquw-itkalbr01_safeway_com.pem                              100% 2476    14.6KB/s   00:00

C:\Users\aalci00>
```

Run the keytool command below to create trust store and import root certificate into the trust store.
Input your desired password. Keep this as this will be used for the trust store password.

```
C:\Users\aalci00>keytool -keystore KafkaTrust.jks -alias comodo_ca -import -file
COMODO_RSA_Certification_Authority.pem
Enter keystore password:
Re-enter new password:
Owner: CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester,
C=GB
Issuer: CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester,
C=GB
Serial number: 4caaf9cadb636fe01ff74ed85b03869d
Valid from: Tue Jan 19 08:00:00 SGT 2010 until: Tue Jan 19 07:59:59 SGT 2038
Certificate fingerprints:
         SHA1: AF:E5:D2:44:A8:D1:19:42:30:FF:47:9F:E2:F8:97:BB:CD:7A:8C:B4
         SHA256:
52:F0:E1:C4:E5:8E:C6:29:29:1B:60:31:7F:07:46:71:B8:5D:7E:A8:0D:5B:07:27:34:63:53:4B:32:B4:02:34
Signature algorithm name: SHA384withRSA
Subject Public Key Algorithm: 4096-bit RSA key (3)
Version: {10}

Extensions:

#1: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
  CA:true
  PathLen:2147483647
]

#2: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
  Key_CertSign
  Crl_Sign
]

#3: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: BB AF 7E 02 3D FA A6 F1   3C 84 8E AD EE 38 98 EC  ....=...<....8..
0010: D9 32 32 D4                                        .22.
]
]

Trust this certificate? [no]:  yes
Certificate was added to keystore

C:\Users\aalci00>dir KafkaTrust.jks
 Volume in drive C is Windows
 Volume Serial Number is 729F-31E6

 Directory of C:\Users\aalci00

08/23/2022  02:07 PM             1,566 KafkaTrust.jks
               1 File(s)          1,566 bytes
               0 Dir(s)  331,673,001,984 bytes free
```

Transfer the JKS file to AKS Jump host (172.25.227.100)

```
C:\Users\aalci00>scp KafkaTrust.jks aalci00@safeway.com@172.25.227.100:~
This feature is now deprecated. Learn more at https://aka.ms/AADSSHLogin

To sign in, use a web browser to open the page https://microsoft.com/devicelogin and enter the code
EPFHYGWHN to authenticate.

Press ENTER when ready.
KafkaTrust.jks
100% 1566     8.3KB/s   00:00

C:\Users\aalci00>
```

6. Login to AKS jump host via SSH. Follow the code authentication instructions.

```
[aalci00@pgv010188 ~]$ ssh -l aalci00@safeway.com 172.25.227.100
This feature is now deprecated. Learn more at https://aka.ms/AADSSHLogin

To sign in, use a web browser to open the page https://microsoft.com/devicelogin and enter the code
FSHB5JPTX to authenticate.

Press ENTER when ready.
```

7. Login to Azure. Follow the code authentication instructions.

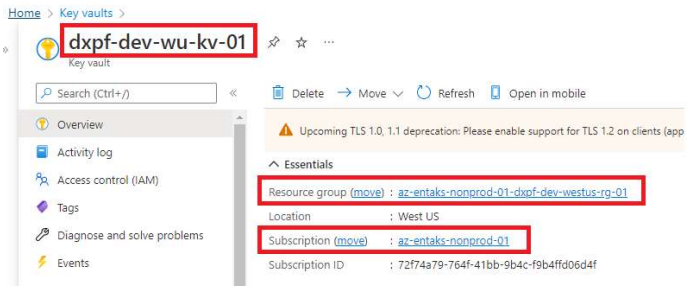
```
[aalci00@safeway.com@esco-jumphost-prod-svc-vm-01-escojump000001 ~]$ az login
To sign in, use a web browser to open the page https://microsoft.com/devicelogin and enter the code
R8CFYQZFE to authenticate.
```

8. Change context to point to the subscription where the key vault was created.

```
[aalci00@safeway.com@esco-jumphost-prod-svc-vm-01-escojump000001 ~]$ az account set -s az-entaks-
nonprod-01
```

Example:
Azure Key Vault: dxpf-dev-wu-kv-01
Subscription: az-entaks-nonprod-01
Resource Group: az-entaks-nonprod-01-dxpf-dev-westus-rg-01

Note:
You can get the subscription name and resource group on the Overview Blade of the target key vault. See sample below.



9. Upload the JKS file to the target Azure Key Vault.

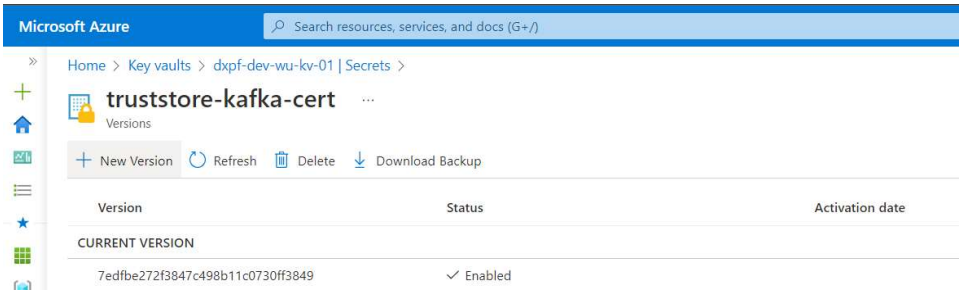
Syntax:

```
az keyvault secret set --vault-name <keyvault_name> --encoding base64 --name <secret_name> --file
<file_name>
```

Sample Command:

```
az keyvault secret set --vault-name dxpf-dev-wu-kv-01 --encoding base64 --name truststore-kafka-cert -
-file KafkaTrust.jks
```

10. Validate the secret was updated.



11. Update the trust store password on your key vault using the password you configured on Step Number 5.